2017

The business of fraud

Jessica Marie Berkshire
University of Northern Iowa

THE BUSINESS OF FRAUD

A Thesis Submitted

in Partial Fulfillment

of the Requirements for the Designation

University Honors

Jessica Marie Berkshire

University of Northern Iowa

May 2017

This Study by: Jessica Berkshire

Entitled: The Business of Fraud

has been approved as meeting the thesis requirement for the Designation of University Honors.

_____	_____
Date	Dr. Amy Igou, Honors Thesis Advisor
_____	_____
Date	Dr. Jessica Moon, Director, University Honors Program

Purpose

This paper will focus on fraud within companies in order to discover overarching themes of why, when, and where corporate fraud occurs. Fraud has significant financial, economic, and social implications that negatively impact a company's business standing. Research will be based on recent frauds that have been tried through the United States Attorney's office. Correlations will be drawn regarding the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) framework, which is a foundation for companies who want to improve their internal controls. Based on the comparisons between the COSO framework and recent fraud activity, individual COSO principles can be analyzed for areas that are violated frequently. Evaluating specific weaknesses in internal controls will elicit trends to identify control areas that should be strengthened. From these results, it can be concluded how to integrate technology, internal controls, and other security measures in order to decrease fraud within a company. This analysis will provide a basis for companies looking to prevent, detect, and correct internal controls in relation to fraud.

Literature Review

Corporate crime, or corporate corruption, has become a topic of public interest since the American 'Great Recession' of 2007-2009. According to the Harvard Law Record, corporate crime has done more damage to society than all street crimes combined (Mokhiber, 2015). The Federal Bureau of Investigation (FBI) estimates street crimes, such as burglaries and robberies, cost $4.5 billion a year, whereas money lost by fraud can amount to $6.3 billion (ACFE, 2016). Corporate corruption is rarely evaluated through government regulation, creating a small risk for repercussions or punishments. The undermining of such crimes allows the public to view

corruption as a routine business activity, when in fact, it is quite detrimental.

Fraud is defined as “the use of one's occupation for personal enrichment through the deliberate misuse and misapplication of the employing organization’s resources or assets” (Wells, 2007, pg. 2). There are four criteria used in the legal system that determine if fraud is present within the case, whether civil or criminal. These factors provide a strong basis in understanding what fraud is and the repercussions that can follow from fraudulent acts. The criteria include “a material false statement, knowledge that the statement was false, a victim’s reliance on the false statement, and damages resulting from this reliance” (Wells, 2007, pg. 3). When applied to a corporate setting, fraud can be regarded in two facets: misappropriation of assets or financial statement fraud. The American Institute of Certified Public Accountants (AICPA), provides definitions on both these types. In the AICPA’s Statement of Auditing Standards (SAS) No. 82, misappropriation of assets involves the theft of an entity’s assets where the effect of the theft is not presented on the financial statements (AICPA, 2002, pg. 1722). This same section describes financial statement fraud as intentional misstatement, or omission, of amounts, or disclosures, in financial statements, designed to deceive statement users (AICPA, 2002, pg. 1722).

SAS No. 82, also identifies conditions in which fraud generally occurs. The system described is known as the fraud triangle, depicted as Figure 1. The AICPA sees that, first, employees must demonstrate an incentive or a reason to commit fraud, known as *pressure*. Pressure can come from several factors including personal financial concerns or workplace troubles. Next, ineffective controls must be present within a company to provide an *opportunity* to commit fraud. For example, if an employee had the ability to write checks and also the duty of

Figure 1: The Fraud Triangle
(Association of Certified Fraud Examiners, 2016)

reconciling the bank statements, there is an internal control lapse, which provides opportunities to commit fraud. Finally, a person must be able to justify, or *rationalize*, their actions both while committing a fraudulent act, and also after the crime. Frequent fraud rationalizations involve the fraudster seeing themselves as a victim, rather than as a criminal. With all three factors present, the AICPA considers the environment to be more prone to fraudulent threats, whether the intent is misappropriation of assets or financial statement fraud.

Subsequent to an uncovered fraud, there are several consequences a company must face, as well as changes that must be implemented. A company must relieve a fraudster of their duties and proceed to hire, train, and monitor a new employee for that position. Next, the corporation's internal culture and ethical standards should be assessed. With the discovery of fraud, all company employees should be reevaluated and briefed on the company's moral standing and policy in order to prevent future fraudulent acts. Finally, a company must evaluate their internal

controls on how they detect and prevent fraud, and ultimately, how their system must adapt based on the current discovered fraudulent actions. While a company reasserts their internal structure, they must simultaneously evaluate the public damage the corporation faces. Fraud can impact investors' trust in the company, leading to a decrease in capital for the corporation (Romney and Steinbart, 2015, pg. 68).

These implications allude to the fact that fraud has a significant financial impact that affects both the company responsible and the economy. According to Financial Statement Fraud: Prevention and Detection, "it is impossible to determine the actual total costs [of fraud] since not all fraud is detected, not all detected fraud is reported, and not all reported fraud is legally pursued" (Rezaee, 2002, pg. 8). Despite these difficulties, there is an investigative interest with accounting professionals, business managers, government agencies, and the media to understand and assess the costs associated with fraud. According to the Association of Certified Fraud Examiner's (ACFE) *Report to the Nations On Occupational Fraud and Abuse: 2016 Global Fraud Study*, valuing fraud is important because, "understanding the size of the problem brings attention to its impact, enables organizations to quantify their fraud risk, and helps management make educated decisions about investing in anti-fraud resources and programs" (ACPE, 2016, pg. 8). Fraud causes a company to have increased insurance and legal costs, as well as expenses from a loss in productivity. Other non-monetary fraud deficiencies include a decrease in employee morale and customer goodwill, loss of credibility, and negative stock market reactions.

As indicated earlier, there are two main forms of fraudulent business activities, asset misappropriation and financial statement fraud. These two types of frauds can be broken down

and assessed in monetary terms. Asset misappropriation is understood to be the most common type of fraud committed. According to the ACFE *Report to the Nations*, an estimated 83% of the fraud cases studied were asset misappropriation. However, these cases were financially immaterial because they had lower costs/losses. The ACFE study found that the median asset misappropriation loss from fraud was $125,000 (ACFE, 2016, pg. 5). The same information valuation can be assessed for financial statement fraud. Only 10% of cases studied by the ACFE were considered financial statement fraud, indicating financial statement fraud is far less common than asset misappropriation. However, financial statement frauds did have a higher median loss at $925,000 (ACFE, 2016, pg. 5). These statistics are indicative as to why government regulation on fraud is seen as undermined. Government agencies, such as the Securities and Exchange Commission (SEC), are concerned with company financial statement frauds because of their larger financial impact on the economy.

The accounting profession has several oversight boards and institutions that regulate a corporation's accounting practices. Notably, the SEC, an agency of the federal government, administers the trading of assets, or securities, through laws, rules, regulations, and other activities. When a company is suspected of committing fraudulent acts, the SEC has the power to begin an investigation involving the corporation's financial statements and other accounting documents.

Another form of government regulation for fraudulent acts is through the Sarbanes-Oxley Act (SOX). Congress passed this act in 2002 in response to scandals involving Enron and WorldCom. SOX implemented rules and regulations for managers, accountants, and

stakeholders, alike. From an accounting prospective, it took the industry from being relatively autonomous, to heavily governed (Franklin, 2016, pg. 56). SOX Section 404 is considered to have the biggest impact on company management and accountants. It is written as: "issuers are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures" (Sarbanes-Oxley Act, 2002, par. 2). SOX created the importance of implementing internal controls, along with updating and assessing their effectiveness.

One of the more significant implications of SOX is that companies have a responsibility to create and maintain internal controls. An internal control is "a process effected by a company, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" (Romney and Steinbart, 2015, pg. 345). This definition provides a broad statement of how a company looks to prevent, detect, and correct fraud. Preventing fraud is seen as a preemptive action, where internal controls reduce the likelihood of fraudulent acts. Segregating duties is an example of a preventative control, as it aims to deter fraud from happening. The AICPA defines segregation of duties as: "shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department" (Ghosn, 2017, pg.1). Segregation of duties allows for procedures to be disbursed across a company in order to prevent the opportunity of committing fraud. Detecting fraud involves discovering problems quickly when they arise. Fraud detection can come from simple measures such as validating a bank reconciliation. Finally, corrective controls provides a remedy to problems that have occurred within an organization. Corrective controls look to identify a

cause, to correct the errors, and also to modify a system in order to prevent future problems.

Figure 2: Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework, 2013

When analyzing a company's internal controls, it is suggested to utilize the framework devised by COSO. This organization combines several accounting organizations including the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the National Association of Accountants, which is now the Institute of Management Accountants (IMA). With the partnership of several influential accounting parties, COSO has been able to develop an evolving framework which helps companies "design and implement internal controls, increase control effectiveness, and decrease vulnerable areas" (McNally, 2013, pg. 3). The framework can be seen as Figure 2. Visually, this framework promotes coherent regulations across a company. Business objectives, internal control functions, and the employees of a company must all be synchronized in order for the framework to be successful.

In order to analyze COSO's effectiveness in preventing fraud through internal controls, it is necessary to break down the different components in the COSO framework. This evaluation will

continue to reference Figure 2. The top of the cube is concerned with a business' objectives, which include operations, reporting, and compliance objectives. Operations objectives effectively and efficiently maintain company performance and profitability. Reporting objectives involve the accuracy, completeness, and reliability of company reports and statements. Finally, compliance objectives hold a company responsible for following the laws and regulations enacted by government agencies, such as the SEC. The right side of the cube outlines the various levels of employees working at a company. This articulates that a company must impose a top-to-bottom approach when implementing internal controls in order to unify all areas of the business. The front facing side of the COSO framework involves the components for effectively creating, maintaining, and managing internal controls. Each provides an essential element to the success of a company's internal control system.

The five components of the COSO framework are as follows: control environment, risk assessment, control activities, information and communication, and monitoring activities. Each is described as follows. The combination of these components offers a guidance for companies looking to improve their existing internal control systems (COSO, 2014, par. 1-5).

- **The Control Environment**

  The control environment establishes a culture of a company which serves as the foundation for awareness and support of company policies. Factors involved in the control environment are management philosophy, ethical values, and human resource standards.

- **Risk Assessment**

  Risk is the possibility an event will occur to adversely affect organization objectives. Risks are assessed in order to determine a company's ability to achieve its objectives.

- **Control Activities**

  The control activities component creates policies and procedures that can provide reasonable assurance for company objectives. Control policies and procedures are established and implemented throughout an organization in order to achieve a cohesive internal control structure. Examples of controls can include authorizations, document design, safeguards, and independent checks.

- **Information and Communication**

  Information and communication allows a company's internal control system to collect and exchange information needed to maintain its operations. Effective communication is facilitated up, down, and across a company in order to provide a clear understanding of business operations and control activities.

- **Monitoring Activities**

  Monitoring activities are used to assess the quality of an internal control system. Monitoring can include evaluation of system design, as well as, a function of a system's effectiveness in preventing, detecting, and correcting problem areas.

Each COSO component has several principles underneath. The principles are requirements and initiatives set to maximize the relevance of the internal control component. Both the components and principles of COSO are outlined in Table 1 below (COSO, 2014, par. 1-5).

Table 1: COSO Internal Control Framework Components and Principles

Control Environment	1. Commitment to integrity and ethical values. 2. Board of directors is independent of management and exercise oversight for the development and performance of internal controls. 3. Management establishes structures, reporting lines, and appropriate authority and responsibility in pursuit of objectives. 4. Organization commits to attract, develop, and retain competent individuals in alignment with objectives. 5. Organization holds individuals accountable for their internal control responsibilities.
Risk Assessment	6. Organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. 7. Identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risk should be managed. 8. Considers the potential for fraud in assessing risks. 9. Identifies and assess changes that could significantly impact the system of internal control.
Control Activities	10. Selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. 11. Selects and develops general controls activities over technology to support the achievement of objectives. 12. Deploys control activities as manifested in policies that establish what is expected.
Information and Communication	13. Generates and uses relevant, quality information to support the functioning of other components of internal controls. 14. Internally communicates information including objective and responsibilities for internal controls. 15. Communicates with external parties regarding matters affecting the functioning of other components of internal control.
Monitoring Activities	16. The organization selects, develops, and performs ongoing evaluations to ascertain whether the components of internal control are present and functioning. 17. Evaluates and communicates internal control deficiencies in a timely manner to parties responsible for taking corrective action.

Retrieved from: coso.org (2014)

The COSO framework provides a company with a foundation for effective internal controls. However, there are requirements for the framework's success. The components and principles outlined above must be present and functioning within a company (COSO, 2014, par. 1-5). To be present and functioning within a system, a control must first exist, and then be conducted in a manner that achieves organizational objectives. Another requirement is that the COSO components are integrated; the components are interdependent and have multiple interrelationships and linkages, which requires that they all operate together (COSO, 2014, par. 1-5). The successful implementation of the COSO framework is necessary for its effectiveness. Deficiencies can cause a company to be susceptible to fraudulent acts.

Technology has become integrated within companies and can be used effectively as an internal control. Correctly implementing preventative, detective, and corrective controls will be an impactful tool in deterring the likelihood of fraud within a company, which can be assisted through the use of control technology. Elaborate information systems and resource management programs often involve complex codes, protections, and safeguards. While the magnitude of these functions are beneficial to an extent, integrating basic technology procedures in a company can be the ultimate determining factor in whether fraud is committed, or not.

Research Questions to be Answered

1. What set of internal controls could have been used to prevent recent actions of fraud?
2. How could internal controls be improved with technology?
3. Which COSO components/principles are undermined most frequently when fraudulent acts are committed? How do vulnerabilities within the COSO framework correlate to recent fraud cases?

Methodology

The research method used throughout this thesis was empirical and analytical. Research was focused on recent fraudulent acts posted through the United States Attorney's Office. The press releases issued by this office provided sources of recent claims of fraud that were compared categorically. As a way of providing consistent research, the search was limited to frauds with press releases in 2016, which approximated 1,900 case files. It was assumed that most fraudulent acts happened in years prior to the court hearing issued by the U.S. Attorney's Office. In this way, all information corresponds will press releases dated in 2016, regardless of the year the fraud was committed. Another filter applied to the search was based on location. The court cases and fraudulent acts that were analyzed were based in: Illinois, Iowa, Minnesota, Missouri, and Wisconsin.

Table 3: Number of Frauds Gathered per State

State	Number of 2016 Cases Used in Data Set
Illinois	30
Iowa	11
Minnesota	7
Missouri	21
Wisconsin	4

Elimination of cases based on type of fraud was necessary in order to provide a cohesive data set. For example, governmental frauds, such as insurance and health care fraud, and individual's frauds were not used in the sample. Research was narrowed down by keywords and phrases based on the type of fraud committed. Examples of these terms included: fraud, embezzlement, laundering, etc. Based on the source parameters, the following data was collected for each case:

- Company/Institution
- Type of Company
- Individual(s)
- Position
- Guilty of (type of fraud)
- Convicted (yes or no)
- U.S. State Crime was Committed
- U.S. Attorney's District
- U.S. State Crime was Tried in
- Level of Court
- Outcome of Case
- Year(s) of Crime
- Year of Press Release (U.S. Attorney's Office)
- Description of Fraud
- Fraud Hierarchy (Wells, 2013, pg. 72)
- COSO Component(s)
    - Control Environment
    - Risk Assessment
    - Control Activities
    - Information and Communication
    - Monitoring Activities
- COSO Principle(s)
    - Main four principles documented
- Internal Control(s)
- Technology Functions
- Other Recommendations

The companies and fraud cases in this table will serve as the basis for evaluation of technology based internal controls (See Appendix A). Information collected from recent fraud cases will test COSO components and principles for vulnerabilities. Conclusions will be dependent on the

deficiencies of the COSO framework and the implementation of specific technology functions within a company's internal control structure. These factors can be assessed based on the internal control's effectiveness at preventing, correcting, and detecting fraud. This thesis will expand on the information within the table, providing examples on the types of fraudulent acts committed and assessing the internal controls.

Results

Research of the frauds within the study helped to determine weaknesses in COSO principles when fraud occurred. These areas are indicators of vulnerabilities, which were then analyzed based on principles of the framework. Through the determination of the most violated framework areas, conclusions on internal controls were made. The results provided a more in-depth analysis on ways to prevent fraud, data is shown in Appendix A. Evaluation of these fraud cases creates generalizations that other companies can use in order to minimize their susceptibility to fraud. It also ascertains which parts of COSO to emphasize when connecting fraudulent cases to internal control systems. As outlined throughout this report, decreasing fraudulent risk is beneficial for a company's financial position and the economy as a whole.

The results of this study combine both similarities and differences of the fraud cases in order to gain a more wholistic conclusion. By researching companies across different industries, the capacity of fraud and its prevalence in even well-known corporations is articulated. Since there are a variety of types and variations of fraud, it will be necessary to remain free of absolutions. There is no guarantee of the prevention of all types of fraud, however, certain measures can be put in place to reduce the risk. These measures are articulated in the findings. The COSO

framework outlines requirements of internal controls which are proven to mitigate fraud risk. This thesis looks to show the importance of internal controls, and specifically technology measures to implement and enhance these controls. Trends based on the information collected are highlighted below. Each conclusion relates the sample of fraud cases to internal controls and the COSO framework. The results are beneficial to companies looking to mitigate their susceptibility to fraud because of the conclusion's versatility and adaptability.

Position Analysis

Data collected from the sample included the perpetrator of the fraud and their position within the company. Analysis of position is important because it relates to the first component of the COSO framework, *control environment*. COSO defines the control environment as: "the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization" (COSO, 2014, par. 1-5). The control environment is defined at the top of the organization, in positions such as the board of directors and senior management, if applicable. For smaller, local businesses, the top of the organization may be limited to the owner/operator. In either instance, the control environment sets the standard for integrity, ethical values, corporate responsibly, and a hierarchy of authority within a company (COSO, 2014, par. 1-5).

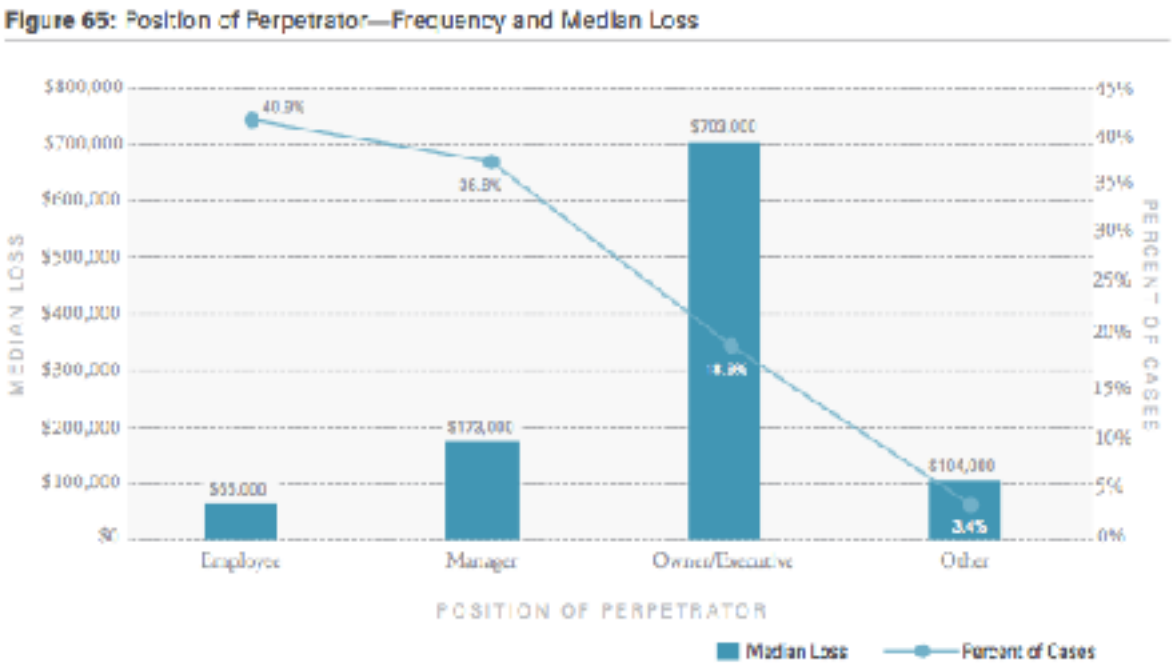

Figure 3: *Report to the Nations On Occupational Fraud and Abuse: 2016 Global Fraud Study* (ACFE, 2016, pg. 49).

The ACFE *Report to the Nations On Occupational Fraud and Abuse: 2016 Global Fraud Study*, has determined trends in fraud cases around the world. One of their conclusions relates to the control environment by analyzing fraud cases based on the position of the perpetrator. Their data is depicted as Figure 3 above.

The relevant component of this graph is the line, depicting the percent of fraud cases that relate to each position. Employee level positions comprise of 40.9% of fraud cases studied, manager, 36.8%, owner/executive, 18.9%, and other, 3.4%. The bar graph component measures median financial loss of the company based on the frauds committed in each position, this information was not evaluated in the thesis project. The control environment influences each level of authority in a company. Lenient regulation or poor supervision of

employees can be explanations for why 40.9% of company employees were able to commit fraud. This correlation can be drawn because a lack of a control environment creates a lack of responsibility and authority within the organization.

The fraud cases examined through the U.S. Attorney's Office produced contrasting results to the *Report to the Nations*. Figure 4 depicts the data collected for the purpose of this thesis:

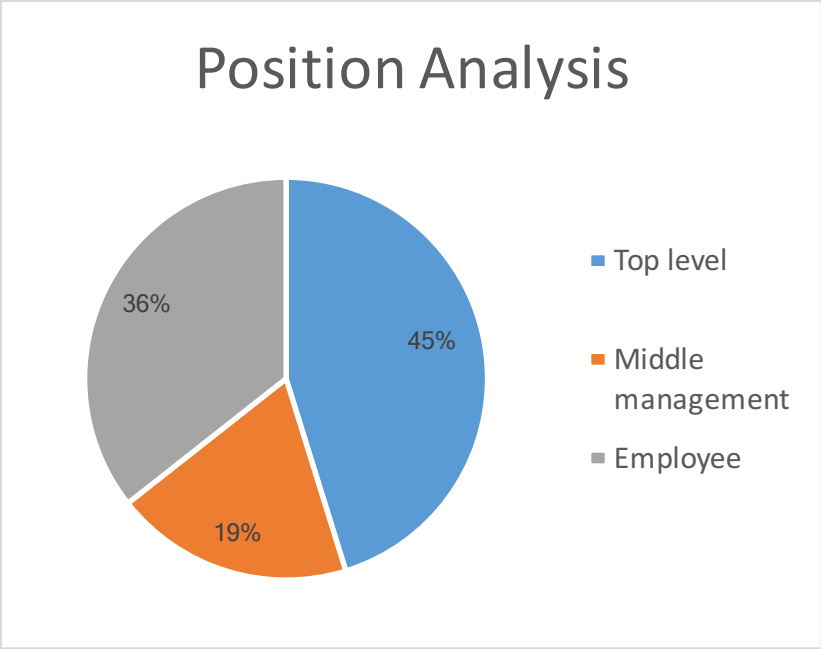

Figure 4: Position Analysis for Fraud

For the purpose of this study, the following labels were created: top level, middle management, and employee. The composition of these roles include:

- Top level — owner, co-owner, operator, executive director, president, vice-president, CEO, CFO, COO, CIO, partner, superintendent, board officer, director, and financial comptroller

- Middle management — general manager, treasurer, supervisor, office manager, senior payroll specialist, administrative manager, portfolio manager, business manager, IT manager, and sheriff
- Employee — employee, customer, financial advisor, business relationship coordinator, bookkeeper, trader, accountant, city clerk, financial secretary, investment broker, sales representative, and customer service representative

The graph depicts that top level management committed 45% of fraud cases, middle management, 19%, and employees, 36%. Differences from the *Report to the Nations* and this thesis data can be attributed to the scope of the data gathered. The thesis data was composed of smaller scale frauds, evaluated in a limited geographic area in the United States. Despite these differences, common conclusions can be drawn from the results.

The control environment of a company has a significant impact on the level within a company where fraud is committed. Executive level frauds establish a negative tone for employees regarding the ethical standards and responsibility of all employees. This can contribute to fraud being committed at lower levels within a company. Companies have a responsibility to successfully create a strong control environment. The environmental structure of a company, if incorporated effectively, is an internal control.

Type of Fraud Committed

There are two types of fraud recognized by the American Institute of Certified Public Accountants (AICPA): financial statement fraud and asset misappropriation. As indicated

earlier, financial statement fraud is the intentional misstatement of financial statements, whereas misappropriation of assets is the theft of company assets (AICPA, 2002, pg. 1722). For the purpose of this research, analysis focused on financial statement fraud, asset misappropriation, and corruption. Corruption is seen as a third type of fraud in the Corporate Fraud Handbook by J.T. Wells. In this publication, corruption is defined as "an act done with the intent to give some advantage inconsistent with official duty and the rights of others" (Wells, 2011, pg. 259). Each category, financial statement fraud, asset misappropriation, and corruption, is broken down based on a hierarchy and sub network. The hierarchy is described below:

- Financial statement fraud
    - Financial
        - Asset/revenue overstatements — timing differences, fictitious revenues, concealed liabilities and expenses, improper disclosures, improper asset valuations
        - Asset/revenue understatements
    - Non-financial — employment credentials, internal documents, external documents
- Asset misappropriation
    - Cash
        - Larceny — of cash on hand, from the deposit, other
        - Skimming
            - Sales — unrecorded
            - Receivables — write-off schemes, lapping schemes, unconcealed
            - Refunds and other
        - Fraudulent disbursements
            - Billing schemes — shell company, non-accomplice vendor, personal purchases
            - Payroll schemes — ghost employees, commission schemes, workers' compensation, falsified wages
            - Expense reimbursement schemes — mischaracterized expenses, overstated expenses, fictitious expenses, multiple reimbursements
            - Check tampering — forged maker, forged endorsement, altered payee, concealed checks, authorized maker
            - Register disbursement — false voids, false refunds
    - Inventory and all other assets
        - Misuse
        - Larceny — asset requisition and transfers, false sales and shipping, purchasing and receiving, unconcealed larceny
- Corruption
    - Conflicts of interest — purchase schemes, sales schemes, other
    - Bribery — invoice kickbacks, bid riggings, other
    - Illegal gratuities
    - Economic extortion

This breakdown of fraud allows for consistent analysis and classification for fraud cases. The hierarchy was used for this purpose in the thesis research data set. Following a standard for classification and using common terminology when researching fraud cases allowed for conclusions to be made based on the frequency each type of fraud occurs. Figure 5

documents the three categories of fraud, and their occurrence within the thesis data.

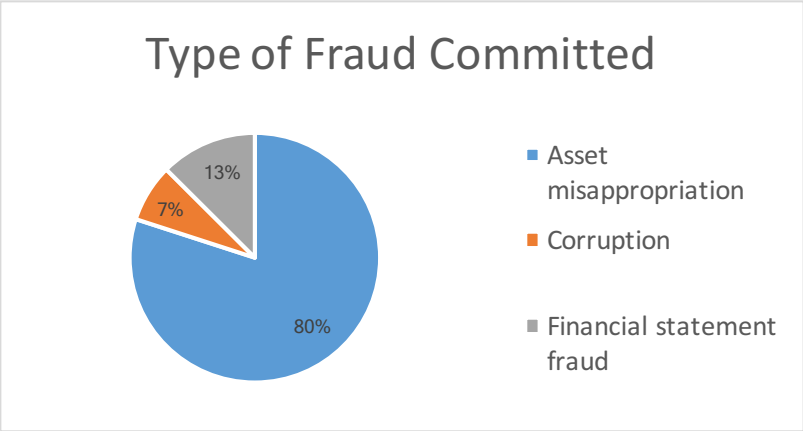

Figure 5: Type of Fraud Committed

Asset misappropriation is the most common type of fraud from the data set, which is consistent with research done through the ACFE *Report to the Nations*. Both financial statement fraud and corruption make up smaller percentages of the overall data. In order to document the use of Well's fraud hierarchy, each category of fraud was broken down based on various levels.

First, financial statement fraud was analyzed based on the initial layer of characterization, financial or non-financial. Figure 6 is depicted below, highlighting the prevalence of financial instances. ACFE *Report to the Nations* emphasizes that, although financial statement fraud is not as common, it is very costly to an organization. According to the ACFE data, financial statement fraud occurred in less than 10% of cases, but caused a median loss of $975,000 (ACFE, 2016, pg. 4). This loss is significantly higher than the monetary implications of asset misappropriation and corruption.

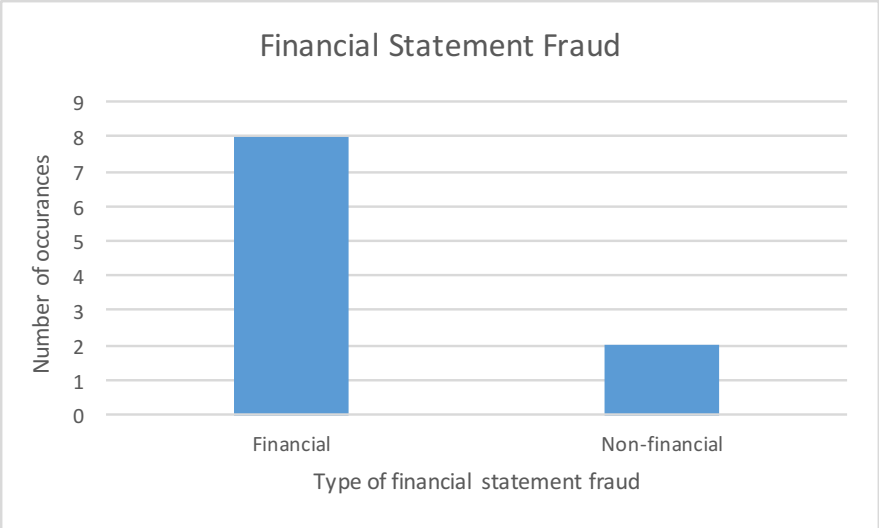

Figure 6: Frequency of Financial Statement Fraud

Next, asset misappropriation was evaluated based on the theft of cash and the occurrence of larceny, skimming, and fraudulent disbursements. According to the thesis data, the theft of cash was more common at 90%, than the misappropriation of inventory and other assets, which composed of 10% of the cases studied. The ACFE reports that asset misappropriation was the most common type of fraud, indicated in more than 83% of cases, but it was the lowest median loss at $125,000 (ACFE, 2016, pg. 4). Larceny, skimming, and fraudulent disbursements are the second layer of characterization based on Wells hierarchy. The frequency of each type of cash asset misappropriation is depicted as Figure 7.

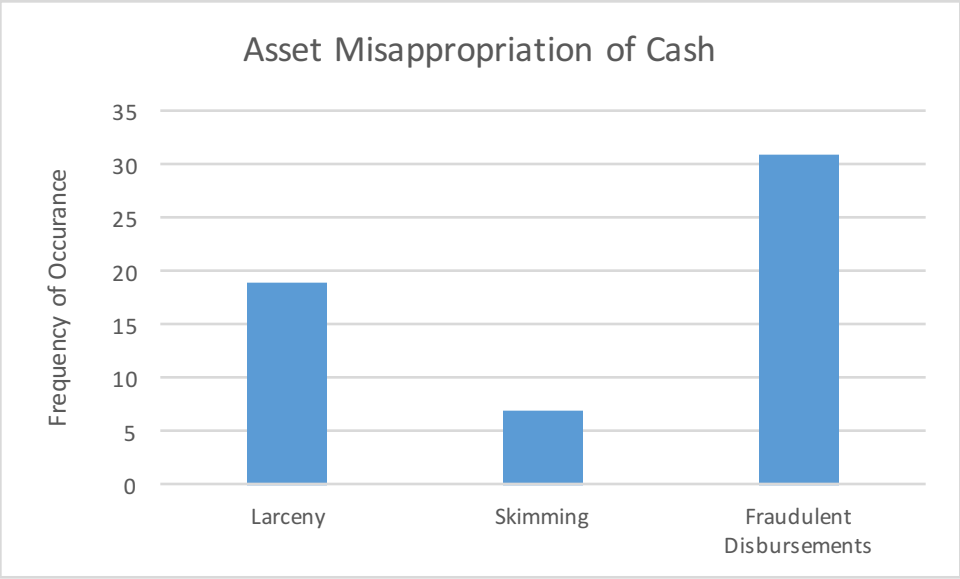

Figure 7: Frequency of Asset Misappropriation Based Fraud

Finally, forms of corruption were analyzed to determine the frequency of their occurrence within the data set. Corruption has one layer of characteristics, and of that, only two were determined to be present within the cases researched. It was determined that conflicts of interest and economic extortion were the types of corruption within the data. The ACFE data determined that corruption cases were in the middle of financial statement fraud and asset misappropriation with 35.4% of cases being reported as such, and a median loss of $200,000 (ACFE, 2016, pg. 4). Figure 8 depicts the frequency of conflicts of interest, composed of sales schemes and purchasing schemes, compared to economic extortion.

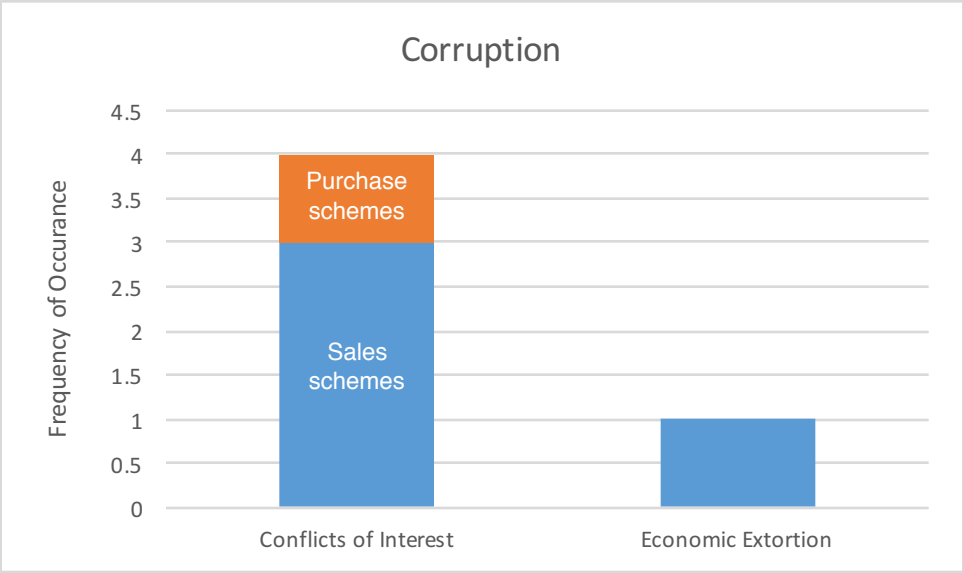

Figure 8: Frequency of Corruption Based Fraud

The culmination of primary thesis data and ACFE research draws similar conclusions. Asset misappropriation is the most common type of fraud, in comparison to corruption and financial statement frauds. By documenting each type of fraud and characterizing based on Well's hierarchy, comparisons and trends across the different cases can be analyzed. These trends can be compared to the COSO framework, which evaluates internal controls. Risk assessment is a COSO component that can be directly related to fraud prevention and detection.

Risk assessment manages business risk from both external and internal sources. It involves the identification and assessment of risks, as well as, risk tolerances (COSO, 2014, par. 1-5). COSO had determined that management has the responsibility to establish company objectives in relation to operations, reporting, and compliance standards (COSO, 2014, par. 1-5). Risks are then analyzed based on those objectives. A source of risk for a company is

fraud. Management objectives should successfully outline the responsibility of employees in relation to fraud risk. Operation objectives look to minimize the risk of asset misappropriation, reporting objectives minimize financial statement fraud, and compliance standards set regulations for corruption. Successful risk management of a company identifies weaknesses in internal controls which can be influenced by both internal factors, such as fraud, and external factors.

COSO Components and Principles

The COSO framework involves both components and principles, which are outlined and described previously. The data was categorized and analyzed based on both the COSO components and principles violated within each fraudulent act. The frequency of violations can determine a pattern of weaknesses in company internal controls. Fraud cases were assessed independently, and it was found that each case violated one or more COSO component and principle. Figures 9 and 10 show the frequency each COSO component and

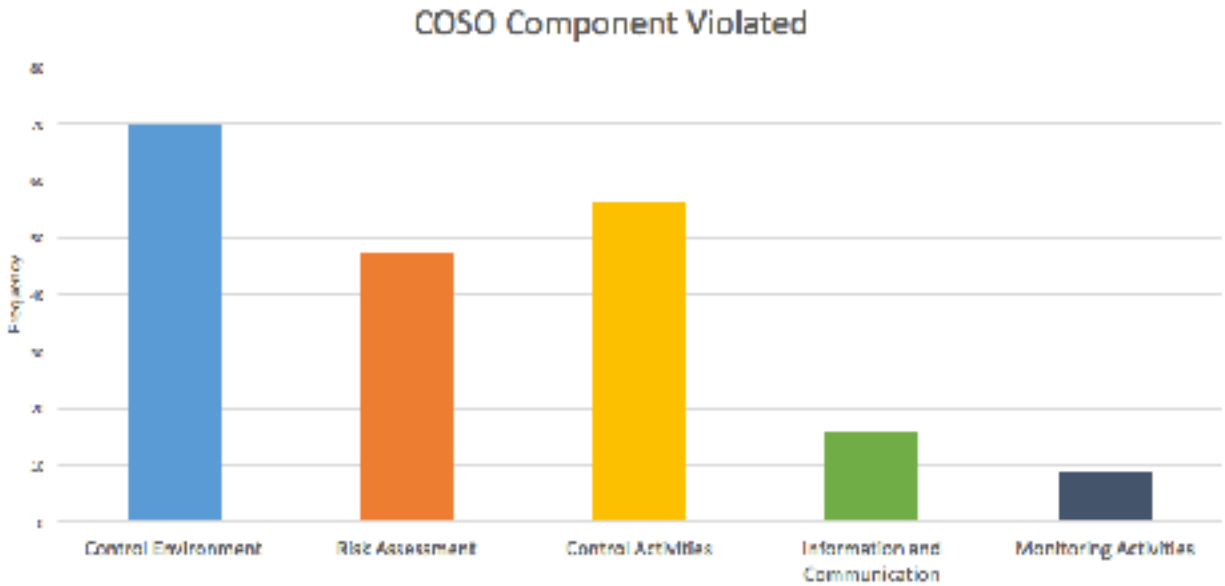

Figure 9: Frequency of COSO Component Violation

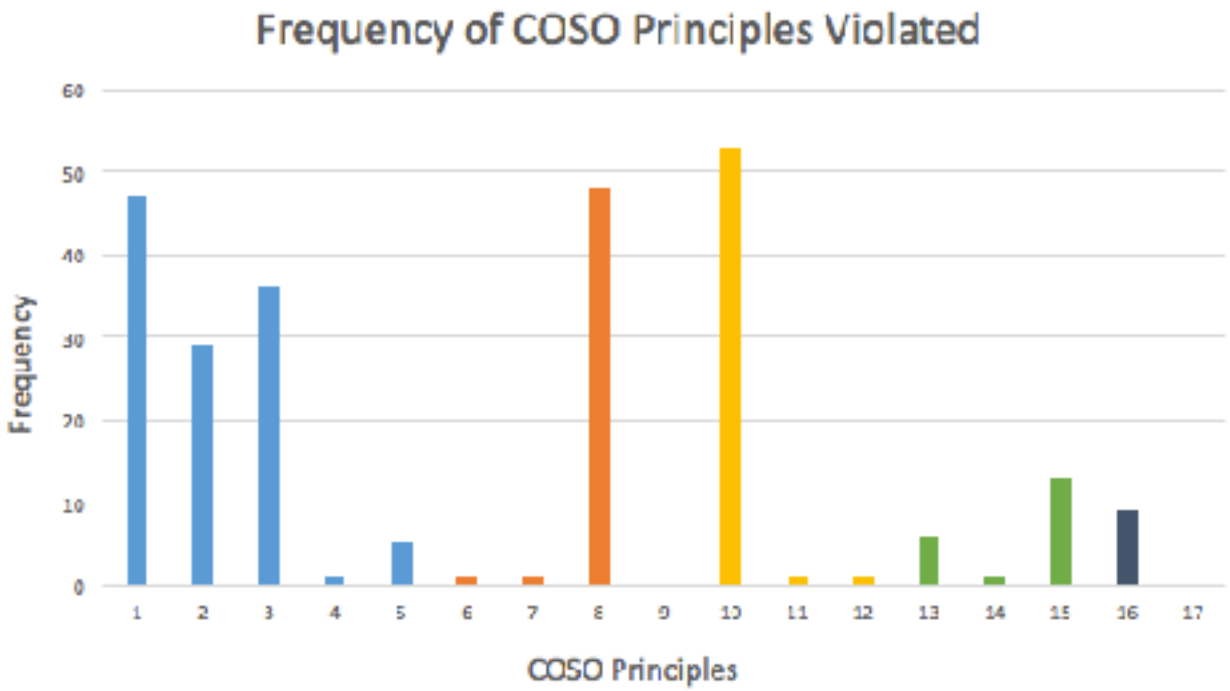

Figure 10: Frequency of COSO Principle Violation

principle was faulted, respectively. The COSO principles are coordinated to the components via color.

Discussion of each COSO component is provided below with COSO principles embedded within the analysis. This section describes the elements within fraud cases that designated a violation, and includes an example from the data set that emphasizes the violation of each principle.

Control Environment

The control environment was the most prominently violated COSO component. This result is expected since an entity's ethical standards and obligations directly relates to fraud risk and

the control environment. To violate the control environment component, the fraud case must have depicted any of the following factors: lack of integrity, no management oversight of internal controls, no hierarchy of authority or responsibility for employees, faltered alignment of organizational objectives, or lack of accountability for internal controls. These criteria are directly related COSO principles of the control environment.

An example of a control environment violation from the thesis data set is Fraud Case #53. As a brief summary, Stuart B. Millner and Associates is an auction business in the eastern district of Missouri, owned and operated by Stuart Millner. Millner misdirected profit and sales revenue from auction clients to pay company expenses. He reported to customers that auctioned items had sold for less than they actually were (Department of Justice, 2016).

The control environment was violated in this example due to the fact the owner of the company did not act ethically when selling customer property. Top management is expected to "establish directives, guidance, and control to enable management and other personnel to understand and carry out their internal control responsibilities" (COSO, 2014, par. 1-5). The design and evaluation for authority responsibility were not executed with respect to internal controls functions. These weaknesses were discussed as part of the data evaluation for each case. Possible internal controls and technology functions of the internal controls were addressed for each case as well. For this example, possible internal controls for Fraud Case #53 include the requirement of client approvals for deposits and withdrawals, and also segregation of duties between custody of goods and reporting of sales. Also, the reconciliation of company revenue accounts and customer revenue accounts to verify sales

price would be beneficial. Technological functions include automatically entering sales transactions into the company accounting system so no falsification can be made. It was also noted as an additional recommendation that oversight is important because the owner of the company committed the fraud. In this example, oversight could be potentially from city governance.

COSO principles can also be evaluated. In Fraud Case #53, several principles can be identified as being negligent within this organization. With relation to the control environment, this case violated COSO principle number three. The principle states: "management establishes structures, reporting lines, and appropriate authority and responsibility in pursuit of objectives" (COSO, 2014, par. 1-5). As indicated above, Stuart B. Millner and Associates disregards internal controls and ethical standards. Specifically, their lack in segregation of responsibilities within the company provided an opportunity to commit fraud, which directly correlates with COSO principle number three. Each level of the company should have designated authorities and responsibilities which provide for a distinct hierarchy of the control environment. The implementation of these internal controls would create a system of accountability for the company, set a tone of compliance, and reduce fraud risk.

A lack of a strong control environment, or any COSO component, makes a company more susceptible to fraud. The control environment in particular sets a strong foundation for a company which reinforces the expectations throughout the various levels of an organization (COSO, 2014, par. 1-5). When there is a lack in the control environment, the support for the

other COSO components is also lacking, which increases a corporations fraud risk. Investing in the development of a sufficient control environment can be instrumental in a company's success.

Control Activities

The next most violated COSO component was control activities. A lack of control activities provides an opportunity for fraud, which is illustrated above as a component of the fraud triangle. Control activities are defined as "actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out" (COSO, 2014, par. 1-5). Violation of this component requires evidence of any of the following aspects: lack of development in internal controls for organizational objectives, no technological controls to support organizational objectives, or no expectations deployed regarding control activities. Again, these criteria directly relate to the control activity COSO principles.

An example involving the violation of the control activities component is Fraud Case #3. This case involved Stadium Grill, a restaurant in the central district of Illinois. James Michael Hill, the general manager, committed wire fraud from 2009-2013. Hill had access to the restaurant accounting system in order to correct employee errors in entering purchases. He changed records to delete certain cash sales, decrease the amounts of cash sales, and classify cash sales as gift card purchases. He then stole and used the cash generated for his personal use (Department of Justice, 2016).

This is an example of the control activities violation because there were no internal controls activities to prevent the misuse of accounting functions, indicating COSO principle number ten and eleven were misappropriated. Principle ten states: “selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels” (COSO, 2014, par. 1-5). While principle eleven dictates: “selects and develops general control activities over technology to support the achievement of objectives” (COSO, 2014, par. 1-5). These principles allow for successful implementation of internal controls within an organization, such as segregation of duties, in order to support business objectives. Suggestions for internal controls for Fraud Case #3 include implementation of an approval system that requires verification of the changes made in the company accounting system by an independent party, such as the owner. As a technology function, documentation should be maintained on the system in order to alert personnel of changes being made. These additions can successfully address the lack on control activities within a company.

The control activities of an organization mitigate the opportunities for the occurrence of fraud. The COSO framework is a dynamic and integrated model, meaning that all the functions build off each other to create a cohesive set of standards for internal controls. The development of control activities can impact operating functions, reporting functions, and compliance functions within a business. In this sense, control activities can maintain dual purposes and promote the objectives of an organization in multiple values. The implementation of control activities is essential for a company to achieve its objectives.

Risk Assessment

Risk assessment is an important component within a company's internal control network, and it was also frequently violated within the fraud case study. To understand risk assessment, the definition of risk related to fraud and internal controls is: "the possibility that an event will occur and adversely affect the achievement of objectives" (COSO, 2014, par. 1-5). Subsequently, COSO defines risk assessment as a "dynamic and iterative process for identifying and assessing risks to the achievement of objectives" (COSO, 2014, par. 1-5). For the purpose of this study, violation of the risk assessment components include the misuse of risk assessment principles; examples include: unclear definition of organizational objectives, no risks were identified or analyzed, lack of consideration in the potential of fraud, or no assessed changes or implementation of changes that could have impacted the internal control system.

An example of faulty risk assessment is documented as Fraud Case #26. Marty Turner Farms operates in the central district of Illinois. Amy Ward was the bookkeeper in this institution and she committed bank fraud from 2011-2015. The owners of the company left pre-signed checks in Ward's care when they were expected to be gone for long periods of time. Ward wrote these checks to herself and deposited them in an account she shared with her husband. She created fraudulent entries in the accounting software program to conceal her actions (Department of Justice, 2016).

This case illustrates a lack of risk assessment principles, specifically principle number eight which states: "considers the potential for fraud in assessing risks" (COSO, 2014, par. 1-5).

The owners of the company did not evaluate the potential risks of fraud or how these actions could go against company objectives based on their actions regarding the management of their business. Internal controls that could be implemented in regard to Fraud Case #26 include the requirement for reconciliation of accounting records to account balances. Also, segregation of duties should be implemented, one employee should write the checks, and an independent employee should enter the information into the accounting system. As a technology function, there could be a notification system that alerts an outside management member of account disbursements. These functions could effectively demonstrate risk assessment procedures and mitigate the opportunity for fraud.

In reiteration, the COSO frameworks is an all encompassing tool for a company. Risk assessment is dependent on the prior establishment of organizational objectives, authority and responsibility platforms, and the creation of control activities (COSO, 2014, par. 1-5). All organizations face risk independent of size, structure, industry, and level. Assessing risks requires the identification of various internal and external possibilities that may adversely affect a company. Although risks cannot be reduced to zero, strategic risks can be monitored and evaluated, and unfavorable risks can be set to tolerant levels through internal controls.

Information and Communication

Information within an organization is a constant, dynamic tool. Information documentation and communication is a regularly occurring activity within an internal control system. COSO denotes that it is management's responsibility to "obtain or generate and use relevant and quality information from both internal and external sources to support the functioning of

other components of internal controls" (COSO, 2014, par. 1-5). Violations of the information and communication component include: generation of faulty or error-based information, lack of internal communication, or lack of external communication. These violations correlate with the information and communication principles outlined by COSO.

For example, Fraud Case #4 describes a fraud committed within John Deere and Company by Harvey Ulfers, an employee. Ulfers committed wire fraud and money laundering from 2004-2013. He created falsified internal documents that allowed him to sell scrap metal below market value. He also used a third party to launder the fraudulent proceeds for his own personal use.

Ulfers violated the information and communication COSO component and principles. There were weaknesses in John Deere's internal controls in regard to creating these documents, providing Ulfers with the opportunity to produce and communicate fraudulent information. These activities are related to COSO principle number thirteen. Principle thirteen states: "generates and uses relevant, quality information to support the functioning of other components of internal controls" (COSO, 2014, par. 1-5). Within this principle is the requirement and expectation to identify factors such as the timeliness, accuracy, accessibility, and completeness of information used by a company. Also, data processing and transformation based on this information should be monitored in order to continuously generate relevant and quality information. Types of internal controls that could have been initiated within Fraud Case #4 include maintaining a valid price list that documents the range of acceptable selling prices for a product. Also, sales should be verified based on the

selection of reputable and approved purchasers. For technology functions, sales should be required to be entered based on the price list. In addition, the sales should be verified with the accounts receivable and revenue account in order to maintain accurate information. Likewise, the purchases should be verified with the approved list of companies. These controls would increase the reliability of both information and communication within the organization and externally.

Company generated information relies on the functions of the other COSO components. Relevant and accurate information will be gathered based on proper control environment standards and implementation of control activities. Even more, the issuance of quality information will return to support the other functions of the COSO components by ensuring the authenticity of the organization. Both internal and external sources use company produced information, therefore the quality of communication regarding this information also supports organizational objectives.

Monitoring Activities

The last COSO component, and least violated according to the thesis data set, is monitoring activities. Monitoring activities are defined as "ongoing evaluations, separate evaluations, or some combination of the two used to ascertain whether each of the five components of internal control are present and functioning" (COSO, 2014, par. 1-5). Violations of the COSO component are likewise violations of the COSO principles, including: no evaluations regarding an entity's internal controls, or lack of communication regarding internal control deficiencies.

An example of violation of monitoring activities is Fraud Case #43. Starkey Laboratories Inc. located in Minnesota faced several fraudulent actions. Jerome Ruzicka, Scott Nelson, Lawrence Miller, Jeffrey Taylor, and Lawrence Hagen were employees of the company and were charged with embezzlement. The employees created a fictitious company to which Starkey was required to pay consulting fees and commissions to. The money was directed to the fraudsters' bank accounts, and no services were provided. Also, they used their fake company to buy discounted merchandise, which they then re-sold to other manufacturers for profit. The employees also forged signatures to transfer assets to their fake companies. Starkey's company reports were falsified in order to conceal the transfer of money (Department of Justice, 2016).

Due to the large number of fraudulent acts committed by these employees, it is evident that Starkey lacks sufficient monitoring activities. Evaluation of internal controls should prove shortcomings in several processes, which should be influenced by all five COSO components, and several COSO principles. A specific principle violated is number sixteen: "the organization selects, develops, and performs ongoing evaluations to ascertain whether the components of the internal control are present and functioning" (COSO, 2014, par. 1-5). The lack of such evaluations contributes to the fraud risk within the organization. Internal controls that should be present for Fraud Case #43 include the monitoring of employee activists to determine risks associated with certain authorization procedures, the assessment of employee accountability, and the segregation of duties within the accounting system. For technology functions, the company accounting system should automatically enter

transactions. There should also be a system for monitoring account activity, in which there is a detection process for unusual and suspicious activities. Finally, there should be an approved vendor list in which a company approves the suppliers of services. These records should be maintained and updated by authorized personnel.

Monitoring activities can be broken down into two categories: ongoing evaluations and separate evaluations (COSO, 2014, par. 1-5). Ongoing evaluations provide timely information by continuously referencing a specific business process; whereas separate evaluations are determined by management based on business objectives. Both types of monitoring activities assess whether internal controls are present and functioning. Evaluating the effectiveness of an internal control is necessary in order to prevent, detect, and correct fraudulent acts.

Limitations

The limitations of this research provide a holistic analysis of the data set. In particular, the number of sources evaluated was limited in scope. All data is attributed to the Department of Justice press release files, which documents prosecuted, high-profile cases. This source had limitations individually, as it provided concise and limited details regarding the cases evaluated. In addition, data from this source was filtered to only encompass financial fraud in the Midwest during 2016. Further details and a broader scope would have provided a richer analysis and created a stronger support for the applied conclusions.

Conclusion

Fraud has financial, economic, and social bearings for an organization. Understanding why, when, and where corporate fraud happened provided conclusions on how to mitigate fraud risk within an organization. The evaluation of positions concludes the likelihood of fraud based on level of employee, while the evaluation of the type of fraud indicates which type of fraud is most likely to be committed within an organization. Through the assessment of each COSO component, in relation to COSO principles, generalized internal control activities and technology functions were identified. These results portrayed trends which can be versatile and applied to a variety of organizations; while the documentation of these cases provided insights on how to routinely improve internal control functions. Understanding each component and principle within the COSO framework allowed for recommendations to be made to decrease the opportunity and potential for fraud risk.

Literature Cited

American Institute of Certified Public Accountants. (2002). *Statement of Position 82, Section 316:* Consideration of Fraud in a Financial Statement Audit.

Association of Certified Fraud Examiners. (2016). Report to the Nations on Occupational Fraud and Abuse. Retrieved April 28, 2017, from http://www.acfe.com/rttn2016.aspx

Charleston Man Charged with Embezzling from Former Employer. (2016, September 08). Retrieved April 23, 2017, from https://www.justice.gov/usao-cdil/pr/charleston-man-charged-embezzling-former-employer

Civic Impulse. (2017). H.R. 3763 — 107th Congress: Sarbanes-Oxley Act of 2002. Retrieved from https://www.govtrack.us/congress/bills/107/hr3763

Components and Principles. (2014, November 9). Retrieved February 6, 2017, from http://aaahq.org/COSO/Content/COSO-Frame-1/coso-frame1_components_and_principles

Components of Internal Control. (2014, November 9). Retrieved February 6, 2017, from http://aaahq.org/COSO/Content/COSO-Frame-1/coso-frame1_components_of_internal_control#coso-frame1_control_environment

COSO Internal Control — Integrated Framework Principles [Digital image]. (2013). Retrieved January 29, 2017, from coso.org

Effective Internal Control. (2014, November 09). Retrieved February 05, 2017, from http://aaahq.org/COSO/Content/COSO-Frame-1/coso-frame1_effective_internal_control

Eisinger, J. (2004, January 02). Year of the (Shrugged Off) Scandal. Retrieved January 18, 2017, from http://www.wsj.com/articles/SB107273198326302800

The Ever-Rising Cost Of Fraud. (2016, August 30). Retrieved January 31, 2017, from http://www.pymnts.com/fraud-attack/2016/fraud-costs-security-hackers/

Five Indicted For Massive Fraud Perpetrated Against Starkey Laboratories. (2016, September 21). Retrieved April 23, 2017, from https://www.justice.gov/usao-mn/pr/five-indicted-massive-fraud-perpetrated-against-starkey-laboratories

Former Deere Employee Charged with Wire Fraud, Money Laundering. (2016, April 05). Retrieved April 28, 2017, from https://www.justice.gov/usao-cdil/pr/former-deere-employee-charged-wire-fraud-money-laundering

Franklin County Man Indicted on Fraud Charges. (2016, April 07). Retrieved April 23, 2017, from https://www.justice.gov/usao-edmo/pr/franklin-county-man-indicted-fraud-charges

Franklin, M. (2016). Sarbanes-Oxley Section 404: A Historical Analysis. Journal of Accounting & Finance, 16(4), 56-69. Retrieved January 25, 2017.

The Fraud Triangle [Digital image]. (2017). Retrieved January 29, 2017, from http://www.acfe.com/fraud-triangle.aspx

Ghosn, A (2017). Segregation of Duties. Retrieved February 05, 2017, from https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Auditing/InternalControl/Pages/value-strategy-through-segregation-of-duties.aspx
From the American Institute of Certified Public Accountants (AICPA).

McNally, S. (2013). The 2013 COSO Framework & SOX Compliance: One Approach to an Effective Transition. Committee of Sponsoring Organizations of the Treadway Commission. Retrieved January 18, 2017.

Mokhiber, P. B. (2015, September 08). 20 Things You Should Know About Corporate Crime.

Retrieved January 18, 2017, from http://hlrecord.org/2015/03/20-things-you-should-know-about-corporate-crime/

Rezaee, Z. (2002). Financial Statement Fraud: Prevention and Detection. New York: Wiley.

Romney, M. B., & Steinbart, P. J. (2015). Accounting Information Systems (13th ed.). NJ: Pearson Education Inc.

Rushville Woman Pleads Guilty to Defrauding Former Employer. (2016, December 02). Retrieved April 23, 2017, from https://www.justice.gov/usao-cdil/pr/rushville-woman-pleads-guilty-defrauding-former-employer

Sarbanes-Oxley Act Section 404 . (2002). Retrieved May 05, 2017, from http://www.soxlaw.com/s404.htm

Wells, J. T. (2011). Corporate fraud handbook: prevention and detection (3rd ed). Hoboken, NJ: John Wiley & Sons.

Appendix A

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
1	Diversified Behavioral Comprehensive Care (DBCC)	George E. Smith	Owner and operator	Mail fraud and money laundering	Illinois	2008-2009
2	Kankakee Valley Park District	Roy Collins	Executive director	Wire fraud and mail fraud	Illinois	2013-2015
3	Stadium Grill	James Michael Hill	General manager	Wire fraud	Illinois	2009-2013
4	Deere and Company	Harvey Ulfers	Employee	Wire fraud and money laundering	Iowa	2004-2013
5	Capital Management Associates Inc.	Charles J. Dushek	President of Lisle-based store	Securities fraud	Illinois	2008-2012
6	Local 6 of the International Union of Bricklayers and Allied Craft workers	David Fleury	President	Embezzlement	Illinois	2011-2014
7	Quadrant 4 System Corporation	Nandu Thondavadi and Dhru Desai	CEO and CFO	Wire fraud and falsifying financial reports	Illinois	n/a
8	A.P. Gold Realty & Management Inc.	Alan P. Gold	Owner and operator	Mail fraud	Illinois	2010-2014
9	Perdel Contracting Co.	Elizabeth Perino	Owner	Wire fraud and mail fraud	Illinois	n/a
10	"Company A"	Salvatore Cribari	Customer	Wire fraud	Illinois	n/a
11	Right Field Rooftops LLC	Marc Hamid and Joseph Gurdak	Owner and accountant, respectively	Mail fraud: illegally structuring financial transactions,; mail fraud: and willfully filing a false income tax return	Illinois	2008-2011
12	Marketaction Inc., Marketaction Advisors LLC, Marketaction Capital Management LLC	Clayton Andrew Cohn	Owner	Wire fraud	Illinois	2010-2013

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)			
1	Corruption	Conflicts of interest	Sales schemes	
2	Asset misappropriation	Cash	Larceny	Of cash on hand
3	Asset misappropriation	Cash	Skimming	Understated sales and receivables
4	Corruption	Conflicts of interest	Sales schemes	
5	Asset misappropriation	Cash	Larceny	From the deposit
6	Asset misappropriation	Cash	Larceny	Of cash on hand
7	Financial statement fraud	Financial	Asset/Revenue overstatements	Concealed liabilities and expenses
8	Financial statement fraud	Financial	Asset/Revenue overstatements	Fictitious revenues
9	Financial statement fraud	Financial	Asset/Revenue overstatements	Fictitious revenues
10	Asset misappropriation	Inventory and all other assets	Larceny	False sales and shipping
11	Financial statement fraud	Financial	Asset/Revenue understatements	
12	Financial statement fraud	Financial	Asset/Revenue understatements	

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
1	X					1	2	5	
2	X	X	X			2	5	8	10
3	X		X		X	4	11	16	
4	X		X			3	10		
5	X			X	X	3	15	16	
6	X	X	X			2	5	8	10
7	X		X			1	2	3	12
8	X			X		2	13	15	
9	X					2			
10		X	X		X	6	8	10	16
11	X			X		1	2	13	15
12	X			X		1	2	13	15

Case #	Internal Control(s)	Technology Functions
1	Funds are automatically entered on the company's financial records. Bank accounts are held separate from owner and records are available to creditors/lenders.	Direct deposit and updated account balances once money enters the company bank account.
2	Require reconciliation of accounting records to credit card statements.	Create a notification system that alerts an outside management member of expenses charged to the account.
3	Approval system that verifies the changes made in the company accounting system.	Documentation maintained on the company accounting system in order to verify changes made.
4	Price list that documents the range of acceptable revenues for a product. Only verify selection of reputable and approved purchasers/suppliers.	Function that requires sales to be entered based on price list. Verifies the sale with accounts receivable and sales revenue account. Verify the purchaser/supplier to the approved list of companies.
5	Segregate the information surrounding cliental and employees.	Form that requires information be entered before proceeding with a transaction.
6	Require reconciliation of accounting records to credit card statements and bank statements.	Create a notification system that alerts an outside management member of expenses charged to the account.
7	Validate changes in financial statement information by requiring sign-offs from various department employees and manager's in order to segregate duties.	Cross reference information throughout an entities accounting system in order to detect any misstatements.
8	Create separate duties -- One person receives and records the cash. One person deposits the cash. One person reconciles the balance.	Require client authorization for the removal and use of cash. Verify the reconciliation balances to the statement account balances.
9	Require sign-offs from client that verify the work was complete. Verify the sign-offs to payments received.	Use punch cards or another method of employee verification in order to document the work was completed.
10	Issue random inspections of customer receipts and verify the purchaser.	Visual monitoring and increase security of store activates to prevent stolen merchandise. Upgrade identity verification process in order to deter the use of fake IDs.
11	Separate accounting duties and owner/operator activities. Require accounting department to submit account balances directly to the service organization.	Automated system that computes ticket sales per game and enters the information into the account balances. Allow Cubs to have visual access to these balances in order to reconcile the numbers at the end of the period.
12	Automatic entry into the accounting system for withdrawals and deposits into client accounts.	Require client authorization for the removal and use of cash. Verify the reconciliation balances to the statement account balances.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
13	D.J. Mosier and Associates	Delores J. Mosier	Financial advisor	Wire fraud	Illinois	n/a
14	First State Bank	Kayla Bergstrom	Vice-President	Embezzlement	Illinois	2010-2014
15	Phezer Enterprises Inc.	Joseph Michael Phelan	President	Concealment of assets from a Bankruptcy Trustee	Illinois	2008
16	International Resorts Resale, Resort Closing Services, Timeshare Consolidators, and Transfer my Timeshare	Gilbert Freeman	Operator	Wire fraud	Illinois	2008-2015
17	McKinsey & Company, Inc. and State Farm	Navdeep Arora and Matthew Sorensen	Partner and consultant, respectively	Wire fraud	Illinois	n/a
18	Windoor	Dean Kreher	Partner	Structuring financial transactions	Illinois	n/a
19	American Federation of State, County and Municipal Employees, Local 415	Jeffrey Magelitz	Treasurer	Embezzlement	Illinois	2012-2013
20	East St. Louis Township	Oliver Hamilton	Supervisor	Wire fraud	Illinois	2011-2016

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
13	Asset misappropriation	Cash	Larceny	Of cash on hand	
14	Asset misappropriation	Cash	Larceny	Of cash on hand	
15	Asset misappropriation	Inventory and all other assets	Misuse		
16	Asset misappropriation	Skimming	Sales	Unrecorded	
17	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Shell company
18	Asset misappropriation	Cash	Skimming	Sales	Unrecorded
19	Asset misappropriation	Cash	Larceny	Of cash on hand	
20	Asset misappropriation	Cash	Larceny	Of cash on hand	

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
13	X	X	X			1	3	8	10
14	X	X	X			1	3	8	10
15	X			X	X	1	3	15	16
16	X			X		1	2	15	
17	X	X	X			1	7	8	10
18	X	X	X			1	3	8	10
19	X	X	X			1	3	8	10
20	X	X	X			1	5	8	10

Case #	Internal Control(s)	Technology Functions
13	Require approval of client deposits and withdrawals. Financial advisors must submit report with their activity which can be reconciled with client records/confirmations.	Verify account validity by having an approved list of investment options. Create notification system which alerts management of activity outside of select investments.
14	Authorization of select individuals to access information of a particular account.	Create a notification system that alerts an outside management member of changes made in an account.
15	Approval system that requires department heads to sign-off on bankruptcy. Reporting system the President must follow to keep executives, board of directors, and employees updated on the company financial position.	Require that higher level board of directors and management team receive reports on the financial capabilities of the company.
16	Automatic entry into the accounting system for withdrawals and deposits into client accounts.	Require client authorization for the removal and use of cash. Verify the reconciliation balances to the client account balances.
17	Separate approval process for executives and employees regarding service work. Require approval from a third party that verifies work that was performed.	Use punch cards or another method of employee verification in order to document the work was completed.
18	Segregate data entry duty and administrative responsibilities.	Automatically enter transactions into company accounting system.
19	Validate disbursements and payments through several executives. Reconcile the bank statement records with the check balance.	Automatically enter deposits and disbursements into company accounting system.
20	Require reconciliation of accounting records to credit card statements.	Create a notification system that alerts an outside management member of expenses charged to the account.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
21	Scott Credit Union	`	Business Relationship Manager	Financial institution fraud, misapplication of assets, money laundering, making a false record with the intent to deceive	Illinois	2005-2014
22	Lotawata Creek Inc. and Lotawate Creek Southern Grill	Rodney Archer and Kenneth Archer	Owners	Conspiracy to obstruct the IRS in the assessment and collection of federal income taxes	Illinois	2010-2015
23	Doctor's Office	Jerry Akin	Employee	Wire fraud	Illinois	n/a
24	Pinckneyville Rural Fire Protection District	Tammy Kallerman	Bookkeeper	Mail fraud	Illinois	2004-2013
25	U.S Department of Veteran's Affairs	Terrance Starks	Employee	Wire fraud and aggravated identity theft	Illinois	n/a
26	Marty Turner Farms	Amy Ward	Bookkeeper	Bank fraud	Illinois	2011-2015
27	First Farmers Financial LLC	Nikesh Patel	CEO	Wire fraud	Illinois	2012-2014
28	First Farmers Financial LLC	Timothy Fisher	President and COO	Money laundering	Illinois	2012-2014
29	Rock Capital Markets LLC	Thomas Lindstrom	Trader	Commodities fraud and wire fraud	Illinois	2014-2015

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
21	Asset misappropriation	Inventory and all other assets	Misuse		
22	Financial statement fraud	Financial	Asset/Revenue understatements		
23	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Personal purchases
24	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Concealed checks
25	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Altered Payee
26	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Altered Payee
27	Financial statement fraud	Nonfinancial	Internal documents		
28	Financial statement fraud	Financial	Asset/Revenue overstatements	Improper asset valuations	
29	Asset misappropriation	Inventory and all other assets	Misuse		

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
21	X		X			1	3	10	
22	X			X		2	15		
23	X	X	X			1	3	8	10
24	X	X	X			1	3	8	10
25	X	X	X			1	3	8	10
26	X	X	X			3	8	10	
27	X			X		2	13	14	
28	X			X		2	13	15	
29	X		X	X		1	10	13	

Case #	Internal Control(s)	Technology Functions
21	Require approval of client deposits and withdrawals. Financial advisors must submit report with their activity which can be reconciled with client records/confirmations.	Automatically enter transactions into company accounting system.
22	Separate accounting duties and owner/operator activities. Require accounting department to verify account balances.	Leave a digital footprint of changes made in an accounting system. Automatically flag changes that significantly alter the transaction.
23	Require reconciliation of accounting records to account balances.	Create a notification system that alerts an outside management member of expenses charged to the account.
24	Require reconciliation of accounting records to account balances.	Create a notification system that alerts an outside management member of expenses charged to the account.
25	Require reconciliation of accounting records to account balances.	Create a notification system that alerts an outside management member of expenses charged to the account.
26	Require reconciliation of accounting records to account balances. Separate the responsibilities -- one person writes the checks and one person enters the information into the accounting system.	Create a notification system that alerts an outside management member of account disbursements.
27	Separate accounting duties and owner/operator activities. Require accounting department to verify account balances.	Verify account validity by having an approved list of investment options. Create notification system which alerts management of activity outside of select investments.
28	Separate accounting duties and owner/operator activities. Require accounting department to verify account balances.	Automatically enter transactions into company accounting system.
29	Reconcile investment activity with market results. Require confirmation from outside sources to verify the balances of the investments.	Automatically enter transactions into company accounting system.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
30	A Lamp Concrete Contractors Inc.	Joseph Lampignano	Co-owner	Mail fraud	Illinois	2008-2013
31	A Lamp Concrete Contractors Inc.	Giovanni Traversa	Superintendent	Making false statements to the FBI and U.S. Department of Labor Office of Inspector General	Illinois	2008-2013
32	Peosta Warehouse	Chad Michael Saeugling	Supervisor	Mail fraud	Iowa	2004-2014
33	Mason City Dental	Pamela Harris	Office manager	Wire fraud	Iowa	2005-2014
34	Primus Construction Inc.	Teresa Meeks	Accountant	Wire fraud	Iowa	2009-2014
35	Country Bancorporation	Heidi Wagler	Board officer	Embezzlement	Iowa	2004-2013
36	SCICAP Credit Union	Linda Clark	Employee	Embezzlement	Iowa	1978-2015
37	Ames Chi Omega Alumnae Association	Andrea Baker	Treasurer	Mail fraud	Iowa	2000-2014

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
30	Financial statement fraud	Nonfinancial	External documents		
31	Corruption	Economic extortion			
32	Asset misappropriation	Inventory and all other assets	Larceny	False sales and shipping	
33	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Forged endorsement
34	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Altered Payee
35	Asset misappropriation	Cash	Fraudulent disbursements	Payroll schemes	Workers' compensation
36	Asset misappropriation	Cash	Larceny	Of cash on hand	
37	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Altered Payee

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
30	X			X		1	3	15	
31	X					1	3		
32	X	X	X			2	8	10	
33	X	X	X			3	8	10	
34	X	X	X			3	8	10	
35	X	X	X			2	8	10	
36	X	X	X			3	8	10	
37	X	X	X			1	2	8	10

Case #	Internal Control(s)	Technology Functions
30	Require sign-offs to verify the work was complete. Verify the sign-offs to payments received.	Use punch cards or another method of employee verification in order to document the work was completed.
31	Require sign-offs to verify payment was made. Verify the sign-offs with court system and individuals.	Automatically enter transactions into company accounting system. Require authorization to override.
32	Complete inventory counts and reconcile numbers to the shipment/purchase order records.	Have a list of qualified shipment recipients which is updated based on purchase order forms. Alert appropriate personal if customers outside of the list are being used.
33	Separate the duties. One person writes and administers the checks. Another person reconciles the accounts to the bank statement.	Automatically enter transactions into company accounting system.
34	Separate the duties. One person writes and administers the checks. Another person reconciles the accounts to the bank statement.	Automatically enter transactions into company accounting system.
35	Separate human resource duties and board activities. Require HR department to verify and approve salaries. Require accounting department to verify the salary checks being disbursed.	Create a digital footprint of changes being made into accounts and the company system in order to detect fraudulent acts.
36	Require approval of client deposits and withdrawals. Employees must submit reports with their activity which can be reconciled with client records/confirmations.	Automatically enter transactions into company accounting system.
37	Separate the duties. One person writes and administers the checks. Another person reconciles the accounts to the bank statement.	Automatically enter transactions into company accounting system.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
38	City of Casey	Dorothy Dillinger	City clerk	Mail fraud	Iowa	2009-2014
39	People's Savings Bank of Crawfordsville	Russell Wagler	President	Embezzlement	Iowa	2002-2013
40	M.H.I. Credit Union	Lori Bentler	Employee	Bank fraud	Iowa	2009-2011
41	Patriot Bank	Barbara Baker	CFO	Misapplication of bank funds	Iowa	2012-2013
42	Dblaine Capital, LLC	David Walliver	CEO and CIO	Securities fraud	Minnesota	2010-2011
43	Starkey Laboratories Inc.	Jerome Ruzicka, Scott Nelson, Lawrence Miller, Jeffrey Taylor, and Lawrence Hagen	Employees	Embezzlement	Minnesota	2006-2016

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
38	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Altered Payee
39	Asset misappropriation	Cash	Skimming	Receivables	
40	Corruption	Conflicts of interest	Other		
41	Asset misappropriation	Cash	Larceny	Of cash on hand	
42	Asset misappropriation	Cash	Larceny	Of cash on hand	
43	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Shell company
	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Forged endorsement
	Corruption	Conflicts of interest	Sales schemes		
	Asset misappropriation	Cash	Larceny	Of cash on hand	

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
38	X	X	X			1	2	8	10
39	X	X	X			1	2	8	10
40	X	X	X		X	3	8	10	16
41	X	X	X			2	8	10	
42	X		X		X	2	10	16	
43	X	X	X		X	3	8	10	16

Case #	Internal Control(s)	Technology Functions
38	Separate the duties. One person writes and administers the checks. Another person reconciles the accounts to the bank statement.	Automatically enter transactions into company accounting system.
39	Require approval of client deposits and withdrawals. Separate employee accounts and authorizations from upper level management.	Automatically enter transactions into company accounting system.
40	Specific monitoring for employee investment accounts. Account is overseen by a manager or another employee, authorization for changes is limited.	Automatically enter transactions into company accounting system.
41	Separate accounting duties and executive activities. Require accounting department to verify account balances.	Automatically enter transactions into company accounting system.
42	Separate accounting duties and executive activities. Require accounting department of both the parent and subsidiary to verify account balances. Monitor executive activities.	Automatically enter transactions into company accounting system.
43	Monitoring of employee activities to determine the risks associated with certain authorization procedures.	Automatically enter transactions into company accounting system. Require a system of monitoring for accounts to detect unusual and suspicious activities.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
44	AgQuest Financial Services, Inc.	Diane Eiler	Director of Accounting	Wire fraud	Minnesota	2007-2015
45	Agape House for Mothers and Sierra Young Family Institute	Roberta Barnes	President	Defrauding the State of Minnesota	Minnesota	2002-2012
46	International Association of Heat and Frost Insulators and Allied Workers, Local 34	Scot McNamara	Financial secretary	Embezzlement	Minnesota	2007-2012
47	Wells Fargo	Bradley Smegal	Investment broker	Securities fraud	Minnesota	2007-2013
48	Community Action of Minneapolis	William Davis	CEO	Mail fraud, wire fraud, theft concerning programs receiving federal funds	Minnesota	2007-2014
49	Fairview Ridge, LLC	Patrick Sweeney	Customer	Wire fraud and identity theft	Wisconsin	2007-2011
50	Four Seasons Wood Products	Lisa Buchholz	Bookkeeper	Wire fraud	Wisconsin	2008-2012
51	Wisconsin Coalition Against Sexual Assault	Laura Ewing	Employee	Embezzlement	Wisconsin	n/a
52	Spectrum Brands, Inc.	Brad Volkmann	Sales representative	Wire fraud	Wisconsin	2005-2014

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
44	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Forged endorsement
45	Asset misappropriation	Cash	Skimming	Receivables	Write-off schemes
46	Corruption	Conflicts of interest	Purchase schemes		
47	Asset misappropriation	Cash	Larceny	Of cash on hand	
48	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Personal purchases
49	Asset misappropriation	Inventory and all other assets	Larceny	Asset requisition and transfers	
50	Asset misappropriation	Cash	Fraudulent disbursements	Payroll schemes	Ghost employees
	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Forged endorsement
51	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Altered Payee
52	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Altered Payee

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
44	X		X		X	2	8	16	
45	X					1	2	5	
46	X	X	X			1	3	8	10
47	X	X	X			1	3	8	10
48	X		X		X	2	10	16	
49		X	X			8	10		
50	X	X	X			1	3	8	10
51	X	X	X			1	3	8	10
52	X	X	X			1	3	8	10

Case #	Internal Control(s)	Technology Functions
44	Separate accounting duties and executive activities. Monitor executive activities.	Automatically enter transactions into company accounting system.
45	Funds are automatically entered into the company's financial records. Bank accounts are held separate from owner and records are available to creditors/lenders.	Direct deposit and updated account balances once money enters the company bank account.
46	Require reconciliation of accounting records to credit card statements.	Create a notification system that alerts an outside management member of expenses charged to the account.
47	Require approval of client deposits and withdrawals. Financial advisors must submit report with their activity which can be reconciled with client records/confirmations.	Verify account validity by having an approved list of investment options. Create notification system which alerts management of activity outside of select investments.
48	Separate accounting duties and executive activities. Monitor executive activities.	Automatically enter transactions into company accounting system. Limit changes to select authorized employees which must be reconciled with other accounts.
49	Require approval of client deposits and withdrawals. Reconcile the bank accounts with the customer accounts.	Authorization system which verifies the customer identity in order to prevent the risk of fraud.
50	Segregate bookkeeper duties and require that information entered is reconciled to records to determine fraud risk.	Automatically enter transactions into company accounting system.
51	Reconcile the check records with the balance in the company bank accounts.	Automatically enter transactions into company accounting system.
52	Reconcile the check records with the balance in the company bank accounts.	Automatically enter transactions into company accounting system.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
53	Stuart B. Millner and Associates	Stuart B. Millner	Owner and operator	Bank fraud, mail fraud, and wire fraud	Missouri	n/a
54	F.S	Linda Sweazy	Employee	Mail fraud	Missouri	n/a
55	Garmin	Patricia Webb	Senior payroll specialist	Wire fraud	Missouri	n/a
56	University of Missouri	Carla Rathmann	Administrative officer	Mail fraud and credit card fraud	Missouri	2005-2014
57	Public School and Education Employee Retirement Systems of Missouri	Danny Colgan	Superintendent	Wire fraud	Missouri	1992-2005
58	Hanson Holdings, LLC	Christopher Hanson	Owner	Wire fraud and money laundering	Missouri	n/a
59	Bank of America	Elisha Araiza	Portfolio officer	Embezzlement	Missouri	2011-2015
60	Federal Financial Services, LLC	Billings Chapman	Owner	Wire fraud and mail fraud	Missouri	2011-2014

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
53	Asset misappropriation	Cash	Skimming	Sales	Understated
54	Asset misappropriation	Cash	Fraudulent disbursements	Payroll schemes	Falsified wages
	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Personal purchases
55	Asset misappropriation	Cash	Larceny	Of cash on hand	
56	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Personal purchases
	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Shell company
57	Asset misappropriation	Cash	Fraudulent disbursements	Payroll schemes	Falsified wages
58	Asset misappropriation	Cash	Larceny	Of cash on hand	
59	Asset misappropriation	Cash	Larceny	Of cash on hand	
60	Asset misappropriation	Cash	Skimming	Receivables	Lapping schemes

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
53	X			X		3	15		
54	X	X	X			1	3	8	10
55	X	X	X			1	3	8	10
56	X	X	X			2	8	10	
57	X		X			1	2	10	
58	X			X		1	15		
59	X	X	X			1	3	8	10
60	X			X		1	15		

Case #	Internal Control(s)	Technology Functions
53	Require approval of client deposits and withdrawals. Reconcile the bank accounts with the customer accounts.	Automatically enter sales transactions into company accounting system.
54	Reconcile the check records with the balance in the company bank accounts. Require authorization to change information in the system.	Automatically enter transactions into company accounting system. Track changes and send alerts to management for changes made in specific accounts.
55	Require authorization to change information within the system, approvals from management and department heads. Reconcile original data with records at the end of the year.	Automatically enter transactions into company accounting system. Track changes and send alerts to management for changes made in specific accounts.
56	Create and approved vendor/supplier list. Authorization and background information must be approved in order to add/change information on the list. Reconcile account balances to statements.	Automatically enter transactions into company accounting system. Track changes and send alerts to management for changes made in specific accounts.
57	Require authorization to change information within the system, approvals from Board of Education. Reconcile original data with records at the end of the year.	Automatically enter transactions into company accounting system. Track changes and send alerts to Board for changes made in specific accounts.
58	Require approval of client deposits and withdrawals. Reconcile the bank accounts with the customer accounts.	Automatically enter sales transactions into company accounting system.
59	Require approval of client deposits and withdrawals. Reconcile the bank accounts with the customer accounts. Increase management supervision and confirmation of employee activities.	Automatically enter sales transactions into company accounting system.
60	Require approval of client deposits and withdrawals. Reconcile the bank accounts with the customer accounts.	Automatically enter sales transactions into company accounting system.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
61	Community National Bank	Jo Ann Nickell	Customer service representative	Bank embezzlement	Missouri	2009-2013
62	Assured Management Company	Thomas Hauk	Accountant	Bank fraud, wire fraud counterfeit securities, and money laundering	Missouri	2006-2015
63	ACI Boland Architects	Jane Barnes	Office manager	Wire fraud and bank fraud	Missouri	2006-2011
						2010-2016
64	Nativity of Mary	David Townley	Business manager	Wire fraud	Missouri	2011-2013
65	Joplin South Little League	Diane Heikkila	President	Wire fraud	Missouri	2010-2014
66	Smith Paper and Janitor Supply	Abbie Stemper	Bookkeeper	Bank fraud	Missouri	2010-2015
67	BCC Merchant Solutions	John Kruse	Financial comptroller	Wire fraud	Missouri	2010-2014
68	Reliant Financial Services	Kimberly Padgett	Bookkeeper	Wire fraud	Missouri	2007-2015

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
61	Asset misappropriation	Cash	Larceny	Of cash on hand	
62	Asset misappropriation	Cash	Larceny	Of cash on hand	
63	Asset misappropriation	Cash	Fraudulent disbursements	Payroll schemes	Falsified wages
	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Forged endorsement
64	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Concealed checks
65	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Personal purchases
66	Asset misappropriation	Cash	Fraudulent disbursements	Billing schemes	Shell company
67	Asset misappropriation	Cash	Larceny	Of cash on hand	
68	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Concealed checks

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
61	X	X	X	X		1	3	8	10
62	X	X	X			1	3	8	10
63	X	X	X			1	3	8	10
64	X	X	X			1	3	8	10
65	X	X	X			1	2	8	10
66	X	X	X			1	3	8	10
67	X	X	X			1	2	8	10
68	X	X	X			1	3	8	10

Case #	Internal Control(s)	Technology Functions
61	Require approval of client deposits and withdrawals. Reconcile the bank accounts with the customer accounts. Increase management supervision and confirmation of employee activities.	Automatically enter sales transactions into company accounting system.
62	Require approval of client deposits and withdrawals. Reconcile the bank accounts with the customer accounts. Increase management supervision and confirmation of employee activities.	Automatically enter sales transactions into company accounting system. Alert management if there are changes in certain accounts.
63	Require authorization to change information within the system, approvals from management and department heads. Reconcile original data with records at the end of the year.	Automatically enter transactions into company accounting system. Track changes and send alerts to management for changes made in specific accounts.
64	Require authorization to change information within the system, approvals from management and department heads. Reconcile original data with records at the end of the year. Separate duties regarding the handling of cash.	Automatically enter transactions into company accounting system. Track changes and send alerts to management for changes made in specific accounts.
65	Require reconciliation of accounting records to credit card statements.	Create a notification system that alerts an outside management member of expenses charged to the account.
66	Create and approved vendor/supplier list. Authorization and background information must be approved in order to add/change information on the list. Reconcile account balances to statements.	Automatically enter transactions into company accounting system. Track changes and send alerts to management for changes made in specific accounts.
67	Separate accounting duties and executive activities. Monitor executive activities.	Automatically enter transactions into company accounting system. Limit changes to select authorized employees which must be reconciled with other accounts.
68	Reconcile the check records with the balance in the company bank accounts.	Automatically enter transactions into company accounting system.

Case #	Company/Institution	Individual(s)	Position	Guilty Of	U.S. State Crime was Committed	Year(s) of Crime
69	Clarkson Construction Company	Rodney Tatum	IT manager	Mail fraud	Missouri	2013-2014
70	Christian County	Joseph Kyle	Sheriff	Money laundering	Missouri	2011-2014
71	Hawthorn Bank	Katherine Brown	Head teller	Embezzlement	Missouri	2012-2014
72	First Home Savings Bank	Diana Emery	Bookkeeper	Making false entries in banking documents	Missouri	2008-2012
73	American Federation of State, County and Municipal Employees, Local 1707	Lowell Wreh	President	Wire fraud	Missouri	2012-2014

Case #	Fraud Hierarchy (Wells, 2013, pg. 72)				
69	Asset misappropriation	Cash	Skimming	Sales	Unrecorded
70	Asset misappropriation	Cash	Fraudulent disbursements	Expense reimbursement schemes	Mischaracterized expenses
71	Asset misappropriation	Cash	Larceny	Of cash on hand	
72	Financial statement fraud	Financial	Asset/Revenue understatements		
73	Asset misappropriation	Cash	Fraudulent disbursements	Check tampering	Concealed checks

Case #	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities	COSO Principle(s)			
69	X	X	X			1	2	8	10
70	X	X	X			1	2	8	10
71	X	X	X			1	3	8	10
72	X	X	X	X		1	8	10	15
73	X	X	X			1	2	8	10

Case #	Internal Control(s)	Technology Functions
69	Require reconciliation of accounting records to credit card statements.	Create a notification system that alerts an outside management member of expenses charged to the account.
70	Monitoring of employee activities to determine the risks associated with certain authorization procedures. Verify invoices and purchase orders with the accounting department. Separate duties.	Automatically enter transactions into company accounting system. Require a system of monitoring for accounts to detect unusual and suspicious activities.
71	Monitoring of employee activities to determine the risks associated with certain authorization procedures. Separate duty for someone to maintain count of inventory in the bank vault.	Install security cameras inside the vault in order to deter stealing. Create a key code system to determine which employees accessed the money and at what time.
72	Monitoring of employee activities to determine the risks associated with certain authorization procedures. Separate duty for someone to access financial records and someone who has access to the inventory. Require authorization procedures.	Create a notification system that alerts an outside management member of expenses charged to the account.
73	Separate accounting duties and executive activities. Monitor executive activities.	Automatically enter transactions into company accounting system. Limit changes to select authorized employees which must be reconciled with other accounts.