Have Accounting Information Systems Significantly Helped in Detecting Fraudulent Activities in Accounting?

Daniel H. Boylan
Purdue University, Fort Wayne

Jaylen E. Hull
Purdue University, Fort Wayne

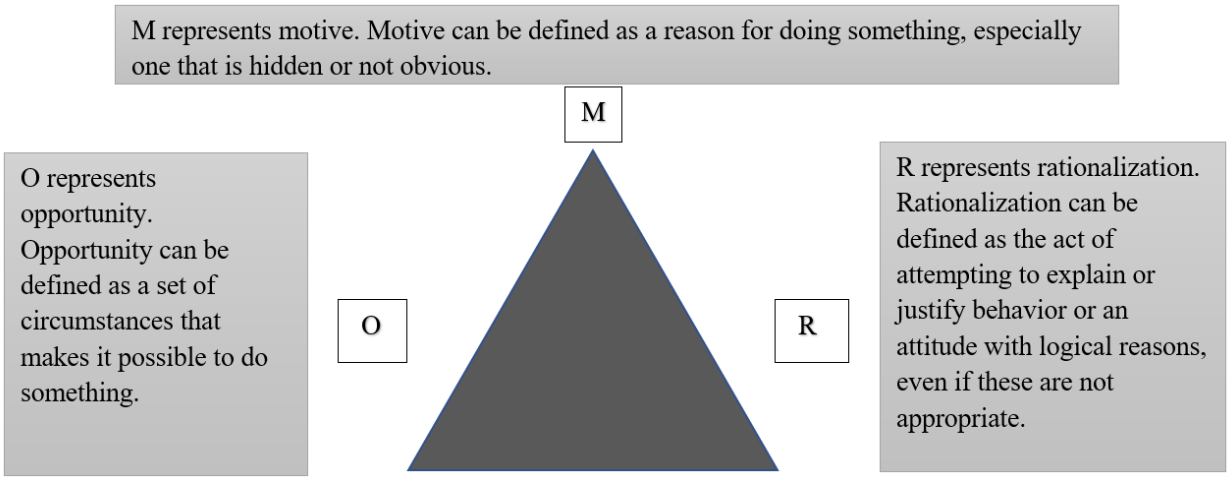
Fraudulent activity corrupted public companies in several ways for years. Accounting information systems have been recently implemented in public companies to help with fraud in financial statements. Accounting information systems have been reported to detect fraud, but the question is whether the systems can prevent fraud. Relevant literature is researched concerning this topic. Comparison and implementation of the software systems were the basis for this research. Public companies, shareholders, and auditors are all at the benefit of this research as money, time, and uncertainness can all be saved. It was concluded that information systems implemented in accounting detect fraudulent activity.

Keywords: accounting information systems (AIS), securities and exchange commission (SEC), public company, fraud, fraudulent activity, internal controls

INTRODUCTION

Fraud in the accounting profession is not a new topic. It is important to look at the fraud triangle as a key to understanding why it happens. The fraud triangle represents three reasons that individuals commit fraud. The three areas are motive, opportunity, and rationalization. If the three areas are present, then there is an increased likelihood that fraudulent activities will occur. The fraud triangle is shown below.

FIGURE 1
FRAUD TRIANGLE EXPLANATION. RESEARCH FROM THE HELMKE LIBRARY AT PURDUE UNIVERSITY FORT WAYNE



From the figure above, it can be seen that each letter on the angle represents a reasoning for why fraud is committed. The M stands for motive. When there is an issue with someone that could be solved with money, they are more likely to commit the fraud for personal gain. The letter O stands for opportunity. If there is a breakdown of internal controls and the fraud would be easy to cover up, then there is a greater opportunity for an employee to commit fraud. The R in the triangle stands for rationalization. When an individual can rationalize their fraudulent activities, they will be more likely to commit the fraud. When this triangle all meets the criteria of an employee, they will commit fraud repeatedly. If all three areas of this triangle are present in any situation, the potential for fraudulent activity is at its highest. This does not necessarily mean it is a guarantee it will happen, but there is an increased risk for fraud to occur and for no one to notice in a timely manner.

Fraud is defined as "an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception that results in a misstatement in financial statements that are the subject of an audit" (Dennis et al., 2013). Management can misstate or misappropriate assets on the financial statements to deceive shareholders and investors. Auditors' jobs are to uncover these deceitful acts to help shareholders make decisions. Auditors do not want to be held liable for any type of missed fraud. Auditors are hopeful that accounting information systems will decrease any threats to the validity of the financial statements. The thought of increased information systems allows auditors to catch fraud earlier on than if there is no information system present. The purpose of the information systems, in an auditor's life, is to detect any fraud within the accounting period. The perfect approach would be to develop an information system that will also prevent any crimes from being committed.

In 2016, $6.3 billion was stolen from companies across the United States. This amount resulted in about a 5% decrease in annual revenues (Dai, 2017). Shareholders are experiencing these revenue losses and are not happy about the issue. Audits are completed by the auditor, but their findings may not uncover any of the fraudulent activity going on due to the lack of information systems. Those who commit fraud are going to do their best in covering up what they have done. This brings in the need for an accounting information system that will aid managers and auditors in assuring the validity of the financial statements. A technological program can help management and the auditor in finding those issues (Gettry, 2016). The system will also be able to track who is making journal entries that shouldn't be. An accounting information

system (AIS) is capable of logging any and all activity. This is useful to management as well as the auditors in ensuring that the financial statements are represented fairly.

AIS has evolved to help prevent and detect any fraudulent activities within the company. Before this type of technology became universal in all companies, it was much easier for an employee to manipulate some balance sheet accounts or falsify accounts payable and receivable documents. These types of activities are what is causing the misstatements in the financial statements. AIS systems can track who is making journal entries, when they were completed, and the accounts that were affected. This gives management and the auditors the ability to evaluate and uncover any crimes (Dai, 2017).

The definition of an audit is stated as, "an official inspection of an individual's or organization's accounts, typically by an independent body" (Krishnan et. al., 2005). Auditors' purposes are to uncover these fraudulent activities and to ensure that the financial statements are accurately presented. Any publicly held firm is required to have annual audits to be in compliance with GAAP (Generally Accepted Accounting Principles) rules. The Sarbanes-Oxley Act of 2002 upheld this rule. The purpose of the annual audits is to protect any current or future investor. Investor's trust the work completed by the auditors, not the words and affirmations of management.

Blockchain innovation is an emerging technology that serves as a way to take the opportunity part in the fraud triangle away from those who are tempted to steal from the company. Blockchain technology is a system that can track computer clicks and movements from each employee. It becomes difficult for auditors to complete this task if there is not an effective AIS system or there is a flaw in internal control implementation. Fraudulent financial reporting or misappropriation of assets are the most common types of fraud that will arise in the accounting world (Seetherarm, 2015).

The question at hand is whether or not these AIS systems have significantly helped in detecting fraudulent activities within the accounting world. AIS systems have not prevented fraud, according to statistics provided by auditors. Alternatively, it is possible that AIS systems have helped in detecting fraud, but that it doesn't catch everything. If there is a smart employee/manager that knows the system well, it is possible that they can cover up their criminal acts through manipulation using computer systems to cover up their digital footprints (Huang et. al., 2021).

The following sections of this article will summarize other academic journals relevant to this topic. The purpose of the literature review is to show what information is available to be able to conclude about the efficiency of AIS systems. The literature review will explain how each article relates to the other and how it affects the research question. It will also support the hypothesis and other theoretical frameworks developed from the academic journals.

From the article summaries, there will be a section that will state what quantitative and qualitative data will be used to conclude. The data will be presented in a non-biased way. Facts will be presented fairly and in a common way so that it is all understood. From the data presented, there will be an initial rejection or acceptance of the hypothesis: AIS systems have not prevented fraud, according to statistics provided by auditors. The next section of this article will present the findings from the data collected. The data that will be used will be relevant to the research question: has accounting information systems significantly helped in detecting fraudulent activities in accounting?

The concluding paragraphs will summarize the findings of the research relevant to answering the research question. The hypothesis will either be accepted or rejected with an explanation as to how it was determined. Here is where any limitations of the research question will be explained. There will also be a summary as to what type of future research could be done to provide more data on the research question.

LITERATURE REVIEW

In an article written by Gettry Marcus' Certified Fraud Examiners, titled "Fraud Statistics", there are several different statistics given to further prove that fraud happens too often. Reinforcing the idea above, the average organization loses about 5% of its annual revenues (Marcus Gettry News, 2016). The Association of Certified Fraud Examiners (ACFE) conducted this study on around 1,500 different cases. The majority of those cases reported a loss of $200,000 or less. The article also stated that the costliest form

of fraud was the misstatements on the financial statements. However, fraud is typically uncovered before it hits the auditor's desk. Most fraud is detected by employee tips (42.2%), management review (16.0%), or internal audits (14.1%) (Marcus Gettry News, 2016). The CFE's in the study found that there was a large weakness in internal controls across the 1,500 companies (Marcus, 2016).

Internal controls are the most effective way to prevent fraudulent activity. Implementation of accounting information systems will help companies improve (or implement) internal controls. The most common people to commit fraud were the employees, followed by management, and then the owners and executives (Hutchinson, 2020). However, there is an inverse relationship with the dollar amount of money that was taken. The common white male in an executive position is more likely to steal large amounts of money from the company compared to the common employee who directly deals with cash movement. The use of AIS systems will tip-off management and other owners about the fraudulent activities (Hutchinson, 2020).

The most common fraudulent activity is misstatements and misappropriations on the balance sheet. An article was written by Sidney I. Simon titled, "Fraud in the Balance Sheet" explains the common misstatements in the balance sheet. The article evaluates the issues that arose when GAAP and the SEC did not have any oversight. Judges were finding reporting issues in accounts that were not treated the same way as other companies were treating them. This made it difficult for auditors and creditors to accurately assess a company. Before GAAP, managers were able to cover up fraud in the balance sheet relatively easily. This furthers the need for computer software to catch fraudulent misrepresentations (Simon, 1965).

Among the Enron and WorldCom scandals, it was evident that something needed to be done to protect US investors. According to an article written by Mark A. Nickerson, CPA, CMA titled, "Fraud in a World of Advanced Technologies", in the early 2000s there were off-balance-sheet loans, manipulation of commodity prices, improper accounting practices, falsified financial results, and many others that left the US market in pieces. This all could have been predicted according to Sidney Simon's article. With the passing of the Sarbanes-Oxley (SOX) act in 2002, more responsibility was put on managers and an internal control assessment was required by auditors. The act also forced auditors to be 100% independent (Nickerson, 2019). Ineffective internal controls over financial reporting (ICFR) have drastically decreased since the enactment of SOX section 404(b). Blockchain has proven to be an emerging technology that could hinder most fraudulent activities in the future. The technology makes it nearly impossible for basic fraud to take place from a balance sheet standpoint (Dai, 2017).

Computer information systems have become an everyday tool in professional and personal life. Researchers have found that information systems can be very beneficial when it comes to fraud prevention. An article published by Capital Business Solutions titled, "How nonprofit accounting software can help prevent fraud" states that accounting information systems are important when it comes to all organizations. This article focuses on the nonprofit sector and how detrimental fraud can be to those organizations. This can also relate to publicly held companies as many US investors are at risk without fraud prevention software. Publicly held companies are expected to have external audits done yearly. Integrating software that can easily pull account information cleanly and uniformly is easy for both management and the auditor (Huang et al., 2021).

Enterprise Resource Planning (ERP) refers to a type of software that organizations use to manage day-to-day business activities such as accounting, procurement, project management, risk management and compliance, and supply chain operations. An ERP system helps to prevent and detect fraud committed by everyday personnel such as secretaries and lower-level managers. ERP software is common in the procurement and accounting phases of a company. Misappropriation of assets is very likely to occur in these departments without any type of software to create a check and balances system across coworkers. An article titled, "ERP Accounting Software: Preventing Fraud", written by Chandler Hutchinson summarizes the uses of ERP software in common day-to-day activities and how it protects the company from fraud. The article was written shortly after the University of Louisville scandal where the former dean, executive director, and equine program coordinator were all convicted of mail fraud, wire fraud, money laundering, theft, and bribery. It was determined at the time that if an effective ERP software had been installed, the crimes would have been caught much sooner.

"Anatomy of Computer Accounting Fraud," an article written by Seetharaman et al. (2015), analyzes the reasons for fraud within the accounting system. The article breaks fraud down into three major categories:

- Asset Misappropriation; stating assets at incorrect values
- Corruption: people wrongfully using their power
- Fraudulent Statements; false financial statements

The article goes into depth with related information on the best ways to prevent and deter fraudulent activities within an organization. The article focuses on the monetary valuations of fraud losses, as well as the potential outcomes of implementing fraud preventative software (Seetharaman et al., 2015).

One aspect of the issue at hand that has not been explored often is the use of qualitative analysis in an interview setting. "Auditing Techniques to Minimize Accounting Related Fraud and Errors: A Qualitative Analysis with the Interview Model," written by Cevdet Kizil, analyzes the different techniques that can be used when assessing fraud. In a world that has become technological, this article dives into what history has already proven: questioning and interviewing employees and managers will bring out the truth. In the light of whether technology systems work or not, qualitative interviews paired with the technology are a tool that will give the upper hand (Kizil & Yimaz, 2021).

An article written by Ramayya Krishnan, James Peters, Rema Padman, and David Kaplan titled "On Data Reliability Assessment in Accounting Information Systems" analyzes data gathered from the technology implemented in a company. Managers have proven that they can manipulate financial statements. This article analyzes how much an employer can manipulate computer data returned from an AIS. The article implements an approach to quantifying this idea (Krishnan et al., 2005).

Blockchain technology can be defined as a system that tracks and creates an unalterable record of transactions with encryption that makes it nearly impossible for a fraudster to hack. The system denies anyone without access to gain its files and stored data. The data is stored across a network of computers, unlike the traditional computer where it is all stored together in servers. This is the key new technology to limit the amount of access to any unauthorized user.

In an article titled, "How Blockchain Technology Can Prevent Fraud", the author defines blockchain technology and how it can benefit the prevention of fraudulent activities. The article states that there is a history of fraud going undetected for long periods of time, making it susceptible to never be uncovered the more time passes. It also leaves an open door for the fraudster to continue their habits of stealing from the company.

Theoretical Framework

The theoretical framework for this research entails the need for awareness of fraud within the accounting departments of different-sized companies. Auditors have continued to detect fraud through the use of their audit procedures and advancing Accounting Information Systems. The Sarbanes-Oxley Act have forced publicly held companies to obtain an audit of their financial statements and their internal controls each year. This is to ensure that the financial statements are presented in a fair representation for shareholders and future investors. Management of a company is held liable for the representation of the financial statements, not auditors.

Accounting Information Systems that can keep track of each employee's actions (journal entries, cash transactions, accounts receivable, accounts payable, etc.) will help companies and auditors when it comes to the audit procedure. Auditors will be able to complete their duties more efficiently and cost effectively. This will reduce costs for the company. Public companies who have an effective Accounting Information System will be more likely to receive an unmodified opinion issued by the auditor.

Enterprise Resource Planning (ERP) systems are a type of AIS that will help in detecting fraudulent activities. Along with ERP systems, numerous software packages can be used to protect against fraud. However, there is no type of software or AIS system that will be able to prevent fraud within the workplace.

Fraudulent acts cannot be completely prevented simply because there are people who know how to work the system. Other than blockchain technology, there is no accounting information system that is able to collectively prevent and detect fraud. The articles above and the future sections of this paper will prove

that AIS systems significantly help in detecting fraud, but that no AIS system will be able to prevent it entirely.

METHODOLOGY

Sample

The best data when it comes to accounting fraud comes from auditors. Managers may report fraudulent activity to the police if it was committed by a low-level employee. However, they want to conceal the issue as much as they can to limit the amount of damaged reputation. The research was conducted through the online Helmke Library database from the Purdue University Fort Wayne campus. The research was gathered to see if AIS systems can detect and prevent fraud. The Null Hypothesis is that AIS systems can detect fraud, but that they cannot successfully prevent fraud. The Alternative Hypothesis is that AIS systems can detect fraud and show a significant decrease in future cases after AIS implementation. The Null hypothesis will be rejected if three out of the five AIS systems fail to prevent fraud.

It was important to take a look at several different types of AIS systems to come to the right conclusion based on data from several locations. Within each article, the data was gathered in a way that would answer whether the Null hypothesis would be rejected or not. The AIS systems that were tested were as follows:

- Blockchain Technology
- Nonprofit Accounting Information Systems
- Target System, Log of Events, AIS Engines, Behavioral Engines, and Risk Score
- ERP Accounting Software E: Preventing fraud - Clients first: Acumatica and Dynamics ERP Partner
- Fraud in a world of Advanced Technologies; Enter the Robots: The Good, the bad, and Potentially Ugly

Procedures

For this research, the authors are utilizing existing and the most recent research and data. These are used to determine what is the best route to determine how auditing can detect money laundering. The researchers have used the EbscoHost, ABI/INFORM, and Gale Business search engines to locate articles. Specifically, articles that contain keywords such as "audit," "crime," "accounting," "money laundering," and "detection." The following table reveals the results.

TABLE 1
THE VOLUME OF ARTICLES FOUND ON THE PURDUE UNIVERSITY, FORT WAYNE LIBRARIES ON AUDIT AND MONEY LAUNDERING

Search Words	Number of Peer-reviewed Journal Articles
"audit" and "crime"	21,283
"audit," "crime," and "accounting"	7,801
"audit," "crime," "accounting," and "money laundering"	1,025
"audit," "crime," "accounting," "money laundering," and "detection"	454

Those keywords were used together in different combinations to pull up several peer-reviewed articles. When searching using "audit" and "crime" there were over 21,000 peer-reviewed articles. As terms were added, the volume decreased. When using the terms "audit," "crime," "accounting," "money laundering," and "detection" the volume diminished to just under 500 articles.

Statistical Analysis and Measurement

Blockchain is an evolving technology first used with Bitcoin transactions. Some organizations have implemented blockchain into their accounting department to detect any fraudulent activity. The research was conducted to verify whether the implementation was detecting or preventing fraudulent activities.

Nonprofit AIS systems were created specifically for nonprofit companies. Fraudulent activity is not good for any company, but especially when it comes to donation dollars trusted in the hands of these companies. The nonprofit systems explained more that it could detect fraudulent activity, but that it cannot prevent it.

The Target Systems technology provided some great findings on the topic. Target Systems are created to track every action of the end-user. It logs the data for every incorrect password entered, a correct password, failed transaction, and successful transaction. When users sign in, they are assigned an IP address that can track everything that the user does. Target systems have shown that they can detect and prevent (to a certain extent) any fraudulent activities.

ERP systems allow companies to implement audit tracking. This is similar to the target systems as it can track each user's activity. The ERP system can store data about each user and their activities throughout the day. The ERP software can create reports showing any outlier transaction. With the right approval, a user can look up all cash transactions and look back at any source documents related to the transaction. This is a check and balances tool to require source documents to be entered whenever making cash transactions.

Robots in accounting seem like the right thing to do as robots have been implemented in every other part of the world. However, this article defines the bad and the ugly when AIS systems are interconnected with robots.

FINDINGS

TABLE 2
ARTICLE ACCEPTANCE AND REJECTION OF NULL HYPOTHESIS. PEER-REVIEWED ACADEMIC JOURNALS FROM HELMKE LIBRARY, PURDUE UNIVERSITY, FORT WAYNE

	Accepts Null Hypothesis: Detect Fraud	Accepts Null Hypothesis: Prevent Fraud
Machine Learning	Yes	No
Blockchain Technology	Yes	Yes
Nonprofit Accounting	Yes	No
ERP	Yes	No
AIS Fraud Detection	Yes	No
Totals	**Yes: 5 No: 0**	**Yes: 1 No: 4**

The above table shows whether or not each article accepted or rejected the null hypotheses presented above. For either of the hypothesis to be accepted, the article must explicitly state that AIS systems prevent or detect fraudulent activity within the company. This is useful for auditors and managers to evaluate the internal controls of the company. The overall acceptance or rejection of the null hypothesis will be concluded from the results of the table above.

The first article examined is titled, "Detecting accounting fraud in publicly traded U.S. firms using a Machine Learning Approach." Researchers found that using raw data provided from publicly held companies. The SEC's Accounting and Auditing Enforcement Releases (AAERs) were the foundation of this research conducted. The AAERs show material misstatements within audited financial statements from public companies registered with the SEC. Detection of fraud was stated as difficult, but attainable through the use of their benchmarks for two fraud prediction models. The research combined into one prediction model based on the raw data gathered. The prevention of fraud was found as not possible. Machine learning was used to predict future fraud within financial statements.

Researchers found with the machine learning approach that fraud would typically be committed in block sections in consecutive years. The data that was found shows that in some scenario's fraud can be predicted, however, the fraud model did not prove that accounting fraud could be prevented.

The second article evaluated above deals with the advancement of blockchain technology. Blockchain technology is an emerging software system that puts controls in place. When used in the accounting world, the technology can track what each employee is doing. Anyone in real-time can see what users are clicking and processing what buttons. Blockchain technology notifies every party in the network when a "block" is created.

Authors stated that "Because blockchain keeps the record of an asset transfer, any type of misappropriation can be detected by tracing through the blockchain" (Dai & Vasarhelyi, 2017, pg. 3). Blocks are created when a transaction is in its early stages. For the block to continue, those in the network have to approve the transaction as valid. Once the transaction is complete, managers can click on a block and see who initiated the transaction and which associates approved it. This solidifies that blockchain technology can detect any fraudulent actions within the company.

Casey Evans, a blockchain expert and professor of finance and accounting at American University's Kogod School of Business, studies how blockchain advancements shares information in real-time to enable all participants the ability to visualize the transactions that are happening at the current time. This feature of blockchain technology takes away the opportunity part in the fraud triangle.

Authors go on to state that fraud can be prevented with this technology because of the blocks that are created that need approval before entering the next stage. This is the first article that tells readers that it is possible to completely prevent fraudulent activity. In a company with effective internal controls, the prevention of fraud is a lot more likely. However, the article states that if a CEO of a company had exclusive rights to initiate, approve, and complete a transaction, then fraud can occur and appear on the financial statements. However, auditors can use blockchain technology to uncover any misappropriation of assets or any type of fraudulent reporting.

Blockchain technology is a system of interrelated storage networks that prevents any manipulation of the data. There are blocks in place that make it virtually impossible for a hacker to gain access. If someone is able to gain access to the computer system and conduct any fraudulent activity, the system makes it impossible for the fraudster to cover up their tracks.

Nonprofit accounting is very important to have no or little fraud committed. Nonprofit money is donated or raised through company programs, not based on profit funds. The article states how the software can easily be audited to search for any fraud; however, it does not state that fraud can be prevented within the software. As for comparing accounting software for-profit companies versus non-profit, there are not many differences. Nonprofit AIS systems can be just as detailed as other systems used by for-profit companies.

The purpose of an ERP system is to organize the day-to-day business activities within an organization. ERP refers to accounting, procurement, project management, risk management and compliance, and supply chain operations. The purpose of the ERP is to lower the risk of fraudulent activity of incorrect data entries or paper transactions. ERP systems allow for documents to be transmitted without the possibility of an alteration.

ERP software is an accounting information system that can track what each user is doing. The software can also track the date and time of who is completing what transactions. Researchers state that the ERP software system can prevent fraud, similar to the claim with the nonprofit software. They claim that the controls and blocks put in place are efficient enough to prevent fraud. However, as with any software, it is virtually impossible to say that a software package can prevent fraud within a company.

In the accounting aspect of an ERP system, the information system allows your employees to feel secure about its automated function. The ERP system directly downloads the data from an order into the account payable computer system. This allows for fewer errors as there are no manual data entries. Most companies have some sort of ERP system that cuts down on the possibility of an error or fraudulent crime to occur. Companies sometimes have issues where their financial statements are not presented fairly due to an error of data entry, not necessarily an ill intention by an employee or a member of management.

ERP systems can restrict access to users, as well as create an alert system when fraudulent activities may be occurring. For the detection of fraud, this is a great asset to possess when auditors are combing through the financial statements. ERP systems also offer an audit tracking package that helps auditors. The ERP system can issue activity reports showing transaction history and other important information when it comes to evaluating a transaction. A user, time, and date are all assigned to each transaction within the system. Overall, ERP systems cannot prevent fraud, but they assist in many ways in detecting it.

ERP systems take away the O (opportunity) and the R (rationalization) in the fraud triangle. The automated system does not allow for an employee to gain access to manipulate any source documents that could directly affect the financial statements. ERP systems also make it easier for management and/or auditors to uncover the crime if anything were to happen. This is the feature that takes away the rationalization part of the fraud triangle.

The fifth article evaluated is a broad overview of a basic accounting information system. The article evaluates what a typical AIS system could do in terms of detecting and preventing fraud. The article analyzes what is seen in most systems. There is a target system that creates a dynamic IP address for each user connecting to the system. AIS engines and Behavioral engines track user activity and then determine a risk score. For the AIS systems that are "audit-friendly," the risk score tied to each user and transaction throw error messages to the system.

Eventually, the reports will build, making it easy for the auditor to audit the system. The system is great at detecting fraud. The target system combined with the AIS and behavioral engines to create the risk score is how auditors can uncover fraudulent activity or reporting. Like with other systems created, there is no fool-proof way to say that AIS systems prevent fraud within the company. This system is no different, which is stated by the authors of the article. The system described is a reactive system, not a proactive one. This means that the information system described cannot be proven to prevent fraud.

CONCLUSIONS

Researchers have found that the prevention of fraud is nearly impossible to prove. AIS systems have come a long way in helping the detection of fraudulent activity and reporting on the financial statements. The question at hand, though; is whether or not an accounting information system can prevent fraud, or if it is just able to sufficiently detect fraud.

There was a total of five different types of technology advancements that have been proven to improve the accounting role. The five articles each discussed how its technology has improved the accounting world in terms of efficiency and traceability.

Blockchain technology is the one AIS system that stood out among the other four. Blockchain technology is a new emerging technology that is finding its way in many different industries across the world. The most promising technology that can say that it can "prevent" fraud would be blockchain.

ERP systems are another important information system to look at when it comes to uncovering and detecting fraudulent activities. The automated issuance of documents and reports from the ERP system takes away parts of the fraud triangle. It is important for companies to adopt some sort of ERP system as it is notably one of the stronger information systems to result in lowered fraud rates.

However, it is impossible to say that there is any type of AIS system that can completely prevent fraudulent activity. As shown above, there are very few other technologies that can accurately prevent fraud. All of the technologies presented can use its features to detect most fraud, but nothing is ever a 100% guarantee.

Auditors can make their work easier through the use of public company AIS use. Reports are generated and time-and-user stamps are kept on record. If there is any type of fraudulent activity or reporting, an auditor will find much success in uncovering it through the type of accounting information system the company chooses to go through.

The detection of fraud is a given with any type of AIS system discussed in previous sections. An auditor should be able to uncover any fraud. The AIS system should be used as a tool when the audit is underway. AIS systems can detect fraud but are unable to prevent it.

The purpose of an AIS system development is to minimize the fraud triangle. When one or more of the triangle pieces are hindered, the likely that fraud will even be committed is minimized. Even if fraud has still occurred, the likelihood that it will be uncovered within a reasonable amount of time skyrockets.

Implications for Management

This research has many benefits as it shows to upper management and owners of public companies what effective information systems can help when managing internal controls. Public companies need security for investors to trust in them. Investors that know that the company has an effective internal control system will more than likely buy into them, causing stock prices to increase and the overall value of the company to rise.

Implementing an accounting information system can also decrease auditing costs. Auditors will be able to complete their pre-audit work in less time through the use of reports and other historical data kept within the AIS system.

Auditors' risk scores will ultimately lower the greater control an AIS system has over the company's financials, causing less audit work. Manager's and shareowners' money will be saved through the use of a one-time implementation of a large blockchain or ERP software (or both).

A safe, secure company who implements an AIS system will see decreased costs in auditing expenses as well as increased investor awareness. Increasing the bottom line of a company at the same time as improving internal controls will show an improvement in the accountability of its employees. Potential future investors and current shareholders view that as a positive aspect of the company.

For the management of a nonprofit business, an accounting information system will increase trust among the top executives and the donors. Donors trust their money to be put to the use that they allocated it for.

Limitations

Information systems for accounting are relatively new and are constantly changing to stay current with accounting rule changes. It is hard to compare a financial statement for one specific year as to if they did or did not have an information system installed. It is possible that fraud was not uncovered near as much as it is now, simply because of auditor fails. It is possible to say that fraud was not committed to earlier years as well. A growing company that is in search of an information system now might be uncovering fraud due to the more employees dealing with any records.

There are very little data available from public companies stating whether the AIS system is what uncovered the fraud, or if an employee tip or basic audit through red flags. The lack of data available could alter the conclusion to the research question. However, the sample current research and development prove that the conclusion that was reached is accurate.

The lack of time is another limitation of the research. The research was conducted, and this report was put together in about 8 weeks. Time restraints paired with the everchanging advancements in technology could alter the research conclusion. Blockchain seems to be the front runner in answering the null hypothesis of whether an AIS system can prevent fraud.

Unfortunately, there is a lack of prior research in this area. There are articles stating how each system works and how it can benefit a company, but none are related to the research question of if an AIS system can detect or prevent fraudulent activity.

The lack of data and research relevant to blockchain technology creates a limit on this research. Blockchain technology is the only technology that could have accepted the alternative hypothesis. However, blockchain is still advancing and was not discovered until recent years.

Future Research

Time restrictions and technology advancements did not allow further research into company versus company effectiveness with the same accounting information system. Future research of company use of AIS systems would further prove or alter the conclusion.

Research among company use of AIS systems will bring a stronger understanding of the way managers can benefit from the large initial expense. A relevant topic to research would be the use of an AIS system and its stock price to see if there are any correlations between the two.

There is a lack of information on the results of company outcomes after implementing an AIS system. Making its employees aware of the implementation of the system would inherently halt any fraudulent activity that could have been occurring. The most effective way to determine if implementation of the system has worked is to create a run-through of the system. For example, after implementation of the information system, it would be important for a fake "fraudulent activity" to occur. This will prove to everyone involved if the system were to throw an error or not. Keeping some of the managers in the dark about the situation will also test to see how accurate your managers are at reviewing reports they are responsible for.

One topic that could see future research would be the use of a singular AIS system across several different companies. Creating the same system across different industries can show the positives and negatives of each system. The reports that are generated can be helpful to some managers, but not necessarily to others within different companies. The Auditor's use of the reports is another area to research, within a public company, that would provide more insight as to if the correct conclusion was reached.

ACKNOWLEDGEMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

Bao, Y., Ke, B., Li, B., Yu, Y.J., & Zhang, J. (2020). Detecting accounting fraud in publicly traded U.S. firms using a Machine Learning Approach. *Journal of Accounting Research*, *58*(1), 199–235. https://doi.org/10.1111/1475-679X.12292

Capital Business Solutions. (2020, September 21). *How Nonprofit Accounting Software Can Help Prevent Fraud*. Retrieved from https://www.capitalbusiness.net/resources/how-nonprofit-accounting-software-can-help-prevent-fraud/

Dai, J., Yunsen, W., & Vasarhelyi, M.A. (2017). Blockchain: An emerging solution for fraud prevention. *CPA Journal*, *87*(6), 12–14. Retrieved from https://www.cpajournal.com/author/mvasarhelyi/

Dennis, L., Hornik, S., Jones, K., Riley, R., & Trompeter, G. (2013). Integrating fraud-related research into accounting, auditing, and accounting information systems curricula. *Journal of Forensic Studies in Accounting & Business*, *5*(1), 38–55. Retrieved from https://www.worldcat.org/title/journal-of-forensic-studies-in-accounting-business/oclc/828103317

Gettry Marcus. (n.d.). *Fraud Statistics*. Retrieved from https://www.gettrymarcus.com/fraud-statistics/

Huang, R., Tawfik, H., & Nagar, A. (2021, April 21). *Fig 3. AIS-based fraud detection system*. ResearchGate. Retrieved from https://www.researchgate.net/figure/AIS-based-fraud-detection-system_fig3_220307817

Hutchison, C. (2020, November 20). *ERP accounting SOFTWARE: Preventing fraud - Clients first: Acumatica and Dynamics ERP Partner*. Clients First | Acumatica and Dynamics ERP Partner. Retrieved from https://cfbs-us.com/erp-accounting-software-preventing-fraud/#:~:text=ERP%20Accounting%20Software%3A%20Fraud%20Detection%20and%20Prevention&text=According%20to%20auditors%20and%20analysts,fraudulent%20conversions%20of%20any%20sort

Kizil, C., Muzir, E., & Yimaz, V. (2021). Auditing techniques to minimize accounting related fraud and error: A qualitative analysis with the Interview Method. *EMAJ: Emerging Markets Journal*, *11*(1), 95–104. https://doi.org/10.5195/emaj.2021.232

Krishnan, R., Peters, J., Padman, R., & Kaplan, D. (2005). On data Reliability assessment in accounting information systems. *Information Systems Research, 16*(3), 307–326. https://doi.org/10.1287/isre.1050.0063

Nickerson, M.A. (2019, July 10). Fraud in a world of advanced technologies. *The CPA Journal*, June 2019 Issue (all pages). Retrieved from https://www.cpajournal.com/2019/07/01/fraud-in-a-world-of-advanced-technologies/

Seetherarm, A. (2015). Anatomy of Computer Accounting Fraud. *Emerald Research*.

Simon, S.I. (1965). Fraud in the balance sheet. *The Accounting Review*, *40*(2), 401–406. Retrieved from https://www.jstor.org/stable/242310?seq=1#metadata_info_tab_contents