2016

Accounting Information Systems: Ethics, Fraudulent Behavior, and Preventative Measures

jasmine s. smith
student

Accounting Information Systems: Ethics, Fraudulent Behavior, and Preventative Measures

Jasmine S. Smith
College of Business Administration
Information Systems
Emphasis: ERP using SAP
Faculty Mentor: Dr. Thomas Case

Table of Contents

Abstract

Most business organizations have implemented Accounting Information Systems to improve efficiency and to help optimize use of company resources. The evolution of Information Technology within financial and accounting processes has brought new ethical issues, forms of fraudulent behavior, and mechanisms to prevent compromising confidential, sensitive, and personal information. This investigation focuses on the evolution of Accounting Information Systems and their controls for limiting fraud and misconduct in financial and accounting processes.

I. Introduction

Review of Literature

The purpose of this literature review is to provide an overview of the recent evolution of Accounting Information Systems (AIS) and their controls for combatting fraud and misconduct. Many completed and ongoing studies have demonstrated the beneficial impacts of AIS on organizations. These studies also summarize potential threats to AIS from employee and/or management ethical misconduct or attempts to commit fraud. Such threats can result in misrepresentation in Financial Accounting reporting for both external and internal and can have undesirable impacts on the integrity and exactitude of the organization's financial reporting and its overall corporate image.

Accounting Information Systems

An Accounting Information Systems is an integral component of an organization's business computing fabric. AIS is the systems that classifies, collects, stores, monitors and converts the organization's financial data into information used for reporting and internal control **(**Meymandi, Roosta, Rajabdoory**)** With accounting information systems in place, organizations are able to keep accurate records, and manage organizational assets; they are also used by management to ensure that appropriate access and separation of duty controls are in place. Such controls enable management to hold workers accountable for their interactions with the system.

II. Ethics and AIS

Ethics

The evolution of Information Technology and Accounting Information Systems has brought new opportunities for ethical misconduct and fraud. A cornerstone of ethical behavior is an understanding of how one's personal behaviors and actions impact the welfare of the other individuals. Ethical guidelines can help individuals avoid harming others and to act in ways that have the potential to help or aid others. Some government regulations are designed to minimize some forms of unethical behavior and also enact laws to deter illegal behavior. In society, social norms are often implied ethical guidelines that tend to change in response to different environments, communities, and the passage of time.

Accounting and Ethics

In the accounting discipline, professional standards have been created to inhibit accounts from engaging in unethical behavior. Such standards play an important role in accounting because accounting processes aid management in decision-making processes that impact a wide range of other individuals and the organization as a whole. It is important for accountants to understand Accounting Information Systems from an ethical perspective because they have the professional responsibility to protect and safeguard assets and financial information. In accounting, standards of ethics are defined as implied or expected norms of accountant conduct (Chunhui, Lee, Nan). Ethical guidelines are viewed as equally applicable to each individual within the profession. (Mastracchio Jr, Jimenez-Angueira, Toth 2015)

The International Federation of Accountants (IFAC) is a worldwide organization that serves as an umbrella organization for many national accounting organizations including the

American Institute of Certified Public Accountants (AICPA) and the National Association of State Boards of Accountancy. The mission of the IFAC is "the worldwide development and enhancement of an accountancy profession with harmonized standards, able to provide services of consistently high quality in the public interest." (Clements, Neill, Stovall). IFAC seeks to synchronize the quality of accountants' works with the intent and the ethical standards on which it is based. IFAC stresses to member and potential member organizations that they don't have to develop standards that follow IFAC codes exactly, but they "may not apply less stringent standards than those stated in this code." (Clements, Neill, Stovall). This stipulation encourages member organizations to develop codes of conduct that exceed those set by the "parent organization". (Clements, Neill, Stovall)

AIS and the Protection of Confidential Information and Integrity

Because Accounting Information Systems are integral components of business computing platforms organization, controlling the risk of unauthorized access to sensitive information is important. Failure to control access to important information can result in the information being altered or being seen by employees or outsiders who have no business seeing the information. (Zhensheng, 2014) Accountants and AIS auditors could use the AIS to violate other individuals' privacy and rights by collecting, selling, and using their data or information for personal gain. In some cases, employees have gained access to other workers' confidential information, which could be used for blackmail or identity theft. In other cases, workers have obtained financial information from an AIS to tip off outsiders whom may or may not have a stake in the company. Such behavior is not just unethical; it is also a form of fraudulent behavior.

III. Purpose of Accounting Information Systems

Reporting in the Accounting Information Systems

A primary purpose of AIS is to serve as a systematic and comprehensive system that records and reports financial transaction, which are integral to business operations. (Trigo, Belfo, Estebanez). Reporting can be defined as the process of analyzing and summarizing the organization's transactions in order to provide information that is utilized in decision making (Trigo, Belfo, Estebanez). Reporting has traditionally been conducted on a periodic basis, whether it daily, weekly, monthly, quarterly or annually. In the reporting process financial information is summarized and given to stakeholders of the company, be it government officials, suppliers, investors, manager, auditors, etc. Reports illustrate the organization's financial position. Reports are used by auditors to assess the integrity of the company's accounting processes.

IV. AIS Security

Accounting Information Systems Security and Access Controls

In many organizations, Accounting Information Systems have a multitude of users who can simultaneously access a database that contains a vast amount of data. This is especially true in organizations that have Enterprise Resources Planning (ERP) systems as their primary transactional computing systems. One of the attractions of ERP systems as a business-computing platform is its single, comprehensive data that holds both transactional data and master data about suppliers, customers, materials, products, etc.

In order to minimize concerns about the security of data and information in an AIS database, it is important to ensure that appropriate user access controls are in place (Zhensheng,

2014). In a business environment, it is vital to have a database that ensures adequate security for both internal and external stakeholders. When the AIS database is vast in size and depth, there is increased risk of data and information being inaccurate or misappropriated.

Access controls are a first line of defense in protecting the integrity of AIS systems and their databases. There are numerous types of access controls for AIS databases, which include Discretionary Access Control, Role Based Access Control, and Mandatory Access Control. Role Based Access Control has been successfully implemented and integrated into AIS due to its flexibility and logical reasoning. With RBAC, users are delegated and assigned specific roles within the system that will only grant them access to things relevant to their assignments. With this method, it eases the transition of employee turnovers, in regards to security configurations, due to its central managerial control. Management does not have to reconfigure the system because it is assigned by position (Uzun).

V. AIS and Fraudulent Behavior

Accounting Information Systems and Fraudulent Behavior

Fraudulent behavior among AIS users is a perpetual accounting and auditing concern. Financial fraud is an activity that can affect more than one person or company and it may have indirect effects on external entities. Employees that are authorized users of an AIS may have the opportunity to misappropriate AIS data and information. When authorized users are members of the organization's accounting department the misappropriation of AIS data and information may be a form of occupational fraud, the illegal action of converting or concealing information for personal gain. The Association of Certified Fraud Examiners defines occupational fraud as the misappropriation of assets (Glodstein). For example, an accounting employee with authorized

access to the AIS database may be able to alter payroll, billing, or reimbursement data for personal gain. Fraudulent behavior by accounting employees can also involve the intentional manipulation of the content or the structure of financial reports. (Bressler 2011)

In the absence of appropriate controls, accountants can also utilize AIS systems to access private or sensitive information about fellow employees and other organizational stakeholders including, suppliers, customers, or other business partners. This may involve the acts of obtaining, hoarding, private or sensitive information for personal gain.

VI. Preventative Measures for Addressing the Potential for Fraudulent Behavior

Ethics Education

Instilling the importance of ethical behavior should not begin when an organization hires an employee. Organizations that are truly concerned with ethical behavior on the part of employees and fraud deterrence should begin by hiring graduates from colleges and universities with a track record of producing ethically inclined students. Such schools typically go beyond highlighting ethics and professional codes of conduct in textbooks used in their courses; they often have stand-alone courses that focus on ethics. Unfortunately, such schools are rare rather than plentiful and there is ample evidence that universities often come up short of the mark for ethical education.

In 2014, 64 students at Dartmouth College were charged with cheating on an exam of ethics. The involvement of 64 students is troubling, but the fact that the content of the exam was ethics, makes this truly disturbing. A study conducted by Donald McCabe found that business majors are more likely to engage in cheating, plagiarism, and unethical behavior than majors in

other colleges or disciplines (Mastracchio Jr., Jimenez-Angueira, Toth). If the results of this study are generalizable to business programs at other institutions, the future of ethics among accountants and AIS auditors may be dim because they typically graduate from a college of business or business program. These findings suggest that much work remains to be done to ensure that ethics education appropriately infiltrates academia. They also suggest that business schools and accounting programs should become more vigilant about instilling their students with a sense of professional ethics, both in thought and action. To be better positioned to combat unethical behavior and fraud and to thereby gain the trust of society, it is important for accounting professionals and auditors to follow professional ethics guidelines (Meymandi, Rajabdoory, Asoodeh).

Ethics Focused Onboarding and Training

Ethics policies and guidelines should be in place in organizations to provide guidance to newly hired workers and accounting employees. These serves as guides for employee behavioral and professional action. The existence of ethics policies demonstrate to new hires that the organization takes ethics seriously. During the onboarding and training process, there should be a separate module or program that emphasizes the ethics policies and how they should be applied to daily operations.

Information and Data Controls

Encryption is a process that converts data from its original to an indecipherable (scramble) form. Prior to transmission over a network, encryption can be used to scramble it so that if it is intercepted in transit it will be difficult or impossible to understand. Data in an AIS database can be stored in encrypted form to deter its unethical or fraudulent use. Government regulations, including HIPPA, require some forms of private or sensitive data to be transmitted in

encrypted form. However, HIPPA does not require organizations to store data in encrypted form in its databases (database encryption is recommended but not required by HIPPA). The 2015 Anthem hack was enabled by data being stored in unencrypted form.

There are four main objectives for using encryption to transmit or store data, there are confidentiality, integrity, authentication, and nonrepudiation. In an AIS database, there is personal information, which can be compromised in malicious ways (Marcella 2014). Encryption helps to prevent the malicious used of AIS data by presenting it to unauthorized users in an indecipherable form. Encryption also helps to maintain data integrity by making it difficult to modify. Because only authorized users or recipients who hold the decryption key are able convert the indecipherable data back into its original form, encryption provides a mechanism for confirming and authenticating their identity (Busta 2002).

Data management is paramount in organization's quest to protect data assets and information from unethical and fraudulent behavior. Companies should employ data management controls to ensure that users are accountable for their use of the database. An example of a data management control is segregation of duties. Companies should implement appropriate accounting data controls for its financial transactions. For example, a "three way match" should be used in the Procure to Pay process that checks for discrepancies between purchase orders, goods receipt, and vendor invoice documents. In accord with role-based access controls and segregation of duties, three separate individuals or groups within the organization should process these three documents. This system allows for each entity to be held responsible for any problems that may arise in the amount of goods received and the invoice amount before any payment is made.

Real-time Reporting Impacts on Company

Real-time reporting capabilities for AIS offer organizations many benefits in comparison to the traditional, "periodic reporting". As the technology wave continues to spread vastly, society is continuously turning into an immediate gratification society. Traditionally in accounting, financial and non-financial reports are done periodically, annually and [or] quarterly, which limits the accuracy of the measurements that help to improve the company (Trigo, Belfo, Estebanez). Real-time reporting holds the potential for organizations to make improvements, respond to change, and better understand issues that affect their operations. It also has the potential to give them confidence in the structure and performance of the company and its employees. This type of reporting can serve as a preventative measure or AIS control and can allow for certain information reporting to be automated thereby lessening the risk of human error and interference. For example, in the past few years SAP has developed AIS controls that run on its HANA system and enable AIS real time reporting. Analytics are produced as AIS transactions are performed which in instant feedback on AIS transactions and data in real time (SAP HANA).

Real-time Database Monitoring

Automatic or Real-time database monitoring allows management to quickly identify who or what is responsible for transactions and changes AIS data. It automatically detects and reports issues that pose real or potential risks to the system or company. Such monitoring can include monitoring of transaction executions, resource utilization, and process exceptions. When an issue is detected, it is analyzed and managed in real-time via mitigation or preventative tactics. (Oracle)

Continuous Auditing

Continuous auditing is a technology-driven process that seeks to provide organizations with risk assurance in real time. This offers organizations continuous compliance monitoring and the ability to detect attempted fraud and AIS user misconduct in real time. Continuous accounting uses algorithms and other models to evaluate both high impact and less serious risks. Compliance monitoring processes update regulatory changes when they occur and help ensure compliance with these regulations. (Rikhardsson, Dull)

VII. Conclusion

An accounting information systems is an integral computing component in many organizations and the business processes that drive them. Accounting is a component of every business process and the AIS is an important aspect of business process integration. Due to the nature of the transactional and master data in AIS databases, it is important to establish controls and preventative measures to ensure the security and integrity of the data that they contain. In the overview of AIS summarized in the previous literature review, it is apparent that there are numerous risks surrounding AIS as well as numerous controls that can be implemented to manage AIS risks. For future accountants and auditors, AIS risk management should begin with ethics education and an understanding of professional ethics in accounting practices. Universities have been inconsistent in including ethics courses in their business and accounting curricula and it will be increasingly difficult for accounting professionals to address emerging AIS risks associated with information technology advancements without a firm grounding in professional ethics.

By implementing appropriate structures and controls, organizations can help themselves safeguard AIS data and information and thereby improve their business processes. Data management controls, including continuous database monitoring, can help ensure data integrity by tracking individual roles and responsibilities and the AIS transactions in which individuals are involved. Access controls can/should be implemented in order to prevent individuals from accessing data that they are not authorized to see. Role-based access controls is one of the most common and efficient controls for AIS data. Role-based access controls should be used in conjunction with segregation of duties when more than one individual is needed to complete a business process transaction. Such controls deter fraudulent behavior and help prevent human error from compromising AIS security and data integrity.

Real-time Reporting and Continuous Auditing provide additional mechanisms for limiting fraud and accounting information systems misconduct. Both are technology-driven processes that provide automated AIS database monitoring in real time and facilitate rapid, if not immediate, responses to attempted fraud and misconduct. Continuous auditing and real-time reporting is already widely used and serve as cornerstones to the future of AIS auditing.

Much research being conducted today and to be done in the future will focus on configuring accounting information systems to create stronger controls to deter fraud and to prevent the unethical use of AIS data. Although Accounting Information Systems are integral components of business computing platforms, there are many more parts, some of which cross-traditional organizational boundaries to interface with the systems of business partners and other stakeholders. Technological advancements will continue to strain AIS security and the integrity of AIS data and the years ahead will include considerable research that focuses on addressing AIS vulnerabilities and risks.

IX. References

References

Brandas, Claudiu, Dan Stirbu, and Otniel Didraga. "Integrated Approach Model Of Risk, Control And Auditing Of Accounting Information Systems." Informatica Economica 17.4 (2013): 87-95. Business Source Complete. Web. 03 Jan. 2016.

Bressler, Linda. "Forensic Investigation: The Importance Of Accounting Information Systems." International Journal Of Business, Accounting, & Finance 5.1 (2011): 67-77. Business Source Complete. Web. 03 Jan. 2016.

Busta, Bruce. "Encryption In Theory And Practice." CPA Journal 72.11 (2002): 42. MasterFILE Elite. Web. 05 Feb. 2016.

Chunhui, Liu, Yao Lee J., and Hu Nan. "Improving Ethics Education In Accounting: Lessons From Medicine And Law." Issues In Accounting Education 27.3 (2012): 671-690. Business Source Complete. Web. 16 Jan. 2016.

Clements, Curtis, John Neill, and O. Stovall. "An Analysis Of International Accounting Codes Of Conduct." Journal Of Business Ethics 87.(2009): 173-183. Business Source Complete. Web. 03 Jan. 2016.

Glodstein, David. "Occupational Fraud: Misappropriation Of Assets By An Employee." Journal Of The International Academy For Case Studies 21.5 (2015): 81-86. Business Source Complete. Web. 05 Mar. 2016.

Marcella Jr., Albert J.1. "Encryption Essentials." Internal Auditor 71.6 (2014): 55-59. Business Abstracts with Full Text (H.W. Wilson). Web. 05 Feb. 2016.

Journal Of Business Ethics 127.1 (2015): 189-203. Business Abstracts with Full Text (H.W. Wilson). Web. 14 Jan. 2016.

Mastracchio Jr., Nicholas J., Carlos Jiménez-Angueira, and Ildiko Toth. "The State Of Ethics In Business And The Accounting Profession." CPA Journal 85.3 (2015): 48-52. Business Source Complete. Web. 05 Feb. 2016.

Meymandi, Azam Roosta, Hossein Rajabdoory, and Ziba Asoodeh. "The Reasons Of Considering Ethics In Accounting Job." International Journal Of Management, Accounting & Economics 2.2 (2015): 136-143. Business Source Complete. Web. 05 Feb. 2016.

Oracle. "4 Monitoring Real-Time Database Performance." Monitoring Real-Time Database Performance. Oracle, n.d. Web. 25 Mar. 2016.

Rikhardsson, Pall, and Richard Dull. "An Exploratory Study Of The Adoption, Application And Impacts Of Continuous Auditing Technologies In Small Businesses." International Journal Of Accounting Information Systems 20.(2016): 26-37. ScienceDirect. Web. 30 Mar. 2016.

"SAP HANA Live Overview." SAP HANA Tutorial. SAP HANA Tutorial, n.d. Web. 25 Mar. 2016.

Trigo, António, Fernando Belfo, and Raquel Pérez Estébanez. "Accounting Information Systems: The Challenge Of The Real-Time Reporting." Procedia Technology 16.CENTERIS 2014 - Conference on ENTERprise Information Systems / ProjMAN 2014 - International Conference on Project MANagement / HCIST 2014 - International Conference on Health and Social Care Information Systems and Technologies (2014): 118-127. ScienceDirect. Web. 16 Jan. 2016.

Uzun, Emre, et al. "Security Analysis For Temporal Role Based Access Control." Journal Of Computer Security 22.6 (2014): 961-996. Business Source Complete. Web. 14 Mar. 2016.

Zhensheng, Zhuang. "Research On The Security Model Design Of Accounting Information System Based On The B/S Model." Applied Mechanics & Materials 687-691.(2014): 1840-1843. Engineering Source. Web. 16 Jan. 2016.