Advances in Economics, Business and Management Research, volume 215
Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)

Risks in the Design and Analysis of Accounting Systems

Ping Zhou[1,*]

[1]*School of Accountancy, Central University of Finance and Economics, Beijing, China.100098*
**Corresponding author. Email: 2018210658@email.cufe.edu.cn*

ABSTRACT
This research covers risks associated with accounting system design and analysis. In addition, the paper will look at how the accounting system aids firms in keeping track of and managing their financial activities. The goal of this study is to better understand the risks associated with accounting system design and the internal control framework's components, which include control activities, control environment, monitoring, communication, and information. An accounting system is a set of activities and records used by a company to execute transactions and maintain track of finances. Security breaches, fraud, outages, and changes in financial legislation are all threats to accounting systems. The impact of security breaches, outages, fraud, and financial restrictions is investigated in this research. Threats are the possibility for unanticipated occurrences or actions that do not jeopardize both the accounting and organizational information systems. The research was carried out by evaluating some articles linked to developers' awareness of the hazard of accounting system security. This study also looks at the many sorts of internal controls, such as preventive, corrective, and detective controls.

Keywords: *Accounting Systems, Financial institutions, Risk Management, Organizational performance*

1. INTRODUCTION

An accounting system is a set of activities and records used by a company to execute transactions and maintain track of finances. Among other things, such a system identifies, integrates, processes, computes, categories, records, summarizes, and reports. Accounting systems help businesses enhance productivity, save operating expenses, and make better choices in the long and near term.

Understanding the risks associated with the area of financial accounting is one of the most essential things to do to solve or prevent them. This aids in the creation of the most efficient accounting system possible, ensuring that all transactions are executed correctly. Moreover, an accounting system's good design aids in the development of investor sentiment. As a result, I'm intrigued in learning about the potential risks associated with developing an accounting system in strategy to garner more investments and create a system with the fewest possible errors. Understanding the several sorts of risks, such as operational risk, strategic risk, financial risk, compliance risk, and reputational risk, can extend the subject and help others completely see why one should be cautious while designing an accounting system. Financial information is very sensitive to any company, so understanding how to minimize dangers like unlawful backups, data theft, and illegal sharing of information to third parties will be a valuable addition to my accounting system expertise.

The purpose of this research is to address the following question: "What are the Risks in The Design and Analysis of Accounting Systems and their influence or reflection of the risks of accounting system inputs on administrative, accounting, and internal control in commercial banks?"

2. LITERATURE REVIEW

Globalization and interaction have been the defining characteristics of the economic environment throughout the previous several decades. Accounting is a formal corporate communication language that enables a firm to be represented both internally and publicly. It should also be able to swiftly adapt to the current global business environment, which is constantly changing and evolving. Without the new communication and computing architecture centring around the World Wide Web, this change would be unthinkable. The usage of

telecommunication systems and networks may be dangerous since it can lead to unforeseen events such as communication system failures, information loss, or faulty judgments[1]. The term "information infrastructure" describes a variety of information resources, such as communication networks, entities, and experts in the subject[2]. Society has become more reliant on accounting systems, which have become increasingly complicated to fulfil the growing demand for data. Companies have a higher danger of the system being contested as the system becomes more complicated and dependent on the system. Almost every year, more than 60% of organizations fail to manage the confidentiality and reliability of accounting systems [3]. The following are the reasons behind this: Information is accessible to a high number of workers, and information spread throughout the accounting system is hard to regulate; society has become more reliant on accounting systems, which have become more complicated in response to the growing need for data. As an open system, an accounting system cannot be assured to be error-free or devoid of fraud. Internal control allows systems to defend themselves from potentially dangerous activities. Because the danger to the Accounting System grows in both kind and severity, the notion of control is becoming more significant and holds a strategic position. Companies confront higher risk for systems that are being designed and negotiated, under the rise in complexity and reliance systems have on the system. The major sources of risk for accounting systems are discussed below.

2.1 Attackers

People inside a firm, as well as catastrophes or natural disasters, are the major sources of risk for accounting systems [4]. Furthermore, persons outside the firm, in certain situations, constitute a significant source of danger since they are more dedicated and tougher to identify and probe than employees.

The following 'agents' are likely to create difficulties with the accounting information system's security: Personnel: They are trusted and have exposure to the Accounting Systems, which allows them to get a deeper understanding of the system's flaws, undertake activities that are harmful to the organization, and remove digital data; rivals: Other persons or businesses that stand to profit from the company's losses as a consequence of such assaults on the accounting Systems; Crackers Professional criminals/mercenaries in the fields of information technology and information security. Espionage specialists; those who unlawfully access information systems and purposely inflict harm, with a variety of motivations. They are experts in gathering information on behalf of other businesses. Accidents/natural catastrophes might result in the loss of crucial information or render it inaccessible. These persons have highly technical skills; they are well taught and can most frequently follow their goals without being noticed.

Attackers on information systems generally fall into one of four groups, depending on their motivation: Social motivation. This kind of attacker tries to achieve a sense of dominance or control, as well as acceptance from other attackers or absorption into a certain group. Motivation to learn new skills. As a form of intellectual contest, attackers in this category aim to 'defeat' the system. This kind of attacker tries to get political consideration to support a certain cause. Attackers in this group are looking for personal gain (i.e. spies or even people that deal with confidential information, etc.). A password cracker is software that can break passwords, bypass password security, or disable it. Attacks using "brutal force" and attacks using dictionaries are prominent strategies used to "guess" the password. Human nature is used in social engineering attempts to obtain access to sensitive information. Most of the time, such assaults target the organization's gullible employees. Database attacks have certain distinct characteristics when compared to other types of data in the company, such as the fact that databases contain the most data; databases may disclose personal information by processing public data. Direct, indirect, and monitoring assaults are the most common forms of database attacks.

2.2 Threats

Threats to the accounting information system's infrastructure are acts that might be done or are now being taken to attack the system. Security threats may be classified into three categories: natural/physical, unintentional, and purposeful [5]. The ones that are done on purpose are the most common. They are divided into two groups: internal and external. Internal risks originate from inside the company, where personnel have easier access to information since there are fewer hurdles to overcome. Furthermore, they are aware of the company's security policies.

Fundamental threats, enabling threats, and indirect threats are the three types of threats that might affect the accounting information system's infrastructure. What an attacker intends to achieve is represented by fundamental threats. Information leaks, data manipulation, rejection, denial of service, and unauthorized usage are examples of such risks. Threats that facilitate access to basic threats are known as facilitating threats. Masquerade, malicious programs, security by-pass, and authorization breaches are all examples of facilitating risks. Interception, scavenging, indiscretion, and administrative mistake are all examples of indirect dangers that arise from the fundamental properties of the Internet and information infrastructure.

2.3 Security

Accounting system security is achieved by achieving four goals: confidentiality, integrity, availability, and non-repudiation. Security is not a goal in and of itself. Security as a goal might be considered a state. Regardless matter the safeguards put in place, security will never be flawless [6]. Access management, firewalls, antivirus software, file encryption, digital identity, physical security, and other security technologies are used to eliminate risks and reduce losses. To this end, the following activities must be carried out: intrusion prevention, detection, and response. Encryption is seen on multiple tiers inside information systems, including hardware, application, data transport, files, and directories. When it comes to antivirus software, corporations and businesses may run into issues. Virus scans, for example, are tough to do from each workstation; upgrading antivirus software is difficult, and monitoring antivirus software performance on each workstation is complex.

A firewall is a system that implements rules to limit access to a business system or access across companies. It will guard a machine or a network against unauthorized access. When picking a firewall, keep the following parameters in mind: the level of security, the operating system, and the management system [7]. The deployment of an intrusion detector will aid the firm in terms of detecting, stopping, and responding to attacks, as well as assisting in the assessment of losses suffered and providing proof acceptable in court against those accused of abusing infrastructure components. A particular sort of intrusion detector may be chosen depending on the specificity and size of the firm. Such intrusion detectors are included in the firewall used in small businesses. The invasive attempts will be detected by analysing the firewall records or router logs. In addition, operating systems may aid in the detection of intrusions.

2.4 Risk Analysis

Risk is described as a possible hazard that might take advantage of flaws in accounting information systems. A risk is an occurrence that is predicted to happen. Specific actions should be made to avoid an occurrence that might compromise the security of the information system from happening. Security measures are what they're called. Risk analysis is a component of risk management, which encompasses a wide range of measurements. The outcome of risk analysis is risk assessment. Risk management may be described as a set of procedures for recognizing, checking, deleting, or minimizing occurrences that may have an impact on the system's resources.

The risk may be tackled from a variety of perspectives, some of which are included below: quantitative analysis, qualitative analysis, and workstation analysis. These risk assessments are mostly carried out by major firms and a few medium-sized businesses. Small businesses do not have specialized people or the financial resources to pay for such an evaluation. Nonetheless, a minimal level of security must be implemented. It is a well-known reality that business executives are hesitant to engage in projects that do not provide a direct return. When they are convinced of the need of assigning the amounts necessary to ensure security, the quantities are frequently less than the standards' maximum limit. In these instances, the business must guarantee that the cost of the security system does not exceed the budgeted amount. This is referred to as "financially restricted security." In this circumstance, there are two options: covering dangers that are most likely to materialize while keeping the original checking procedures, or covering all threats while minimizing expenses associated with checking measures [8].

The former provides the greatest level of protection against certain risks, but it may leave other threats partly or unprotected. The latter necessitates a reduction in the amount of money spent to guarantee that all potential hazards are addressed. This may be reflected in the way checking measures are modified and configured. This is preferable to the former since it prevents vulnerabilities from being discovered by checking measures. Security is difficult to measure, although it may be graded as a great, medium, low, or none at all. Nonetheless, the amount of security may be defined, at least from a financial standpoint. Costs associated with equipment and human resources will always be incurred while implementing, testing, or updating a security system.

The process by which a firm or organization guarantees its security is known as establishing a security program [9]. This program consists of five steps: appointing security people, deciding the major phases of implementing security, defining security requirements, educating employees about needed security measures, auditing, and monitoring security. In certain circumstances, guaranteeing security necessitates the involvement of specialized organizations. They may do both the research and the implementation, or just the study, with the implementation being handled by the company's staff. Small businesses often engage in specialized services when updating the skills of staff in charge of security involves a significant financial investment. Outsourcing is a company's decision for having security services provided by a third party. They deliver security services as well as security management. Security Service Management (SSM) will be handled by the services provider, not the firm. Security is a continuous process, not a destination [10].

3. METHODOLOGY

This process involves deciding on a study plan that will drive and allow the researcher to respond to the research questions. This study was based on a survey of various studies that focus on the security vulnerabilities to accounting systems. This research mostly consists of print books and internet articles that are specifically related to my subject. The research also concentrates on determining the best path to success in terms of developing the most efficient accounting system. I am convinced that the risks associated with accounting system design and analysis need sufficient time and knowledge to prevent errors that may spook investors. In addition, after performing a review, classification of what constitutes a danger to the accounting system is completed.

The first element of the goal is to investigate and understand how accounting system inputs affect administrative, accounting, and internal control in commercial banks. Accordingly, the following design was used for this research: For this research, a secondary data study using regression analysis was used to determine the influence of how accounting system inputs affect administrative, accounting, and internal control in commercial banks. For the following goals, SPSS statistical software was utilized in the analytical process: Because there were multiple independent variables, Multiple Liner Regression was applied. The link between the dependent and independent variables was investigated using the T Distribution test, which was applied for the presented hypothesis. The F-Test was used to determine if the model as a whole was suitable. The overlap (relationship) between the independent variables was investigated using the Variance Inflation Factor. The ratio of the sum of squares of consecutive differences of residuals to the sum of squares of errors is known as the Durbin–Watson Test in statistics.

4. RESULTS AND DISCUSSION

Hackers are a frequent danger, according to the findings of reviews of numerous articles. When there are no physical boundaries and controls are centralized, the danger of hackers becomes extremely real. A computer virus is the outcome of a programmer's labor that successfully infiltrated the virus into someone else computer system, either with malevolent purpose or merely to fulfil their programming thirst. Viruses may penetrate a computer system in some ways, including Share files, such as copy-paste, with other computers infected with the virus; E-mail, since the virus has been linked to an e-mail file, perusing e-mails from questionable sources can result in infection; Chat channels may be used to introduce viruses into a computer.

The following is the influence of the risks of accounting information system inputs on administrative control. The occurrence of duplicate accounting data entry influences the efficiency of administrative choices, implying that banks must record accounting system data from several controls. The tampering of accounting system inputs has harmed the documentation of the bank's activities to clients, perhaps resulting in the loss of their rights. The distribution of competences and competencies across personnel is influenced by the generation of solid accounting data. This implies that creating a good organizational structure in the bank is challenging, and this is reflected in the bank's activities.

The following is the influence of the risk of the accounting system's inputs on accounting control. The deletion of certain inputs before their usage influences financial control and, as a result, the validity of the bank's financial statements, necessitating the integration of accounting system data entry to activate the prevention of inaccurate data entry on the accounting system. The deletion of particular information from the systems has impacted the bank's ability to maintain comprehensive data on banking activities, necessitating a review of accounting data input after the first entry by another person to ensure self-control.

The following is the influence of the risk of accounting system inputs on internal control procedures. The alteration of primary manuscripts after they have been entered into the accounting software influences the efficacy of obtaining control over the bank's assets. This entails differentiating the terms of reference for personnel who receive original documents from those who input the original documents into the accounting software. Inappropriate usage of the accounting software has an impact on the bank's ability to maintain effective control and avoid asset misappropriation. Several items that the information system management should consider after looking at certain issues that constitute a danger to the security of the health information system given in the evaluated articles are: To secure information assets, do a security risk analysis; Implement safeguards in terms of policies, procedures, processes, and activities to protect data from a variety of risks; Provide enough protection in the areas of secrecy, integrity, and investigative availability.

5. CONCLUSION

The paper's arguments allow us to see the digitized environment as a source of new threats. Any company must perform comprehensive risk assessments and analyses to assure effective data security. The realization around us necessitates a three-fold attitude to the risks that the accounting infrastructure faces, namely, threats defined as events or activities (typically from outside the system evaluated) that may affect the security flaws within any system, resulting in implications, defined as

damage or a repercussion that the corporation or enterprise may suffer in the short, medium, or long term. Risk cannot be eliminated from a business; it will always exist. It is within the power of corporate management to bring it down to a tolerable level.

REFERENCES

[1] Aanestad, M., Monteiro, E., & Nielsen, P. (2007). Information infrastructures and public goods: Analytical and practical implications for SDI. Information Technology for Development, 13(1), 7-25.

[2] Vasiu, L., & Vasiu, I. (2004). Dissecting computer fraud: From definitional issues to a taxonomy. 37th Annual Hawaii International Conference on System Sciences, 2004. Hawaii. 115-117.

[3] Vasiu, I., & Vasiu, L. (2020). Break on through: An analysis of computer damage cases. https://doi.org/10.31228/osf.io/ugj5v.

[4] Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. Computers & Security, 88, 25-26

[5] Pathan, A. K. (2014). The state of the art in intrusion prevention and detection. CRC Press.

[6] Panko, R. R. (2012). Computer security incident response teams (CSIRTs). Handbook of Computer Networks. 632-638.

[7] Panko, R. R. (2004). Computer security incident response teams (CSIRTs). The Internet Encyclopedia. 56, 8-10.

[8] Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. Proceedings of the 2001 workshop on New security paradigms - NSPW '01. https://doi.org/10.1145/508171.508187 In Proceedings of NSPW, Cloud croft, New Mexico, USA.

[9] Bishop, M. (2002). Trends in academic research: Vulnerabilities analysis and intrusion detection. Computers & Security, 21(7), 609-612.

[10] Vasiu, L., & Vasiu, I. (2004). Dissecting computer fraud: From definitional issues to a taxonomy. 37th Annual Hawaii International Conference on System Sciences, 2004. Hawaii. 15-17.

[11] ISO (2008) ISO 27799: 2008 about Health Informatics -Information Security. Management in Health using ISO / IEC 27002. Geneva: ISO.