Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

The Effectiveness of Internal Control Procedures in Providing Electronic Information Security

Danah Abdulaziz Alfares

Abstract

The study aimed to demonstrate how internal control processes effectively provide electronic information security. The study used the qualitative method. Results showed that the Bank has an effective and efficient control environment. Several of its processes still need to be improved and strengthened, especially those that deal with determining the number of workers required to manage the various operations. By identifying numerous deviations and delivering exact operational management recommendations for shifting company processes, internal control methods enable the bank to promptly make adjustments. Based on the findings, the study came out with several recommendations. First, the necessary to provide management support for internal control activities involving information security, including the provision of qualified cadres in the internal audit department and the provision of the training they require to recognize emerging threats to information security and appropriate counter measures. Second, the necessity of educating the financial management team about the value of information assets and how to protect them, particularly against technological threats, with a focus on less-experienced staff. Third, encouraging staff members to obtain professional certifications in information security management. Fourth, maintaining the confidentiality of the company's information is one of the crucial components of its strategic development, thus it is necessary to encourage small businesses to implement effective internal control measures appropriate to the scale of their activity to maintain the security of their information.

Keywords: *Internal Control; Information Security; Information Technology (IT); Internal Audit Function (IAF).*

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

Introduction

If organizations want to survive in a fiercely competitive environment; efficient operational control, strategic direction and the exploitation of high-quality information must be taken into account and dependent on, organizations of all shapes and sizes must enthusiastically embrace information systems and technologies. In order to ensure that all the information buried within organizational information systems maintains its integrity, confidentiality, and availability; it is crucial that suitable security and control measures be implemented (Dhillon & Backhouse, 2001). The threat to the security of organizational information and information systems, however, is also strongly supported by evidence, including an increasing number of threats, a more comprehensive range of threats, and most crucially, a more serious impact (Angell, 1996). For example, natural disasters, theft of equipment and software, unauthorized access, and human error are some of the more conventional threats to the security of information and systems (Loch et al, 1992), while viruses are among the more recent threats (Post & Kagan, 2000) and hacking and cyber terrorism (Furnell & Warren, 1999).

Such dangers are expanding mostly as a result of increased interconnection within and across enterprises (Dinnie, 1999; Barnard & von Solms, 1998). Particularly, as information security moves from being just a "domestic" concern to one that involves third parties, such as external business partners, the rise of intra-organizational systems is causing issues for businesses (von Solms 1998).

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

Information security is the collective term for any measures taken to safeguard data and information systems from unauthorized access, use, disclosure, interruption, alteration, or destruction. United States Code 2008 computer technology Information security requires an important role for IT. IT refers to any technology, including a mix of computer hardware, software, and related communications systems that facilitates the management, processing, or dissemination of information. Since financial reporting, information security, and IT are closely related, the majority of businesses have put in place a range of IT controls to abide by SOX rules 2005's Damianides (Wallace et al., 2011).

Information security is the collective term for any measures taken to safeguard data and information systems from unauthorized access, use, disclosure, interruption, alteration, or destruction (United States Code 2008). Information security requires a strong foundation in information technology (IT). IT refers to any technology, including a mix of computer hardware, software, and related communications systems, that facilitates the management, processing, or dissemination of information. Since financial reporting, information security, and IT are closely related, the majority of businesses have put in place a range of IT controls to abide by SOX rules (Damianides, 2005).

Although the accuracy of an organization's financial information and the efficacy of internal controls are the key objectives of SOX, SOX does not specifically address how IT should be integrated into the SOX compliance process. Additionally, the SEC provides minimal advice on the use of IT, leaving for ambiguity in how much and what kind of IT is

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

used in complying with SOX (Brown and Nasuti, 2005). Most firms do not require individuals with IT skills to engage in compliance activities, according to a 2003 Gartner poll (Leskela and Logan, 2003). Others contend that even if IT specialists are participating in the compliance process, they might not be knowledgeable about the nuances of internal control, which could cause problems with communication, implementation, and effectiveness (ITGI 2006). According to an ISACA (2011) report, information security risk management should involve more than simply a specific group within the information technology (IT) function and should also engage other organizational functions, such as the internal audit function (IAF).

For study on internal audit as a governance and risk management method, the issue of information security risk management thus provides an essential framework (Steinbart et al., 2018). The IAF may have a favorable impact on the quality of risk management and internal control systems, according to Sarens (2009). The IAF is expected to actively contribute to the improvement of procedures and internal controls in order to make up for the loss of control that (Sarens & De Beedle, 2006).

Problem and Questions of The Study

Research Problem:

The proliferation of electronic accounting information systems, with all its advantages, has led to the emergence of modern risks that were not previously known in the paper system, including the security of electronic information, which is related to the possibility of information and data being stolen, lost or modified by individuals from outside the organization or by individuals using the system in addition It is not possible for programmers to view all the data stored within the databases.

Questions of The Study

The problem of the current study can be summarized in the following questions:

1. What is the internal control framework?
2. How Accounting information systems security effect on the banking sector?

The Study Objectives

The study seeks to achieve the the following objectives:

1. To explain the internal control framework.
2. To suggest how the accounting information systems effect on banking sector.

Methodology

The study will use the qualitative method. This method aims to first ascertain the current state of a specific occurrence before attempting to explain it. As a result, it is dependent on the study of reality or the event as it actually occurs and is concerned with accurately portraying it (Creswell, 2003).

Because it is regarded as a fundamental scientific inquiry and is widely regarded as the sole approach capable of studying many human fields, the qualitative method is significant in research. According to its definition,

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

the qualitative method entails treating the phenomenon as it actually is and is concerned with accurately defining it and communicating it both qualitatively and statistically (Williams, 2007).

The study followed the qualitative approach to clarification the effectiveness of internal control procedures in providing electronic information security through the literature review.

Definitions

Internal control is a procedure carried out by a board of directors, management, and other staff members of a company and intended to give reasonable assurance about the accomplishment of goals related to operations, reporting, and compliance (Committee of Sponsoring Organizations of the Treadway Commission, 2012).

Information security is defined by the international standard ISO/IEC 27002 (2005) as the maintenance of the confidentiality, integrity, and availability of information (ISO/IEC 27002, 2005, p. 1). Information can exist in a variety of forms according to ISO/IEC 27002 (2005). It can be typewritten or printed on paper, electronically stored, sent by email or other methods, displayed on film, spoken out, or any number of other ways (ISO/IEC 27002, 2005, p. 1).

Literature Review

The Objectives of Internal Control

Three categories of objectives are outlined in the Framework, allowing organizations to concentrate on various facets of internal control

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

(Committee of Sponsoring Organizations of the Treadway Commission, 2012):

- Operations Objectives: These concern the efficiency and effectiveness of the entity's operations, including objectives for operational and financial performance and protecting assets from loss.
- Reporting Objectives: These cover reliability, timeliness, transparency, and other criteria outlined by regulators, standard-setters, or the entity's rules and apply to internal and external financial and non-financial reporting.
- Compliance Objectives: These deal with following the rules and laws to which the entity.

These diverse but overlapping categories handle various requirements and may even be the direct responsibility of various individuals. One purpose may come under more than one category. Additionally, the three categories show what to anticipate from internal control. An organization should have a reasonable level of assurance from an internal control system that its goals for external reporting and legal and regulatory compliance will be met. The manner in which operations under the supervision of the organization are carried out will determine whether those objectives, which are largely based on laws, rules, regulations, or standards created by lawmakers, regulators, and standard setters, are met. Internal reporting goals that are not largely influenced by such external parties are typically created with more latitude by management and/or the

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

board. To allow internal reporting to better support the entity's external reporting, the business may choose to align its internal and external reporting objectives (Committee of Sponsoring Organizations of the Treadway Commission, 2012).

Internal Control

The information security policy has not, to now, been the focus of clear, empirical analysis in the academic literature, despite the fact that its importance is widely accepted. An exploratory study project was started to look into the adoption, content, dissemination, and impact of information security rules in order to assist close this gap. To achieve this, senior IS executives in significant UK-based firms were mailed a questionnaire. A total of 208 valid replies were received. Although policies are now reasonably prevalent, at least among our sample, the findings of this study show that there is still a significant amount of variation in terms of their substance and dissemination (Fulford and Doherty, 2003).

Businesses have increased the number of resources devoted to efficient internal control monitoring as a result of the Sarbanes-Oxley Act of 2002. The Masli et al. (2010) study adopts a method for evaluating potential outcomes of internal control monitoring practices by taking into account explicit benefits associated with monitoring technology as represented by internal assurance outcomes, such as the strength of the internal control system, and external assurance outcomes, such as the efficiency and timeliness of the audit. The findings of the study taken as a whole lend

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

credence to the benefit-related claims incorporated into the conceptual application of efficient internal control monitoring techniques.

The focus of the paper was on evaluating the financial security of insurance company operations as one of the implementation stages for all forms of economic control, particularly internal control. In the current stage of economic development, the internal management of business processes related to the assessment of financial security and the assessment of risks in insurance businesses is a pressing concern. Furthermore, this area of internal control is not sufficiently developed for application in the insurance industry. The article offers an algorithm for evaluating an insurance company's financial security in internal control and suggests phased monitoring of the evaluation of an insurance company's financial risks. The methods of determinative factor analysis and an indicative method for setting the standards for evaluating indicators were used in the study's methodology. It is determined that the internal control of evaluating the financial security of an insurance firm must be used as one of the sections of the approach. The study's output was the creation of an algorithm for carrying out one of the internal control sections utilizing an evaluation of an insurance company's financial stability. The article's practical importance comes from the fact that its conclusions and recommendations are intended to advance contemporary economic control and support genuine company optimization. According to a survey the authors conducted, the new reality has caused people's attitudes on the employment of conventional methods to shift, making it necessary to modernize existing ones and

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

adopt fresh perspectives on economic control methods (Turgaeva et al., 2020).

Internal Control Framework

The internal control framework of an organization should include IT controls. IT controls and SOX regulations both call for the protection and oversight of a company's financial data. Information security management is a challenging process that, when properly managed, aids firms in achieving and maintaining SOX compliance. The conclusions of this study not only describe the IT controls already in use, but also offer suggestions for future research that will build on the existing findings to create tactics to help firms install information security controls that support and sustain SOX compliance.

The internal control framework of an organization should include IT controls. IT controls and SOX regulations both call for the protection and oversight of a company's financial data. Information security management is a challenging process that, when properly managed, aids firms in achieving and maintaining SOX compliance. The conclusions of this study not only describe the IT controls already in use, but also offer suggestions for future research that will build on the existing findings to create tactics to help firms install information security controls that support and sustain SOX compliance (Wallace et al., 2011).

Accounting information systems security is significant in the banking sector due to its critical role in generating high-quality financial services. Additionally, terminals strive to give decision-makers reliable

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

information, enhancing and developing the performance of these services, and boosting their sufficiency and efficacy in the banking industry. The purpose of the current study is to investigate how putting in place information technology governance structures might improve the security of electronic accounting systems. Additionally, it aims to evaluate the prerequisites for applying the COBIT framework processes for the Trade Bank of Iraq's implementation of information technology governance. The findings demonstrate that the Bank has a suitable and suitable control environment. It still has to be improved and enhanced in several of its processes, particularly those that deal with estimating the number of employees needed to run the Bank's various operations and assigning authority and responsibility to the banking industry. As these units take some of the essential steps to address those banking risks, there are also banking units in charge of controlling the risks related to information security. The internal control team's responsibilities, however, center on debating adequate monitoring of the process of providing banking services and risk assessment. The Bank also engages in appropriate supervision operations to keep an eye on its accounting and financial performance. However, they need to pay more attention to the sentences that discuss how to properly divide up the jobs given to the employees as well as how to make sure that each person may use the complaint box. Therefore, the segregation of jobs can function as a helpful monitoring tool for increasing client confidence, observing the performance of autonomous employees, and continuously enhancing and developing performance (Al-Fatlawi et al., 2021).

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

Information Security

Companies must now manage information security risks due to the growing financial effect of cybercrime. The internal audit function (IAF), according to the practitioner literature, can be crucial in both providing assurance regarding information security and producing ideas about how to enhance the organization's information security. However, there is little empirical data to back up this assertion. This study investigates the impact of objective measures of the overall efficacy of an organization's information security activities on the quality of the interaction between internal audit and the information security functions using a distinctive data set. The degree of this association has a favorable impact on the quantity of reported internal control flaws, instances of noncompliance, and security events discovered both before and after they caused the company material harm. Additionally, we find that having the chief information security officer (CISO) report independently from the IT function and having higher levels of management support for information security have a positive impact on the quality of the partnership between the internal audit and information security functions (Steinbart et al., 2018).

The information security policy is one of the most significant information security measures. This crucial direction-giving document, however, is not always simple to create, and its authors struggle with issues like what counts as a policy. As a result, the architects of the policy go to already-existing sources for assistance. The many worldwide information security standards are one of these sources. These criteria are an excellent place to

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

start when deciding what the information security policy should include, but they shouldn't be the only source of information. They lack complete coverage, to start with, and they also tend to focus more on the procedures required for successfully implementing the information security policy. The organization's culture must be considered while developing the information security policy as it is considerably more crucial than it does so (Höne and Eloff, 2002).

Conclusion and Recommendation

The aim of the study is to explain the effectiveness of internal control procedures in providing electronic information security through the literature review. The study employs qualitative research, a technique designed to first determine the current context of a particular event before attempting to provide an explanation. As a result, it is reliant on the examination of reality or the event as it actually transpires and is concerned with faithfully capturing it.

The results show that the business may decide to align its internal and external reporting objectives in order to allow internal reporting to better support the entity's external reporting. Internal reporting goals that are not significantly influenced by such external parties are typically created with more latitude by management and/or the board. The findings demonstrate that the Bank has a suitable and suitable control environment. It still has to be improved and enhanced in several of its processes, particularly those that deal with estimating the number of employees needed to run the Bank's various operations and assigning authority and responsibility

Multi-Knowledge Electronic Comprehensive Journal For
Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

to the banking industry. As these units take some of the essential steps to address those banking risks, there are also banking units in charge of controlling the risks related to information security. The internal control team's responsibilities, however, center on debating adequate monitoring of the process of providing banking services and risk assessment. The Bank also engages in appropriate supervision operations to keep an eye on its accounting and financial performance. Internal control procedures allow you to quickly make adjustments as a result of discovering various deviations and producing precise operational management recommendations for changing business processes. They not only optimize business processes at an early stage of their implementation.

Based on the conclusions reached by the study, the study came out with the following recommendations:

- The need for management support for internal control activities on information security by providing qualified cadres in the internal audit department, in addition to providing the necessary training for them to identify new challenges facing information security and methods of combating them.
- The need to provide training and awareness to the financial management staff on the importance of information assets and methods of preserving them, especially from electronic risks, with a focus on less experienced employees.
- Encouraging employees in companies to obtain professional certificates related to information security oversight.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

- The need to encourage small companies with the importance of applying effective internal control measures commensurate with the size of their activity to maintain the security of their information, because maintaining the confidentiality of the company's information is one of the important elements for its strategic development.
- The need for continuous cooperation and coordination between the Internal Audit Department, the Information Technology Department, and the Financial Department with regard to information security.

References

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. Webology, 18(Special Issue on Information Retrieval and Web Search), 294-310.

ANGELL, I. O. (1996). Economic crime: Beyond good and evil. Journal of Financial Regulation and Compliance.

Barnard, L. and von Solms, R. (1998) "The evaluation and certification of information security against BS 7799", Information Management and Computer Security, 6 (2), pp. 72-77.

Brown, W., & Nasuti, F. (2005). Sarbanes-Oxley and enterprise security: IT governance-what it takes to get the job done. Inf. Secur. J. A Glob. Perspect., 14(5), 15-28.

Committee of Sponsoring Organizations of the Treadway Commission. (2012). Internal Control—Integrated Framework: Framework and Appendices, September 2012.

Creswell, J. (2003) Research design: Qualitative, quantitative and mixed methods approaches (2nd ed.). Thousand Oaks, CA: SAGE Publications

Damianides, M. 2004. How does SOX change IT? Journal of Corporate Accounting & Finance 15 ?6: 35–41

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information systems journal, 11(2), 127-153.

Dinnie, G. (1999). The second annual global information security survey. Information Management & computer security.

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications(MECSJ)
Issues 82 (2025)
ISSN: 2616-9185

Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium?. Computers & Security, 18(1), 28-34.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. Computers & security, 21(5), 402-409.

ISO/IEC. ISO/IEC 27002: code of practice for information security management 2005

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting. ISACA.

Leskela, L., & Logan, D. (2003). Sarbanes-Oxley compliance demands IS involvement. Gartner, available at: www. gartner. com.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. Mis Quarterly, 173-186.

Masli, A., Peters, G. F., Richardson, V. J., & Sanchez, J. M. (2010). Examining the potential benefits of internal control monitoring technology. The Accounting Review, 85(3), 1001-1034.

Post, G., & Kagan, A. (2000). Management tradeoffs in anti-virus strategies. Information & Management, 37(1), 13-24.

Sarens, G. (2009). Internal auditing research: Where are we going? Editorial. International Journal of Auditing, 13(1), 1-7.

Sarens, G., & De Beelde, I. (2006). The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. International Journal of Auditing, 10(3), 219-241.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29.

Turgaeva, A. A., Kashirskaya, L. V., Zurnadzhyants, Y. A., Latysheva, O. A., Pustokhina, I. V., & Sevbitov, A. V. (2020). Assessment of the financial security of insurance companies in the organization of internal control. Entrepreneurship and Sustainability Issues, 7(3), 2243.

United States Code. 2008. Public Printing and Documents: Definitions. Title 44, Section 3552. Washington, D.C.: United States Code

Von Solms, R. (1998). Information security management (1): why information security is so important. Information Management & Computer Security.

Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information security and Sarbanes-Oxley compliance: An exploratory study. Journal of Information Systems, 25(1), 185-211.

Williams, C. (2007). Research methods. Journal of Business & Economics Research (JBER), 5(3).