



International Journal of Multidisciplinary Research and Growth Evaluation



International Journal of Multidisciplinary Research and Growth Evaluation

ISSN: 2582-7138

Received: 01-06-2021; Accepted: 16-06-2021

www.allmultidisciplinaryjournal.com

Volume 2; Issue 4; July-August 2021; Page No. 207-209

Controls, Security, and audit in online digital accounting

Siti Hardiyanti Marpaung ¹, Sri Lestari Saragih ², Sri Rizki Marbun ³, Iskandar Muda ⁴

Faculty of Economics and Business, University of North Sumatra, Medan, Indonesia

Corresponding Author: Siti Hardiyanti Marpaung

Abstract

The purpose of this study implement the use of the Internet and Web-based tools, as seen so far, permeates almost every functional area of business. Information technology, networks and computing systems, along with possible collaborating people from all over the world who may not have met in person because millions of transactions are processed in minutes due to automation, manual controls are not very useful in Internet transactions. Issues of privacy and assurance services in the online world also receive special attention. Privacy relates to the confidentiality of information; however, it also has to deal with security, because unsafe information is not personal information. As

such, privacy audits have to deal with internal controls and actual organizational behavior. Internal control is basically a system of checks and balances. The goal is to keep the organization moving along the desired line as the owner wishes and to protect the assets of the business. Internal control has received attention from auditors, managers, accountants, fraud examiners and legislative bodies. This is where the role of the company's internal control system is needed. Management designs an internal control system so that they get the reliability of financial reports, the efficiency and effectiveness of operations, and compliance with laws and regulations.

Keywords: Information Technology, Privacy Audit, Internal Control, Digital Accounting

1. Introduction

The use of technology in the business world is not something new, especially in the era of the industrial revolution 4.0 or digitalization. Technology is an important component in information systems that are expected to produce information quickly and precisely (Winarni and Rahmawati, 2015), so that the development of computer-based information systems is growing very rapidly. The use of information technology can improve internal control by adding new control procedures performed by computers and by replacing controls that are usually carried out manually which are prone to human error. (Elder, et al: 2013). The objectives of internal controls in the online world are similar to internal controls in the physical world — protect assets and information, provide reliable and relevant information, promote operational efficiency and comply with managerial policies. The online environment presents a mix of technological, human and physical elements, and threats to business can arise from any of these elements. Generally, in the security literature, technical solutions have received the most attention. However, there is no technological silver bullet to solve security problems, since technology is but one piece of the problem. Security solutions and internal controls must cover every aspect of the online environment. The Internet is a global collection of networks and connects myriad operating systems, applications, databases and machines. The explosive growth of the Internet and commercial applications has sidelined security issues; and to begin with, the Internet was designed to promote communication, not security. A white paper published by the CERT® Coordination Center (2003) gives the following reasons for security problems on the Internet.

Additionally, the Internet has a large user population that is accessing a large and dynamic pool of computer services and resources. Programs can be accessed, trans- ported and executed by remote and anonymous users. Numerous protocols run Internet transfer of data and are difficult to debug and monitor. Authentication and authorization mechanisms are different at each Web site; users may have multiple IDs and can be geographically scattered.

The efficiency and effectiveness of internal controls in the online environment encompasses technical, human, legal and audit considerations. A number of accounting firms offer privacy audit services. These services are also offered by other service firms and even done by businesses internally. Privacy — the ability to keep designated information safe from prying eyes — is a problem for both organizations and individuals. The U.S. Constitution does not specifically mention right to privacy. Historically, law has protected an individual from intrusive efforts to collect personal information. As automation became widespread, collection, aggregation and dissemination of personal information became easier. Privacy issues are beginning to

be taken seriously by individuals, organizations and legislatures.

2. Literature Review

Online Internal Controls

Internal controls, no matter the exotic terminology, have standard objectives. The objectives of online controls can be classified as validity of transactions, mutual authentication of identity, authorization, end-to-end data integrity and confidentiality, non-repudiation and auditability of transactions. These areas are not mutually exclusive, but provide a way to conceptually organize and discuss internal controls in the online world. Let us take a detailed look at elements of the conceptual framework. Some of the controls mentioned below are covered in detail in a later section.

- *Validity of transactions:* The primary question in online transactions is its legal status. Transacting parties in EDI take care of this problem by using trading agreements. New laws, such as UETA, UCITA and E-SIGN, have facilitated validity of transactions in the online world, though compliance with these laws remains an important internal control issue.
- *Mutual authentication of identity:* Authentication is a process of verifying identities of the transacting parties. It involves determining whether someone or something is, in fact, who or what it is declared to be. Authentication of identity has two facets: identity of the machines and identity of the humans operating the machine.
- Such authentication can be carried out by means of static or dynamic passwords or PINs, passwords or PINs and security tokens, automatic callbacks and biometric techniques. The use of digital certificates is also increasingly common. Establishing identity of a human at the end of the machine is primarily a matter of intra-organizational controls. It requires review of access controls and separation of duties within the organization. The human user is identified by something the user knows or carries. These criteria include passwords, ID cards or biometric measures, such as fingerprints.
- *Authorization:* Authorization is the step after authentication. The machine and user are identified and allowed access to the computer system in the authentication phase. Then, the authorization phase deals with granting rights to the user to perform certain functions. These rights define types of resources and actions allowed to the user; for example, the user can read, write or modify but cannot delete files. The rights can be assigned via Access Control List (ACL). Accounting, which may follow authorization, involves collecting statistics and usage information for a particular user or class of users. This information is used for authorization control, billing, trend analysis, resource utilization and capacity planning.
- *Data integrity and confidentiality:* Data integrity refers to transfer of data without any modification, intentional or unintentional, in the transit. Data confidentiality refers to inability of unauthorized parties to access data. Standard controls in this area include encryption, security algorithms and communication protocols such as SSL.
- *Non-repudiation:* Non-repudiation refers to proof that the electronic document was sent by the sender and received by the receiver. The three aspects of

nonrepudiation are: non-repudiation of origin, non-repudiation of receipt and nonrepudiation of submission. Non-repudiation covers the problem of post-facto denial of an electronic transaction by transacting parties. First, it proves that the transaction took place, and second, it establishes identity of the transacting parties. Controls such as digital signatures and digital certificates address nonrepudiation.

- *Auditability of transactions:* Auditability of transactions refers to the existence of an audit trail and the ability to verify past transactions. The transactions should be validated, controlled and recorded properly. A log of users, resources used by the users, and various system functions is also required for auditability.

Internal Control Techniques

Internal control techniques must address technical, legal, human and audit dimensions of security in the online world. A well-designed internal control system should be supported by top management and cover a wide range of technical and managerial strategies and tactics. No single method provides reasonable, absolute — it is never absolute — protection. A mix of security mechanisms needs to be in place to protect information assets. Security and internal controls are an ongoing and evolving process.

This process must be monitored as business situations change. The consensus of experts in this area indicates a layered approach to security. The different layers of a security system are given below. This is but a broad classification, and these areas intersect at various levels.

- Security policy for the organization
- Perimeter security
- Message content security
- Back-end infrastructure security

Privacy Audits

The privacy policies posted on the Web site are often legalistic in nature and difficult to understand. Privacy policies are often flouted since a consumer cannot find breaches easily. Privacy audits not only evaluate the online company's compliance with privacy policies but also evaluate areas such as data security and access controls, password administration, database administration, personnel security, network administration and physical security of the Web site. The requirements of WebTrust and SysTrust clearly underscore the interconnected nature of privacy and security issues. Privacy deals with confidentiality of information; however, it must also deal with security, since unsecured information is not private information. As such, privacy audits have to deal with internal controls and actual organizational behavior. Privacy Knowledge Base (www.privacyknowledgebase.com) provided the following objectives for the privacy audit.

- *Notice and disclosure:* What does the company's privacy policy promise consumers as to its information practices? How does the company collect, capture, use and disseminate personal information?
- *Access:* Does the company provide consumers with access to data collected about them?
- *Choice (opt out/opt in):* Does the company give consumers a clear choice with respect to using information supplied through visits to Web sites?
- *Enabling technology:* Does the company have the proper technology to ensure anonymity of consumers?

information?

- Security: Does the company ensure that consumers' data is safe and secure?
- Redress: Does the company provide due process for consumers that have grievances or are harmed? The privacy audit market is fragmented among various service providers.

The demand for privacy audits may increase as customers and users become more aware about how personal information is being collected, used and abused. Currently, due to legislative requirements such as the Health Insurance Portability and Accountability Act (HIPPA) and the U.S. Patriot Act, many corporations are paying close attention to the privacy and security of information. Hopefully, there will be progress in this area in the near future.

3. Conclusion

The controls, security and audit area on the Internet is a vast field. This chapter is but just a brief overview of the complicated control requirements on the Web. First, the concept of internal controls was reviewed. Internal controls are important for accountants, auditors, managers and legislatures for different reasons. Internal controls have been defined differently by different organizations; however, there are common themes in those definitions. The COSO framework was discussed in detail, since it is applicable to the online world.

Security and control issues on the Internet are multidimensional and not only restricted to technical areas. The Internet is inherently an unsecure environment, used by millions of users around the globe, and is created to facilitate the free flow of information. Technical problems in this area include protections against physical and logical attacks directed at networks, facilities and people. Logical attacks include malicious code, active content, or probes and scans to penetrate the network. Social engineering is often used to illegally acquire information from legitimate employees. Human error generally plays a larger role in successful hacking. Also, various laws, such as UETA, UCITA, E-SIGN and the U.S. Patriot Act, which affect e-commerce transactions, were investigated. Finally, auditing considerations, such as maintenance of audit trails and backups, were discussed. A conceptual framework for internal controls was presented to aid our understanding of controls on the Internet. The objectives of internal controls were stated as validity of transactions, mutual authentication of identity, authorization, data integrity and confidentiality, non-repudiation and auditability of transactions. This framework enables us to ask intelligent questions regarding internal controls, even if we do not have a full technical understanding of them.

Finally, privacy and security issues, which are intertwined, were reviewed primarily for B2C transactions. Different types of seals were discussed, and the Trust Services offered by the AICPA were reviewed in detail. A number of assurance and advisory services, such as privacy solutions, are offered by accounting and other firms. Consumers are more aware of privacy issues, and new laws are in progress to protect the privacy of personal information. As such, these areas may witness positive developments in the near future.

4. References

1. Baumer DL, Maffie RL, Ward AL Cyberlaw dan e-commerce: Perspektif audit internal. *Audit Internal*. 2001; 17:24-31.
2. Bernstein GL, Campbell E. Kontrak elektronik: Kondisi hukum dan praktik terbaik saat ini. *Jurnal Hukum Kekayaan Intelektual & Teknologi*. 2002; 14:1-11.
3. Pusat Koordinasi CERT. Gambaran umum insiden CERT / CC dan tren kerentanan (buku putih). Pittsburgh, PA: Pusat Rekayasa Perangkat Lunak, Universitas Carnegie Mellon, 2003.
4. Deshmukh A. Kerangka konseptual untuk pengendalian internal online. *Jurnal Manajemen Teknologi Informasi*. 2004; 3-4, 23-32.
5. Dreazen Y. 25 Juni). Konsumen tidak tahu apa-apa tentang privasi situs web. *The Wall Street Journal*, Bagian Keuangan Pribadi, 2003, D2.
6. Givens B. Juni). Daftar Periksa untuk praktik penanganan informasi yang bertanggung jawab. *Kredit Bisnis*. 2001; 103:47-52.
7. Lee P, Hui S, Fong A. Analisis struktural dan berbasis konten untuk pemfilteran Web. *Riset Internet*. 2003; 13(1):27-37.
8. Merkow M. Mandikan situs Anda dalam segel jaminan privasi. *Wawasan-EC Outlook*, 2000.
9. Buletin. Manajer TI percaya bahwa Spyware bukanlah sebuah laporan masalah. *Telecomworldwire*, Coventry, 2004, 1.