JISMA
JOURNAL OF INFORMATION SYSTEMS AND MANAGEMENT
Vol. 02 No. 02 April 2023 https://jisma.org e-ISSN: 2829-6591

General Control of Information Systems

Devita Wahyu Azhari[1*], Masduki Asbari[2]
[1.2]Universitas Insan Pembangunan Indonesia
Corresponding email: devitawhyzh@gmail.com

Abstract *– In society and various fields of life, the advancement of information systems is very important. Controls must be installed to detect and resolve system disturbances in the information system. The purpose of this article is to learn about general information control systems. The methodology of this article is descriptive qualitative and refers to secondary data from books, research findings published in journals, and topics related to the findings and discussion of this article. The focus of this article is on general controls in information systems, which are divided into several categories: documentation controls, hardware damage controls, organizational controls, physical security controls, and data security controls.*

Keywords*: management control, information system, internal control*

Introduction

Advances in information systems today have the potential to make them a significant component of society. People's perspectives and behavior have changed as a result of advances in information systems and technology. In addition, advances in technology and information systems have an impact on various fields. Good controls are needed to avoid and prevent activities that may affect various parties in the future, given the importance of information systems in society and various important industries.
The system is a collection of two or more parts that are connected and work together to complete a task (Romney & Steinbart, 2015). Information, however, is data that has been handled and processed to give it significance and facilitate decision-making (Romney & Steinbart, 2015). Consequently, a system built on a collection of computer and manual components that are stored, processed, and issued to users is described as an information system (Gelinas & Kusam). This is also in line with the idea that information must be considered a structured and intact aspect of the control process because it is a permanent component of that process (Marciariello, 1984). To avoid system disturbances, information systems require control devices. In general, control refers to the outermost controls on an information technology system that users have to take into account and deal with initially. Organizational controls, documentation controls, hardware controls, physical security controls, and data security controls are common divisions of information systems controls. The purpose of this article is to identify each control in the overall information system.

Method

This paper will use a qualitative descriptive methodology. Qualitative research techniques are research techniques that produce descriptive data from spoken or written people and observed behavior (Panorama & Muhajirin, 2017). Descriptive research, on the other hand, seeks to provide methodical, factual, and accurate reports of facts. A more thorough description of a symptom or phenomenon can be provided through descriptive research (Panorama & Muhajirin, 2017). This is the secondary data source that will be used in this essay. Secondary data sources are sources that indirectly provide data to data collectors (Sugiyono, 2013). Books, journal research results, and topics relevant to the topics discussed are secondary data sources used in this article.

JISMA
JOURNAL OF INFORMATION SYSTEMS AND MANAGEMENT
Vol. 02 No. 02 April 2023 https://jisma.org e-ISSN: 2829-6591

Results and Discussion

Control devices must be in place to identify and stop system disturbances in the information system. General control and application control are two types of controls in information systems. Control generally refers to the outer control of an information technology system, which the system user must initially take into account and deal with. Application controls can be enabled if the controls can be generally overridden and bypassed. Organizational controls, documentation controls, hardware damage controls, physical security controls, and data security controls are common divisions of controls. Organization Control comes first. In this section, we define good organizational control as having well-organized systems and good planning. This organizational control can be achieved if there is a clear division of roles and responsibilities; for example, the information department and the department itself may have separate roles and responsibilities. separation of roles and responsibilities within departments, such as between the transaction authority and the part that deviates from the assets concerned, between the transaction authority and the part that processes data, between the part of asset storage and the part of the implementation, between the part of the implementation and the part that processes data, and between the part asset storage and data processing section.

There are many functions performed by the information systems department, which is responsible for its duties and responsibilities. First, the sector data control division acts as a liaison between the information department and several other departments. Second, the part that completes and verifies the data ensures its completeness and accuracy so that it can be entered into the information system. The third part, computer operations, processes data to provide report findings. Fourth, is data storage, which stores data libraries, and space for data storage. The purpose of this data library is to provide a clear line of authority between the parts that store the data and the parts that will use them for activities, thus preventing unauthorized access to the data. Fourth, data analysis is carried out in the programming and system development section. Fifth, the information center, assists managers in developing their application programs for end-user computing (EUC) or end-user development (EUD). Documentation control comes next. This control over documentation is presumed to provide information about the problem through written content. This documentation includes examples of information system items as well as descriptions, justifications, flowcharts, checklists, printouts on computer results, and more. Documentation is needed for several reasons, including learning how to use the system, as training information, as a basis for future system development, as a basis for modifications, and as reference material for the auditor.

The following are some of the documents in the information systems division. First, Basic Documentation Documentation is a document that composes several basic documents used to prove system transactions. Second, account registration documentation is a record that contains details about account-related issues that are relevant to transactions. The list of accounts includes information about each account, including its code, name, categorization, and instructions. Third, manual method documentation is a record that describes how the basic paper is distributed within the business. The fourth is process documentation, which lists the many actions that must be taken under certain conditions. And finally, system documentation. program documentation is the sixth. working documentation is the seventh. The eighth item is data documentation.

Hardware damage control comes in third. If there is a hardware failure or if a process jam occurs, the data processing process may be interrupted. This can be avoided and resolved by managing the hardware, offering backup equipment, and purchasing insurance. The controls that have been built into the computer by its manufacturer can be used to manage the hardware inside it. This control is designed to be able to identify hardware faults. Hardware controls can take the form of parity checks, echo checks, read-after-write checks, dual-read checks, and validity checks.

Fourth, supervision of physical security. To keep enterprise hardware, software, and personnel secure, physical security controls must be in place. Theft, sabotage, power failures that can damage databases, fires, extreme temperatures, dust, and natural disasters are some of the things that can make a system physically insecure. The following physical security measures may be implemented:
1. The first control is physical access control, which offers security by limiting who can enter sensitive areas. Installing security guards, completing visiting agendas, using identity cards, and using cards are methods that can be used in this supervision.
2. The location of the computer room is an important factor in security planning. Control over the ideal physical location of the computer room, including a quiet area away from other buildings and potential environmental hazards.
3. The application of safety measures, including additional safety devices, may be used to prevent events that could result in death. Water lines, fire extinguishers, and uninterruptible power supplies are some of this safety equipment (UPS). Stabilizers, air conditioners, and fire detectors are additional physical safety controls.

The fifth control is data security. To prevent the security of data stored on external storage from being lost, damaged, or accessed by unauthorized persons, maintaining data integrity and security is one method of prevention. For this purpose, various control techniques, including the following, have been widely used.

Data logs are used, and agendas (logs) can be used in data processing to be able to monitor, record, and identify data. To protect files, several tools or techniques are available to protect files from improper use which can cause corruption or change of data with incorrect values, such as a tape protection ring, write-protect tabs, external labels, and labels. internal, and read-only storage. Access restrictions (Access Restriction), an important security goal is to prevent unauthorized personnel from being able to access data. Accessing data by unauthorized persons usually has the intention of diverting company property. Data backup and recovery. Backup and recovery controls are needed in case files or databases are damaged or lost or data errors occur.

Conclusion

Good controls are needed to avoid and prevent activities that may affect various parties in the future, given the importance of information systems in society and various important industries. Control devices must be in place to identify and stop system disturbances in the information system. Organizational controls, documentation controls, hardware damage controls, physical security controls, and data security controls are common divisions of controls in information systems.

References

Amani, T., Vidiyastutik, E. D., & Hudzafidah, K. (2018). Dampak Teknologi Informasi Terhadap Audit Internal. *UNEJ e-Proceeding*, 58-66.

BERBASIS KOMPUTER (Sebuah Tantangan bagi Internal Auditor). *Account: Jurnal Akuntansi, Keuangan dan Perbankan*, *9*(1).

Cantika, W. N. (2020). Pengendalian Audit Sistem Informasi. *Fakultas Komputer, TUGAS*, 1-88675543.

Effendi, M. R., & Saputra, J. (2022). Design and Build an Employee Leave Application System. *Journal of Information Systems and Management (JISMA)*, *1*(4), 42-53.

Hermansyah, R., & Asbari, M. (2022). Edifying In The Industrial Revolution 4.0 With The Role Of Islamic Education. *Journal of Information Systems and Management (JISMA)*, *1*(5), 7-11.

Indra, F., Juliana, J., Hubner, I., & Sitorus, N. B. (2022). Development Of Gastronomic Tourism Potential In Pontianak West Kalimantan. *Journal of Information Systems and Management (JISMA)*, *1*(5), 28-42.

Jasin, M. (2022). How The Role of online and viral marketing and competitiveness ability on business performance of SMEs. *Journal of Information Systems and Management (JISMA)*, *1*(2), 28-35.

Jasin, M. (2022). The Role of Social Media Marketing and Electronic Word of Mouth on Brand Image and Purchase Intention of SMEs Product. *Journal of Information Systems and Management (JISMA)*, *1*(4), 54-62.

Laoli, E. S., & Ndraha, T. P. (2022). Pengaruh Sistem Pengendalian Manajemen Terhadap Kinerja Pegawai. *Jurnal Akuntansi, Manajemen Dan Ekonomi*, *1*(1), 15-20

Muchtar, A. M., & Agha, R. Z. (2022). PENGENDALIAN PADA SISTEM INFORMASI

Novitasari, D. (2022). Hospital Quality Service and Patient Satisfaction: How The Role Service Excellent and Service Quality?. *Journal of Information Systems and Management (JISMA)*, *1*(1), 29-36.

Novitasari, D. (2022). SMEs E-commerce Buying Intention: How the Effect of Perceived Value, Service Quality, Online Customer Review, Digital Marketing and Influencer Marketing. *Journal of Information Systems and Management (JISMA)*, *1*(5), 61-69.

Patmawati, S., Dewi, V. M., & Asbari, M. (2023). THE EFFECT OF SHORT-TERM AND LONG-TERM LEARNING IN QUALITY MANAGEMENT AND INNOVATION. *Journal of Information Systems and Management (JISMA)*, *2*(1), 21-26.

Purwanto, A. (2022). WHAT IS THE ROLE OF CUSTOMER BEHAVIOR FOR ELECTRONIC E-COMMERCE AND MODERN MARKET VISIT INTENTION?. *Journal of Information Systems and Management (JISMA)*, *1*(6), 46-57.

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara Journal of Information and Library Studies (N-JILS)*, *1*(1), 39-51.

Sudirman, A., Muttaqin, M., Purba, R. A., Wirapraja, A., Abdillah, L. A., Fajrillah, F., ... & Simarmata, J. (2020). *Sistem Informasi Manajemen*. Yayasan Kita Menulis.