Transekonomika: Akuntansi, Bisnis dan Keuangan
https://transpublika.co.id/ojs/index.php/Transekonomika
Online ISSN 2809-6851 | Print ISSN 2809-7866

https://doi.org/10.55047/transekonomika.v5i2.866

Literature Review

Information Security of Management System Using ISO 27001: 2013 in the Industrial Revolution 4.0

Lusmitasari[1*], Tri Siwi Agustina[2]

[1,2]Department of Management, Faculty of Economic and Business, Universitas Airlangga, Surabaya, Indonesia
Email: [1)] lasiminsari@gmail.com, [2)] siwi@feb.unair.ac.id

Received : 28 December - 2024
Accepted : 02 February - 2025
Published online : 04 February - 2025

Abstract

The design of the Information Security Management System that is made includes all existing processes in a company. Organizations such as universities or institutions need to have a clear security management system. One of the standards that can be used to analyze the level of information security within an organization is ISO 27001:2013. This standard is continuously being developed for the purpose of completing the requirements in terms of implementation of a security system. This study aims to find out how ISO 27001 works and its benefits for an organization. The study employed a literature review methodology. Sources included books, academic papers, internet resources, and personal experiences related to the topic. This study is also expected to be able to help provide a reference for companies to determine the most appropriate security system for the company. In conclusion, the integration of ISO 27001 into an organization's security management system is crucial in today's complex digital landscape. Embracing ISO 27001 not only enhances the overall security framework within an organization but also instills trust among stakeholders and customers in the organization's dedication to data protection.

Keywords: ISO 27001: 2013, Information Security Management, Industrial Revolution 4.0, Management System, SSE-CMM.

1. Introduction

Higher education is one of the institutions providing public services where universities are required to provide the best service for those who need information, such as students, employees, or other parties. Therefore, the college formed a special division that serves the information management system and university interconnection services. Along with the development of information technology, according to Darmawan & Fauzi (2013), information becomes an important asset because apart from being confidential, information also has risks from unauthorized access, data modification, data, human error, hardware & software damage, as well as risks from natural disasters.

The increasing need and use of ICT in supporting an organization of business activities will increase the value of the risk of information security disturbances. The increased risk of disruption in organizations that rely heavily on ICT services will greatly affect the achievement of the organization's goals. Thus, the organization must be aware of and implement an appropriate policy to protect its information assets. One of the policies that can be taken by organizations to overcome information security disturbances is to implement information of security management (Karlsson et al., 2022; Meriah & Rabai, 2019). The Government of the Republic of Indonesia through the Directorate of Information Security Team – Kemenkominfo

has also played an active role in managing information security. This was evidenced when a guide document for the implementation of information security governance was issued for public service providers.

The Government of the Republic of Indonesia realizes that the implementation of Information and Communication Technology governance has now become a need and demand every public service provider agency considering the increasingly important role of ICT for efforts to improve service quality as one of the realize of good corporate governance. In the implementation of ICT governance, the information security factor is a very important aspect to consider considering that the performance of ICT governance will be disrupted if information as one of the main objects of ICT governance experiences information security problems involving confidentiality, integrity and availability.

Based on data from Data Loss DB (2015) until October 2015 there have been 1,416 incidents related to information security in private and government organizations, 12% of these incidents occurred in the education sector (Olifer, 2015). This is a serious concern for the company. One of the standards that can be used to analyse the level of information security in organizations is the ISO 27001 standard in accordance with incidents that often occur in the education sector. One source from the international journal shows that ISO 27001 is the most widely used framework by organizations. Therefore, the measurement of the maturity level will be carried out by referring to ISO 27001 and referring to the maturity assessment criteria using SSE – CMM.

The primary objective of this study is to examine the functionality and advantages of implementing ISO 27001 within an organization. By understanding how ISO 27001 operates, organizations can enhance their security measures and mitigate potential risks effectively. Moreover, this research endeavor seeks to serve as a valuable resource for companies in selecting the most suitable security system tailored to their specific needs and requirements.

2. Literature Review

According to Darmawan & Fauzi (2013) information is the result of data processing that can provide meaning or meaning and is useful for someone. Meanwhile, according to Laudon et al. (2007), an information system is understood as a series of interrelated components. That is starting from processing to decision making in an organization. According to Weber (in Sutabri (2012)), an information system audit is a collection and evaluation step that aims to determine whether the system being implemented is able to protect assets, integrity, and help the organization effectively. Next is the ability to maximize the available resources (Singh & Pandey, 2014; Susanto et al., 2011). ISO 27001 certification can be a sign or indicator that the company already has a good information security management system. In this way, it can also indirectly increase the trust of potential consumers or third parties and related stakeholders.

Context Diagram (CD) is the top level or often known as level 0 of the DFD. On the CD, the system is described with a process, then the external entities that interact with the single process are identified. Data Flow Diagram (DFD) is a graphical representation of a system that uses four symbols to illustrate how data flows through interconnected processes. DFD development usually uses a tiered method. Starting from the Context Diagram, DFD level1, level2 and so on according to the complexity of the system being developed. Balancing in DFD is used to store input and output streams of different levels.

3. Methods

This research was conducted by searching for literature and sources of information on the internet related to the problems discussed for further analysis by researcher. The purpose of searching the literature and existing sources is to obtain and find out relevant information and understand all the information related to each other, whether they support each other or not.

The researcher gathers existing sources of information and literature, both from books, the internet, pre-existing papers, own experiences, and other materials related to this topic

a. Read and understand the sources that have been obtained
b. Identify whether the information obtained and read is relevant to the topic to be discussed in the article
c. The researcher summarizing the key points of each relevant literature
d. Write a paper

4. Results and Discussion

4.1. ISO 27001 Overview and Benefits

ISO 27001 is a standard used to ensure the security of an information system and is used as a reference to produce recommendations. ISO 27001:2013 is an Information Security System standard document that provides an overview of what an organization or company should do in an effort to implement the concept of information security. Therefore, companies that want to implement ISO 27001 must pay attention and understand the whole concept of this rule (International Standards Organization, 2013). ISO 27001:2013 has 113 controls in securing information (Disterer, 2013). A company can choose which controls are most relevant to conditions on the ground by conducting a risk and asset assessment at an early stage. However, this selection is not an easy job, because many parameters must be considered. For this reason, the selection process for information security controls based on ISO 27001 generally relies on the services of an information security consultant.

One of the advantages of ISO 27001 is that it is a flexible standard. ISO 27001 is a standard for auditing the security of an information system (Fenz et al., 2016). The point is that if you apply this standard, the company can adapt to the conditions of an organization. Recommendations for the CD/DFD model of the academic information system and the maturity level of each control under study. Data analysis was carried out with gap analysis to compare the extent to which the ISO/IEC 27001 clauses had been implemented, both in terms of policy/procedure documentation, implementation, and evaluation. Before the data was analysed using gap analysis, first the data from the interviews, observations and documentation were collected, the results of the interviews were developed into a verbal team, then grouped according to the question category of each research variable, and also the results of observations were used to make field notes and documentation. used as evidence of implementation by the organization. The final result of the data is an assessment table for measuring the level of maturity.

The next challenge that may arise is mapping the complexity of information assets related to data processing systems, monitoring and related to concerns about the security of information assets. This should be assessed with other related approaches. ISO 27001 has its own requirements to be applied in a company. This standard covers how to handle and control information according to company needs. According to BSI UK, this requirement aims to be

implemented in all organizations although they are of different type, nature and size. The clauses in ISO/IEC 27001: 2013 consist of 7 clauses, namely:

a. an Organizational Context
b. Planning
c. Leadership
d. Clause of an Operation
e. Clause of a Support
f. Clause of an Evaluation
g. Clause of an Upgrade

Whatever your business industry, it's a good idea to start implementing ISO as a standard because it has many benefits, be it for company management, or for consumers. The general benefits of ISO 27001 are as follows:

a. Protecting employee and consumer information
b. Anticipating cyber attacks
c. Manage information system security risks more effectively and more precisely.
d. Reducing the information security budget, because you only have to implement. security controls that are really needed, but with maximum results.
e. Will be more obedient in terms of work, because there is a predetermined standard.
f. Increase the credibility and branding of the company.
g. Help to attract new customers as well as retain existing clients.

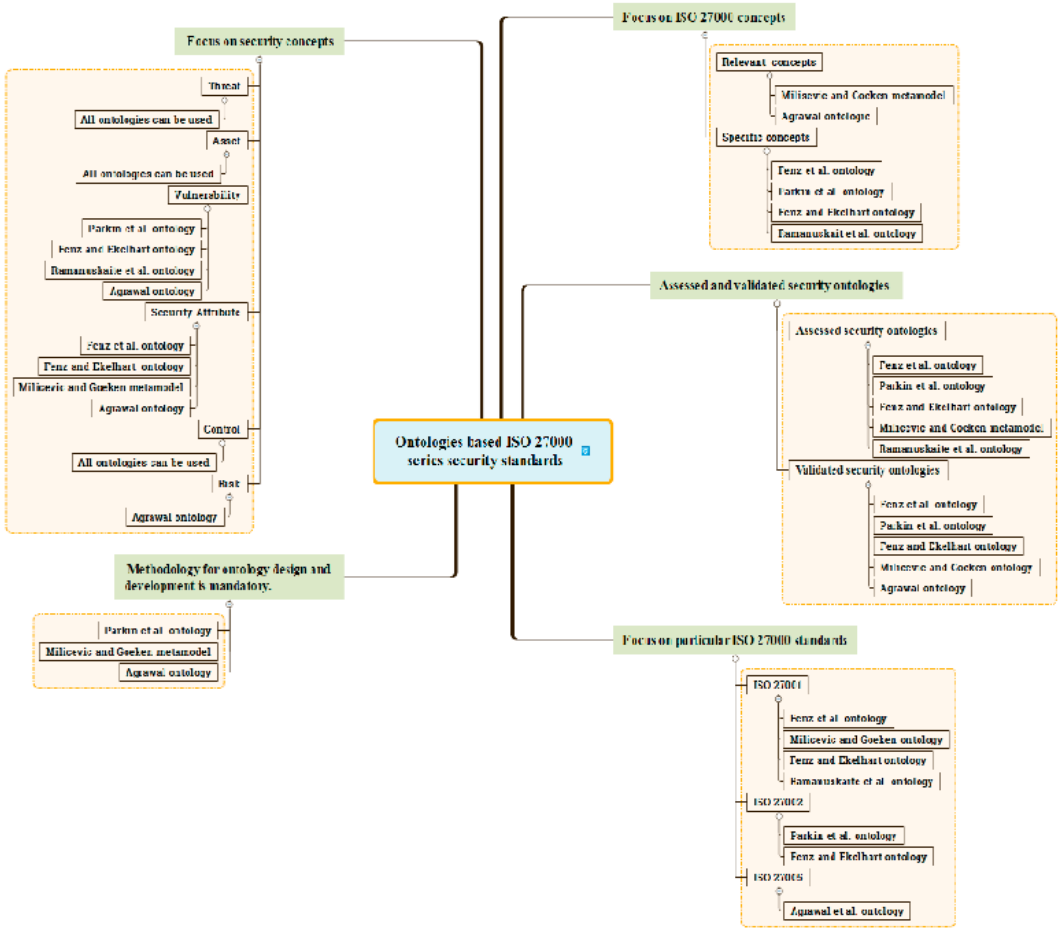

Figure 1. Summary of recommendations of ontologies based ISO 2700

a. Standard Ontology for ISO 27001: In essence, companies must understand which type of ISO standard is appropriate for their organization. If a company wishes to implement ISO 27001, it must thoroughly understand the requirements (Al-Hassan, 2014).
b. Concept: If a company needs a concept or object related to the ISO 27000 series standard, then the company needs to identify: the appropriate standard and have a clear related concept. If the company requires all the relevant concepts in a particular standard, it may be advisable to use ISO 27001.

4.2. Control in ISO 27001

The following is a list of controls from Annex A regarding ISO 27001:

1) Information Security Policy

This control checklist ensures that policies are carefully monitored and written according to directives from existing information security organizations. Companies implementing ISO 27001 must create a control list to ensure they can be monitored according to existing guidelines.

2) The Organization of Information Security

This list includes specific responsibilities and duties, divided into two main components:

a. Ensures the company has established a framework capable of maintaining and implementing information security effectively.
b. Addresses issues related to remote working and mobile devices. Employees working from home or on the go must adhere to established rules.

3) Human Resources Security

Employees must understand their rights and duties within the company. It is the company's responsibility to ensure employees are working according to their designated roles.

4) Asset Management

Asset management is a way how a company can identify information and also determine protection in accordance with existing standards. In this case it contains three main parts, namely:

a. Regarding companies that identify information assets.
b. Regarding the classification of informations which ensures that information assets are in accordance with existing standards.
c. It is about media handling that ensures that any data may not be modified, deleted, destroyed, and even disclosed if its purpose is not legitimate.

5) Access Control

The purpose of access control is to ensure that company employees manage information according to their capacity and position in a company. Within the company there are four parts, namely user access, control, access, business needs, user responsibilities, and also access control in a system and application.

6) Cryptography

It will discuss various things related to data encryption and also managing sensitive information. In addition, cryptography will also ensure that companies are able to use cryptography appropriately and effectively to protect the integrity, confidentiality, and also the availability of existing data.

7) Physical and Environmental Security

It discusses various matters related to physical security and also the environment in an organization or company.

8) Operations Security

Operations security must ensure that information processing facilities move in a safe and controlled manner.

9) Communications Security

Communication security in this case is more focused on how companies protect information in a client's network

10) System Acquisition, Development and to Maintenance

This list will ensure that information security becomes the central and most important part of the company.

11) Supplier Relationships

It contains contractual agreements owned by the company with third parties. As well as ensuring that each party can maintain a level of information security and also deliver agreed services.

12) Information Security Incident Management

This section deals with reporting as well as managing a security incident. The process in it involves explaining which employees should be in charge of certain actions, so that the form of handling will be more consistent and more effective.

13) Business Continuity Management,

This stage was formed in order to create a more effective system to be able to manage various business interruptions.

14) Compliance

In this stage, company management should be able to ensure that organizations are able to identify more appropriate laws and regulations to assist in understanding their legal and contractual requirements, minimizing the risk of non-compliance, as well as penalties. In ISO 2700, there are 10 clauses of the management system, namely scope, rules and definitions, context, normative reference, support, leadership, planning and risk management, performance evaluation, operation, as well as improvement or improvisation. Meanwhile, security that must be evaluated in information management includes information security governance, risk management related to information security, information security management framework, information asset management, and information security technology.

5. Conclusion

The conclusions of this study highlight that ISO 27001 serves as an international standard for implementing, establishing, monitoring, operating, reviewing, maintaining, and improving the information security management system (ISMS) within a company. The implementation of ISO 27001 offers numerous benefits to the company, as clients or customers will recognize the company's credibility and trustworthiness. Information security encompasses all processes within the organization, and a catalog of ISMS findings has been developed based on the international standards applied by ISO 27001:2013.

Furthermore, ISMS modeling has been carried out by identifying information security controls. The steps for implementing an information system security audit include making statements, identifying information assets, formulating questions, and determining controls based on the ISMS findings.

6. References

Al-Hassan, M. N. M. (2014). *A Semantic Ontology based Concept for Measuring Security Compliance of Cloud Service Providers*.

Darmawan, D., & Fauzi, K. N. (2013). *Management Information Systems*. Rosdakarya Youth.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2).

Fenz, S., Plieschnegger, S., & Hobel, H. (2016). Mapping information security standard ISO 27002 to an ontological structure. *Information & Computer Security*, *24*(5), 452–473.

International Standards Organization. (2013). *ISO/IEC 27001 Information Technology, Security Techniques – Information Security Management System-Requirements*.

Karlsson, F., Kolkowska, E., & Petersson, J. (2022). Information security policy compliance-eliciting requirements for a computerized software to support value-based compliance analysis. *Computers & Security*, *114*, 102578.

Laudon, K. C., Laudon, J. P., Hall, P. P., & Education, P. (2007). Management Information Systems: Managing the Digital Firm–9th Edition. *Studies in Informatics and Control*, *16*(1), 147.

Meriah, I., & Rabai, L. B. A. (2019). Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science*, *160*, 85–92.

Olifer, D. (2015). Evaluation metrics for ontology-based security standards mapping. *2015 Open Conference of Electrical, Electronic and Information Sciences (EStream)*, 1–4.

Singh, V., & Pandey, S. K. (2014). A comparative study of cloud security ontologies. *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, 1–6.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23–29.

Sutabri, T. (2012). *Analisis sistem informasi*. Penerbit Andi.