An Analysis of Physical and Environmental Security in Communication and Information Department Mojokerto

Eristya Maya Safitri*, Ramadhani Aditya, Doddy Ridwandono and Dhian Satria Yudha Kartika
Department of Information System, University of Pembangunan Nasional Veteran Jawa Timur, Indonesia

Abstract. This study aims to provide an overview to the Communication and Information Department Mojokerto regarding the maturity level of physical and environmental security management at the agency, as well as to provide future recommendations. The results of research related to physical and environmental safety using the ISO 27002 standard, indicate that the level of physical and environmental security at the Communication and Information Department Mojokerto is still relatively low. Things that are still lacking include the lack of protection from external threats such as natural disasters, as well as the lack of care and maintenance of infrastructure. The maturity level of physical and environmental security control is 0.85 which is still at level 1 or Initial Ad Hoc from a maximum value of 5, which is at the Optimized level. It can be concluded that Communication and Information Department Mojokerto only knows that there are things that need attention but there is no standardization of the process. With this research, it is hoped that the Communication and Information Department Mojokerto can make improvements to improve physical and environmental security. In addition, it is also a consideration to obtain ISMS Certification with the ISO 27002 standard in the future.

Keyword: ISO 27002, Environmental Security, Maturity level

1 Introduction

The era of globalization encourages the implementation of Information Technology – based on business operations [1]. It has inspired the reengineering of traditional business processes to transform to be more efficient, improving communication within the company, between companies, and between customers and suppliers. Increasingly massive role of IT, organizations are required to manage information technology well [2]. Good management of Information and Communication Technology will encourage the presence and realization of good governance. Methodology and good governance are prerequisites that are mandatory in managing a good system [3]. With good governance, an accountable and sustainable system can be achieved for an agency or institution and can provide the widest possible benefit to the public. Under these conditions, data and information become a very valuable asset. As stated, that the data and information produced by the organization have a very valuable value because of the many resources that have been expended to produce the data and information. Information and data have now become very valuable, it can even be said to be very vital, so that damage or leakage of information in an organization can result in the organization being stopped or closed.

Based on the results of observations and interviews conducted at the Communication and Information Department Mojokerto, especially in the field of informatics, based on information obtained from informants, the Mojokerto communication and information department was only established in 2017 and the section that handles security issues in the informatics field is still in the planning stages of formation. Therefore, it is necessary to evaluate the level of physical and environmental security at the Communication and Information Department Mojokerto for now so that it can provide recommendations based on the findings at the time of the research in order to facilitate policy making related to physical and environmental security.

There is no standard reference on the standard that should be used or chosen by the company to carry out an information system security audit. The selection of standards is determined jointly with the agency itself. The ISO 27002:2013 standard was chosen with the consideration that this standard is very flexible to be developed depending on the needs of the organization, organizational goals, security requirements, business processes, number of employees and the size of the

* Corresponding author : maya.si@upnjatim.ac.id
organizational structure [4]. In addition, another consideration is that ISO 27002 provides an internationally recognized Information Security Management System (ISMS) implementation certificate called Information Security Management System (ISMS) certification [5]. ISO/IEC 27002 was developed to provide guidance on implementing information security. ISO/IEC 27002 is widely used in solving problems related to information security [6]. ISO 27002 is able to provide guidance in planning and implementing programs to protect information assets. Physical and Environmental Security is used because according to previous research researched by the control in this clause explains the most about risk mitigation.

2 Literature Review

An information is considered very important so that in some cases an information is only wanted to be accessed by certain people. If the information is in the wrong person, it can cause huge losses for the owners of the information. So that an information system used must have security so that it can be guaranteed.

Information security itself is an effort to secure information assets from all threats that may occur to reduce the negative risks received [7]. The more information stored in an organization, the more risks that will occur such as damage, loss, or also personal information that can be spread to irresponsible parties.

Three goals will be achieved from the existence of system security, namely confidentiality, availability and integrity [8]. Two major areas are included in the scope of information security, namely the existence of physical information security and logical information security [9].

Information security threats can include people, organizations, mechanisms, or events that have the potential to harm the company's information resources, threats can be internal or external and intentional or unintentional. Some of the benefits that can be obtained by implementing ISO 27001, there are data confidentiality is better maintained and reduces the threat of data theft. This standard also covers many important aspects of business. The following are some previous research in table 2.1 below [10].

| Title | Method | Results |
|-------|--------|---------|
| Implementation of ISO/IEC 27001:2013 for Information Security Management System (SMKI) at the Faculty of Engineering, Uika-Bogor | Using the method of observation, distributing questionnaires, and data processing. The type of questionnaire used in this study using an open structured questionnaire | The results stated that the security management on the hotspot network based on ISO 27001 Clause 11 Access Control, proved to be "unsafe". |
| Evaluation of Academic Information System Security Using ISO 17799:2000 | The research methods are, 1. Tracing library sources 2. Understanding the standards used 3. Collecting primary and secondary data, 4. Assessing case studies according to standards 5. Providing recommendations for research results | Based on the assessment criteria of Peltier (2002), it can be concluded that the security of SIA PT. X is in the less secure category. |
| Information System Security Audit Based on ISO 27001 Standard At PT. East Java BPR | The methods include determining the scope, collecting data, conducting a fit and proper audit, determining the maturity level, determining the results of an information system security audit, and compiling a report on the results of an information system security audit. | Maturity level audit results overall score of 2.90 which means security controls are placed at level 2 planned and tracked |
| Research conducted at STIMIK Tunas Bangsa uses qualitative research methods with a maturity level approach. Then to obtain data about the current state of information security management | Overall, the maturity value obtained in the information security audit at STIMIK Tunas Bangsa is 2.6 which indicates that information management has been carried out but has not been defined and documented. | The audit results show that the use of ISO/IEC 27001:2013 has been implemented well because it has an average maturity level of 97.25% with a level of 5 Optimised. |

Table 2.1. Previous Research
3 Methodology

In this chapter, it will be explained how the research was carried out so that it can be seen the sequence of steps that are made systematically. The steps or stages in this research are shown in Figure 3.1 below [11].

Fig 3.1. Methodology

The first step is to conduct a literature study by studying several previous studies, then identify business processes by conducting observations, then selecting clauses, analysis methods that are useful for selecting suitable methods to use, analyzing the level of maturity of the expected conditions through interviews, analyzing maturity levels current conditions through interviews and examination of interview results for assessment, and compiling a list of findings and recommendations based on ISO 27002 [12].

4 Results and Discussion

This chapter discusses the results and discussion of thesis research on the implementation of an information security audit at the Mojokerto District Communication and Information Technology using the ISO 27002:2013 standard. The audit itself consists of a series of stages, such as analysing the maturity level of the expected condition, then analysing the maturity level of the current condition.

4.1 Expected Condition Maturity Level Analysis

Before analyzing the current maturity level, the researcher first analyzed the condition maturity level expected by the relevant agency, namely the Communication and Information Department Mojokerto, by conducting interviews with the Information Technology Manager, his name is Mr. Ulin Nuha Nashirudin, S.Kom. The following results of the expected maturity level analysis of the relevant agencies are shown in Table 4.1 below.

Table 4.1. Expected Condition Maturity Level Analysis

| Clause | Information                        | The expected conditions |
|--------|------------------------------------|-------------------------|
| 11     | Physical and Environmental Security| 3                       |

4.2 Maturity Level Analysis Current Condition

The maturity level analysis of the current condition is carried out by calculating the maturity level of physical and environmental security. This maturity assessment is obtained based on the results of survey assessments and interviews with stakeholders within the organization. This calculation is carried out by means of each statement being assessed for its maturity level in accordance with the results of interviews and existing examinations using the assessment criteria contained in the maturity level assessment standard. The level of the criteria used includes non-existent which has a value of 0 (zero) to the optimal level which has a value of 5 (five) [13]. After assessing the maturity level of each question, then doing an average so that the level of security in the security control is obtained, then doing an average of the security controls so that the value of each control objective is obtained, after that doing the average of each control objective so that the value is obtained of the maturity of the clause [14].

The result of the maturity level calculation process of physical and environmental security is 0.85, namely initial which means no management for repairs, no documentation, no IT expert who knows everything about the software or hardware being developed, and still relying on individual abilities and responsibilities [15]. These results indicate that the physical and environmental security processes in this agency are carried out inconsistently and unofficially. [16]

This can be seen by the number of undocumented procedures and many controls that have not been carried out, for example, special handling of external threats, installation of danger signs, logs of visitors coming and going not optimal, no identification for visitors, neglected equipment maintenance, not the existence of a record of borrowing equipment, and others. The following results of the maturity level analysis of the current condition are shown in Table 4.2 below.

Table 4.2. Maturity Level Analysis Current Condition

| Clause | Information                     | Index | Level |
|--------|---------------------------------|-------|-------|
| 11     | Physical and Environmental Security | 0,85  | 1     |

After analyzing and obtaining the maturity level of physical and environmental security at the Communication and Information Department Mojokerto, then compiling findings and recommendations as a result of carrying out physical...
and environmental security analysis. From the results of the analysis, recommendations and suggestions are then given that can be used to improve physical and environmental security at the relevant agencies. The following recommendations are given in accordance with ISO 27002 based on security controls in the physical and environmental security clauses are shown in table 4.3 below:

| Table 4.3. Recommendation |
|-----------------------------|
| **Security Controls** | **Analysis Result** | **Recommendation** |
| Physical security barrier/parameter | No automatic fire alert, no danger signs installed, No restrictions for access to buildings | Install automatic fire alerts and extinguishers, Gives warning signs in sensitive areas, Install security devices in the room (for example: alarms, temperature gauges, and humidity) |
| Physical Entry Control | Security control in the form of logs of visitors coming and going has not been maximized, there is no requirement to wear a clear badge, Periodic updates for access rights to safe areas are missing | Record all arrivals and departures of visitors by adding a guest book, Adding entry access controllers (eg the use of access control cards, PINs, biometrics, and alarms), Reinforcing policies regarding mandatory use of IDs for guests and employees |
| Securing offices, rooms, and facilities | There are no specific regulatory standards for the selection and design of areas, there are no standards for the placement of doors and windows | Studying several standards on area selection and design, including health and overall standards, Applying these standards as a reference for area selection and design for improvement and environmental security improvements |

5 Conclusion and Suggestion

This section contains conclusions from the overall research results and also suggestions that will be given from this research.

5.1 Conclusion

There are two conclusions from the results of this research, there are maturity level of physical and environmental security at Communication and Information Department Mojokerto is still at the first level (Initial Ad Hoc) with a value of 0.85. The next conclusion is the recommendations are given based on ISO 27002 for each security control based on the findings. However, based on the value of the gap, the resulting gap is quite large, so it requires more effort for future improvements.

5.2 Suggestion

In this study there are also suggestions, first suggestions it is hoped that Communication and Information Department Mojokerto can improve information system security management, rules, and information system security procedures so that external and internal threats related to information security can be controlled [17]. The second suggestions it is hoped that the Communication and Information Department Mojokerto carry out a security analysis of the information system again by using the entire ISO 27002 security clause and control after the Communication and Information Department Mojokerto performs physical and environmental security improvements [18]. The third suggestions researcher hopes that future researchers can conduct research using the same topic but with a different ISO 27002 clause, as well as using other methods, for example such as the KAMI Index so that perspectives can be known from the point of view of different clauses and methods [19] [20].

References

[1] O. M. e. all, “Methodology for Creating, Implementation and System Effectiveness Evaluation of the Business Processes Information Security System,” in *International Conference of Quality Management, Transport and Information Security, Information System*, Yaroslavl, Russia, (2020).
[2] e. Semi Yulianto, “Information security maturity model: A best practice driven approach to PCI DSS compliance,” in *IEEE*, Bali, Indonesia, (2016).
[3] J. A. et.all, “Integrating ISO/IEC 27001 and other Managerial Discipline Standards with Processes of Management in Organizations,” in 2012 *Seventh International Conference on Availability, Reliability and Security*, Prague, Czech Republic, (2012).
[4] e. Sevgi Ozkan, “Collaborative risk method for information security management practices: A case context within Turkey,” *International Journal of Information Management*, vol. 30, no. 6, pp. 567-572, (2010).
[5] N.V.Syreyschchikova, “Information Safety Process Development According to ISO 27001 for an Industrial Enterprise,” *Manufacturing System*, vol. 32, pp. 278-285, (2019).
[6] Y. Zhiwei, “A Survey on the Evolution of Risk Evaluation for Information Systems Security,” Energy Procedia, vol. 17, pp. 1288-1294, (2012).

[7] M. S. et.al, “Information security evaluation using KAMI index for security improvement in BMKG,” in 2017 5th International Conference on Cyber and IT Service Management (CITSM), Denpasar, Indonesia, (2017).

[8] e. Syopiansyah Jaya Putra, “Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company,” in 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, (2020).

[9] e. Muhammad Yasin, “Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ),” in 2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Bandung, Indonesia, (2020).

[10] S. Zhang, “A model for evaluating computer network security systems with 2-tuple linguistic information,” Computers and Mathematics with Application, vol. 62, no. 4, pp. 1916-1922, (2011).

[11] e. Dmitri Palko, “Model of Information Security Critical Incident Risk Assessment,” in 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, (2020).

[12] V. Monev, “Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002,” in 2020 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, (2020).

[13] I. V.Mashkina, “Issues of information security control in virtualization segment of company information system,” in 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, Russia, (2016).

[14] e. a. Milena, “Information system integrated security,” in 2008 7th Computer Information Systems and Industrial Management Applications, Ostrava, Czech Republic, (2008).

[15] e. Christopher Schmitz, “LiSRA: Lightweight Security Risk Assessment for decision support in information security,” Computers and Security, vol. 90, p. 101656, (2020).

[16] e. Mariana Gerber, “Information security requirements – Interpreting the legal aspects,” Computers and Security, vol. 27, pp. 124-135, (2008).

[17] e. Christopher Schmitz, “Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities,” Computers and Security, vol. 108, p. 102306, (2021).

[18] e. Nelli V.Syreyschchikova, “Information Safety Process Development According to ISO 27001 for an Industrial Enterprise,” Procedia Manufacturing, vol. 32, pp. 278-285, (2019).

[19] G. Pernul, “Information systems security: Scope, state-of-the-art, and evaluation of techniques,” International Journal of Information Management, vol. 15, no. 3, pp. 165-180, (1995).

[20] S. C.Patel, “Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements,” International Journal of Information Management, vol. 28, no. 6, pp. 483-491, (2008).