International Journal of Education, Information Technology And Others (IJEIT)
https://jurnal.unibrah.ac.id/index.php/IJEIT

Vol. 3, No.3, December 2020

The Use of ISO 27001 Framework for Government's Online E-Monitoring System Implementation

Pini Singgrit*[1], Geraldi Catur Pamuji[2]

[1, 2]Master of Information Systems, Indonesian Computer University, Indonesia
*Email: timkonferensi4@gmail.com

Article Info

Article History:
Received : October 21, 2020
Revised: October 28, 2020
Published: December 2020

e-ISSN: 2623-2324
p-ISSN: 2654-2528

DOI: 10.5281/zenodo.4308121

ABSTRACT

This research aims to discover the security level of online e-monitoring information system in Karawang Regency Government. We used Information Security Management System (ISMS), ISO 27001 11th paragraph access control Annex A 11.2, and Annex A 11.3 as the orientation of information security governance. It also used to actualize good government's information security system. This research method was done using Plan-Do-Check-Act (PDCA) questionnaire. The questionnaire was addressed to two kinds of respondents: users and leaders. The results of this study is that (1) users' trust the security level is 52% dan (2) leaders trust the security level is 48%. According to the results, ISMS on the online e-monitoring system in Karawang Regency Government is unsafe because it is under 64% based on ISO 27001 Standardization. In this research, we propose an ISMS framework designed to manage the secrecy aspect, integrity, and information security. This framework was developed based on ISO 27001 Standardization. By applying this ISMS framework in Karawang Regency Government, this research is expected to reduce the information security threat in data center and support organization in the future.

Keyword: E-Monitoring, Information System, Government, Audit, Information System, SIMDA, OCTAVE Allegro.

INTRODUCTION

The leaking of data center has been one of the information problems in the world with so many irresponsible people to leak and steal information or to break the proceed, sent, and saved data. Data can be used for selling and buying personal data of individuals or institutions. The leaked data have a significant impact for individuals or institutions to enrich the seller. It also have a significant impact in digital world nowadays. There are many examples that have occurred due to the minimum level of data security in the network. Almost every individual or institution has the potential to be affected by cyber attacks. Cybersecurity is also a reflection of an institution's progress in terms of technology. Ease of service is a reference for the success or failure of an institution in managing, processing, and maintaining data. Cybersecurity is one of the main factors to determe the success of data management. It is also the first shield that should not be penetrated by irresponsible parties. Many institutions are willing to allocate large amounts of funds for data security.

As a state institution, Karawang Regency Government needs to have good government information security management to give optimal service in order to support the success of data reported in the online e-monitoring system by Information Security Management System (ISMS) paragraph 11 access control in ISO 27001 Standardization. ISO 27001 Standardization is an essential Information Security Management System (ISMS) in the information security world (Shojaie, B et al, 2015). ISO 27001 Standardization for information security indicates the framework to apply and to finalize information management’s security process in an organization (Communications, N. C., et al,2017).

Previous research related to this research from several references, information is very valuable for a governmental organization, so it is common that so many irresponsible individuals or groups try to steal the data through an online e-monitoring information system, in that case, a good information system management to protect it from a structural cyber-attack. A relevant e-monitoring is essential for every control that managed by ISMS like application security monitoring (Hajdarevic, K., et al, 2016). ISO 27001 Standardization gives a specification for ISMS. Officially, ISO 27001 defines ISMS as a “management system that establishes, operates, maintains, monitors and develops information security continuously” (Hsu, C., et al, 2016). While the challenge is to ensure international trust in IT-Security level based on objective evidence and independent audit. ISMS evaluation is relevant to certification standards recognized internationally by the third party, national certification institution, under the IAF control (International Accreditation Forum) (Shojaie, B et al, 2015). Because national institution has a role in managing information data, the management must have good information security management. Nevertheless, the circumstance does not have a guide about information security adoption by the government and the usage level (I Livshitz, I. I., et al, 2016) based on ISO 27001 standardization (Susanto, A., and Shobariah, E, 2016), also introduces cycle model knowns as “Plan-Do-Check-Act” (PDCA). It is designed to establish, to apply, to monitor and to develop organizations’ effectivity. This research is developing and different from before.

This research is aimed to discover the security level of online e-monitoring information system in Karawang Regency Government by method using Information Security Management System (ISMS), ISO 27001 11th paragraph access control Annex A 11.2 and Annex A 11.3 (Yoseviano, H. F., & Retnowardhani, A, 2018) to be used as the Orientation of information security governance and to actualize good government’s information security system (Tsang, T., et al, 2010). An international standardization in applying information security management or more known as Information Security Management Systems (ISMS) in many aspects of information security is shown in Figure 1 (Almeida, R., 2018).

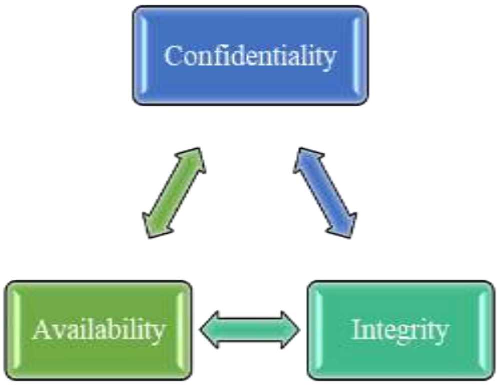

Figure 1. Information Security Aspect

RESEARCH METHOD

This research was implemented in the Karawang Regency Government. The substances of this e-monitoring system research was based on 11 access control clause that used only on Annex A 11.2 and Annex A 11.3 ISO 27001 Standard according to the need of the government, by data collecting, data allocating and data analyzing that needed to ease job in information system security management. This method was implemented by collecting observational data, spreading questionnaire and data management (Achmadi, D., et al, 2018). The taking of conclusion with Plan-Do-Check-Act (PDCA) process approach was based on ISO 27001 (Shrivastava, A. K.,. et al, 2013). The explanation for the PDCA approach method is shown in Figure 2 (Talib, M. A., et al,2012):

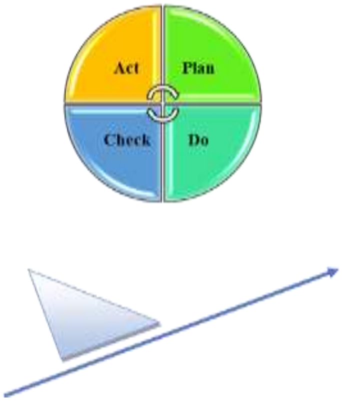

Figure 2. Plan, Do, Check, Act (P D C A)

- Plan: Planning and designing to do research analytic
- Do: The control, process, and ISMS procedure planned in “plan” step, the making of questionnaire that turned over to government employee user
- Check: The implementation of evaluation and audit on ISMS. Process from the Questionnaire is based on ISO 27001 Standard
- Act: The continuous improvement and ISMS development in Karawang Regency Government
- Constitution: Continuous improvement and development of the ISMS in the Karawang Regency Government

ISMS target control with access control clause 11 of ISO 27001 Standard is shown in Table 1.

Table 1. Annex A – 11 Akses Kontrol Klausa ISO 27001

Annex A – 11 control access clause ISO 27001		
A.	5	Information Security Policy
A.	6	Information Security Organization
A.	7	Asset management
A.	8	Human Resource Security
A.	9	Physical and Environmental Security
A.	10	Communication and Management of Operation
A.	11	Access Control
A.	12	Acquisition, Development and Improvement Information System
A.	13	Security Incident's Information Management
A.	14	Business Management
A.	15	Obedience

RESEARCH RESULTS AND DISCUSSION

This research was conducted using ISO 27001 standard framework which was a structural method of Information Security Management Systems (ISMS). It is used to determine Information Security Management by analyzing the online electronic monitoring system in the Karawang Regency Government based on access control 11 ISO 27001 Annex A 11.2 and Annex A 11.3. The results were obtained by two respondents, which are users and leaders. The questionnare was given to ten people and one leader. The results obtained was 52% and 48% of users and leaders, respectively. From that perspective, an information security system can be considered as unsafe based on ISO 27001 standards. Based on the results, it ought to do the PDCA method according to ISO 27001 standard as follows:

Plan

This step is done to analyze the needs including in analysing and processing.

Data Analyze

Data analyze with ISO 27001 standardization Annex A 11.2 and Annex A 11.3 is shown in Table 2.

Table 2. Annex A 11.2 and Annex A 11.3

No.	Criteria	Controls	Number of Questions
1	A.11.2 User Management Access	User Registration	15
		Special Privacy Management	20
		User Password	15
		User Access Rights Review	15
2	A.113 User Responbility	Password Usage	15
		Tool Usage without Supervision	10
		Table Cleaning and Clean Screen Policy	10

Analyze Process

Analyze process on the online e-monitoring system in Karawang Government based on ISO 27001 standardization 11th clause control access Annex A 11.2 and Annex A 11.3 according to the needs, explains an expected system process. This analyzing process describes the questionnaire constructive process given to the respondents. The criteria for analyzing process bases on ISO 27001 standardization is shown in Table 3.

Table 3. Analyzation Results from the Criteria of Research Process Using ISO 27001 Standardization

Percentage	Criteria
>74	Safe
64-73	Safe Enough
53-63	Less Safe
42-52	Not Safe
<42	High Risk

Do

The action discusses how to make a questionnaire that is suitable and relevant to the 11th ISO 27001 standard access control Annex A 11.2 and Annex A 11.3 according to the needs of the Karawang Government. This questionnaire is divided into two parts, namely for users and leaders. Only four answers can be selected as follows :

1. Yes
2. No
3. Not Realized
4. Other

Question examples:

1. Is there any Information Security Policy?
2. Does the user report to their leader after making changes in the current Information Security Policy?
3. Has anyone exited the authorization process for the information processing facility which includes hardware and software?
4. Is there an inventory asset associated with each information system?
5. Is the verification check on permanent staff was carried out at the start of work?
6. Are there any potential threats?
7. Are operational procedures and responsibilities documented?
8. Is the allocation and re-allocation of passwords controlled through a formal management process?
9. Is the risk assessment has complete before the system development started?
10. Is the software product licensed?

Check

Check is an explanation about evaluation on files and pieces of evidence on the questionnaire filled by government employees user or non-government employees and also a leader of Karawang Government. Security target uses ISO 27001 standardization criteria 11th clause access control with Annex A 11.2 and Annex A 11.3 as shown in Figure 3.

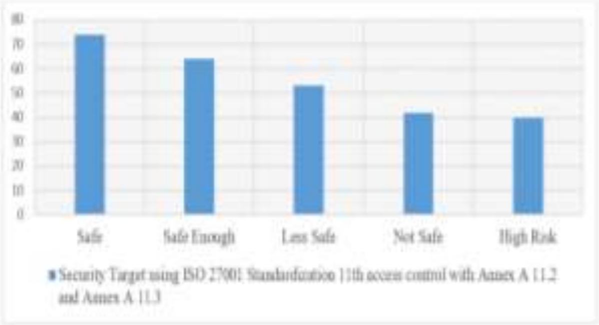

Figure 3. Security target using ISO 27001 Standardization 11th Clause Control Access with Annex A 11.2 and Annex A 11.3

Questionnaire obtained from users

Questionnaire obtained from user government employees or no government employees. This questionnaire has ten individuals' sample with fifty questions, according to 50 questions and 10 respondents, it has 500 questions in total, there are 260 points who answered "yes" and 240 points who answered "no" to make a percentage, (260/500) x 100% = 52%. Meanwhile, the percentage for the other one is 48%. In addition, the other answer has 0% percentage because the Karawang Regency Government acknowledge the IT fundamental and has good individuals' education (See Figure 4).

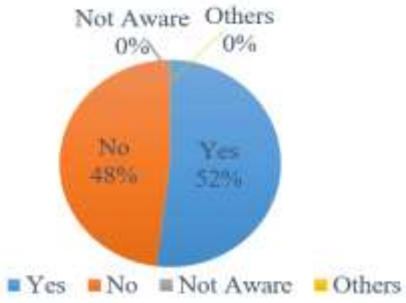

Figure 4. Results from User Questionnaire

Questionnaire for leaders

Questionnaire for leader was filled by the leader of Karawang Regency Government and contained 100 question points. According to 100 questions and 1 respondent, it has 100 questions in total, there are 48 points who answered "yes" and 42 points who answered "no" to make a percentage, (48/100) x 100% = 48%, meanwhile percentage for the other one is 42%. In addition, the other answer has 0% percentage because the Karawang Regency Government acknowledge the IT fundamental and has good individual education (See Figure 5).

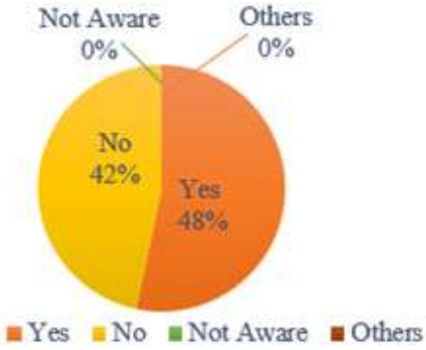

Figure 5. The results from leader Questionnaire

Act

Act is a continuous improvement and development on information security system. Karawang Government will be using ISO 27001 Standardization not only with Annex A 11.2 and Annex A 11.3 but also the whole 11th control access clause with all used annex A or new released one published by ISO 27001.

CONCLUSION

According to the research of online e-monitoring system in Karawang Regency Government, it can be concluded by the given questionnaire to 10 individuals with 500 questions, there were 52% who answered "yes". Based on ISO 27001 with the result above means categorized as "not safe". Research analyzation through questionnaire from the leader that contains 100 questions has 48% can be concluded based on ISO 27001 standardization is also categorized as "not safe". According to the two kinds of questionnaires, information security management on online e-monitoring system is under 64% that is not safe if we observe ISO 27001 11th clause access control on Annex A 11.2 and Annex 11.3. In this research, we propose an ISMS framework designed to maintain the secrecy aspect, integrity, and information security based on ISO 27001 Standardization. For continuous improvement and development on Karawang Regency Government's information security system and for further improvement, Karawang Regency Government should consider using ISO 27001 Criteria Standardization not only Annex A 11.2 and Annex A 11.3 but also with the whole 11 control clause access Annex A that is currently used or the new-will-be-released one published by ISO 27001 that developed to support the organization in the future.

BIBLIOGRAPHY

Achmadi, D., Suryanto, Y., & Ramli, K. (2018, May). On developing information security management system (isms) framework for iso 27001-based data center. In 2018 International Workshop on Big Data and Information Security (IWBIS) (pp. 149-157). IEEE., doi: 10.1109/IWBIS.2018.8471700.

Almeida, R., Lourinho, R., da Silva, M. M., & Pereira, R. (2018, July). A model for assessing COBIT 5 and ISO 27001 simultaneously. In 2018 IEEE 20th Conference on Business Informatics (CBI) (Vol. 1, pp. 60-69). IEEE., doi: 10.1109/CBI.2018.00016.

Communications, N. C., Queues, T., and Queues, O. (2017). Net Centric Communications S OFT -W IRE R OUTER, Framework, pp. 3–5.

Hajdarevic, K., Allen, P., & Spremic, M. (2016, November). Proactive security metrics for bring your own device (byod) in iso 27001 supported environments. In 2016 24th

Telecommunications Forum (TELFOR) (pp. 1-4). IEEE., doi: 10.1109/TELFOR.2016.7818717.

Hsu, C., Wang, T., & Lu, A. (2016, January). The Impact of ISO 27001 certification on firm performance. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 4842-4848). IEEE., doi: 10.1109/HICSS.2016.600.

I Livshitz, I. I., Nikiforova, K. A., Lontsikh, P. A., & Karaseva, V. A. (2016, October). The evaluation of the electronic services with accordance to IT-security requirements based on ISO/IEC 27001. In 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS) (pp. 128-131). IEEE, doi: 10.1109/ITMQIS.2016.7751921.

Shojaie, B., Federrath, H., & Saberi, I. (2015, August). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. In 2015 10th International Conference on Availability, Reliability and Security (pp. 159-167). IEEE., doi: 10.1109/ARES.2015.25.

Shrivastava, A. K., Kumar, A., Rai, A. K., Payal, N., & Tiwari, A. (2013, September). ISO 27001 Compliance via Artificial Neural Network. In 2013 5th International Conference and Computational Intelligence and Communication Networks (pp. 339-342). IEEE. doi: 10.1109/CICN.2013.77.

Susanto, A., & Shobariah, E. (2016, April). Assessment of ISMS based on standard ISO/IEC 27001: 2013 at DISKOMINFO Depok City. In 2016 4th International Conference on Cyber and IT Service Management (pp. 1-6). IEEE, doi: 10.1109/CITSM.2016.7577471

Talib, M. A., Khelifi, A., & Ugurlu, T. (2012, October). Using ISO 27001 in teaching information security. In IECON 2012-38th Annual Conference on IEEE Industrial Electronics Society (pp. 3149-3153). IEEE. doi: 10.1109/IECON.2012.6389395.

Tsang, T. M., Yeung, T. M., Chiu, D. K., Hu, H., Zhuang, Y., & Hu, H. (2010, November). Security Alert Management System for Internet Data Center Based on ISO/IEC 27001 Ontology. In 2010 IEEE 7th International Conference on E-Business Engineering (pp. 178-183). IEEE., doi: 10.1109/ICEBE.2010.78.

Yoseviano, H. F., & Retnowardhani, A. (2018, September). The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: case study in xyz, ltd. In 2018 International Conference on Information Management and Technology (ICIMTech) (pp. 21-26). IEEE., doi: 10.1109/ICIMTech.2018.8528096.