ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University

Alit Yuniargan Eskaluspita
Master of Information System, Faculty of Postgraduate, Universitas Komputer Indonesia
Bandung City, West Java 40132
Email: eskaluspita@gmail.com

Abstract. School of applied science is one of the faculty that Telkom University had. It focused on vocational education which leads to the implementation of practicum activities in daily lectures. The number of facilities and the needs to support the practicum is not small, also its value is not cheap. So to manage that data faculty use an information system that focused to organize and manage all data of laboratory and practicum needs, called SIMLAB. Information security is important so that the crucial information is not leaked to an unwilling party. It does not have the management of information security to prevent that possibility. This research was conducted by identifying the level of information security by ISO 27001:2013 in that department to be used as a framework in the implementation information security system.

1. Introduction
Telkom University is one of the private universities located in Bandung which established by Telkom Education Foundation. This university was formed based on the decision of the Education and Culture's Minister Number: 309/E/0/2013 on August 14, 2013, and Number: 270/E/O/2013 on July 17, 2013, about the basis merging of Telkom Technology Institute, Telkom Management Institute, Telkom Polytechnic, and Telkom School of Art and Design became Telkom University [1]. All diploma degrees are merged into one faculty, is School of Applied Science which has eight study programs now. Because it is prioritized for diplomas, the education model is focused on vocational, which means that practicum activities have a big influence during lectures. All of the practicum activities are held in the laboratory according to the group of scientific subjects, in total there are 41 laboratories [2, 3]. Generally, the laboratory is divided into three groups, there are computer group, engineering group, and hospitality group, which for the management of laboratory facilities and all activities are handled by the Laboratory Unit. In the operational activities of the Laboratory Unit is supported by an information system that was built specifically to assist each unit's business processes and store all data related to facilities, assets, resources, and even administration and finance. That system called SAS Laboratory Management Information System (SIMLAB) that has been used since 2016 until now and registered at Indonesian Intellectual Property Rights in 2019 with domain simlabfit.telkomuniversity.ac.id.

6 accesses are available in SIMLAB with different access according to the access level. SIMLAB mostly used in work hours from 8 a.m. until 5 p.m., during practicum activities as well as for meeting support. With the quite dense data traffic used and so on the data transfer, the gap for data and information retrieval by irresponsible parties is quite large. Other attacks targeted laboratory data continue to come by times. They will become a threat to the security of the information system. The threat itself means effect from the accident threaten 3 aspects of information security, are Confidentiality, Integrity, and Availability.
[4, 5]. Realized there are so many information threats, information system security becomes an urge to be improved. Information security is secured information from all threats that may occur in an effort to ensure the continuity of business processes, minimize risks, and maximize opportunities. [6, 7].

To find out the level of security in SIMLAB, the information security measured by ISO 27001:2013 as the information security requirements specification standard. ISO 27001:2013 is an international standard for assessing system specifications and assessing system performance in the reliability and accuracy of the system to protect information. ISO 27001 itself is an international standard published by International Organization for Standardization (ISO), described methodology of information security management in the organization, with the latest revise in 2013 so produced ISO 27001:2013 [8, 9, 10, 11].

ISO 27001 is the best-known standard in ISO 2700 family that provides requirements to the information security management system (ISMS). The latest revision of this standard is ISO 27001:2013 which released in October 2013 by ISO that describes the requirements for creating, implementing, executing, monitoring, analyzing, maintaining and documenting the ISMS standards. ISO 27001:2013 defines 14 management clauses and 114 controls (Annex A) that can be applied to ISMS [10, 11, 8].

2. Methods

In this research data collected by observation and interview with the user and unit’s managerial. Based on ISO 27001:2013, defined scopes and choose clauses that suitable for research background to measure maturity level in every aspect of the object. Clauses used are explained in table 1.

| No | Clauses (Control Annex A)                |
|----|------------------------------------------|
| 1  | A.7 : Human Resource Security            |
| 2  | A.8 : Asset Management                   |
| 3  | A.9 : Access Control                     |
| 4  | A.11 : Physical and Environmental Security |

Defined controls measured based on the value criteria of SCE-CMM, process-oriented methodology to develop secure systems. The processes define what needs to be accomplished by the security engineering process, and the maturity levels categorize how well the process accomplishes its goal [12, 13]. The maturity levels explained in table 2.

| Level     | Maturity Levels               | Descriptions                                                                 |
|-----------|-------------------------------|-------------------------------------------------------------------------------|
| 1         | Performed Informally         | Base processes are performed                                                  |
| 2         | Planned and Tracked           | Project-level definition, planning, and performance verification issues are addressed |
| 3         | Well-Defined                 | The focus is on defining and refining a standard practice and coordinating it across the organization |
| 4         | Quantitatively Controlled     | This level focuses on establishing measurable quality goals and objectively managing their performance |
| 5         | Continuously Improving        | At this level, organizational capability and process effectiveness are improved |

A list of statements made and customized based on ISO 2701:2013 according to researched clauses, the maturity level results for each objective control. The statements made and distributed to the Head of Laboratory Unit for the assessment of objective controls. The Example of value maturity level calculation can be seen in table 3, for example of result maturity level can be seen in table 4.
Table 3. Example Maturity Levels Calculation

| No | Statement | 1 | 2 | 3 | 4 | 5 | Value |
|----|-----------|---|---|---|---|---|-------|
| 1  | Asset inventory procedure and system |   |   | √ |   |   | 4     |
| 2  | Asset inventory standard includes detailed asset information |   |   | √ |   |   | 4     |
| 3  | All detailed asset information stored |   |   | √ |   |   | 3     |

Level of proficiency: 3.67

Table 4. Example Result Maturity Levels Clause 8

| Clause | Objective Control          | Security Control | Ability Level | Average / Objective Control |
|--------|----------------------------|------------------|---------------|----------------------------|
| 8.1.1. Responsibility for Assets | 8.1.1. Inventory of Assets | 3.67            |               |                            |
| 8.1.2. Ownership of Assets | 4.00 | 2.79 |
| 8.1.3. Acceptable Use of Assets | 2.00 | |
| 8.1.4. Return of Assets | 1.50 | |
| 8.2.1. Classification of Information | 2.50 | |
| 8.2. Information Classification | 1.50 | 2.00 |
| 8.2.2. Labeling of Information | 2.00 | |
| 8.2.3. Handling of Assets | 2.00 | |
| 8.3. Media Handling | 1.00 | 1.33 |
| 8.3.2. Disposal of Media | 1.00 | |
| 8.3.3. Physical Media Transfer | |

8.3. Media Handling

Maturity Level Clause 8: 2.04

Based on the obtained data and information, a compliance analysis is made. The current compliance levels with the principle of the practices code have been categorized using the following definitions: 1) Compliant, fully compliant with the specific standard of ISO 27011:2013; 2) Partially compliant, towards being compliant but still requires a lot of work to go; 3) Non-compliant, does not have the controls to satisfy the requirements of ISO 27001:2013.

3. Results and Discussion

Data were analyzed after the result of statements from Head of Laboratory Unit gathered. The first analysis done was maturity level analysis. The clause used to measure is 4 clauses, 45 security controls, and 73 customized statements based on ISO 27001:2013. By those statements, the maturity level result obtained for each objective controls according to clauses. The summary result of the maturity level can be seen in Table 5.

Table 5. Summary Result of Maturity Levels Calculation

| Clause                                      | Level |
|---------------------------------------------|-------|
| A.7 : Human Resource Security               | 2.61  | 3 |
| A.8 : Asset Management                      | 2.04  | 2 |
| A.9 : Access Control                        | 3.24  | 3 |
| A.11 : Physical and Environmental Security  | 3.16  | 3 |
| Maturity Level All Clause                   | 2.76  | 3 |

Well-Defined
Planned and Tracked
Well-Defined
Well-Defined
Separately, each clause is between level 2 to level 3 of maturity levels. It shows that within 4 clauses, the whole system is at level 3, categorized as well-defined, in the use of information security based on ISO 2700:2013. Besides maturity levels, also obtained compliance level for the selected requirements controls, and it can be seen that:

- 16% of the controls reviewed found out to be compliant with ISO 27001 standards.
- 49% of the controls reviewed found out to be partly compliant with ISO 27001 standards.
- 36% of the controls reviewed found out to be non-compliant with ISO 27001 standards

The representation of compliant level results can be seen in figure 1.

![Figure 1. Representation Compliance Level Result in All Clause](image)

After knowing the maturity level of information security for selected controls, and determining the expected maturity level, which equals 5 (optimized), as a compliance level in SIMLAB. The value gap for each clause obtained to calculate the average value of the overall gap [4]. The summary result maturity level value gap for all clauses can be seen in table 6.

| Clause | Maturity Level | Current | Expected | Gap  |
|--------|----------------|---------|----------|------|
| A.7    |                | 2.61    | 5.00     | 2.39 |
| A.8    |                | 2.04    | 5.00     | 2.96 |
| A.9    |                | 3.24    | 5.00     | 1.76 |
| A.11   |                | 3.16    | 5.00     | 1.84 |
|        | Maturity Level All Clause | 2.76 | 5.00 | 2.24 |

The representation of the maturity level gap can be seen in figure 2, which is illustrated by comparing the current maturity level with the expected maturity level. The value of the expected maturity level itself is based on the standard of ISO 27001:2013.
4. Conclusion
With ISO 27001:2013 standards, evaluate and measure the security of the information systems easier to be done supported by specific security controls. After analysis and evaluation of the security in SIMLAB, it obtained level 2 at maturity level, with just 4 clauses. Clause A.7 Human Resource Security reach level 3 of maturity level (Well-Defined), information security is done partly compliant to ISO standards. It also does not has yet some implementation documentation and complete procedures as well as policy to security in the human resource area. Clause A.8 Asset Management reaches level 2 of maturity level (Planned and Tracked), there are several controls that do not have yet implementation documentation, and procedures which not mature enough as well as evaluation. Clause A.9 Access Control reach level 3 of maturity level (Well-Defined), it has enough procedures but no implementation yet, some controls do not have a policy, but some controls have completed ISO requirements. Clause A.11 Physical and Environmental Security reach level 3 of maturity level (Well-Defined), physically mostly ISO requirements completed, though partly. But in some controls are still need support documentation and procedures. From evaluation also found out that procedures and documentation are not in the same template and format. Generally speaking, it means SIMLAB still needs to plan and completed all of ISO 27001:2013 standards.

Acknowledgement
Special thanks to Universitas Komputer Indonesia for the given opportunity, and Laboratory Unit of Telkom University Applied Science School for being willing to be the object of this research.

References
[1] T. University, "Telkom University," [Online]. Available: https://telkomuniversity.ac.id/. [Retrieved 20 January 2020].
[2] L. FIT, "SAS Laboratory," Telkom University, [Online]. Available: http://www.fit.labs.telkomuniversity.ac.id. [Retrieved 20 January 2020].
[3] S. o. A. Science, "School of Applied Science," Telkom University, [Online]. Available: https://sas.telkomuniversity.ac.id/en/. [Retrieved 15 January 2020].
[4] A. A. Nasser, "Information Security Gap Analysis Based on ISO 27001:2013 standard: A Case Study of The Yemeni Academy for Graduate Studies, Sana'a, Yemen," International Journal of Scientific Research in Multidisciplinary Studies, 03(11), pp. 4-13, 2017.
[5] C. M. Y. D. Beninda and Y. Priyadi, 2016. Analysis of Information Security Audit Using ISO 27001:2013 & ISO 27002:2013 at IT Division - X Company, In Bandung, Indonesia, International Journal of Basic and Applied Science, 04(04), pp. 77-88.
[6] F. N. Simbolon and D. Y. Hardiyanti, 2019. Security Audit on Loan Debit Network Corporation System Using Cobit 5 and ISO 27001:2013," IOP Conference Series : Journal of Physics :
Conference Series, (1196), pp. 1-9.

[7] M. Bärsan, 2019. Aspects Regarding The Implementation of Information Security Standards in Organizations, Romanian Journal of Library and Information Science, 13(1), pp. 21-26.

[8] A. E. S. Ltd, "27001 Academy : ISO 27001 and ISO 22301 Oline Consultation Center," Croatia, 2017.

[9] M. Goeken and T. Sattler, Implementation Guideline ISO/IEC 27001:2013, Berlin: ISACA Germany Chapter e.V., 2017.

[10] BSI, Information Technology - Security Techniques - ISMSs Requirements ISO/IEC 27001:2013, UK: BSI Standards Publication, 2013.

[11] ISO, "International Standard ISO/ISEC 27001 Information Technology - Security Techniques – Information Security Management Systems - Requirements," Iec, vol. 27001, no. 27001, 2013.

[12] SSE-CMM, "System Security Engineering - Capability Maturity Model," 2020. [Online]. Available: http://www.sse-cmm.org/model.htm.

[13] A. A. Nasser, A. A. Al-Khulaidi and M. N. Aljober, 2018. Measuring the Information Security Maturity of Enterprises under Uncertainty Using Fuzzy AHP, International Journal Information Technology and Computer Science, 4, pp. 10-25.