International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 02, 2020
ISSN: 1475-7192

Information System Security Analysis at PT. TELKOM Using KAMI Index

[1]SY.Yuliani , [2]Heri Heryono , [3]Ai Rosita, [4]Ulil Surtia Zulpratita, [5]Eka Angga Laksana, [6]Feri Sulianta

Abstract---*by the development of information technology, it provides convenience way for every individual or institution to perform its duties and functions. Information security used by institutions must be maintained, yet they can manage and further they can avoid failure. Therefore it is important to assess the relevant institutions to determine the level of maturity and completeness of information security. The assessment carried out was by using the Information Security Index (KAMI) issued by the Ministry of Communication and Information that has fulfilled the requirements and aspects of information security that refer to ISO 27001. Currently, PT Telekomunikasi Indonesia (TELKOM) has implemented information technology. At PT TELKOM there are well-implemented access controls including security or supervision of important work locations (server room, archive space); only employees are given a username and password to access it and also have implemented security to detect and prevent network access usage (including network wireless).*

Keywords---*Information Security, KAMI index*

I. INTRODUCTION

Information is very valuable organizational asset. Therefore, information becomes one thing that are susceptible to be exploited. The Indonesia Cyber Security Report published by ID-SIRTII found data on the total number of attacks in 2016 of 136,672,948 (increased of more than 50% from 2015). the total number of attacks was only 89,691,783 internet security attacks in Indonesia). The most common type of attack is DDOS , and attack that most many happen on in April 2016, which was 46,338,965 attacks. Whereas the go.id government domain that became Host Phising was 17.73% and id 13.64%. These various forms of attack and incident trends use the instruments of cyberspace as the main channel in carrying out their actions. One policy that can be taken by organizations to overcome information security disruptions is to implement an Information Security Management System (ISMS). Although in reality until now it has not or there will not even be a perfect Information System security so that can 100% secure information from any interference.

KAMI Index as a tool prepared by the Information Security Directorate of the Ministry of Communication and Information Technology to measure and analyze the level of preparedness or maturity of information security in an agency. The results of this measurement will produce a level of information security at PT. Indonesian Telekomunika (TELKOM), which will be evaluated and used as a reference to increase the level of information

[1]***University of Widyatama, Bandung, Indonesia***
[2]***University of Widyatama, Bandung, Indonesia***
[3]***University of Widyatama, Bandung, Indonesia***
[4]***University of Widyatama, Bandung, Indonesia***
[5]***University of Widyatama, Bandung, Indonesia***
[6]***University of Widyatama, Bandung, Indonesia***
sy.yuliani@widyatama.ac.id

DOI: 10.37200/IJPR/V24I2/PR200618
Received: 02 Jan 2020 | Revised: 15 Jan 2020 | Accepted: 28 Jan 2020

security of PT. Indonesian Telekomunika (TELKOM) in the future.

II. LITERATUR STUDY

II.I. Information Security

Information security is the maintenance of confidentiality, integrity and availability of information. One might ask, why is "information security" and not "information technology security" or IT Security. These two terms are actually interrelated, but refer to two completely different things. "Information Technology Security" or IT Security refers to business ventures to secure IT infrastructure from disturbances in the form of prohibited access and unauthorized network utilization. while "security information" focus on data and information belong to organization.

In this concept, the efforts taken are to plan, develop and supervise all activities related to the data and business information that can be used and utilized in accordance with its functions and not misused or even leaked to unauthorized parties (Sulianta, 2019). Based on this explanation, information technology security is part of whole aspect information security. Information technology is one of the important tools used to secure access and use of organizational data and information. So, information technology is not the only aspect that allows the realization of the concept of information security at organization.

II.II. KAMI Index

KAMI Index is an evaluation tool to analyze the level of readiness of information security in government agencies. This evaluation tool is not intended to analyze the feasibility or effectiveness of existing forms of safeguards, but rather as a tool to provide an overview of the conditions of readiness (completeness and maturity) of the information security framework for agency leaders.

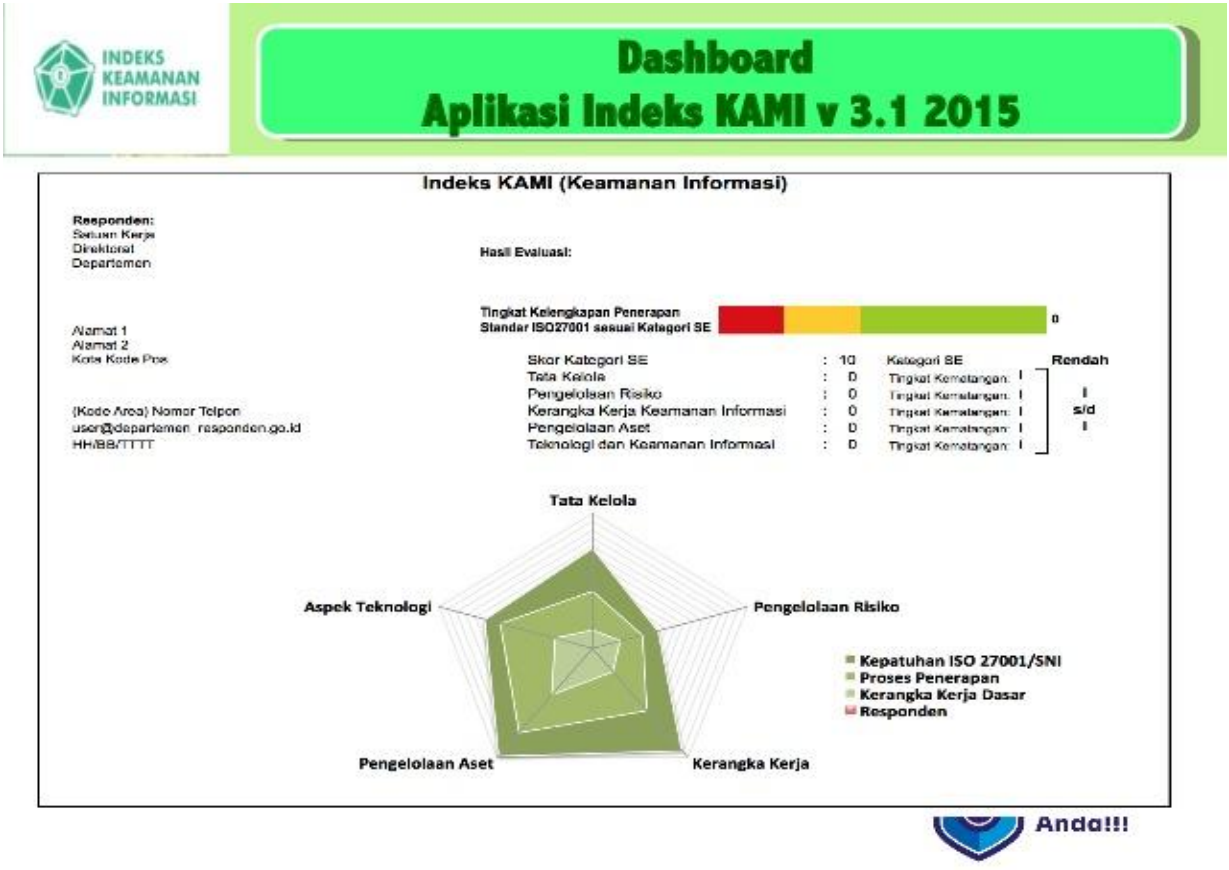

Figure 1:*KAMI Index Dashboard*

Evaluation was carried out on various targeted areas application security information with room scope of discussion that also meets all aspects of security defined by the SNI ISO / IEC 27001: 2009 standard. The

DOI: 10.37200/IJPR/V24I2/PR200618
Received: 02 Jan 2020 | Revised: 15 Jan 2020 | Accepted: 28 Jan 2020

evaluation results of KAMI index describe the level of maturity, the level of completeness of the application of SNI ISO / IEC 27001: 2009 and the map of the area of information system security governance in the agency government.

The form of evaluation applied in the KAMI Index is designed to be used by government agencies of various levels, sizes, and levels of interest in the use of ICT in supporting the implementation Task Principal and Function that there is. Data which will be used in this evaluation will provide a portrait of the readiness index of the completeness and maturity aspects of the information security framework applied and could be used as comparison in order to compile steps for improvement and priority setting.

This evaluation tool then can be used regularly to get an overview of changes in information security conditions as a result of the work program being carried out, as well as a means to convey increased readiness to the parties concerned (stakeholders).

The use and publication of the evaluation results of the KAMI Index is a form of responsibility for the use of funds the public that is also a means to raise awareness about information security needs in government agencies. Exchange of information and discussions with agencies government others as part from the use of the KAMI Index evaluation tool also creates a communication flow between information security managers in the government sector so that all parties can benefit from the lessons learned passed through.

This KAMI Index evaluation tool is generally intended to be used by government agencies at the central level. However, the work unit at the level of the Directorate General, Agency, Central or Directorate can also use this evaluation tool to get an overview of the maturity of the information security work program that it is running. This evaluation is recommended to be carried out by officials who are directly responsible and authorized to manage information security throughout the scope his institution.

Assessments in the KAMI Index are carried out with the overall scope of security requirements listed in the ISO / IEC 27001: 2009 standard, which are rearranged into 5 (five) areas below this:

1) Information Security Governance - This section evaluates the readiness of the form of information security governance along with the agencies / functions, duties and responsibilities of the security manager information.
2) Information Security Risk Management - This section evaluates the readiness of the application of information security risk management as the basis for implementing security strategies information.
3) Information Security Framework - This section evaluates completeness and readiness framework work (policies & procedures) for managing information security and strategy its application.
4) Information Asset Management - This section evaluates the complete security of information assets, including the entire asset use cycle that is.
5) Information Technology and Security - This section evaluates the completeness, consistency and effectiveness of using technology in securing information assets.

The rearrangement into 5 (five) components is carried out to obtain a form of self-evaluation that is easy to respond to where the results are the evaluation itself will be used as a guide for improvement or enhancement the performance system manage information security. In each area, the evaluation process will discuss a number of aspects needed to achieve the main objectives of security in the area that is.

The assessment process is carried out through 2 (two) methods. The first method will evaluate the extent to which the respondent agencies have implemented safeguards in accordance with the control requirements requested by the ISO / IEC 27001: 2009 standard. For the five evaluation areas, what is meant by controls is briefly explained below:

1) Information Security Governance - Control needed is a formal policy that defines roles, responsibilities, authority for managing information security, from the head of the work unit to to executor operational. Including in this area also there is a continuous work program, budget allocation, evaluation programs and strategies to improve the performance of information security governance.

Management of Information Security Risks - The form of governance needed is the existence of a management framework risk with definition that explicit related to the risk threshold, risk management programs and mitigation measures that are regularly reviewed for effectiveness.

2) Information Security Framework - Completeness of controls in this area requires a number of operational

DOI: 10.37200/IJPR/V24I2/PR200618
Received: 02 Jan 2020 | Revised: 15 Jan 2020 | Accepted: 28 Jan 2020

work policies and procedures, including implementation strategies, measuring the effectiveness of controls and corrective steps.

3) Information Asset Management - Control needed in this area is a form of security regarding existence asset information, including whole technical and administrative processes in the asset use cycle that is.

4) Information Technology and Security - For the benefit of the KAMI Index, the security aspect in the technology area requires a strategy that is related to the level of risk, and does not explicitly mention the technology or brand of the manufacturer certain.

Details of the forms of safeguards discussed in each area can be understood from the questions (independent study) provided in the area. The second method is an extension of the evaluation of completeness and is used to identify the level of maturity of security applications with categorization that refers to the level of maturity used by the COBIT framework (Objective for Information and Related Technology) or CMMI (Capability Maturity Model for Integration) framework. This level of maturity will later be used as a tool to report mapping and rating of information security readiness in Ministries / Institutions.

Mapping and ranking will be carried out by a Team determined by the Ministry of Communication and Information (KOMINFO) and will become the basis for the provision of Communication and Information OPINION regarding the condition of information security governance in Ministries / Institutions related.

KAMI Index is a tool for evaluating the implementation of information security governance that is carried out continuously, and is used to provide an overview of the progress of the application periodically. If the change happens on infrastructure or the unit work that is in the initial scope of the evaluation of the KAMI Index, a review is useful to ensure the completeness and maturity of the forms of governance that are implemented in early. For project procurement system large-scale and strategic applications, KAMI Index can also function as a checklist of governance implementation for system security that is.

III. RESEARCH METHODOLOGY

This research used pure qualitative methods with the purpose of describing the results of the research of the object under study, they are the Data and Information Center. In line with the research objectives, this method is also able to explore the object of research with a series of interview procedures with related parties.

This study used triangulation data collection techniques. The tool used in this study is to use work paper, interviews, cameras, and other documentation.

The analysis technique in this study was carried out by means of analysis for maturity, namely by comparing the current level of maturity with the intended maturity. Processing data with the level of maturity is done using a simple technique that is by interactive counting using Microsoft Excel. Assessment criteria used for processing data using the KAMI Index.

IV. RESULT

Implementation of KAMI Index at PT. TELKOM, use KAMI Index. In the measuring instrument, there are 1 4 1 (one hundred and forty one) questions which are divided into 6 parts. In Part I, informants were asked to define the Role of Electronic Systems in their respective units. Parts II to Part VI contain a number of questions regarding the level of information security maturity.

Figure 2:*Results of System Security Evaluation at PT. TELKOM*

DOI: 10.37200/IJPR/V24I2/PR200618
Received: 02 Jan 2020 | Revised: 15 Jan 2020 | Accepted: 28 Jan 2020

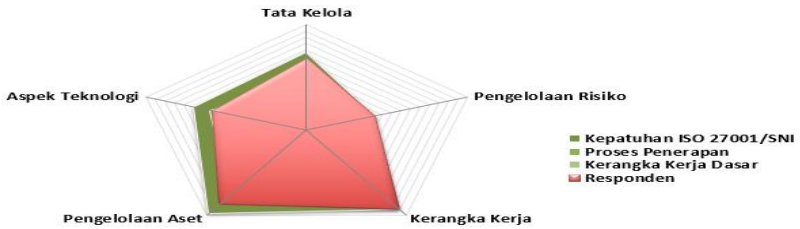

Figure 3:*Radar Evaluation Diagram of the ISMS*

Based on the information in Figure 2 it can be concluded that:

The role of Information System interests at PT. TELKOM is at a High level with a score of 30.

While the level of completeness of the application of the ISMS (Information Security Management System) is at the level of "Good" with a total score of 597, which is the sum of all the average scores in each area of Information Security evaluated.

The level of completeness of the application of the ISMS can also be seen in Figure 3 above, the pink diagram is the condition of the ISMS PT. TELKOM is based on the results of filling out questionnaires by informants. Can be observed that:

All aspects of information security exceed the standards of the Application Process applied and also in the Framework Area beyond the specified Basic Framework.

And for Compliance with ISO 27001 the aspects that have already reached these standards are Risk Management and Framework. While for Governance, Technology Aspects, and New Asset Management approaching Compliance with ISO 27001.

The level of completeness of the ISMS PT. TELKOM based on the results of the KAMI Index data collection shows in the red area on the image bar chart 2. This achievement provides an indication that the existing ISMS is quite good and there only needs to be improvement in several aspects.

Priority improvement in these aspects based on radar diagram in Figure 3 and percentage of the score of informant scores in Table 2 are Asset Management, Technology Aspects, and Governance.

The Governance Score has a value of 116 with a level of security reaching II +. Of the total 22 questions submitted in this area, 1 (4.55 %) of them were responded to "Not Done", 0 of which were responded "In Planning ", 2 (9.09 %) of which were responded to" In the Application / Partially Applied ", and the remaining 19 (86.36 %) were responded to" Completely Applied ". To increase the level of completeness of the application of the ISMS in this area, PT. TELKOM needs to make improvements including to allocate responsibility for deciding, designing, implementing and managing business continuity and disaster recovery plans.

The Risk Management Score has a value of 72 with a level of security reaching V. Of the total 16 questions asked in this area, 0 of which were responded to "Not Done", 0 of which were responded to "In Planning", 0 of which were responded to "In Implementation / Partially Applied", and the remaining 16 (100%) were responded to "Completely Applied".

The Information Security Framework Score has a value of 159 with a security level reaching V. Of the total 29 questions asked in this area, 0 of which were responded to "Not Done", 0 of which were responded to "In Planning", 0 of which were responded to "In the Implementation / Partial Application" , and the remaining 29 (100%) of them are responded to "Completely Applied".

The Information Asset Management Score has a value of 150 to achieve the security level II I. From a total of 38 questions asked in this area, 4 (10.53 %) were responded to "Not Done", 0 of which were responded "In Planning ", 0 of which were responded to" In the implementation / Partial Application ", and the remaining 34 (89.47 %) were responded to" Completely Applied ". To increase the level of completeness of the application of the ISMS in this area, PT. TELKOM needs to make improvements including:

1. It is necessary to destroy the data that is not needed and determine the data requirements that must be destroyed.
2. It is necessary to report information security incidents to external parties or authorities.
3. Make rules about the use of computing devices when used outside the work location.

The Information Technology and Security Score has a value of 1 00 with a security level reaching II +. Of the total

DOI: 10.37200/IJPR/V24I2/PR200618
Received: 02 Jan 2020 | Revised: 15 Jan 2020 | Accepted: 28 Jan 2020

2 6 questions asked in this area, 4 (15.38 %) were responded to "No Done", 0 of them responded "In Planning ", 1 (3.85 %) of which was responded to" In the implementation / Partial Application ", and the remaining 21 (80.77 %) were responded to" Completely Applied ". To increase the level of completeness of the application of the ISMS in this area, PT. TELKOM needs to make improvements including:
1. There needs to be a standard in the use of encryption and applying security to manage encryption keys
2. Applying a special form of security to protect from outside the agency.
3. Has the latest desktop and server operating system.

V.CONCLUSION

Based on research conducted at PT. TELKOM to measure the level of information security by using an index (US), this conclusion can be drawn:
1) The level of information security maturity at PT. TELKOM has been classified as GOOD and only needs to be maintained or if possible improve in several aspects and for the role / level of dependence on ICT is classified as High. All aspects have high scores, only a few aspects need only a slight increase.
2) The final score of KAMI Index at Telkom is 597 of the 645 maximum scores or 92.56 %. With this score, PT. TELKOM is classified as good and has achieved good safety standards.

V.I. Suggestion
Suggestions that can be taken from the results of information security evaluation at PT. TELKOM . using the Information Security index (US) is:

PT. TELKOM has been very good at information security awareness; it's just a matter of implementing the rules that have been determined .
PT. TELKOM must maintain the level of maturity that has been achieved from the evaluation of the KAMI index, even better if it is improved in accordance with current international standards,
A new assessment instrument needs to be made, because the KAMI Index is currently still adapting to the ISO 27001 standard in 2013. Whereas currently there is ISO 45001 in 2018.

REFERENCES

[1] Sulianta, F., Heryono, H., Zulpratita, U.S., Yuliani, S., Rosita, A., Laksana, E.A., Different Kinds of Modern Technique to Develop Various Information System, International Journal of Advanced Science and Technology,Vol. 28, No.6, (2019), pp.68-75.
[2] http://sam-berbagi.blogspot.com/2013/08/ancaman-dan-kelemahan-keamanan-sistem.html
[3] https://www.academia.edu/9760290/keamanan_sistem_informasi
[4] https://www.academia.edu/13063207/Ancaman_keamanan_sistem_informasi
[5] https://kominfo.go.id/index.php/content/detail/3326/Indeks+Keamanan+Informasi+(KAMI)/0/kemanan_informasi
[6] https://media.neliti.com/media/publications/193043-ID-evaluasi-manajemen-keamanan-informasi-me.pdf
[7] https://drive.google.com/file/d/13-fq8nT1s99mk4DvV7TZFYxh0soT75ql/view
[8] https://drive.google.com/file/d/1XRM74RMKIpxtuvTeJDYlNBlBDxwvpkD_/view
[9] https://www.nesabamedia.com/pengertian-firewall-dan-fungsi-firewall/
[10] http://ejurnal.its.ac.id/index.php/teknik/article/download/8289/2085
[11] Badawi, H., Abass, M., Hamam, O., Diab, M., El Said, M., Ismail, A., Badawy, A., Mostafa, G., Samir, S., El-Dabaa, E., Saber, M. Molecular and in-situ hybridization detection of human papillomavirus genotypes among Egyptian patients with bladder cancer(2018) International Journal of Pharmaceutical Research, 10 (4), pp. 402-405. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062655664&doi=10.31838%2fijpr%2f2018.10.04.056&partnerID=40&md5=671f4d1a022e6ddf8b334a66602038b6
[12] M. S. Neeharika, b. Jeevana jyothi (2015) chronotherapeutics: an optimizing approach to synchronize drug delivery with circadian rhythm. Journal of Critical Reviews, 2 (4), 31-40.
[13] P. K. Lakshmi, B. Kalpana, D. Prasanthi. "Invasomes-novel Vesicular Carriers for Enhanced Skin Permeation." Systematic Reviews in Pharmacy 4.1 (2013), 26-30. Print. doi:10.4103/0975-8453.135837

DOI: 10.37200/IJPR/V24I2/PR200618
Received: 02 Jan 2020 | Revised: 15 Jan 2020 | Accepted: 28 Jan 2020