International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1

Mardi Kurnianto[1], Dyah Anggraini[2]
[1, 2]Business Information System, Gunadarma University, Depok, West Java, Indonesia-16424
Email Address: [1]mardi.kurnianto@gmail.com, [2]d_anggraini@staff.gunadarma.ac.id

***Abstract*—** *Social Insurance Company is a government company that protects workers to overcome socio-economic risks due to workplace accidents, workforce deaths, dropping out of work, and reaching old age, which is implemented using a social insurance mechanism. The obligation of companies to register workers in the Social Insurance program makes the number of membership data Social Insurance Companies increase every year, but the more data and information stored, managed and shared, the greater the risk of data and information being stolen by irresponsible parties. The purpose of this study is to analyze the level of completeness and maturity to improve the quality of information security in Social Insurance Companies. This research is a type of quantitative analysis research using primary data and secondary data. Data collection was carried out by conducting library studies, focus group discussions, questionnaires, and observations. This analysis was carried out using the Information Security Index (KAMI Index) tools, the information security evaluation tool released by the Ministry of Communication and Information for government agencies. The results of the analysis of the level of information security of Social Insurance Companies are at the level of "SUFFICIENT", that is, the Social Insurance Company has fulfilled at least Managed and Measured implementation of ISO 27001: 2013 with a maturity level II to IV+. To achieve evaluation result at a good level it is necessary to increase the level of maturity in the area of Risk Management, Information Security Framework, Technology, and Information Security.*

***Keywords*—** *Social Insurance; Security Information; ISO27001: 2013; KAMI Index.*

I. INTRODUCTION

Every citizen has the right to get social security from the state, as their constitutional rights. This is as mandated in the 1945 Constitution article 34 paragraph (2) which states that "the State operates a social security system for all people and empowers all people who are weak and unable to comply with human dignity". Therefore the government is obliged to make a policy to organize National Social Security so that the citizens' constitutional rights can be fulfilled.

Following law number 24 of 2011 concerning Social Security Institutions article 15 paragraph 1, that employers must gradually register themselves and their workers as participants to BPJS following the Social Security program that is followed. And referring to article 17 paragraph 1 states, employers other than state administrators who do not implement the provisions referred to in Article 15 paragraph (1) and paragraph (2), and anyone who does not implement the provisions referred to in Article 16 is subjected to administrative sanctions.

The obligation of companies to register workers in the Social Insurance program makes the number of membership data of the Social Insurance Company increase every year, but the more data and information stored, managed and shared, the greater the risk of data and information being stolen by irresponsible parties.

The need for disbursement of information about the Social Insurance Company as a social security institution in Indonesia becomes a necessity that must be provided by the Social Insurance Company, one of the innovations of the Social Insurance Company is the realization of e-service services. With e-Service, participants can easily access Social Insurance Company information and services through the internet, anytime, anywhere, without being limited to space and time, but the rapid development of e-Service website technology is proportional to the development of security threats faced.

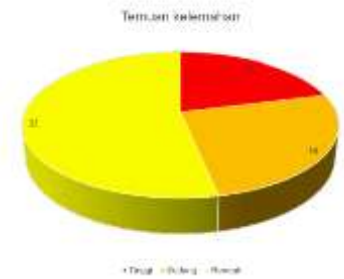

Figure 1 Diagram of Penetration Testing Findings

Data from the results of IT penetration testing (information technology) security against Social Insurance Companies at the end of 2018 stated that the discovery of some vulnerabilities in information systems and network security is quite dangerous. Among them are 13 vulnerabilities with a high level of risk, 16 vulnerabilities with a moderate level of risk, and 33 vulnerabilities with a low level of risk.

Guaranteed data security can indirectly ensure continued business continuity, optimize return on investment and open new business opportunities. But the more data and information stored, managed and shared, the greater the risk of data and information being stolen by irresponsible parties [1].

Information Security Management is one aspect of Good Corporate Governance. Given the importance of managing information security in Social Insurance Companies, it is

Mardi Kurnianto and Dyah Anggraini, "Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 340-346, 2019.

necessary to measure the conditions of the information security framework readiness. Have all data management and presentation at the Social Insurance Company integrated work processes based on ISO / IEC 27001: 2013?

By using the Information Security Index (KAMI) tool, an evaluation tool released by the Ministry of Communication and Information, the researcher wants to know the level of maturity and completeness of information security at the Social Insurance Company. The assessment is carried out in the areas of importance for electronic systems, information security governance, information security risk management, information security management frameworks, information asset management as well as technology and information security.

It is expected that the results of evaluations using the US index can provide confidence and assurance to participants or partners, that the Social Insurance Company already has a good information security management system according to ISO 27001: 2013 standards, giving maximum contribution to the business continuity of the Social Insurance Company. In the final section, GAP Analysis researchers to achieve the evaluation results at a good level, it is necessary to increase the level of maturity in the areas of Risk Management, Information Security Framework, Technology, and Information Security.

II. Literature Review

A. Research Data Sources

Data collection is done by conducting a literature study, Focus Group Discussion (FGD), surveys (questionnaires), and observations, and the research method used in this paper is quantitative because this method is following the tools used by the author, the KAMI Index. Where the use of the tool is carried out in a systematic, structured, and detailed manner because, in its implementation, the KAMI Index tool focuses on the use of figures, tables, graphs and diagrams to display the results of data or information that has been processed.

A literature study is an activity to gather the information that is relevant to the topic or problem that is the object of research. Such information can be obtained from books, scientific papers, theses, dissertations, encyclopedias, the internet, and other sources. By conducting library studies, researchers can utilize all the information and thoughts relevant to their research [1]. The literature study in this research was conducted by searching digital files and archives and hardcopy documents relating to the theory and literature about information security, concepts, and application of information security policies in Social Insurance Companies.

Researchers also used the Focus Group Discussion (FGD) method with resource persons. Researchers also used the FGD method with resource persons. FGD or focus group discussion is a data collection method commonly used in qualitative social research, not least in nursing research. This method relies on the acquisition of data or information from an interaction of informants or respondents based on the results of discussions in a group that focuses on conducting discussions in solving certain problems.

Data or information obtained through this technique, besides being group information, is also a group's opinion and decision. The advantages of using FGD methods are that they provide richer data and add value to data that was not obtained when using other data collection methods, especially in quantitative research [2]. In the FGD the questions contained in the KAMI index application are given to responders to be assessed following the existing conditions.

Observation is a process of observation and recording systematically, logically, objectively and rationally about various phenomena, both in actual situations and in artificial situations to achieve certain goals [3]. Observations in this study were made by observing the results of penetration testing (pentest) that have been carried out on e-Service services of the Social Insurance Company. Pentest activity is carried out to find out the weakness (Vulnerability) and the level of security of the Social Insurance Company information system. The results of the pentest are expected to be analyzed as evidence in the area of information technology and security.

B. Information Security

Information security is an effort to secure information assets against threats that may arise. So that information security can indirectly guarantee business continuity, reduce the risks that occur, optimize investment returns (return on investment. The more company information is stored, managed and shared, the greater the risk of damage, loss or exposure of data to unwanted external parties [4].

In designing an information system security system there are aspects of information security that need to be considered including:

- Confidentiality

Aspects that guarantee the confidentiality of information or data and ensure information can be accessed by the authorities.

- Integrity

Aspects that guarantee data cannot be changed without the permission of the authorities, safeguarding the completeness of the information and guarding against damage or other threats that can cause changes to the original information or data.

- Availability

Aspects that guarantee that data will be available when needed and ensure users can access information without interference.

C. Information Security Threats

Security in information systems is a very important factor in operating the information system itself. As for how to deal with these threats, then you can use control management methods, where this method is still effective in preventing threats to the information system. Control in the information technology system is divided into two, namely general control and application control [5].

General control (general control) which is the outermost control of the information technology system and must be faced first by the users of the information system. Some controls are organization, documentation, control devices to

Mardi Kurnianto and Dyah Anggraini, "Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 340-346, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

prevent damage to the device, and data security parameters. Application control is a control that is installed in the management of the application in the form of control on the input (access limitation), control of the process (the need for the approval of superiors) and control of output (documentation).

D. Information Security Management System

An organization must implement an Information Security Management System to ensure the security of information and communication technology assets. An Information Security Management System is a collection of policies and procedures to systematically manage sensitive organizational data. The purpose of the ISMS itself is to minimize risk and proactively ensure business continuity to limit the impact of security breaches.

The Information Security Management System must also refer to existing national or international standards so that the quality of the security provided is high and able to overcome any problems. International standards that have been recommended for the application of the ISMS are ISO or IEC 27001: 2013. It contains specifications or requirements that must be met in building an Information Security Management System (ISMS) [4].

E. ISO / IEC 27001: 2013 As a Standard for ISMS

ISO 27001: 2013 is a standard issued by the International Organization for Standardization. This International Standard establishes requirements for the establishment, implementation, maintenance, and improvement of an Information Security Management System (ISMS) in an organizational context on an ongoing basis. The applicable ISO at the time of this analysis was ISO 27001: 2013 which replaced ISO 27001: 2005 (ISMS Requirements).

This standard also includes requirements for the assessment and handling of information security risks that must be carried out by organizations to obtain compliance with this standard. The requirements of this standard are generic and are intended to be applied to all organizations regardless of type, size, and nature. The requirements set out in clauses 4 to 10 are Clause 4 Organizational Context, Clause 5 Leadership, Clause 6 Planning, Clause 7 Supporting, Clause 8 Operations, Clause 9 Performance Evaluation, Clause 10 Improvement [4].

ISO / IEC 27001: 2013 consists of 14 control areas containing core topics that discuss aspects of information security contained in Annex A controls, 34 control objectives, and 114 controls implemented in the Information Security Management System (ISMS).

F. Information Security Index (KAMI) version 3.1 as ISMS Tools

KAMI Index version 3.1 is a tool used to evaluate the level of maturity, the level of completeness of the application of ISO or IEC 27001: 2013 and an overview of information security governance in an organization. The KAMI Index is made by the Ministry of Communication and Information. This evaluation tool is not used to analyze the feasibility or effectiveness of existing forms of security, but rather as a tool to provide a picture of the readiness condition (completeness and maturity) of the information security framework to agency leaders [6].

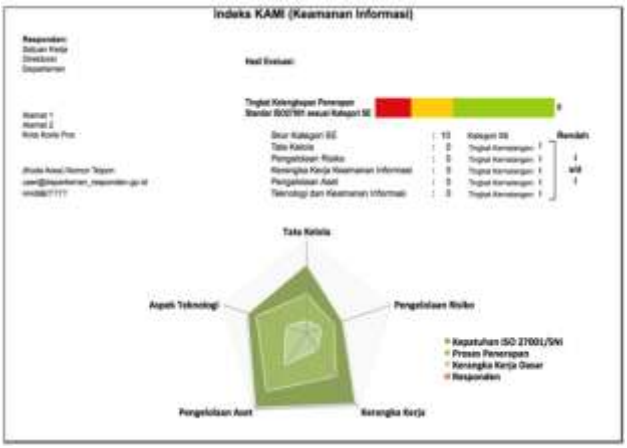

Figure 2 Dashboard Results of KAMI Index Assessment [6]

KAMI Index is an application that is used as a tool to analyze and evaluate the level of application of information security in an organization based on conformity with the criteria in SNI ISO / IEC 27001.

This evaluation tool can then be used periodically 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 relevant parties (stakeholders).

This evaluation is recommended to be carried out by officials who are directly responsible and authorized to manage information security throughout the scope of their institution. The evaluation process is carried out through several questions in each of the areas below:

- Categories of electronic systems used by agencies
- Information security governance
- Management of information security risks
- Information security framework
- Management of information assets, and
- Information technology and security

III. METHODOLOGY

In conducting research, a research methodology is needed, so that the work steps become more systematic and neat. The stages carried out by researchers in analyzing the level of completeness and maturity of information security at the Social Insurance Company.

A. Research Type

This research is a type of quantitative analysis research, where researchers will analyze the level of maturity and completeness of information security at Social Insurance Companies. Data from the analysis are inputted into tables of information security measurements contained in the KAMI index application.

B. Sources and Types of Data

Mardi Kurnianto and Dyah Anggraini, "Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 340-346, 2019.

The type of data used is quantitative data obtained from secondary data and primary data directly collected from the source. Secondary data were obtained from observations of reports on the results of penetration testing on research objects, while primary data were collected from IT Security officials or technical officers with 5 years of experience as IT security responders in Social Insurance Companies using survey methods and field observations.

C. Time and Place of Research

The time of observation and data collection lasts for one year starting from 1 August 2018 until 31 July 2019. Conducted in the IT Operational Division of the Social Insurance Company by observing the process of data management and documentation.

D. Data Collection Techniques

Data collection is done by conducting library studies, Focus Group Discussions (FGD), surveys (questionnaires), and observations.

E. Research Instruments

The research instrument used by researchers to obtain data on the level of completeness and level of maturity of information security in Social Insurance Companies is the questionnaire question of the KAMI index version 3.1 consisting of:

- Electronic system category questionnaire
- Questionnaire 5 Area for Information Security

F. Assessment Process

The assessment process on the KAMI index is done through 2 (two) methods [7] namely:

- Assessment of the number (completeness) of security.
- Assessment of the maturity level of the information security management process.

G. Data Analysis

Data analysis is the process of systematically searching and compiling data obtained from interviews, field notes and other materials so that they can be easily understood, and their findings can be shared with others [8]. Data analysis is carried out after all the required and researched data has been obtained in full. The data analysis method refers to the use of the KAMI index. The results of the summing of scores for each area are presented in two instruments, namely: the level of completeness of the form of security and the level of information security maturity.

H. Evaluation / Assessment Flow

The flow of evaluation/assessment of the level of completeness and level of maturity of information security in Social Insurance Companies is illustrated in Figure 3 below, in the figure explained that the KAMI index is a set of evaluation tools used in the use of information security governance that is carried out sustainably with the aim of providing illustrations of the results of the application. Infrastructure changes occurred in the initial conditions of the KAMI index evaluation, so the review was conducted to provide certainty on the maturity of the evaluation results.

Figure 3 Illustration of KAMI Index Evaluation [9]

- *Defining Scope*

In this study, researchers focused on the problem on the level of completeness and the level of information security maturity of the Social Insurance Company. This measurement is carried out using the KAMI index to analyze and evaluate the level of readiness or completeness and application of information security in Social Insurance Companies following the criteria in SNI ISO / IEC 27001, namely: governance, risk management, frameworks, asset management, technological aspects.

- *Determine the role of electronic interests*

The first stage carried out in the assessment of the KAMI index is that respondents were asked to define the role of the electronic system in the company or agency, respondents were also asked to describe the existing information technology infrastructure in their work units briefly.

The purpose of this Electronic Systems category assessment is to group agencies into specific sizes, namely the low electronic system category with a minimum value of 10 (basic category) to a value of 15, is another electronic system that is not included in the high category or strategic category. While the high-value electronic system category ranges from 16 to 34, is an electronic system that has a limited impact on the interests of certain sectors and / or regions, and the last Strategic achievement of 35 to 50, is an electronic system that has a serious impact on the public interest, services public, the smooth running of the state, or national defense and security.

- *Assessing Completeness of 5 Safety Areas*

Measuring the level of completeness and maturity in the area of information security governance. Governance as a formulation of the implementation of controls which has the scope of which is in the form of general control of the organization, information security in business continuity and compliance management activities. Within this area have been defined readiness of governance forms in the aspect of information security along with the agencies or functions, duties, and responsibilities of information security managers.

Mardi Kurnianto and Dyah Anggraini, "Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 340-346, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Furthermore, measuring the level of completeness and maturity in the area of Information Security Risk Management. The application of controls in this area is the target of organizational control, information asset management, information security in managing business continuity and compliance. The purpose of the strategy in the area of information security risk management is to ensure that all risks are identified and there are planned and measurable mitigations to keep these risks at a predetermined level.

Then take measurements of the level of security and level of maturity in the area of the information security framework. Implementation of controls carried out in this area is the target of organizational control, the security of actors (HR), management of communications and operational standards, management of threats or information security disturbances. Completeness of control in this area is the operational work procedures policy, the competition between human resources including the implementation strategy and measurement of the effectiveness of controls to carry out improvement targets. This area evaluates the completeness and readiness of work (policies and procedures) for managing information security and its implementation strategies.

After those take measurements of the level of security and level of maturity in the area of information asset management. The formulation of the use of controls in managing information assets namely control targets, human resource security, physical and environmental security, access control, and information security in the procurement, development, and maintenance of information systems.

Last is to measure the level of security and the level of maturity in the area of information technology and security. The formulation of the application of controls in this area is the target of controlling access to information security in the procurement, development, and maintenance of information systems, managing information security threats and managing business continuity and compliance. Aspects of this area require the need for strategies related to the level of risk. This area is to identify the completeness, consistency, and effectiveness of the use of technology in the concept of securing information assets.

- *Review KAMI Index Results and Determine Steps for Priority Setting*

Measuring activities on the level of security and level of maturity in the area of information security is carried out as a reference in compiling corrective steps and setting priorities, as well as to provide convenience in evaluation where the results of the evaluation itself can be used as a reference to improve and improve information security performance. Realizing the achievement of the main objective of security in each area requires an evaluation of every aspect.

- *Reviewing Assessment Results*

After getting the results of the assessment of the application of each section, the leadership of the agency can see the necessary improvement needs and the correlation between the various areas of information security application with the importance of the electronic system.

Based on the above thinking framework, it can be concluded that if the ISO 27001: 2013 procedure is applied as a Standard Operating Procedure (SOP) in the areas of information security governance, information security risk management, information security frameworks, information security asset management, and aspects of information security technology, the results of the assessment of the level of maturity and level of completeness through the Information Security Index in the Insurance Company are good. in other words, the application of ISO 27001: 2013 has a relevant relationship with increasing reputation and increasing the number of participants in the Indonesian Insurance Institute.

IV. Results and Discussion

A. *Recapitulation of Data Processing Results*

Data recapitalization and processing of observations and confirmation of the level of maturity and level of completeness through the KAMI Index are presented in the form of the following Table 4.1:

Table 4.1 Summary of evaluation scores in the KAMI Index area

AREA		SCORE
Level of Importance / Role of Electronic Systems	:	41
Information Security Governance	:	119
Information Security Risk Management	:	66
Information Security Framework	:	145
Management of Information Security Assets	:	159
Information Technology and Security	:	108

In accordance with table 4.1 above, that the Social Insurance Company scores 41 points for the importance or role of the electronic system category, 119 points for assessing the maturity level of information security governance, 66 points for assessing the maturity level of information security risk management, 145 points for assessment of the maturity level of the information security framework, 159 points for assessing the maturity level of information asset management, 108 points for assessing the maturity level of information technology and security.

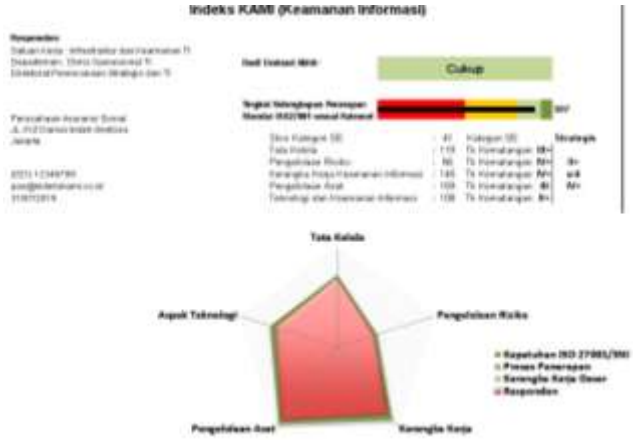

Figure 4 Dashboard of KAMI Index Evaluation Results

In figure 4 of the radar diagram above, the pink diagram is a condition of ISO 27001 Social Insurance Company Compliance based on the results of filling out the questionnaire by the respondents, it can be observed that:

Mardi Kurnianto and Dyah Anggraini, "Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 340-346, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

- From the five information security areas observed, it appears that the Social Insurance Company already has Information Assets Management and Information Security Governance that is far better than other security areas.
- Social Insurance Company has fulfilled at least Managed and Measured in the implementation of ISO 27001: 2013 with maturity level II to IV +.

B. Analysis of the Completeness of the Application of ISO 27001 Standards

Figure 5 Results of the Assessment of the Complete Level of ISO 27001 Application in Social Insurance Companies

Based on the information on the bar chart figure 5 above, it can be concluded that:

- The role or level of importance of the electronic system in Social Insurance Companies is at the STRATEGIC level with a score of 41. Ie the electronic system used has a serious impact on the public interest, public services, the smooth running of the state, or national defense and security if constrained.
- While the level of completeness of the information security level of ISO 27001 implementation, with a matrix range of 536-609, Social Insurance Companies are in the "SUFFICIENT" level in the "Light Green" area with a total score of 597, which is the sum of all scores in each information security area evaluated. The range of security features included in the category is sufficient to obtain ISO 27001 certification. From the results of the assessment, it can be concluded that Safeguards are implemented effectively under the risk management strategy. Evaluation (measurement) of safeguard achievement is carried out routinely, formally and documented. The application of technical safeguards is consistently evaluated for effectiveness. Weaknesses in security management are well identified and are consistently followed upon. Security management is pro-active and applies reforms to achieve an efficient form of management. Incidents and non-conformities are resolved through formal processes by learning the root of the problem. Employees are an inseparable part of implementing information security.
- To achieve good and optimal final evaluation results, it is necessary to increase the level of maturity at the maturity level III, IV and IV of the Risk Management area 1 form of security, Information Security Framework 2 forms of security, Technology and Information Security 4 forms of security.

C. Analysis of Maturity Level Implementation of ISO 27001

Analysis of the level of maturity The application of ISO 27001 Social Insurance Company can be from the results of bar charts, the results of a compilation of KAMI Index application research data as follows:

Figure 6 Results of Assessment of Maturity Level and Completeness of the Application of ISO 27001 Social Insurance Company

Social Insurance Companies are at level II + to IV +, i.e. Managed and Measured in the application of ISO 27001: 2013.

D. Discussion on the Level of Completeness

The level of completeness of the application of ISO 27001: 2013 in Social Insurance Companies based on the results of the questionnaire KAMI index data showed in the yellow area on the bar chart figure 5. This achievement provides a clue that the level of completeness of the application of ISO 27001: 2013 in Social Insurance Companies has been "ENOUGH" meet the criteria of ISO 27001: 2013, but to reach the optimal level requires improvements in aspects of information security governance, information security risk management, information security management, technology, and information security frameworks.

E. Discussion of Maturity Level

- *Maturity Level of Information Security Governance*

Assessors of the maturity level of the information security governance area, there are 5 questions or 23% of them responded with "in planning or partially implemented". And 17 questions or 77% of them responded with "implemented thoroughly". From a total of 22 questions raised in this area, there are 9 questions or 77% at the level of maturity III and IV of which are responded to as "implemented thoroughly".

- *Maturity Level of Information Security Risk Management*

Assessors of the maturity level of the information security risk management area, there are 1 question or 6% of them responded with "in planning" and 15 questions or 94% of them responded with "implemented as a whole".

From a total of 16 questions raised in this area, there is 1 question or 6% at the level of maturity V responding with "In a partially applied or applied".

- *Maturity Level of the Information Security Management Framework*

The framework score with a value of 146 from the maximum value of these acres according to the KAMI index of 145 or 91% of the total maximum value. Of the 29 questions, 2 questions out of a total of them, the information security management framework process at maturity level III and V responded "in planning" meaning that there were still 7% of questions at maturity level III, IV and V with the criteria "implemented thoroughly" not done.

- *Maturity Level of Information Security Asset Management*

Assessors of the maturity level of the information security asset management area, there are 10 questions or 26% of them responded with "in the application or partially applied", and 28 questions or 74% of them responded with "applied in full". Of

Mardi Kurnianto and Dyah Anggraini, "Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 340-346, 2019.

the 39 questions, 2 or 5% of the total maturity process of managing information security assets at maturity level III "in planning", 8 other questions at maturity level II are answered with "in planning" status.

- *Maturity Level of Information Technology and Security*

Assessors of the maturity level of the technology and information security area, there are 2 questions or 8% of them responded with "in planning" and 2 other questions responded with "in the application or partially applied", and 22 questions or 85% responded with "applied in full". Of the 26 questions, 1 question or 4% security level III of the total of them was responded to "in planning", and 2 questions or 8% security level III were answered with the status "in implementation or partially applied".

V. CONCLUSIONS AND SUGGESTIONS

Based on the research results of the Completeness and Maturity Level of Information Security conducted at Social Insurance Companies it can be concluded that:

1. KAMI Index application is very easy to use for evaluating IT security level, all employees can use KAMI Index in evaluating IT security level in Social Insurance Companies. KAMI Index Questionnaire is very easy to understand and digest its language compared to the language of the ISO 27001: 2013 clause. Provision of security level answers can be compared with existing documents as evidence so that the assessment is objective.
2. The level of completeness and maturity of ISO 27001: 2013 in Social Insurance Companies is sufficient to certify ISO 27001: 2013, Social Insurance Companies have implemented information security effectively following risk management strategies. Evaluation of the achievement of security objectives is carried out routinely, formally and documented. The application of technical safeguards is consistently evaluated for effectiveness. Weaknesses in security management are well identified and are consistently followed upon. Security management is pro-active and applies reforms to achieve an efficient form of management. Incidents and non-conformities are resolved through formal processes by learning the root of the problem. Employees are an inseparable part of implementing information security.
3. Dissemination of Information and Communication Technology Governance Guidelines in Social Insurance Companies is still minimal, this causes a low level of awareness of the leaders and employees of Social Insurance Companies about the importance of the Implementation of ISO 27001: 2013. This conclusion is supported by a number of indicators, including:
   - Not yet well-implemented application development procedures, including applications that go-Live productions often exclude penetration testing or application system security testing reliability.
   - Application Security Manager Web Application Firewall feature on a virtual IP application is not actively used to protect attacks.
   - The development of the application of ISO 27001: 2013 has not been prioritized by leaders or institutions, both in terms of infrastructure preparation, work procedures, budgeting, and in terms of supporting human resources.
   - Application development and supporting infrastructure are still reactive in accordance with urgent operational needs and have not been based on medium or long-term planning, so the stages and steps to develop and implement an optimal Information Security Management System are often constrained.

To answer a number of challenges that must be faced related to the application of ISO 27001: 2013 Implementation, the authors suggest a number of things as follows:

1. Carry out a number of programs to increase awareness of leaders and officials about the importance of applying ISO 27001: 2013, both in terms of rules and their application, such as socialization programs, internalization, workshops, seminars and training related to information security by involving third parties who are experts and experienced in the field IT security as the main resource person with the hope that the development of the Implementation of ISO 27001: 2013 can be part of the Social Insurance Company Strategic Plan.
2. Arranging IT Master Plan on Social Insurance Companies that allows the development of applications and infrastructure of Social Insurance Companies that can be planned, integrated and comprehensive.
3. Providing training and socialization of Application Security Manager to programmers, so that when developing new applications the programmer knows good and correct procedures for application deployment.
4. Improve and complete the Standard Operation Procedure regarding the Information Security Management System within the Social Insurance Company.

REFERENCES

[1] "Pengertian Studi Kepustakaan," 5 Agustus 2019. [Online]. Available: http://www.transiskom.com/2016/03/pengertian-studi-kepustakaan.html.
[2] Y. Afiyanti, Focus Group Discussion (Diskusi Kelompok Terfokus) Sebagai Metode Pengumpulan Data Penelitian Kualitatif, Jakarta: Rieneka Cipta, 2008.
[3] Z. Arifin, Penelitian Pendidikan, Bandung: PT Remaja Rosdakarya, 2011.
I. I. Riyanarto Sarno, Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001), Surabaya: ITS Press, 2010.
[4] R. Witaningtyas, "Beberapa Ancaman dan Cara Penanggulangan Ancaman Pada Sistem Informasi," 30 Mei 2016. [Online]. Available: https://www.kompasiana.com/retnowitaningtyas/574bf7dc907a61d906430ca4/beberapa-ancaman-dan-cara-penanggulangan-ancaman-pada-sistem-informasi. [Diakses 4 8 2019].
[5] BSSN, "Indeks Keamanan Informasi (KAMI) 3.1," 15 April 2015. [Online]. Available: https://bssn.go.id/indeks-kami/. [Accessed 31 07 2019].
[6] Kominfo, Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI), Jakarta: Kominfo, 2017.
[7] Sugiyono, Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D, Bandung: Alfabeta, 2014.
[8] N. M. K. Muhammad Rais bin Abdul Karim, E-government in Malaysia : improving responsiveness and capacity to serve, Malaysia : Subang Jaya, 2003.

Mardi Kurnianto and Dyah Anggraini, "Analysis of Complete Levels and Level of Maturity Security Information Social Insurance Companies Using Kami Index Version 3.1," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 340-346, 2019.