Journal of Theoretical and Applied Information Technology
15th March 2018. Vol.96. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI FACTORS IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM: THE INHIBITING

[1]IMAM MARZUKI SHOFI, [2]AHMAD NURUL FAJAR, [2]RULLY TATIARA

[1] Informatics Engineering Department, UIN Syarif Hidayatullah, Jakarta, Indonesia
[2,3] Information Systems Management Department,
BINUS Graduate Program-Master of Information Systems Management,
Bina Nusantara University, Jakarta Indonesia
E-mail: [1] Imam@uinjkt.ac.id, [2]afajar@binus.edu, [3]rullytatiara@yahoo.com

ABSTRACT

The purpose of this research is to propose a follow-up recommendation on the factors that inhibit the implementation of the ISMS from the previous research. Continuously. This research inspired from the critical success factor in implementation of information security management system (ISMS). Its purpose is to analysis the multi factors that are inhibiting in implementation of the ISMS. It is also to propose a follow-up recommendation on the factors that inhibit the implementation of the ISMS In the previous research data were collected from questionnaires to 182 respondents from DCO at BCA, NIT PT TELIN, and DATIN Centre at Ministry of Health Republic of Indonesia. The result from the questionnaires ie 1) implement and operate the ISMS, 2) ISMS documentation management, and 3) continual improvement. This research is focusing on conducting depth interviews to the experts who already have experience in implementing the ISMS in the organizations in Indonesia. It can be concluded that in implementing the ISMS the necessity of the role of all parties in succeeding the implementation of the ISMS continuously.

Keywords: *Multi Factors, ISMS, In Depth Interview, Users, Information Security*

1. INTRODUCTION

This research is to propose a follow-up recommendation on the factors that inhibit the implementation of the ISMS from the previous research in [1]. In this further research authors conducting depth interviews to the experts who already have experience in implementing the ISMS in the organizations in Indonesia. In the previous research in [1], data were collected from questionnaires to 182 respondents from DCO Unit at PT BCA, Tbk, NIT Division at PT TELIN, and DATIN Centre at Ministry of Health Republic of Indonesia. Data were analyzed by using Multiple Linear Regression Analysis and Paired T-test. The result is ie 1) implement and operate the ISMS, 2) ISMS documentation management, and 3) continual improvement. These three factors are inhibiting the implementation of the ISMS. Based on the results authors conducting the further research.

Organization has much valuable assets to support business processes life cycle. The most important and critical valuable assets is information [2].Thus, in order to protect information, information security is an approach to protection against the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission [3].Besides that, information security is the mechanism for preservation three aspects, such as confidentiality, integrity, and availability of information. Meanwhile, the Confidentiality can be described as the information is not available or disclosed for three components. It seems like individuals, entities, and processes are not authorized for access the information. Information Integrity indicates while the information is protected in consistency. Despite of it, availability characteristic is the information can be accessed and used as requested by the entities. They have authority over the information and it will be an important asset to the organization. In order to support decision, leader or decision makers in organization need information clearly, accurate and timely. The important decisions which has been taken from decision makers belonging to information sensitive and critical. This condition forced the organizations should be secured in order not to be accessed by unauthorized parties. The other critical factor in information security is Information leakage. It is very detrimental because

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the impact of it can reduce the competitiveness of the organization. Then, another impact is also reduce the reputation of the organization. In order to achieve the secure information in an integrated, effective and efficient manner, it requires a good management framework. Information security management framework provide guidance and standard in information security management area. The specifically for the management of information security is the ISO 27001 standard on Information Security Management Systems and called the ISMS. Although there are much organizations have been implemented ISMS based on ISO 27001, the successfully implementation is relate and depend on the various factors. It always often encounter significant obstacles such as: the inconsistency of conducting the ISMS activities in accordance with the policies or procedures established.Further more, there are recurring findings of internal audits in the ISMS at any time that would risk disturbance to the organization's information security, external audit findings, and the detention of ISO 27001 certification extension [4]. There are various research which has related with critical success factors in implementing the ISMS based on ISO 27001. It will be inspired and could be to explore the reason, factors, indicators, and the inhibiting of the ISMS implementation. It will be the rationale thinking from the authors to conducting this research. The organizations that have implemented ISMS based on ISO 27001 often encounter significant obstacles such as: the inconsistency of conducting the ISMS activities in accordance with the policies or procedures established and further more there are recurring findings of internal audits of the ISMS at any time that would risk disturbance to the organization's information security, external audit findings, and the detention of ISO 27001 certification extension.
The benefits of this research are to help the organizations to improve the ISMS implementation with provide some of recommendation and suggestion.

2. RELATED WORK

There are various types of researches which is focused on information security and information security management system in various cluster types industry at organizations. The research for measuring the level of information security awareness has been done with [4]. It is using Multiple Criteria Decision Analysis (MDCA) in government organizations [4]. It shows the level of awareness of information security is at "moderate" level. Despite of it, it will be needs to be monitored for possible correction. On the other hand, the conduct an analysis to know problems of information security implementation in the organization has been done by [5]. They are implement technical and operational requirement Combining ISO 27001: 2005 to reach the standard with maturity level [5]. The security system on academic according used is in accordance with the standards and the extent of the readiness of academic information systems in the application of information security standards by combining BS-7799 Standard with SSE-CMM to [6]. The results are the level of information security maturity on the average academic information system is still at the first level (Initial / ad hoc) in on Security Policy clause, Information Security Organization, Asset and Control Classification, Personnel / Human Resources Security, Information Security Incident Management, Aspect Business Sustainability Information Security [6]. Based [7], ISO 27001 international standards are designed to build, implement, operate, monitor, review, maintain and improve the Information Security Management System hereinafter abbreviated as ISMS. This standard adopts the Plan-Do-Check-Act (PDCA) model applied to compile the entire ISMS process. In this standard there are two parts, namely Clause and Annex A. The clause contains the entire ISMS process (starting from clauses 4 to 10) that must be executed by the organization in order to implement the ISMS. The Annex A is a list of information security controls presented by this standard for organizations that will implement the ISMS so that the organization does not miss out on implementing information security controls in its organization. The study about Business processes in dynamic environment should be managed has been done by [8]. According to [5], the critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability. This research has produced critical success factors that can be used for organizations while implementing the ISMS. Despite of [4], it believe that this methodology is useful for evaluating other business organizations with specific CSFs. The other study relate with this research which is discuss about Indonesian government system and regulations explained in [9]. This research has produced CSF that can be used for organizations in implementing the ISMS. According to[5], it believe that this methodology is useful for evaluating other business organizations with specific CSFs. Besides that, relate to [5], it also hope that this method can be applied effectively on several ISO related topics

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

such as ISO 14000, ISO 22000 and OHSAS 18000 assessment to obtain reliable and concrete analytical results for decision makers in their decision-making process

3. RESEARCH METHOD

According to [5], research variables in this study are as follows:

1. Implementation of ISMS (Y)
2. Commitment and leadership from top management (X1)
3. Effective information security policies and objectives (X2)
4. An effective process approach (X3)
5. An effective information security risk management (X4)
6. Implement and operate the ISMS (X5)
7. Assign roles, responsibilities, and authorities for the ISMS (X6)
8. Training, awareness, and competence of effective human resources (X7)
9. ISMS documentation management (X8)
10. Management of incidents, events, and weaknesses of information security (X9)
11. An effective internal audit (X10)
12. Continual improvement (X11)
13. Company wide involving (X12)
14. An effective management reviews (X13)
15. An effective motivation management (X14)
16. Knowledge management (X15)

There are 16 research variables in this study. Relate to these variables, the authors determine the hypothesis in this study. The next stage is create and distribute questionnaires. The author distributed questionnaires to the three companies that were sampled:

1. Data Center Operations (DCO) Unit Bank Central Asia (BCA), located in Jakarta with 50 employees.
2. Network & Information Technology (NIT) Division at Telekomunikasi Indonesia International (TELIN), located in Jakarta with 60 employees.
3. Data and Information (DATIN) Centre of the Ministry of Health of Republic of Indonesia located in Jakarta with 72 employees.

Stages of this research can be illustrated in the following figure:

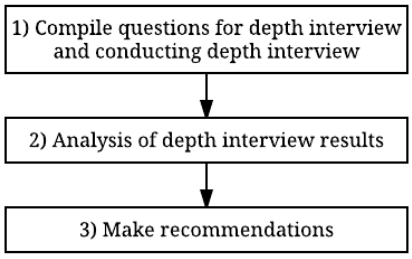

Figure 1: Stages of Research

4. RESULTS AND DISCUSSION

This research results are derived from data analysis from distribute questionnaires and also using in depth interview analysis. The first stage to measure the questionnaires validity is doing the validity test.

Validity Test

According to [7] validity is used to measure the validity or validity of a questionnaire. A questionnaire will be valid if the question in the questionnaire is able to reveal something that the questionnaire will measure. In this study there were 182 populations, using the slovin formula: n = N / 1 + NE2. Then n = 182 / (1 + 182 x 0,052) = 125,08 rounded to 126.

Based on ref [7] a significant test is done by comparing the value of r with r table value for degree of freedom (df) = N-2 where N is 126 and k is the number of variables there are 16, so (df) = 126-2 = 124 For value 124 in r table with significance 0,05 is equal to 0,1750. So after comparison with r table can be seen that the total of all score is bigger than r table, as shown by following table 1 below:

Table1 - Validity Test Result

No	Items	Score	r tabel	Result
1	Y1	0,826	0,1750	Valid
2	Y2	0,688	0,1750	Valid
3	X1-1	0,816	0,1750	Valid
4	X1-2	0,808	0,1750	Valid
5	X2-1	0,692	0,1750	Valid
6	X2-2	0,765	0,1750	Valid
7	X3-1	0,726	0,1750	Valid
8	X3-2	0,724	0,1750	Valid

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

9	X4-1	0,749	0,1750	Valid
10	X4-2	0,661	0,1750	Valid
11	X5-1	0,789	0,1750	Valid
12	X5-2	0,788	0,1750	Valid
13	X6-1	0,848	0,1750	Valid
14	X6-2	0,758	0,1750	Valid
15	X7-1	0,711	0,1750	Valid
16	X7-2	0,782	0,1750	Valid
17	X8-1	0,746	0,1750	Valid
18	X8-2	0,758	0,1750	Valid
19	X9-1	0,712	0,1750	Valid
20	X9-2	0,764	0,1750	Valid
21	X10-1	0,748	0,1750	Valid
22	X10-2	0,642	0,1750	Valid
23	X11-1	0,837	0,1750	Valid
24	X11-2	0,757	0,1750	Valid
25	X12-1	0,779	0,1750	Valid
26	X12-2	0,778	0,1750	Valid
27	X13-1	0,772	0,1750	Valid
28	X13-2	0,859	0,1750	Valid
29	X14-1	0,861	0,1750	Valid
30	X14-2	0,825	0,1750	Valid
31	X15-1	0,793	0,1750	Valid
32	X15-2	0,880	0,1750	Valid

Reliability Test

Relate with [7] this reliability test is used to see whether responses and responses from respondents will produce the same value or results if done in different times and places. According to [9] a construct or variable is said to be reliable if it gives a Cronbach Alpha value > 0.60. After the authors perform calculations using SPSS then obtained the results 0.862 so that the instrument can be said reliable.

Correlation Test and Different Test

The authors conducted a test of correlation and different test using multiple linear regression analysis method and paired t test. The author is assisted by using SPSS application version 23. After using multiple linear regression and getting the results table, the authors then do paired t test to determine whether the author's hypothesis accepted or rejected. The t test results are presented as follows:

DCO Unit at BCA

In t test at DCO Unit of BCA, the total number of samples is 50 employees. By using the formula (df) = obtained result (df) = = 50 - 16 = 34. In t table (df) = 35 with 2 side test (significance 0.025) is 2.032. The test results using SPSS show the following results:

Table2 – Hypothesis Test DCO BCA

Var	t-count	Correlation	t-tab	Result
X1	0,776	<	2,032	Accept H0
X2	1,471	<	2,032	Accept H0
X3	0,869	<	2,032	Accept H0
X4	1,750	<	2,032	Accept H0
X5	0,012	<	2,032	Accept H0
X6	0,911	<	2,032	Accept H0
X7	0,304	<	2,032	Accept H0
X8	0,677	<	2,032	Accept H0
X9	1,740	<	2,032	Accept H0
X10	0,569	<	2,032	Accept H0
X11	0,477	<	2,032	Accept H0
X12	1,579	<	2,032	Accept H0
X13	1,773	<	2,032	Accept H0
X14	0,400	<	2,032	Accept H0
X15	0,037	<	2,032	Accept H0

In the table 2 above can be concluded that all the variables X has no significant effect on the variable Y.

NIT Division at TELIN

In t test at NIT Division of TELIN the total number of samples is 60 employees. Using the formula (df) = obtained result (df) = = 60 - 16 = 44. In t table (df) = 44 with 2 side test (significance 0.025) is 2.030. The test results using SPSS show the following results in table 3 below:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table3 – Hypothesis Test NIT TELIN

Var	t-count	Correlation	t-tabel	Result
X1	1,626	<	2,015	Accept H0
X2	0,447	<	2,015	Accept H0
X3	0,257	<	2,015	Accept H0
X4	1,586	<	2,015	Accept H0
X5	0,589	<	2,015	Accept H0
X6	0,328	<	2,015	Accept H0
X7	0,193	<	2,015	Accept H0
X8	0,082	<	2,015	Accept H0
X9	0,838	<	2,015	Accept H0
X10	0,895	<	2,015	Accept H0
X11	0,511	<	2,015	Accept H0
X12	0,923	<	2,015	Accept H0
X13	0,549	<	2,015	Accept H0
X14	2,233	>	2,015	Reject H0
X15	1,027	<	2,015	Accept H0

In the table 3 above can be concluded that all variables X except X14 does not have a significant influence on the variable Y, while the variable X14 has a significant influence on the variable Y.

DATIN Center of Ministry of Health RI

In t test at DATIN Center the total number of samples is 72 employees. Using the formula (df) = obtained result (df) = = 72 - 16 = 56. In t table (df) = 56 with 2 side test (significance 0.025) is 2,003. The test results using SPSS show the following results:

Table4 – Hypothesis Test DATIN Centre

Var	t-count	Correlation	t-tabel	Result
X1	2,559	>	2,003	Reject H0
X2	0,722	<	2,003	Accept H0
X3	0,986	<	2,003	Accept H0
X4	1,486	<	2,003	Accept H0
X5	0,692	<	2,003	Accept H0
X6	0,527	<	2,003	Accept H0
X7	1,056	<	2,003	Accept H0
X8	0,270	<	2,003	Accept H0
X9	0,626	<	2,003	Accept H0
X10	0,090	<	2,003	Accept H0
X11	0,126	<	2,003	Accept H0
X12	0,426	<	2,003	Accept H0
X13	1,145	<	2,003	Accept H0
X14	1,843	<	2,003	Accept H0
X15	2,207	>	2,003	Reject H0

In the table 4 above can be concluded that all variables X except X1 and X15 do not have a significant influence on the variable Y, while the variables X1 and X15 have a significant influence on the variable Y.

The last stage to compile data analysis, we conduct the qualitative study using depth interview with the users. We choose the experts which is relate to the domain area in information security management system implementation. This research method consists of construct and compile questions for depth interview, doing in depth interview with the users, and analysis of the results. The first stage is Compile Questions for Depth Interview and Conducting Depth Interview. This stage purpose to obtain qualitative supporting data in interpreting the purpose of statistical data obtained by the author, the author conducted depth interviews two experts in the field of ISMS and ISO 27001. The experts have been experienced in assisting organizations in implementing the ISMS based on ISO 27001 from 2002. Both ISMS experts have accompanied the three organizations that have been sampled in this research in implementing the ISMS. In compiling a list of questions to do depth interview the author tries to dig up information based on personal experience of experts in assisting the implementation of ISMS in each organization and by comparing the existing statistical data. The author also made a presentation to the experts related to the results of statistical calculations that have been done by the author. Based on ref [6] Depth interview is an interview designed to find the main motivations and desires commonly used in motivational research. The interview was conducted to investigate the needs, wants and feelings of the respondents. In other words this interview is needed to know the subconscious of respondents and other matters relating to the personality and motivation of respondents. This interview is needed by the author to find out the reasons for the inhibiting factors that arise within the organization in implementing the ISMS.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

To obtain qualitative data, the authors decided to compile the question of depth interview and depth interview to experts / experts in charge of ISMS

4.1. Analysis of Depth Interview Results

Based on interviews with experts, an ISMS implementation is not easy to run in a short time. Based on expert experience, an organization can be said to experience significant improvement of ISMS implementation after passing the fifth year of running implementation. This should be supported by the consistency of the process running and balanced with the competence of human resources and updating technology that continues to increase.

4.1.1. DCO unit at BCA

- ISMS documentation management (X8)

This variable has a value of 12.8%. According to the expert analysis this is because some employees do not understand about the management of documentation in accordance with applicable policies so that the handling of ISMS documentation is not maximal.

- Commitment and leadership from top management (X1)

This variable has a value of 11.8%. According to the expert analysis this can be caused by communication related to the importance of information security in the organization from top management that is less effective or not periodically implemented so that employees feel the lack of top management role in assisting smooth implementation of the ISMS in the organization.

- An effective internal audit (X10)

This variable has a value of 10%. According to the expert analysis this can be caused by lack of communication related to the results of internal audit and audit of ISO 27001 certification to all employees. Communication of internal audit results and certification audit can help employees become more aware of the importance of implementing their duties and responsibilities for managing information security in organizations.

- Continual improvement (X11)

This variable has a value of 8.2%. According to the expert analysis this can be caused by the lack of communication related to the plan to increase the ISMS program to all employees. Communication on the plan of the ISMS improvement program can help employees become more aware of the importance of succeeding the current ISMS improvement program plan.

- An effective motivation management (X14)

This variable has a value of 7.4%. According to the expert analysis this can be caused by the management is less active in providing an example or as a role model for employees in implementing the ISMS in the organization.

- Training, awareness, and competence of effective human resources (X7)

This variable has a value of 5.1%. According to the expert analysis this can be caused by the presence of some employees who have not received training and awareness related to information security in the organization

- Knowledge management (X15)

This variable has a value of 0.6%. According to the expert analysis this can be caused by the lack of knowledge management database of ISMS implementation.

- Implement and operate the ISMS (X5)

This variable has a value of 0.2%. According to the expert analysis this can be caused by the lack of awareness of employees related to the implementation of information security risk management plan, the implementation of the ISMS program, as well as the information security control plan implemented in the organization.

4.1.2. NIT division at TELIN

- An effective management review (X13)

This variable has a value of 6.6%. According to the expert analysis this can be caused by the lack of effectiveness implementation of management review by top management, such as the lack of feedback from top management in providing improvement of the ISMS in the future.

- Information security incident, event, and security management (X9)

This variable has a value of 6.1%. According to the expert analysis this can be caused by the incomplete mechanism of incident handling, incidents, and weaknesses of information security. This is demonstrated by the lack of awareness of employees in reporting all information security incidents, events and weaknesses to the information security incident management section.

- Implement and operate the ISMS (X5)

This variable has a value of 6%. According to expert analysis this can be caused by the lack of awareness of employees related to the implementation of information security risk management plan, the implementation of the ISMS program, as well as the information security control plan implemented in the organization.

- Continual improvement (X11)

This variable has a value of 5.1%. According to the expert analysis this can be caused by the lack of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

communication related to the plan to increase the ISMS program to all employees. Communication on the plan of the ISMS improvement program can help employees become more aware of the importance of succeeding the current ISMS improvement program plan.

- Assign roles, responsibilities, and authorities for the ISMS (X6)

This variable has a value of 3.4%. According to the expert analysis this can be due to the lack of clarity regarding the allocation of tasks and responsibilities and authority related to information security in the organization, although top management has established a decree related tasks, responsibilities and authority related to information security, effective communication to all employees assist the implementation of these variables in supporting the implementation of the ISMS.

- The effective process approach (X3)

This variable has a value of 2.1%. Experts analyze this is caused by the lack of annual ISMS programs related to the implementation of the ISMS so as to make all employees are not clear and understand about what things they should consider in achieving the maximum implementation of ISMS.

- Training, awareness, and competence of effective human resources (X7)

This variable has a value of 1.7%. According to expert analysis this can be caused by the presence of some employees who have not received training and awareness related to information security in the organization.

- ISMS documentation management (X8)

This variable has a value of 0.9%. According to expert analysis this is because some employees do not understand about the management of documentation in accordance with applicable policies so that the handling of documentation ISMS is not following the proper procedure.

4.1.3. DATIN center of Ministry of Health RI

- Effective information security policies and targets (X2)

This variable has a value of 11.5%. According to the expert analysis this can be caused by a lack of communication related to information security policies and targets in the organization.

- Information security incident, event, and security management (X9)

This variable has a value of 10%. According to the expert analysis this can be caused by the incomplete mechanism of incident handling, incidents, and weaknesses of information security. This is demonstrated by the lack of awareness of employees in reporting all information security incidents, events and weaknesses to the information security incident management section.

- Implement and operate the ISMS (X5)

This variable has a value of 8.5%. According to the expert analysis this can be caused by the lack of awareness of employees related to the implementation of information security risk management plans, the implementation of the ISMS program, as well as the information security control plan implemented in the organization.

- Company wide involving (X12)

This variable has a value of 5.7%. According to the expert analysis this can be caused by the target that the information security of each sub unit of work has not been clearly defined.

- Assign roles, responsibilities, and authorities for the ISMS (X6)

This variable has a value of 5.7%. According to the expert analysis this can be caused by a lack of clarity regarding the allocation of tasks and responsibilities and authority related to information security in the organization, although top management has established a decree related tasks, responsibilities and authority related to information security, effective communication to all employees assist the implementation of these variables in supporting the implementation of the ISMS.

- ISMS documentation management (X8)

This variable has a value of 3.7%. According to expert analysis this is because some employees do not understand about the management of documentation in accordance with applicable policies so that the handling of documentation ISMS is not following the proper procedure.

- Continual improvement (X11)

This variable has a value of 1.4%. According to the expert analysis this can be caused by the lack of communication related to the plan to increase the ISMS program to all employees. Communication on the plan of the ISMS improvement program can help employees become more aware of the importance of succeeding the current ISMS improvement program plan.

- An effective internal audit (X10)

This variable has a value of 0.9%. According to expert analysis this can be caused by lack of communication related to the results of internal audit and audit of ISO 27001 certification to all employees. Communication of internal audit results and certification audit can help employees become more aware of the importance of implementing their duties and responsibilities for managing information security in organizations.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2. The Recommendation

Based on the results of statistical data analysis and qualitative data from conducting depth interviews with experts, the recommendations for each organization are as follows.

4.2.1. DCO unit at BCA

In general, DCO unit at BCA has implemented factors that support the implementation of the ISMS although it can be said that it has not been significantly implemented. Some things that must be followed up in order to support the implementation of the ISMS in the future are as follows:

1. Socialize policies and procedures for handling documentation to all employees on a regular basis.
2. Top management is more active in communicating the importance of implementing information security at any coordination meeting or meeting or special events organized by the organization, in order to build a culture of information security in the organization.
3. Communicating internal audit results and external audit results to all relevant employees so that all employees can contribute significantly to the implementation of the ISMS.
4. Communicate to all employees related to the existing improvement plan program every year so that all employees always make improvements related to the implementation of the ISMS in the organization.
5. Superiors and top management are more active in providing examples or as role models for employees in implementing the ISMS in the organization.
6. Provide training and awareness related to information security to all employees on a regular basis.
7. Using information systems in managing employee knowledge related to information security, can be internal website or internal portal.
8. Conduct periodic reviews regarding implementation of the ISMS in accordance with the ISMS annual program, information security risk management plan, information security control plan implemented in the organization.

4.2.2. NIT Division at TELIN

In general, NIT division at PT TELIN has implemented the factors that support the implementation of the ISMS although it has not been significantly implemented. Some things that must be followed up in order to support the implementation of the ISMS in the future are as follows:

1. Top management is more active in conducting management reviews by providing feedback for future ISMS improvements.
2. Socialize policies and procedures related to the management of information security incidents to all employees on a regular basis.
3. Conduct periodic reviews regarding implementation of the ISMS in accordance with the ISMS annual program, information security risk management plan, information security control plan implemented in the organization.
4. Communicate to all employees related to the existing improvement plan program every year so that all employees always make improvements related to the implementation of the ISMS in the organization.
5. Communicate related roles, responsibilities, and related authority of the ISMS to all employees on a regular basis.
6. Make a work program in the implementation of the ISMS every year and then communicate the work program on a regular basis to all personnel to be implemented optimally.
7. Provide training and awareness related to information security to all employees on a regular basis.
8. Socialize policies and procedures for handling documentation to all employees on a regular basis.

4.2.3. DATIN Centre at Ministry of Health RI

In general, DATIN Centre at Ministry of Health Republic of Indonesia has implemented the factors that support the implementation of the ISMS although it can be said has not been significantly implemented. Some things that must be followed up in order to support the implementation of the ISMS in the future are as follows:

1. Communicate the information security policies and objectives that have been assigned to all employees on a regular basis.
2. Socialize policies and procedures related to the management of information security incidents to all employees on a regular basis.
3. Conduct periodic reviews regarding implementation of the ISMS in accordance

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

with the ISMS annual program, information security risk management plan, information security control plan implemented in the organization.
4. Clearly define the information security objectives of each sub-unit in DATIN Centre.
5. Communicate related roles, responsibilities, and related authority of the ISMS to all employees on a regular basis.
6. Socialize policies and procedures for handling documentation to all employees on a regular basis.
7. Communicate to all employees related to the existing improvement plan program every year so that all employees always make improvements related to the implementation of the ISMS in the organization.
8. Communicating internal audit results and external audit results to all relevant employees so that all employees can contribute significantly to the implementation of the ISMS.

Then the authors do further analysis of the variables that have low contribution value to the implementation of the ISMS which the variable is the authors classify as factors inhibiting the implementation of the ISMS in the organization, the inhibiting factors are as follows:

DCO Unit at BCA

There are 8 inhibiting factors in DCO Unit at BCA as follows :

1. ISMS documentation management
2. Commitment and leadership from top management
3. An effective internal audit
4. Continual improvement
5. An effective motivation management
6. Training, awareness, and competence of effective human resources
7. Knowledge management
8. Implement and operate the ISMS

NIT Division at TELIN

There are 8 inhibiting factors in NIT Division at TELIN as follows :

1. An effective management review
2. Information security incident, event, and security management
3. Implement and operate the ISMS
4. Continual improvement
5. Assign roles, responsibilities, and authorities for the ISMS
6. The effective process approach
7. Training, awareness, and competence of effective human resources
8. ISMS documentation management

DATIN Center of Ministry of Health RI

There are 8 inhibiting factors in DATIN Centre at Ministry of Health as follows :

1. Effective information security policies and targets
2. Information security incident, event, and security management
3. Implement and operate the ISMS
4. Company wide involving
5. Assign roles, responsibilities, and authorities for the ISMS
6. ISMS documentation management
7. Continual improvement
8. An effective internal audit

Based on the inhibiting factors of implementation in each organization, the authors also mapping and analyzed which inhibiting factors were repeated in each organization. The result from the mapping and analyzing process shows that there are three factors as follows:

1. Implement and operate the ISMS
2. ISMS documentation management
3. Continual improvement

Seeing this the authors conclude that the implementation of the ISMS of the three organizations must still be a special attention by top management and always improved and supported by all interested parties.

This study examines the inhibiting factors of ISMS implementation based on ISO 27001 in organizations using critical success factors based on previous research from [4] and other supporting literature review. Suggestions for further studies are:

1. Increase the number of samples of organizations that become the object of research, especially organizations that have more than five years to implement the ISMS in the organization.
2. Analyzing the factors inhibiting the implementation of the ISMS by adding research variables derived from information security controls in ISO 27001 Annex A standard.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSIONS

This research is to propose a follow-up recommendation on the factors that inhibit the implementation of the ISMS from the previous research. This research was conducted to analyze the inhibiting factors of ISMS implementation based on ISO 27001 in organizations using critical success factors. The author took a sample of research on three organizations that have implemented the ISMS, the Data Center Operations Unit at Bank Central Asia, , Network & Information Technology Division at Telekomunikasi Indonesia International, Data and Information Center of the Ministry of Health Republic of Indonesia. From the analysis of the authors, each organization has different characteristics of the implementation of the ISMS, in the Data Center Operations Unit at Bank Central Asia, all independent variables have no significant effect on the implementation of ISMS. In the Network & Information Technology Division Telekomunikasi Indonesia International, there is only one independent variable that has significant effect on the implementation of ISMS, that is knowledge management. There are two independent variables that influence the implementation of the ISMS In Indonesia, such as the commitment and leadership of top management, and knowledge management.

REFRENCES:

[1] Rully, T, Fajar,A.N, Siregar.B,Wang.G. (2017), ANALYSIS OF FACTORS THAT INHIBITING IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) BASED ON ISO 27001. 2nd International Conference on Computing and Applied Informatics (ICCAI 2017)

[2] Pavlov, G., & Karakneva, J. (2011). Information Security Managemnet System In Organization. *Trakia Journal of Sciences*, *9*, 4, 20-25. ISSN: 1313-3551.

[3] Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security (Fourth Edition)*. United States of America: Cengage Learning.

[4] (2012). *International Standard ISO/IEC 27000 Second Edition 2012-12-0*. Switzerland.

[5] Hai, Hui-Lin., & Kuei-Min Wang. (2014). The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability. *African Journal of Business Management*. 8, 27, 705-716.

[6] SORA, Daniel. (2012). Securing IT Newtworks with ISMS Family of Standards (ISO 27001 Series). *Defense Resources Management In The 21st Century*.

[7] (2013). *International Standard ISO/IEC 27001 Second Edition 2013-10-01*. Switzerland.

[8] Chazar, Chalifa. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. *Jurnal Informasi*. 7, 2, 48-57.

[9] Fajar,A.N, Shofi,I.M. (2016). Development of SPL Government System with Ontology Web Language. Proceedings of 2016 4th International Conference on Cyber and IT Service Management, CITSM 2016, 7577587. Indonesia

[10] . Landau, Sabine., & Everitt, Brian S. (2004). *A Handbook of Statistical Analyses using SPSS*. London: Chapman & Hall/CRC Press LLC.