Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001

R Tatiara¹, A N Fajar¹, B Siregar² and W Gunawan¹

¹Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management, Bina Nusantara University Jakarta, Indonesia
²Department of Information technology, Universitas Sumatera Utara, Medan, Indonesia,

Email: rullytatiara@yahoo.com , afajar@binus.edu , gwang@binus.edu , baihaqi@usu.ac.id

Abstract. The purpose of this research is to determine multi factors that inhibiting the implementation of the ISMS based on ISO 2700. It is also to propose a follow-up recommendation on the factors that inhibit the implementation of the ISMS. Data collection is derived from questionnaires to 182 respondents from users in data center operation (DCO) at bca, Indonesian telecommunication international (telin), and data centre division at Indonesian Ministry of Health. We analysing data collection with multiple linear regression analysis and paired t-test. The results are multiple factors which inhibiting the implementation of the ISMS from the three organizations which has implement and operate the ISMS, ISMS document management, and continual improvement. From this research, we concluded that the processes of implementation in ISMS is the necessity of the role of all parties in succeeding the implementation of the ISMS continuously.

1. Introduction
According to [1], information is one of the most valuable assets of an organization. According to [2], information security is a protection against the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. According to [3] information security is the preservation of confidentiality, integrity, and availability of information. Confidentiality indicates that an information is not available or disclosed to individuals, entities, and processes that are not authorized for access the information. Integrity indicates that an information is protected against accuracy and completeness. Availability indicates that information can be accessed and used as requested by the entity which has having authority over the information, relate to the important asset to the organization. Decision makers in organization can make the important decisions with accurate and timely information while managing the organization. The information that has belonging to sensitive and critical organizations must also be secured. Meanwhile, the purposes is for protected accessed by unauthorized parties. Besides that, Information leakage is very detrimental because it can reduce the competitiveness of the organization and can also reduce the reputation of the organization. To secure information in an integrated, effective and efficient manner requires a good management framework. One example of a management framework created specifically for the management of information security is the ISO 27001 standard on Information Security Management Systems that called the ISMS. According to [4], there are related research that has been done, such as critical success factors in implementing the ISMS based on ISO 27001 that will be used by the author to conducting this research.
2. Related Work

There are a large number of researches that are focused on information security and information security management system in many organizations. Measuring the level of information security awareness using Multiple Criteria Decision Analysis (MDCA) in government organizations [4]. The results are showed that the level of awareness of information security is at "moderate" level, so it needs to be monitored for possible correction. Besides that, conduct an analysis to know problems of information security implementation in the organization using technical and operational requirement Combining ISO 27001: 2005 that has standard with maturity level [5]. According to [6], it is find out whether the security system on academic information system 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. 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]. Business processes in dynamic environment should be managed with [7]. According to [4], 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.

3. Results and Discussion

Stages in this research are can be described in the figure 1 below:

![Figure 1. Research stages](image)

The stages of this research consists of six step, such as: (1). develop a research hypothesis, (2). Create and distribute questionnaires, (3). analysis of inhibiting factors of ISMS implementation, (4). Compile questions for depth interview and conducting depth interview, (5). Analysis of depth interview results, and (6). make recommendations.

According to [4], the research variables in this study are described in table 1 below:
Table 1. The Research Variable

| Variable Y name | Variable X name                                      |
|-----------------|------------------------------------------------------|
| X1: Commitment  | X8: ISMS documentation management                    |
| X2: Effective   | X9: Management of incidents, events, and weaknesses   |
| X3: An effective | of information security                              |
| X4: An effective | X10: An effective internal audit                      |
| X5: Implement   | X11: Continual improvement                           |
| X6: Assign roles| X12: Companies wide involving                        |
| X7: Training,   | X13: An effective management reviews                  |
| X8: Effective   | X14: An effective motivation management               |
| X9: Management  | X15: Knowledge management                            |
| Implementation  | of information resources                             |
| of ISMS         |                                                      |

Based on these variables, the author determine the hypothesis in this study are:

1. H0: Variable X has no significant effect on Variable Y (implementation of ISMS). This means that the implementation of these factors within the organization is still not significant and a barrier to the implementation of the ISMS.

2. H1: Variable X has significant effect on Variable Y (implementation of ISMS). This means that the implementation of these factors can be quite significant.

The depiction of the relationship between variables X and Y is as follows in figure 2 below:

![Figure 2. Conceptual Framework](image)

3.1. Analysis of Inhibiting Factors of ISMS Implementation

The authors conducted a test of correlation and different test using multiple linear regression analysis method and paired t test [8]. The authors are assisted by using SPSS application version 23. The statistical chart below shows the order of contribution of variable X to variable Y (implementation of ISMS) in each organization, such as figure 3, 4, and 5 below:
3.2. Factors that inhibiting the implementation of ISMS

According to figure 3, figure 4, and figure 5, it can be seen that there is a range of values. The author decides to give the middle value of the range of values by using the median formula of odd numbers:

\[ M_e = \frac{X_{(n+1)/2}}{2} \]  

With \( M_e \) is the order, and \( n \) is the number of data. With 15 variables then the result is which the middle value of the range of values is the sequence to 8. The authors decides for values that fall on the middle value and below the middle value it will be considered as a factor inhibiting the implementation of the ISMS to the organization while the values fall over the middle value will be considered sufficiently implemented in the organization but it needs continuous improvement. The following is a table of author’s conclusions:
Table 2. Factors That Inhibit the ISMS

| Org            | Inhibiting Factors |
|----------------|-------------------|
| DCO BCA,       | X5 X15 X7 X14 X11 X10 X1 X8 |
| NIT TELIN      | X8 X7 X3 X6 X11 X5 X9 X13 |
| DATIN Centre   | X10 X11 X8 X6 X12 X5 X9 X2 |

Table 3. Factors That Need Improvement

| Org            | Need Improvement Factors |
|----------------|--------------------------|
| DCO BCA,       | X3 X6 X12 X13 X2 X4 X9 |
| NIT TELIN      | X2 X10 X12 X15 X4 X1 X14 |
| DATIN Centre   | X13 X7 X3 X4 X14 X15 X1 |

Based on the table 2 and 3 above, the multi factors that inhibiting the implementation of the ISMS from each organization are as explain in table 3 below:

Table 4. factors that inhibiting the implementation of the ISMS from each organization

| DCO unit at BCA | NIT division at TELIN | DATIN centre of Ministry of Health RI |
|-----------------|-----------------------|--------------------------------------|
| ISMS documentation management (X8), Commitment and leadership from top management (X1), An effective internal audit (X10), Continual improvement (X11), An effective motivation management (X14), Training, awareness, and competence of effective human resources (X7), Knowledge management (X15), Implement and operate the ISMS (X5) | An effective management review (X13), Information security incident, event, and security management (X9), Implement and operate the ISMS (X5), Continual improvement (X11), Assign roles, responsibilities, and authorities for the ISMS (X6), The effective process approach (X3), Training, awareness, and competence of effective human resources (X7), ISMS documentation management (X8) | Effective information security policies and targets (X2), Information security incident, event, and security management (X9), Implement and operate the ISMS (X5), Company wide involving (X12), Assign roles, responsibilities, and authorities for the ISMS (X6), ISMS documentation management (X8), Continual improvement (X11), An effective internal audit (X10) |

The authors also gave highlights on several variables to describe which variables are already quite well implemented in the three organizations as well as the X4 (An effective Information security risk management), and the variables that are the inhibiting factors in the three organizations at once are: Implement and operate the ISMS (X5), ISMS documentation management (X8), and Continual
improvement (X11). In order to obtain qualitative data supporting for interpreting and the purpose of statistical data which has obtained by the authors, the authors conducted depth interviews with two experts in the field of ISMS and ISO 27001. The experts are 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 authors trying to dig up information based on personal experience of experts in assisting the implementation of ISMS in each organization and also by comparing the existing statistical data. The authors also made a presentation to the experts related to the results of statistical calculations that have been done by the author. 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 condition 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. Conclusion

In general, the multi factors that support the implementation of the ISMS 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 improvement, (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). Communicate the information security policies and objectives that have been assigned to all employees on a regular basis.

References

[1] Pavlov G and Karakneva J 2011 Information Security Management System In Organization Trakia Journal of Sciences ISSN: 1313-3551.2011 9(4) pp 20-25
[2] Whitman M E and Mattord H J 2011 Principles of Information Security (Fourth Edition) United States of America: Cengage Learning
[3] 2012 International Standard ISO/IEC 27000 Second Edition 2012-12-0 (Switzerland)
[4] Hai, Hui-Lin and Kuei-Min W 2014 The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability African Journal of Business Management 8(27) pp 705-716
[5] SORA and Daniel 2012 Securing IT Networks with ISMS Family of Standards Defense Resources Management In The 21st Century (ISO 27001 Series)
[6] 2013 International Standard ISO/IEC 27001 Second Edition 2013-10-01 (Switzerland)
[7] Fajar A N, Budiardjo E K and Hasibuan Z A 2012 System architecture in the dynamic environment based on commonality and variability business processes ICCM
[8] Landau, Sabine, Everitt and Brian S 2004 A Handbook of Statistical Analyses using SPSS London: Chapman & Hall/CRC Press LLC