Factors Influencing the Establishment of ISO 17799 Standards

Sari Bulan Tambunan[1], Linda Lores[1] and Iskandar Muda[1]
[1]*Universitas Sumatera Utara*

Keywords: Management control, Operational Control, Technical Control, ISO Standard.

Abstract: The purpose of information security management is to protect the confidentiality, integrity and availability of information. Information security management information management system is a set of engineering and technology tools, organizational structure, security policy, responsibility, process, procedure and pact. How data and information are managed, exposed, and maintained, against the background of ISO 17799, the standard for information security management information systems. This research analyzes the factors supporting the establishment of ISO 17799 standard, which consists of control management, operational control, and technical control. The research method used primary data with questionnaires distributed to respondents consisting of employees of IT department, and the students working in information section. Analysis using smart PLS. The results of this study found that management controls support the establishment of ISO 17799 standard and influence its formation, operational control influences the establishment of ISO 17799 standard and technical control has no effect on the establishment of ISO 17799 Standard and has insignificant effect.

1 INTRODUCTION

1.1 Research Background

Concomitant with the development of information technology is very fast and proven system of information is important in economic activities and the implementation of development strategies.. The existence of information systems support the performance of increased efficiency, effectiveness and productivity of government organizations and business world, and encourage the realization of an advanced and prosperous society. In supporting the delivery of an information then utilized information technology, which uses computer technology as the main media in the delivery of information. This term itself is a development of the term Information System. The higher the quality of information technology used, the effectiveness and the better the efficiency

Current information has become a very important commodity. The ability to access and provide information quickly and accurately is very important for an organization, whether in the form of commercial organizations (companies), universities, government agencies, or individuals. This is possible with the rapid development in the field of computer technology and telecommunications. The importance of the value of information makes it often possible that information is only permitted to be accessed by certain people. Falling information into the hands of other parties (for example, business opponents) can endanger the information owner. For example, a lot of information in a company is only allowed to be known by certain people in the company, such as information about the product being developed, algorithms and techniques used to produce the product. For this reason, the security of the information system used must be guaranteed within acceptable limits.

Information is a very valuable asset and is important for the survival of a business enterprise and is presented in various formats: notes, oral, electronic, postal and audio-visual. Therefore, information management is important to improve competitive success in all sectors of the economy.

The purpose of information security management is to protect the confidentiality, integrity and availability of information. Information security management information management system is a set of engineering and technology tools, organizational structure, security policy, responsibility, process, procedure and pact. How

Tambunan, S., Lores, L. and Muda, I.
Factors Influencing the Establishment of ISO 17799 Standards.
DOI: 10.5220/0010072012901295
In *Proceedings of the International Conference of Science, Technology, Engineering, Environmental and Ramification Researches (ICOSTEERR 2018) - Research in Industry 4.0*, pages 1290-1295
ISBN: 978-989-758-449-7

data and information are managed, exposed, and maintained, against the background of ISO 17799, the standard for information security management information systbems.

Information security protects from a wide range of threats to ensure business continuity, minimize corporate loss and maximize return on investment and business opportunity. This security management allows data to be distributed electronically, so that a system is needed to ensure data is safe and well received by the user. Information security can be defined as "Adequately protecting the confidentiality, integrity and availability of information against possible threat manifestations." (Verheul, 2011).

Information security is obtained by implementing a decent set of control tools, which can be policy, practice, organizational structure and software.

ISO1779 is an internationally recognized management standard, which has a broad scope and is conceptual. This approach allows the application of ISO 17799 to various companies and applications. ISO 17799 defines information as a valuable asset and needs to be protected. ISO 17799 covers the selection and management of information security controls. In the 1990s the tech world realized the weakness of the open concept when malwere, the term for malicious software (malicious software), appeared in the form of a virus. Instantly the open concept turns into a weak point of the system that allows viruses to enter and attack.

Then came the thought to protect computers that can only be accessed by authorized only. So it can be said that the security of the system need to pay attention to three aspects of teknoology, human and process. This further emphasizes the importance of every company is always wary of the three aspects of IT system security. In order to minimize the risk of IT system security for the sustainability of its business.

1.2 Problem Formulation

a. Does management controls affect the establishment of ISO 17799?
b. Does operational controls affect the formation of ISO 17799?
c. Do technical controls affect the formation of ISO 17799?

1.3 Research Purposes

a. To know and test empirically management controls is a factor forming ISO 17799
b. To know and test empirically operational controls is an ISO form factor 17799
c. To know and test empirically technical controls is a factor forming ISO 17799

2 LITERATURE REVIEW

2.1 Information Security

Information is an asset must be protected. Security is generally defined as "quality or state of being secure-to be free from danger ". Creating safe is by protecting from enemies and threats of danger. Examples of information security by (Whitman and Mattord 2011) are as follows:

a. Physical Security that focuses on strategies for securing workers or members of organizations, physical assets, and workplaces from various threats including fire hazards, unauthorized access, and natural disasters.
b. Personal Security is overlapped with "phisycal security" in protecting people in the organization.
c. Operation Security that focuses on strategies to secure the ability of an organization or company to work without interruption.
d. Communications Security which aims to secure communication media, communication technology and content, as well as the ability to utilize this tool to achieve organizational goals.
e. Network Security that focuses on securing the organization's data network equipment, its network and its contents, as well as the ability to use the network in fulfilling the function of the organization's data communications.

information. Information security has been treated as a by-product, if not as a ''necessary evil that hinders productivity'' (Conray-Murray, 2003). gradually information security becomes a necessity , surely information security is getting intothe forefront of things, and has been promoted froma by-product to an integral part of business operations (Conner and Coviello, 2003)

According to(BSI 2008), ISMS is part of the management system overall based on a business risk approach to building, implement, operate, monitor, review, maintain and improve information security.

ISMS is a set of policies related to information security management. Concept the key of the ISMS is that the organization / organization designs, implements and maintains the related sequences of processes and systems to effectively manage information accessibility, and ensure confidentiality, integrity and availability of information assets and minimize information security risks

Accounting information security has ISO 17799 standards, including: 10 control clauses (10 articles of observation), 36 control objectives (36 objects / objectives security control), 127 security controls (security control) Information security is to protect information from various threats to ensure business continuity, minimize damage caused by the occurrence of hazard threats, accelerate the return of investment and business opportunities. (Ngqondi 2009) "ISO 17799 defines 133 pieces of security controls that are structured and grouped into 11 clauses to facilitate identifying things that are needed to secure a company's information assets."According to (Ali Haidir, Mochamad Wahyudi,2016) the security of information systems at the BSI scheduling still needs improvement. But there are some clauses that already meet the standards of ISO 17799, the sixth clause of management and organizational communication and seventh clause of access control. ISO 17799 helps businesses in information security with a list of goals and practices. The origin of ISO 17799 goes back to BS7799, which was published by the British Standards Institution in 1995. (Li, et al. 2000) claim that ISO 17799 is a comprehensive model for ISM. (Dhillon, Backhouse 2001) describe this standard as a successful vehicle for addressing ISM issues in the modern organization

2.2 Management Control

Information security aspects are very important in the world of user information and can guarantee that only those who have access to certain information.Information Security is an effort to secure the information assets owned by the company. Users in this case can mean humans or systems that have the right to access that information (Peltier, T. R., 2001).Most people may ask, why "information security" and not "information technology security" or IT Security. These two terms are actually very related, but refer to two completely different things. "Information Technology Security" or IT Security refers to efforts to secure information technology infrastructure from disruptions of illicit access and unauthorized network utilization. In contrast to "information security" which focuses precisely on data and information owned by the company. In this concept, the efforts undertaken are to plan, develop and supervise all activities related to how data and business information can be used and diutilisasi in accordance with its function and not abused or even leaked to unauthorized parties.

2.3 Technical Controls

According to (James O'Brien 2010, p26) the system is a group of components that are interconnected, working together to achieve a common goal by receiving input and producing output in a regular transformation process.
. According to (Gondodiyoto 2007, p112), states that information systems can still be defined as a set of integrated elements or resources and network procedures that are interconnected in an integrated manner, integrated into a certain hierarchical relationship, and aims to process data into information.

3 RESEARCH METHODS

3.1 Type of Research

This type of research is field research (field ressearch) ie direct observation of the object under study in order to obtain relevant data. The method that will be used in this research is by using quantitative analysis research method, that is using deep data analysis in the form of numbers.

3.2 Population and Sample

3.2.1 Population

The population in this study is all information technology departments in the company, Medan city, with employees working in the IT department in one of the PT in Medan and students already working in the information and technology section.

3.2.2 Sample

The samples used in this study are the employees and students who already work in the company. Questionnaires distributed through the website have been filled as many as 70 respondents.

3.3 Variable Operational Definition

The independent variables consist of: management control, operational control and technical control, dependent variable of ISO 17799 standard. Independent variable:

2.3. Management Control, made up of

1. Computer security policy
2. Computer security risk management
3. Security and planning in the life cycle of computer systems
4. Warranty

3.3. Operational Control, comprising,

1. Problems of personnel / users
2. Preparing contingencies and disasters
3. Handling computer security incidents
4. Awareness, training, and education
5. Security considerations in computer support and operation
6. Physical and environmental security

4.3. Technical Control, comprising,

1. Identification and authentication
2. Logical access control
3. Audit trail
4. Cryptography

3.4 Dependent Variables

a. 10 control clauses (10 articles of observation)
b. 36 control objectives (36 objects / security targets)
c. 127 controls securiy (127 security surveillance)

3.5 Data Collection Methods and Procedures

Data will be collected using questionnaire techniques. By spreading the questionnaire to the respondents in this research. Instrument used to measure this research variable by using likert scale 5 points. Respondents answer the choice of five existing alternatives, namely: 1. SS: Strongly Agree 2. S: Agree 3. N: Neutral 4. TS: Disagree 5. STS: Strongly Disagree

3.5.1 Engineering and Data Analysis

A study requires data analysis and its interprestation aims to answer the researcher's questions in order to reveal a certain phenomenal. Data analysis is the process of simplifying the data into a younger form read and interpreted. In this study used qualitative analysis.

3.5.2 Data Analysis Technique and Hypothesis Testing

How the formation of variable indicators using the ratio method of the indicator of research variables. Data processing using Microsof excel application then data is converted using SPSS release 16 application, for provision of path analysis data (path analisys) Data analysis in this research using Partial Least Square (PLS) methde method. PLS can be used on any type of data scale (nominal, ordinal, interval, ratio) as well as more flexible assumption terms. PLS is also used to measure the relationship of each indicator with its construct. In addition, in the PLS bootstrapping test can be done on structural models that are outer models and inner models. Because in this study using indicators to measure each construct, and also the structural model of measurement, it was decided using PLS. PLS can be used for confirmation

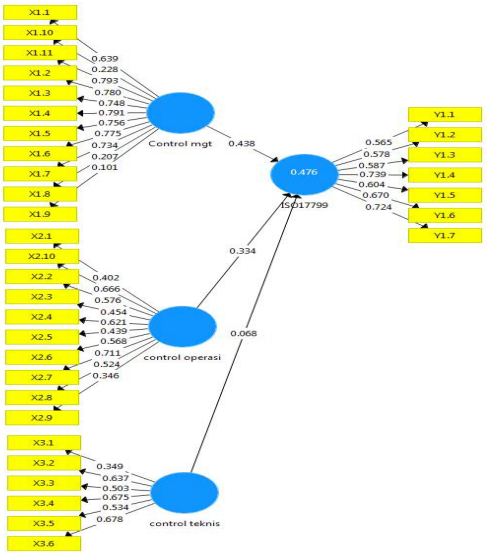
Table 1 : data results

	CM	CO	CT	ISO17799
R-square				0,476
R-squere adjusted				0,452
Composited realible	0,871	0,800	0,739	0,829
Cronbach c alpha	0,827	0,721	0,579	0,761
Avq var extrac	0,522	0,594	0,530	0,612

purposes, such as hypothesis testing and exploration purposes. But PLS prioritizes exploration rather than confirmation. But the main purpose of the PLS is to explain the relationship of the extract and emphasize the notion of the value of the relationship. In this case, the important thing to note is the necessity of a theory that provides assumptions to describe the model, variable selection, analytical approach, and interpretation of results.

4 RESULTS AND DISCUSSION

The results of data processing with outer model algorithm calculations are shown in the following figure, which illustrates the correlation between indicators and variables of management control, operational control and technical controls and contained in table 1.



Picture 1. Processed data

From the results of the test data can be seen all indicators in the model reflect the reliability of the CM reliability composite value of 0.87; CO is 0.800; CT is 0.739 and ISO 17799 standard is 0.829 where the minimum value is 0.7 while ideally is 0.8 or 0.9.

5 CALCULATION OF QUESTIONNAIRE

The respondents of this study consisted of employees at one of the universities in Medan, the Information Technology section, and the students working in the information section. The distribution of questionnaires is done through google, and direct spread among students. The results of questionnaires are selected according to the requirements that must be met, where respondents have worked, according to the field of information technology and have been using applications in their work.

6 DISCUSSION

Data obtained from the results of the questionnaire distribution then processed by using SEM analysis PLS, where the questionnaire using a 5-point likert scale. After the questionnaire is entered in the table, then count the result from 70 resopnden. Based on result of recapitulation result of spreading of questionnaire as follows:

6.1 Management Controls

Management control variables significantly influence the formation of ISO 17799 standards. Management control is divided into 11 indicator indicators, Management Control, comprising Computer security policy, Computer security risk management, Security and planning in the life cycle of computer systems, Guarantees. In the indicator companies still face problems in predicting the risks to be faced, companies still face problems in providing information in accordance with the authorities who get it.

Based on the results of data analysis can also be seen management controls positively influence the formation of ISO 17799 standard, seen from the original value of the sample of 0.583 with a significance of 0.05.

6.2 Operational Control

Operational control variables affect the formation of ISO 17799 Standard significantly and positively. Operational Control consists of 10 indicators of questions given to respondents Operational Control consists of Operational Controls, Personnel / user issues, Preparing contingencies and disasters, Handling computer security incidents, Awareness, training, and education, Security considerations in computer support and operations, Physical security and the environment. The problem that the company found lacks understanding of the possibility of risk in the context of the IT risk portfolio, the Company still faces problems in conducting monitoring plans and further reviews of risks in the IT risk portfolio. The server's storage location is managed by divisions that are not equipped with air conditioning, CCTV, lock and secure from fire. Can be seen also from the analysis results on the original sample of 0.544 with a significance of 0.05, that management control positively affect the ISO 17799 standard.

6.3 Technical Controls

The technical controls affect the formation of ISO 17799 standard. The technical control consists of 6 questionnaires given to the respondent, consisting of Identification and authentication, Logical Access Control, Audit Trace, Cryptography, Service Problems to users experiencing problems so that users experience some problems with service, while the respondent faces many customers. Judging from the original sample data analysis of 0.468 with a

significance level of 0.05, management control has no effect on the formation of ISO 17799.

6.4 ISO 17799 Standard

The respondents face problems in having the information security certificate, from the observation result obtained information most of the respondents still consider the ownership of the certificate is still less important. Respondents' responsiveness that with the enforcement of good security is expected paara customers will feel comfortable and protected. Management control factors, operational controls and technical controls affect the formation of ISO by 0.476 or equal to 47.6% and 52.4% influenced by other factors.

7 CONCLUSIONS AND SUGGESTIONS

a. Based on the results of the discussion can be summarized as follows: Control management, operational control has influence in the formation of ISO 17799 standard, Computer security policy, Computer security risk management, is good but pernting company to improve planning in the life cycle of computer system, and Guarantee of computer system life cycle planning is enhanced because company already have good risk management. This is in contrast to less precise cycle planning.
b. Technical control variables do not affect the formation of ISO 17799 standard.
c. Based on the evaluation results of the modeling of 26 valid indicators in the measurement of each of each Latent variable and can support the establishment of ISO 17799 standard
d. Information System Security enhanced to overcome the weakness of information systems one of them with the ownership of ISO 17799 certificate.

REFERENCES

Verheul, E. (2011). *Introduction to information security Lecture #1.* Radboud University,Nijmegen.

Whitman, Michael E., and Herbert J. Mattord. Principles of Information Security. Independence, KY: Cengage, 2011. 4th edition

Conray-Murray A. 2003,Strategies & issues: justifying security spending. Available online at: http://www.itarchitect.com/articles/NMG20020930S0002.html [accessed 18.07.07]

Conner FW, Coviello AW. 2004 Information security governance: a call to action, corporate governance task force report of 2004.

Bundesamt Fur Sicherheit in der Informationstechnik (BSI). (2008). BSI-Standard 100-1 Information Security Management Systems (ISMS). Bonn.

Ngqondi, T.G. (2009). The ISO/IEC 27002 And ISO/IEC 27799 Information Security Management Standard: A Comparative Analysis From A Healthcare Perspective. Port Elizabeth: Nelson Mandela Metropolitan University.

Ali Haidir Mochamad .Wahyudi..2016 *Jurnal Informatika Kombinasi Standar Iso17799, Sse-CmmUntuk Pengukuran TingkatKematangan Keamanan SistemInformasi Penjadwalan.*

Li, H., King G., Ross M., and Staples,G. (2000). BS7799: A Suitable Model for Information Security Management, America's Conference on Information Systems, Electronic Commerce track, August 10–13, Long Beach, CA, Atlanta, GA: Association for Information Systems

Dhillon, G. and Backhouse, J. (2001) Current Directions in IS Security Research: Towards Socio Organizational Perspectives, Information Systems Journal , (11), pp. 127-153.

Peltier, T. R., 2001, Information Security Risk Analysis, Auerbach Publications.

O'Brien, James A. & George M. Marakas, (2010). Management Information Systems: Managing Information Technology In The Bussiness Enterprise. 15th ed. NY: McGraw-Hill.

Gondodiyoto, S. ,2007 Audit Sistem Informasi: Pendekatan Cobit , Edisi Revisi,Mitra Wacana Media , Jakarta. p112