A Method for Evaluating Information Security Governance (ISG) Components in Banking Environment

M Ula, M Ula and W Fuadi

Informatics Engineering, Malikussaleh University, Jl. Cot Tengku Nie Reuleut, Aceh Utara, Indonesia
Nanggroe@gmail.com

Abstract. As modern banking increasingly relies on the internet and computer technologies to operate their businesses and market interactions, the threats and security breaches have highly increased in recent years. Insider and outsider attacks have caused global businesses lost trillions of Dollars a year. Therefore, that is a need for a proper framework to govern the information security in the banking system. The aim of this research is to propose and design an enhanced method to evaluate information security governance (ISG) implementation in banking environment. This research examines and compares the elements from the commonly used information security governance frameworks, standards and best practices. Their strength and weakness are considered in its approaches. The initial framework for governing the information security in banking system was constructed from document review. The framework was categorized into three levels which are Governance level, Managerial level, and technical level. The study further conducts an online survey for banking security professionals to get their professional judgment about the ISG most critical components and the importance for each ISG component that should be implemented in banking environment. Data from the survey was used to construct a mathematical model for ISG evaluation, component importance data used as weighting coefficient for the related component in the mathematical model. The research further develops a method for evaluating ISG implementation in banking based on the mathematical model. The proposed method was tested through real bank case study in an Indonesian local bank. The study evidently proves that the proposed method has sufficient coverage of ISG in banking environment and effectively evaluates the ISG implementation in banking environment.

1. Introduction

The growth of information technology has been so explosive in the recent decade. Computer has been widely applied in every aspect of our life from business, government, education, finance, healthcare, and aerospace to defense system. With society's increasing dependency on information technology (IT), the consequences of computer *crime* can be extremely grave [1]. Security breach and computer viruses cost global businesses $1.6 trillion a year and 39,363 human years of productivity. In 2009, Symantec has detected 59,526 phishing hosts around the globe, that number is increased by 7% compared to phishing hosts detected in 2008. The percentage of threats to confidential information is increased to 98% in 2009 compared to 83% in 2008, 89% of the threats have the ability to export user data and 86% of them have keystroke-logging component [2].

The information system has become the heart of modern banking in our world today, and information has become the most valuable asset to protect from insiders, outsiders and competitors.

Customers are very concerned about privacy and identity theft. Business partners, suppliers, and vendors are seeing security as the top requirement, particularly when providing mutual network and information access. Banks' ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network services. Having a good reputation for safeguarding information will increase market share and profit. Therefore, banks have to be responsible for fraudulent activity perpetrated via the internet channel. Banks have to reimburse most customers for losses, although the customer clearly compromised their account credentials. An empirical research in Information Security Governance in banking is noted to be lacking [3]. There are some ISG frameworks, have been developed and widely practiced in types of businesses, but each of them has its own advantages and weaknesses. Commonly, it must be customized to fit with organizational structure and environment. ISG frameworks employ in banking system is adopted from general business ISG governance framework. Different business type has different characteristic so that bank need customized framework that's more suitable for bank environment. Hence, this research seeks to fill this research gap. The research aims to identify the degree of importance of each ISG component to be implemented in banking systems. This paper is organized into five sections. This section introduces the background of the study and research concern. Section two portrays the literature review of information security governance in banking. Section three discusses research methodology. The section four discusses the degree of importance of each ISG component. Finally, the paper ends with conclusions.

2. Information security governance evaluation

The ability to evaluate governance processes provides the best measure of governance performance [4]. Practical evaluation of security processes, such as malware statistics, is considered to be the most useful of all security tests. Having metrics provides the necessary quantitative information required to manage information risks and threats [5]. Literature study identifies many papers which proposed a wide range of approaches for evaluating corporate governance, ICT governance and information security governance. There are two ISG evaluation approaches found in the literature which are proposed Corporate Governance Task Force [6] and EDUCAUSE [7]. The security assessment approach developed by EDUCAUSE is a modification from the CGTF (2004) Information Security Governance Framework. EDUCAUSE (2004) developed a scorecard approach to effectively implement information security governance within institutions of higher education such as colleges and universities. However, both of the methods use direct summation method for grading and scoring the ISG implementation. In this research, more realistic ISG evaluation method is developed for banking industry with focus on component importancy and critical components that mapped to bank corporate governance [8].

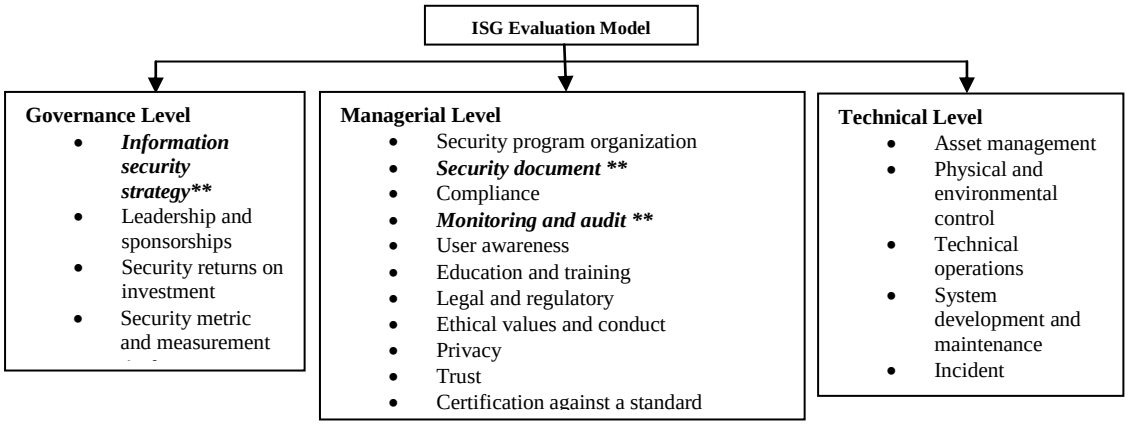

Figure 1. The structure of ISG evaluation model**.**

The structure of the ISG evaluation model is given in Figure 1. For this problem structure, a modified equation from Simple multi-attribute rating technique (SMART), Edwards and Barron proposed a variant named SMARTS (SMART using Swings) that in the course of the comparison of the importance of the criteria also considers the amplitude of the utility values, in examples; the changes from the worst utility value level to the best level among the alternatives [9].

3. Research methodology

The research started by documents and standard review. Almost all security standards available were examined to identify security components suggested by the documents. The information obtained in this preliminary study guides in developing the instrument for the main survey. The population of this study refers to all Bank Leaders, IT/IS professionals and Vendors related to banking industry all over the world which are Bank IT Staff, Security Manager, Security Consultant, IS Auditor, IT Practitioner. The IT/IS professional should have recognized certificates (CCNA, CCP, CEH, CISA, CISM, CISSP, Comptia Security +, ISO2001, ISP, ITIL, RHCT). Sampling come from the bank security professional signed up for linkedin.com social network and some security professional Group in Yahoo group and Google group. Data collection strategy used in this research is a web-based survey using Google document application. A strong reason for choosing web based survey instead of other traditional methods is because of the demography and location of the respondents are scattered around the world [10]. A self-designed and administered survey using Google Document application is developed. This method involves posting a questionnaire on Googledocs web site with respondents typically replying from remote computers. An introductory and acknowledgement page accompanies the questionnaire. 930 personal massage invitations were sent to security professionals at Linkedin.com inviting them to participate in the study. As a result of the effort, it received 189 responses. Within the 189 responses, 7 lacked complete answers for every question; the total number of effective responses is 182. The questionnaire was structured into three parts which are Respondent's Profile, Critical Components, and Importance level.

The survey questionnaire is designed to get feedback and opinion of the respondents. Part I of the questionnaire examines the demographic information about the respondents and their bank, such as respondent's gender, professional level, type of bank and size of bank. Part II was designed to determine the critical components of information security governance to be implemented in banking system. The ISG components used in this questionnaire are derived from information security documents and standards reviews done prior to the survey development. If one of these components is missing, there is no security for the whole system even though all other components are implemented. The respondents were requested to choose several ISG components that he thought as the critical components to be implemented in banking system. The questionnaire questions were structured as follows; "*Please check the items which you consider as the critical components to be implemented at … level in banking system*". Part III of the questionnaire is designed to gather the opinion from respondents about the degree of importance of ISG to be implemented in banking system. The questionnaire questions were structured as follows; *"How important is it that bank …?".* The response option is a Likert type five points scale response categories, ranging from "unrelated" to "extremely important". Each respondent is given a numerical score to describe respondent degree of importance to the preserved each component. The questionnaire is collapsing and mapping for logical groupings (technical level, managerial level, and governance level) to avoid confusing the respondents. By structuring the questions in this manner, would minimize the respondent's burden because of short time consuming to complete the survey and therefore the quality of the data could be maximized. List of component was as structured in Figure 1. The data result from ISG critical components and importance level serve in the mathematical model to develop ISG evaluation Method.

4. Result and analysis

This section describes the survey result of the most critical components should be implemented in banking ISG and the importance of each components. Table 1 shows the the survey result of the

critical component and the importance of each component.

Table 1. ISG critical components and importance.

	Components	Critical Percentage (%)	Importance
Strategic Level	Information Security Strategy*	83.5	4.47
	Leaderships and Sponsorships	48.4	4.37
	Security Return on Investment	24.7	3.74
	Security Metric and Measurement	49.5	3.92
	Auditor Security Program	42.3	3.92
	Security program organization	43.7	4.22
Managerial Level	Security policies, procedure and guidelines*	88.0	4.47
	Compliance	52.5	4.21
	Monitoring and audit*	71.0	4.25
	User awareness	60.1	4.35
	Education and training	51.4	4.2
	Legal and regulatory	41.0	4.15
	Ethical values and conduct	30.1	3.99
	Privacy	35.5	4.46
	Trust	26.8	4.04
	Certification against a standard	20.8	3.63
Technical Level	Risk management	67.2	4.21
	Risk assessment process	48.6	4.14
	Best practice and baseline consideration	29.5	4.26
	Asset management	43.7	4.07
	Physical and environmental control	55.7	4.16
	Technical operations	54.6	3.88
	System acquisition, development and	49.2	3.85
	Incident management	63.4	4.2
	Business continuity plan*	77.6	4.35
	User management	47.5	4.08

4.1 ISG critical components in banking environment

In this section, the survey result of identifying the most critical components of ISG that should be implemented in banking will be discussed. The frequency statistical analysis result for Governance, Managerial and Technical level is provided in Table 1. The survey result in critical component table shows that, for Stategic Lavel , 83.5 % respondents chose Information Security Strategy as a critical security component in banking system. For Managerial Level, 88.0 % chose security policies, procedure and guidelines and 71.0% chose monitoring and audit as the critical security components in banking system. For technical level, 63.4% chose incident management, 77.8% chose business continuity plan, as a critical security components in banking system. This critical components would include in developing the mathematical formula for evaluating ISG implementation in banking system.

4.2 Importance of the ISG components

Regarding the importance, the result in Table 1 shows that all ISG components have means values

higher than 3. It shows that all components discussed are important for banks at Governance Managerial and Technical level. At Governance level, the result shows that the Information Security Strategy and Leaderships and Sponsorships are perceived as the most important components that should be implemented by banks. The security guideline, procedure and policy, and privacy are perceived as the most important components that should be implemented by banks at Managerial level. At Technical level, Business continuity plan is perceived as the most importance component in that should be implemented in banking system.

5. Developing ISG evaluation method

The objective of the ISG evaluation is to identify how much amount of ISG components had been implemented in a bank as a countermeasure to latest security threats. From the structure shows in Figure 1, the mathematical model for ISG Evaluation proposed as in equation 1.

$$ISGLevel = \frac{\left(\sum_{j=1}^{n} W_j M_j\right)\left(\prod_{u=1}^{v} C_u\right)}{\left(\sum_{j=1}^{n} W_j\right)} \quad (1)$$

Where $\boldsymbol{M_j}$ is the level of the j[th] ISG component implementation in a bank. The implementation level of each ISG component in a bank can be determined by using the proposed evaluation document given in Appendix. The document derived from ISO 17799 [11], FISMA and some other security checklists. This proposed tools use six Likert scales scoring to evaluate the implementation level of each ISG component. The scoring is given in Table 2 below.

Table 2. Implementation level scoring.

Score	Stand for
0	Component is not exist
1	Component exists but is not implemented
2	Component that is occasionally implemented
3	Component is implemented with much vulnerability.
4	Component that is implemented with little vulnerability,
5	Component fully implemented.

$\boldsymbol{W_j}$ is the weight of the each ISG component in banking system. The component weighting values are derived from the importance degree resulted from the survey data as shown in Table 1. $\boldsymbol{C_u}$ is critical component of u[th] security component and v is the number of total critical components. he critical components used in this mathematical model also derived from the survey result. The value of $\prod_{u=1}^{v} C_u$ is 1 if the entire critical components are well implemented, otherwise it would be 0, if the critical components not well implemented.

6. Testing the developed method in real bank

X Bank, a local provincial governance bank in Indonesia, selected to use the proposed method. X Bank is an actual bank; however, its name has been changed in this document to comply with its policy. The bank has divided into two business mainstreams which are conventional banking and Islamic (sharia') banking. The testing was done by five evaluators, in main office Banda Aceh, and branches in Sigli, Bireuen and Lhoksumawe. They were asked to evaluate their information security program implementation based on the method provided in the developed method tool. Each evaluator was given a softcopy of the developed method (scorecard) document in Microsoft Excel file with computed using the ISGlevel equation. The summary of the testing result is provided in Table 3.

Table 3. Summary of X bank ISG implementation evaluation result.

Level	S.B. Bireuen	S.B. Sigli	C.B. Bireuen	C.B. Lhoksumawe	Main Office	Average
Governance	2.90	3.13	2.87	2.53	3.19	2.92
Managerial	3.93	3.64	3.48	3.8	3.96	3.79
Technical	4.27	4.06	4.19	4.1	4.28	4.16

Table 3 shows the summary of the testing result done by the evaluators to their branch. This testing done by the evaluator using developed method that given to them as a tool to evaluates ISG components implementation in their bank. The results in Table 3 clearly indicate the weakness areas of X Bank Information Security Program. At governance level, the most of the evaluation score are lower than 3. Refer to the values in Table 2, It can be conclude that, at bank X governance level, the ISG components are occasionally implemented. However, at Managerial level, the most of the evaluation score are higher than 3. It can be conclude that, at bank X Manajerial level, the ISG components are implemented but with much vulnerability. Futhermore, at Technical level, the most of the evaluation score are higher than 4. It can be conclude that, at bank X Technical level, the ISG components are implemented with little vulnerability.

Therefore, it show that the developed method can highlight the weakness of bank X information security program and which level grant the responsibility. Hence, the developed method proves that its can achieve its objectives as an alternative of ISG evaluation method in banking envireonment.

7. Conclusion

To established a proper information security program, a bank need to define the critical component to be implemented in their ISG framework. This study conduct a web-based survey to gathering professional judgment about the critical components must be implemented in bank ISG program. From the survey result, it is found that the critical components for ISG implementation in banking system are: Information Security Strategy, Security policies, procedure and guidelines, Monitoring and audit, Business continuity plan, Disaster recovery plan. The ISG components implemented in banking have different degree of importance. Generally, “Information Security Strategy” and Leaderships and Sponsorships” perceived as very important components should be implemented by a bank at Governance level, “Guideline” and Privacy” perceived as very important components should be implemented by a bank at managerial level, and “Business Continuity Plan” is a very important component at technical level. So that current method on security metric and audit is not realistic because it still use direct summation method and treat all component as the same important. It is need more realistic method which has a weighting coefficient for each ISG component measured in banking environment. In this research, a method to evaluate the ISG implementation was developed and tested in a real bank environment. This developed method used the importance level as a weighting coefficient and the existence of the critical components also taken in to consideration when calculation the level of ISG implementation in a bank. The developed method had highlight the weakness of bank X information security program and which level grant the responsibility, therefore, it proves that its can achieve its objectives as an alternative of ISG evaluation method in banking envireonment.

8. References

[1] Mahncke R J, McDermid D C and Williams P A 2009 *Proceedings of the 7th Australian Information Security Management Conference (Melbourne)* (New York: Springer)
[2] Symantec Enterprise Security 2010 *Symantec Global Internet Security Threat Report Trends for 2009* vol XV (Mountain View: Symantec Corporation)
[3] Kurt B and Tentra G M 2004 *Corporate Information Security Governance in Swiss Private Banking* (Zurich: Master’s Thesis University of Zurich)
[4] Fitzgerald T 2008 *Information Security Governance: What Is It and How can We Accomplish It?* (Milwaukee, WI: ISACA Kettle-Moraine Chapter Meeting)
[5] KabayM E 2009 Security metrics research *Network World*

[6] Corporate Governance Task Force 2004 Information security governance: A call to action *Corporate Governance Task Force Report* (USA: National Cyber Security Summit)
[7] EDUCAUSE 2004 *Information Security Governance Assessment Tool for Higher Education*
[8] Ula M, Ismail Z, Zidek S M 2011 *Journal of Information Assurance & Cybersecurity*
[9] Edwards W and Barron F H 1994 *Elsevier* **60** 306-25
[10] Cooper D R and Schindle P S 2008 *Business Research Method* 10th Edition (Singapore: McGraw-Hill)
[11] Standards Australia 2005 *Information Technology Security Techniques Code of Practice for Information Security Management* (Sydney: Standards Australia Limited)
[12] Brotby W K 2006 *Information Security Governance, Guidance for Boards of Directors and Executive Management* 2nd edision (Rolling Meadows: IT Governance Institute, Rolling Meadows)