Advanced Materials Research Vol 905 (2014) pp 663-668 *Online: 2014-04-28*

doi:10.4028/www.scientific.net/AMR.905.663

Action Design of Information Systems Security Governance for Bank Using COBIT 4.1 and Control Standard of ISO 27001

Idris Gautama So[1,a], N.J. Setiadi[2,b], B. Papak[1], Rudy Aryanto[1,c]

[1] Bina Nusantara University, Jakarta, Indonesia

[2] Widyatama University, Bandung, Indonesia

[a] idrisgs@gmail.com, [b] nsetiadi919@gmail.com, [c] raryanto@binus.edu

Keyword. Information Systems Security Governance, COBIT 4.1, ISO 27000

Abstract. The aim of the study is to design remediation information systems security governance at Bank. This study provided proposed solutions to solve the existing gaps between the current condition and the expected information systems of the bank's security governance. A case study of a commercial bank is used in this study. There are 7 process frameworks of COBIT 4.1 used to measure the maturity level of information systems security governance. Of these processes, appropriate controls within the framework of COBIT 4.1 and ISO27001 are undertaken. As a result, the security of governance information systems is increasing. In conclusion, there is a need of reliable information systems security governance to achieve the intended business goals.

Introduction

Based on Regulation of Bank Indonesia (PBI) number B.9/15/PBI/2007 regarding risk management in the use of information technology by the Commercial Banks that the development of information technology enables the bank to use it to improve operational efficiency and quality of service to customers and the Bank's information technology is also a valuable asset to the Bank so that the management is not only the responsibility of organizing the information technology unit, but also all those who use it [1]. The survey results ISBS (Information Security Breaches Survey) in 2000 showed that most of the data or insufficient information maintained / protected so that the resulting insecurity, the survey also showed that 60% of organizations experienced an attack or corruption of data due to weakness in the security system, security system failure caused more by internal factors than external factors, internal factors such as errors in the operation of the system (40%) and discontinuities power supply (32%).

ISBS survey in 2004-2006 showed that there are many business networks in the United Kingdom (UK) has been under attack from outside [2]. Banking crimes that occurred in Indonesia in early 2011 there has been at least 9 cases of crimes that resulted in losses to the Bank and customers of the Bank with a total loss of IDR 208, 93 billion and $ 110,000, from the various types of crimes are either internal involvement of the Bank as well as from external / outsourced and there is also the role of IT in it [3]. As the beginning of the first 5 months of 2012 there were 1009 reported cases of bank's crimes with losses of IDR. 2.73 billion [4]. Therefore, to prevent crimes related banking IT need for control and good management so that the company or organization can align IT application and business needs [5]. In November 2009 The Bank has successfully connecting all units working in the country in online real-time. Application of this system aims to improve the service, perform operational efficiency and mitigate risk with an integrated control system. The question is "What is the suitable design of remediation systems security governance information system for the bank? ".

Literature review

COBIT was developed by the IT Governance Institute (ITGI). COBIT provides guidance-oriented business, and therefore business process owners and managers, as well as auditors and users, is expected to make use of these directives as well as possible. Business orientation is the main theme of COBIT is designed to be implemented not only by the IT service provider, users and auditors, but more important is a comprehensive reference for management and business process owners.

In order to achieve business objectives, information must meet the criteria referenced by COBIT as follows: Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance, and Reliability. In addition, to need to be defined business goals and IT goals to provide a better basis related to business and better to develop business requirements and develop metrics that can be measured in the achievement of these goals, in relation to the management of IT resources in order to meet business requirements, COBIT identifies resources as IT applications, information, infrastructure and people [5]. COBIT supports IT governance by providing a framework to adjust the alignment of IT with the business, in addition, COBIT framework also ensures that IT enables the business to maximize profits, appropriately manage IT risk and IT resources are used responsibly [6]. According to Schler [7], each domain is clarified and elaborated within 34 (thirty-four) objective is expected to be a reference to COBIT.

COBIT also acts as an integrator of different materials guide, summarizing key objectives under the auspices of the framework is also connected to governance and business needs, to COBIT 4.1, 6 (six) of all the major IT-related standards, frameworks and practices that are focused as a primary reference support to ensure proper coverage, consistency and alignment. The six standards are: COSO (The Committee Of Sponsoring Organization Of The Treadway Commission), ITIL (IT Infrastructure Library) was developed by the Officer of Government Commerce (OGC) in collaboration with the IT Service Management Forum (itSMF) and the British Standards Institute (BSI), ISO27000 (International Organization for Standardization), CMMI (Capability Maturity Model Integration), PMBOK (A Guide to the Project Management Body of Knowledge), ISF (The Standard of Good Practice for Information Security) [5].

COBIT and ISO / IEC 17799:2005 is a standard which is now widely used (ISO / IEC 17799:2005 is the code of practice for implementing security management), and the two are complementary. The scope of ISO / IEC 17799:2005 is the security aspect, while the broader COBIT, is a combination of the principles that have been implanted and is known as the reference model (such as COSO), and aligned with industry standards (such as ITIL, CMMI, BS7799 , ISO9000) [8]. The main function of COBIT is to help companies map IT processes in the company of best practice standards ISACA (Information Systems Control Standard). COBIT is chosen by companies that want to conduct information systems audit, both related to the audit of financial or IT in general, while a security standard ISO27001 scope smaller but deeper than the COBIT [9].

There are more than half of the survey respondents felt that their main threats are from internal information [10]. However, the threat is usually an accident of its own employees. The rest said, the threat came from trojans, hacker attacks, viruses, vulnerabilities of the operating system, and other malicious software (malware). While based on Summer's study [11], which is included in the information security risk are: 1. Human error such as errors or accidents by employees, 2. Deliberate software attacks such as denial of service, worm, or virus, 3. Threats of nature such as fire, floods and earthquakes, 4. Failure or fault of the hardware, 5. Failure or fault of the software as a bug, 6. The technology is outdated.

Dey [12] states that information is something that is important to the company. Therefore the information must be protected so that the information does not fall to that should not be. As a result of information that is not safe or misused can lead to loss of business and even the reputation of the company. Electronic data security becomes very important service providers of information technology (IT) and other industries, such as export-import firms, transportation, education, news, up to the use of banking facilities and placing IT infrastructure as critical / important, information or data is an asset to the company, data security indirectly to ensure business continuity, reduce risk, optimize the return on investment and are looking for business opportunities. More company information is stored, managed and deployed, the greater the risk of damage, loss or exposure of data to unwanted external parties [8].

ISO27001 [13] is an international standard that covers all types of organizations, both profit organizations, government organizations, and non-profit organizations. ISO27001:2005 defines information security by achieving the following aspects: (1) Confidentiality, to make sure the information can only be accessed by authorized parties. (2) Integrity, guarantee the accuracy and

completeness of the information and processes. (3) Availability, ensures that the authorized parties can access the information and associated assets when required.

Method

The method used in this study is case study. The population is the entire subject of research [14]. According Sugiyono [15], the population is a region consisting of generalization objects / subjects that have certain qualities and characteristics are determined by the investigator to be studied and then drawn conclusions. The population in this study is all employees of IT Division of the Bank considered related to or understanding of IT governance processes.

The sample is part of the number and characteristics possessed by the population [26]. Sampling technique in this study is used by purposive sampling technique. Samples in this study were employees of the IT Division of the Bank who are considered relevant or understanding of IT governance processes at the Bank, namely those concerned with IT governance in [5].

Data collection techniques that are used in this study are observation, interviews, questionnaires and a mix of all three (triangulation). (1) Observation is the basis of sciences. Scientists work based on the data, the facts about the reality gained through observation. Hadi [16] suggested that the observation is a a process that is composed of various biological processes and psychological, two of the most important are processes of observation and memory. Moderate participatory observation is used, that in addition to the study employee of the company who becomes the object of research [17]. Observations carried out to observe and obtain data accurate and factual IT Division of the Bank. (2) An interview, which is a meeting of two people to exchange information and ideas through questions and answers so can be constructed into a particular topic [18]. Interviews with relevant parties to obtain initial information on various issues or problems that exist and to obtain information about everyone involved or understanding of IT governance processes from the Bank. (3) The questionnaire is a data collection technique is done by giving a set of questions or a written statement of the respondent to answer, and the questionnaire should be tested first [16], while the validity of this questionnaire approach is content validity and the construction validity, which can be interpreted as judging the validity of the terms of the arrangement, framework or conjecture [19]

From the questionnaire then conducted discussions to crosscheck the contents of the questionnaire which reflected the contents of COBIT 4.1 and to ensure that the indicators are measured in statements and to ensure there are not double barrel question and must also be readable so does not result in bias [5]. The questionnaire will be used to measure the maturity of IT governance processes that are running at the moment and make IT governance process to be achieved by the Bank. The data generated questionnaires are distributed to multiple sources (triangulation of sources / test credibility / validity) consisting of managers, supervisors and staff.

Analysis and discussion

Criteria of information that is referenced by the COBIT 4.1: Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance, and Reliability. Among the processes and criteria will be selected IT processes that meet the three criteria of Confidentiality, Integrity and Availability. Table 1 show the mapping of the entire process and criteria contained.

Table 1. IT Process Analysis.

No	Information Systems Security			IT Process (COBIT)
	Confidentiality	Integrity	Availability	
1.		PO2		Planning and Organization
2.	PO9	PO9	PO9	
3.		AI6	AI6	Procurement and Implementation
4.			DS4	Delivery and Support
5.	DS5	DS5		
6.		DS11		
7.		DS12	DS12	

Tuttle and Vandervelde [20] argue Maturity Model enables company management to evaluate and determine where spectrum control of their internal quality control currently resides. COBIT provides a parameter for the assessment of how well and high an IT management within an organization, the maturity models can be used for assessment management awareness and maturity

level. Maturity models are built from the general qualitative model, the attributes added in increasing attitude at the following levels: 1. Awareness and Communication, 2. Policies, standards and procedures, 3. Tools and automation, 4. Skills and expertise, 5. Responsibility and accountability, 6. Goal setting and measurement.

Evolving from non-existen through optimized processes. This attribute can be used for a comprehensive assessment, gap analysis and improvement planning. From the maturity model is used to control IT processes using a scoring method that can assess an organization's IT processes from the scale of its non-existent to optimized (from 0 to 5), namely: 0: Non Existen, 1: Initial, 2: Repetable, 3: Defined, 4: Managed and 5: Optimized [21, 22, 23].

Before analysis, the data was processed first. Activities in the process the data according Narkubo & Achmadi [24] include: (1) Editing is the list of questions that have been submitted by the data collectors. The goal is to reduce errors or omissions in the list of questions. (2) Coding is the answer of the respondents classified into categories. (3) Scoring is to provide an assessment of the items that need to be assessment or score. (4) Tabulating is work making tables. The answers that have been given a code then inserted into the table 2.

Table 2. IT Process Analysis.

Process/ Respon-dents	DS5						*Maturity / Total Maturity*
	AC	PSP	TA	SE	RA	GS M	
R1	X	x	X	x	x	x	Xxx
R2	X	x	X	x	x	x	Xxx
R ...	X	x	X	x	x	x	Xxx
Rx	X	x	X	x	x	x	Xxx
Maturity / Total Maturity	Xxx	xxx	Xxx	xxx	xxx	xxx	Xxx

R = Respondent
AC = Awareness and Communication
PSP= Policies , Standards and Procedures
TA = Tools and Automation
SE= Skill and Expertise
RA= Responsibilities and Accountabilities
GSM= Goal Setting and Measurement
ValueMaturityLevel=ΣValue Maturity Attribute / 6
Value Maturity Attribute = Σ Value Maturity Attribute / Respondents
Total Value Maturity Level = Σ Value Maturity Level / Respondents

Table 3. Table Summary of Sample Rate Maturity.

Process		**As is**	***GAP***	**To be**
PO2	Define the information architecture	X	x	X
PO9	Assess and manage IT risks	X	x	X
AI6	Manage changes	X	x	X
DS4	Ensure continuous service	X	x	X
DS5	Ensure systems security	X	x	X
DS11	Manage data	X	x	X
DS12	Manage the physical environment	X	x	X
Average		**X**	**x**	**X**

Table 4. Sample Table Design of Remediation

DS5 Ensure systems security	
COBIT 4.1	ISO27001
……	……
……	……
……	……

Conclusion

Based on the calculation of the level of maturity that has been done then average results obtained are the current conditions are at level 3 (Define Process) and to be achieved at the level of 4 (Manage and Measurable). From the analysis of the gap it will look for a solution to cover the existing gap, while the approach used to close the gap is by using the controls contained within the framework of COBIT 4.1 and ISO27001 to achieve Remedial Action Design [15], from the control is yield design remediation for the Bank.

References

[1] Tim Informasi Hukum, Direktorat Hukum, Peraturan Bank Indonesia No. 9/15/PBI/2007 Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum dan Lampiran, http://www.bi.go.id/web/id/Peraturan/Perbankan/PBI9_17_2007.htm , retrieved on 16th of August 2012.

[2] M. Syafrizal, ISO 17799 : Standar sistem manajemen keamanan, Proceeding of Seminar Nasional Teknologi, Yogyakarta, 24 Nopember 2007.

[3] A. Saputra, Ini dia 9 kasus kejahatan perbankan diawal tahun, 2011. http://finance.detik.com/read/2011/05/02/193638/1630794/5/ini-dia-9-kasus-kejahatan-perbankan-di-awal-tahun , retrieved on 27 September 2012.

[4] Y. Purwanto & Shaufiah, Audit Teknologi Informasi Dengan COBIT 4.1 Dan Is Risk Assessment (Studi Kasus Bagian Pusat Pengolahan Data PTS XYZ) (KNS&I10-049, Konferensi Nasional Sistem dan Informatika 2010; Bali, November 13, 2010).

[5] IT Governance Institute, COBIT 4.1, IT Governance Institute, USA, 2007. http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx, Retrieved on 23/09/12

[6] H. Tanuwijaya & R. Sarno, Comparation of COBIT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals, IJCSNS International Journal of Computer Science and Network Security, VOL.80 10 No.6, June 2010.

[7] S. Schler, L. Will & M. Shafer, COBIT and Sarbanes Oxley Act, Galileo Press, Boston, 2007.

[8] Sanyoto, Audit Sistem Informasi; Pendekatan COBIT, Ed.Revisi, Jakarta: Mitra Wacana, 2007.

[9] Information System Auditing Resources (ISAR), Comparison between COBIT, ITIL, and ISO27001, 2008. http://www.securityprocedure.com/comparison-between-cobit-itil-and-iso-27001 , Retrieved on 3rd Oktober 2012.

[10] S. Keller, A. Powell, B. Horstmann, C. Predmore, & M. Crawford, Information Security Threats and Practices in Small Business, Information System Management, 2005.

[11] P. M. Summer, Information Security Threats : A Comparative Analysis of Impact, Probability, and Preparedness, Information System Management, 2007.

[12] M. Dey, Information Security Management – A Practical Approach. IEEE, 2007.

[13] ISO/IEC 27001 : 2005, Information Technology – Security Techniques – Information Security Management System -- Requierments, 2005. http://www.iso.org/iso/catalogue_detail?csnumber=42103 , retrieved on 23 September 2012.

[14] S. Arikunto, Prosedur Penelitian Suatu Pendekatan Praktek, Jakarta: Rineka Cipta, 2009.

[15] Sugiyono, Metode penelitian Kuantitatif, Kualitatif dan R & D, Alfabeta, Bandung, 2012.

[16] S. Hadi, Metodologi Research, Jilid 1,2 UGM, 1986.

[17] S. Stainback & W. Stainback, Understanding & Conducting Qualitative Research, Kendall/Hunt Publishing Company, Dubuque, Iowa, 1998.

[18] K.G. Esterberg, Qualitative Methods in social Reserch, Mc Graw Hill, New York, 2002.

[19] A. Sudijono, Pengantar Evaluasi Pendidikan, Jakarta: Rajawali Press, 2009.

[20] B. Tuttle & S. D. Vandervelde, An Empirical Examination of COBIT as an internal control framework for information technology, International journal of Accounting Information System 8, 2007.

[21] Tribun News Batam, BI Terima Laporan 1.009 Laporan Kejahatan Perbankan, http://batam.tribunnews.com/2012/07/11/bi-terima-1.009-laporan-kejahatan-perbankan, Retrieved on 27 september 2012.

[22] A. Setiawan, Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model COBIT Framework, Seminar Nasional Aplikasi Teknologi Informasi 2008 (SNATI 2008) ISSN: 1907-5022 Yogyakarta, 21 Juni 2008.

[23] Noerlina & D.C Cory, Pengkajian Tata Kelola Teknologi Informasi Menggunakan Panduan Managemen COBIT, Jurnal Piranti Warta Vol. 11 No. 1 Januari 2008: 15-27.

[24] A. Narkubo & A. Achmadi, Metodologi Penelitian Edisi I. Jakarta : PT Bumi Aksara, 2002.

[25] R. Sheikhpour & N. Modiri, An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012

[26] U. Sekaran, Reserch Methods For Business, A Skill Building Approach, Secon Edition, John Willey & Sons, Inc. New York, 1992.

Advances in Applied Materials and Electronics Engineering III
10.4028/www.scientific.net/AMR.905

Action Design of Information Systems Security Governance for Bank Using COBIT 4.1 and Control Standard of ISO 27001
10.4028/www.scientific.net/AMR.905.663