IMPLEMENTATION OCTAVE-S AND ISO 27001CONTROLS IN RISK MANAGEMENT INFORMATION SYSTEMS

Stephanus

Information Systems Department, School of Information Systems, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
stephanus.binus@yahoo.com; stephanus@binus.edu

ABSTRACT

Extensive use of information technology in companies put IT into a position which is of considerable concern, especially in large companies that put IT becomes a strategic part of the company. The importance of IT division, make the companies willing to pay big to get the benefits offered by IT itself, but on the other hand appears disappointment incurred from investments are not comparable with the results obtained. Until the threat appear and disrupt the business of the company. By doing risk management using the OCTAVE-S, particularly in smaller companies, can help companies to be growing, the company can find out the weaknesses and threats that may arise that could disrupt the company's business, helped by the standard controls that are owned by the ISO / EIC 27001 : 2005 helps companies to prepare implement ISO / EIC 27001:2005 later.

Keywords: *risk management, ISO/EIC 27001:2005, OCTAVE-S, risk assesment*

ABSTRAK

Meluasnya penggunaan teknologi informasi dalam perusahaan menempatkan IT dalam posisi yang sangat diperhatikan, terutama di perusahaan besar yang menempatkan IT menjadi bagian strategis dari perusahaan. Pentingnya divisi TI, membuat perusahaan bersedia membayar besar untuk mendapatkan keuntungan yang ditawarkan oleh TI itu sendiri, tetapi di sisi lain muncul kekecewaan yang timbul dari investasi tidak sebanding dengan hasil yang diperoleh. Sampai ancaman muncul dan mengganggu bisnis perusahaan. Dengan melakukan manajemen risiko dengan menggunakan OCTAVE-S, terutama di perusahaan kecil, dapat membantu perusahaan untuk tumbuh, perusahaan dapat mengetahui kelemahan dan ancaman yang mungkin timbul yang dapat mengganggu bisnis perusahaan, dibantu oleh kontrol standar yang dimiliki oleh ISO / EIC 27001: 2005 membantu perusahaan untuk mempersiapkan menerapkan ISO / EIC 27001: 2005 nanti.

Keywords: *manajemen resiko, ISO/EIC 27001:2005, OCTAVE-S, risk assesment*

INTRODUCTION

Extensive use of information technology in companies puts IT into a position which is of considerable concern, especially in large companies that puts IT into a strategic part of the company. Once the importance of IT, companies are willing to pay big to get the benefits offered by IT. However, on the other hand, it appears disappointment incurred from investments that are not compatible with the results obtained. Top management has always wanted an investment that must be issued in accordance with the benefits, regardless of the risks, threats, and weaknesses in the company. Especially on things that are the responsibility of the IT division, which sometimes it is not realized, it will affect the performance of the company's business either directly or indirectly.

Sometimes in the company, there are threats that always appear but never solved. Companies that have not been doing risk management will be difficult to assess the extent of the impact of risks, threats and weaknesses that appear on the company's business continuity. The impacts appear since the risk assessment has not been applied. Risk management is urgently required if there is no standard operational procedure that refers to the action in maintaining the security of information technologies that already exist in the company. The effect is not ready to tackle these risks and threats that arise and it must be handled quickly and appropriately to avoid the company's operations disrupted. Difficulty in communicating the importance of the value of information assets owned, due to lack of documentation or supported data, becomes another trigger for enterprise to apply risk management.

Risk management and risk assessment are important components in information systems management. According to the Technical Department of the European Network and Information Security Agency (ENISA, 2006) risk management is a process, distinct from risk assessment, weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options. Stoneburner, Goguen, & Feringa (2002) states that risk management is a process that allows IT managers to balance between operating costs and economic costs, of the protective measures to achieve gains, according to the company's mission, to protect IT systems and data support the mission of their organization. ENISA (2006) states that risk assessment is a scientific and technology-based process consisting of four steps namely, threat identification, threat characterization, threat assessment and risk characterization. In general, experts accept that risk assessment is part of risk management.

OCTAVE is a methodology developed by the institution of software engineering university Carnegie Mellon, is used to perform a risk assessment that incorporates the analysis of organizational behavior, and weaknesses of the technology. OCTAVE is an important component analyzer that can be built a team of internal company itself that has the technical skills and organizational skills related to the practice of business (Coleman, 2004).

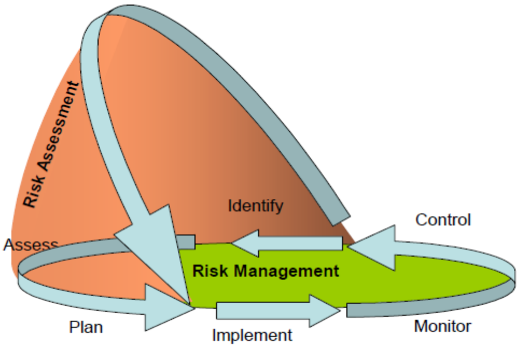

Figure 1 The relationship between risk management
Figure 2 and risk assessment (ENISA, 2006)

OCTAVE method is one method that is widely used by companies to perform risk assessment. OCTAVE method itself has three variants, namely OCTAVE, OCTAVE-S, and OCTAVE Allegro. The method used in this paper is the method of OCTAVE-S. This method is a modification of the OCTAVE method that is adapted to the capacity of the company. The use of the OCTAVE-S is commonly devoted to analyze the risk in companies that have small to medium scale with the number of staff is less than 300, and enabling activities carried out by a team of risk analysis in small quantities.

Table 1 Differences Between OCTAVE and Other Approaches

OCTAVE	Other Metods
There is a stage of improvement of risk management information system.	Does not have a phase of information systems risk management improvement (CRAMM, CORAS)(Bornman &Labuschagne, 2006)
There are formal procedures for the process of "accepting risk"	There is no formal procedure for the process of "accepting risk" (CORAS,CRAMM,COBIT) (Bornman &Labuschagne, 2006)
Focus on risk evaluation of information systems	Focus on the process of building the IT Governance (COBIT) (Bornman &Labuschagne, 2006)
Consider the "People" as an asset in the evaluation of information systems risk	Does not include "People" as an asset in the evaluation of risk information systems. (Alberts, Dorofee, Stevens, & Woody, 2005)

ISO/EIC 27001 is an international standard that is prepared to provide a model to build, implement, operate, monitor, and maintain and develop the Information security management system (ISMS) (ISO & EIC, 2005). This method will be used as a reference in determining the control, after a risk assessment being done with using the OCTAVE-S. ISO / IEC 27001 has been developed to protect the information assets of an organization, "life blood of all the business" (Humfreys, 2005). There are several factors triggering the adoption of ISO / IEC 27001, which is internally the company will create awareness of the vulnerability of the information system and the company's critical processes (Barlette, 2006). Other factors driving the adoption of ISO / IEC 27001 is to demonstrate to partners that the company has been identifying and measuring security risks and implementing corporate security policies and controls that can reduce risk, thereby providing a strong conviction against the company (Saint-Germain, 2005). In addition, that is also what makes ISO / IEC 27001 becomes government policies as in Japan, or a necessity for outsource companies such as Taiwan, Singapore, and India (Backhouse, Hsu, & Silva, 2006).

Applying risk management by combining OCTAVE-S and ISO / IEC 27001 will provide an understanding of the importance of risk analysis for the company and its relation to the company's business. In the other hand it can support companies by providing information about the information technology’s risks, threats, and weaknesses that are found. It also provides solutions to protect corporate information assets, in the form of recommendations that can be applied by the companies that implement risk management, Another positive thing is that it helps to prepare the company when they want to implement ISO / IEC 27001.

METHOD

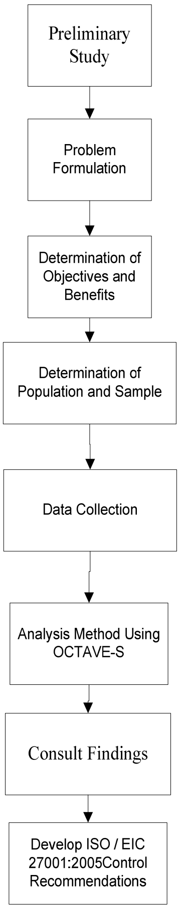
Preliminary Study
Problem Formulation
Determination of Objectives and Benefits
Determination of Population and Sample
Data Collection
Analysis Method Using OCTAVE-S
Consult Findings
Develop ISO / EIC 27001:2005Control Recommendations

Figure 3 Methodology of Research.

Preliminary study describes the process before the beginning of the study was conducted, starting from the submission of proposals to conduct research aimed at the company. At this stage also performed the initial communication with the corporate IT managers, as the tallest structure in charge of all matters related to information technology companies. The discussion is about the idea, a general overview of ideas about the manifest, as well as steps that will be done in the study, to obtain agreement in the form of signing a proposal. The next step is to study the organizational structure of the company and determine and apply the actor who will assist during the process of risk management takes place, besides studying the business processes, systems, and information infrastructure that runs the company.

Formulation of the problem is done so that the research conducted is not widened, which would make the research becoming unfocused. It is necessary to identify problems to be solved. The research is going to determine clear benefits and objectives so that it becomes a meaningful thing for the company in particular, as well as for education in general. The determination of populations and samples will be used as an object. This is the population that will be targeted interviews, and questionnaires regarding the provision of 15 safe practices that exist in the method of OCTAVE-S.

Data collection can be done in several ways. In this way, observation is carefully taken on the process running in the company, the information assets belonging to the company and the possibility of the emergence of risk. In addition, the available documents are collected, such as written policies related to management information systems, implemented controls, the company’s system documentation, the image of enterprise information technology infrastructure, the result of the previous risk management assessment (if any), the report of audit findings (if any) and other documents that can be used as the initial basis to see the initial condition of risk management the company. Data collection through interview by providing questions to the actors who have been mentioned at determination of population and sample step, so the result can provide an overview of the initial condition of the enterprise risk management.

Analysis Method Using OCTAVE-S

Build Asset-Based Threat Profiles

In this phase, the terms of organizational aspects are evaluated and evaluation criteria is defined, which will be used in risk evaluation. There are two processes In this phase: (1) Identify Organizational Information. This process have three activities, first is establishing impact evaluation criteria – in this study four risk criteria tables: table of criteria of impact, table of likelihood criteria, table of risk rating agency criteria, and table of criteria for risk appetite. Second is identifying organizational assets – identification of assets by collecting information assets, in the form of the type, age, size, location, and date of installation, assessment of asset condition and performance, including information about the operation, maintenance and repair history. Third is evaluating organizational security practices. (2) Create Threat Profiles. In this process there are three activities that should be done, first is selecting critical assets, meaning that if the asset is impaired, it will interfere with the performance of an enterprise wide basis, or even worse. Second is identifying security requirements for critical assets. Third is identifying threats to critical assets.

Identify Infrastructure Vulnerabilities

At this stage, followed by examining the extent to which each person participates to be responsible for security practices of information technology processes. In this phase there is a process that must be done, the process is Examine the Computing Infrastructure in Relation to Critical Assets. The process has two activities namely: (1) Examine access paths. (2) Analyze technology-related processes.

Develop Security Strategy and Plans

This phase is the last phase of the OCTAVE-S method to identify risks that may arise and intimidate the company's important asset and decide things that must be done to protect these assets. From the information analysis has been done before, it can be made as the asset protection strategies and develop risk mitigation planning.

In this phase there are two processes: (1) Identify and Analyze Risks. In this process there are three activities that must be done, first is evaluating impact of threats, second is establishing probability evaluation criteria and third is evaluating probabilities of threats. (2) Develop Protection Strategy and Mitigation Plans. In this process there are five activities to do that, first is describing current protection strategy, second is selecting mitigation approaches, third is developing risk mitigation plans, fourth is identifying changes to protection strategy and fifth is identifying next steps. The findings of the risks and weaknesses have been submitted to the company, in order to understand everything that has been done and to find out how the results of assessment activities that have been done.

The team made recommendations in terms of prevention and other matters related to risk management referring to the international standard ISO/EIC 27001. The study will produce a complete document on the assets and company information technology assessment. The risk profile of the company's assets, and control policies and mitigation of the risks and assets held in accordance with the methods referred to the OCTAVE-S and ISO/EIC 27001.

RESULT AND DISCUSSION

From the studies that conducted on small and medium scale companies then obtained the following results, there are four impact of risk that defined, reputation and customer confidence, financial, productivity, fines and legal penalties. All those four can be classified as low, medium, and high levels, according to how large the company is set against the impact of emerging threats and disrupt the company. The next step that should not be missed is conducting interviews with actors who have been determined previously, the questions are in the range of 15 safety practices that exist in the OCTAVE-S, from all questions on 15 security practices owned octave-s, it should be asked to the actors, to get the information about condition of the company, and if there is cooperation between companies and third parties then the answer must be included as well, as the following results shows.

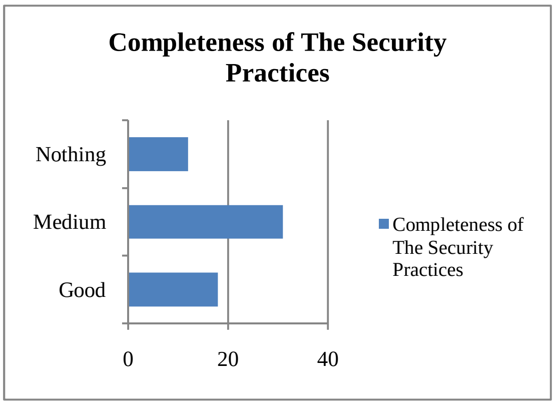

Figure 4 Completeness of the overall security practices

Figure 3 above illustrates the overall completeness of the security of current practices in companies where the number of octave recommended security practices are 15. As figure 4 below illustrates the completeness of the currently security practices priorities in the company.

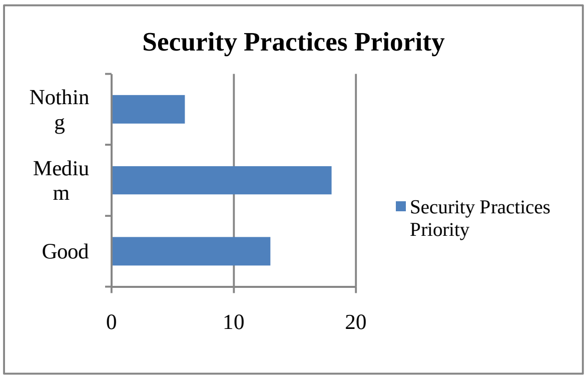

Figure 5 Security practices priority

Table 2 Threat That Apear in The Company Link to Priorities of Security Aspect

ASPECT	THREAT
Security training and awareness.	1. Organization does not make security awareness training to new staff as activities to do. 2. Lack of corporate information security policy documentation. 3. Employees do not understand the responsibility and security policy. 4. Employees still like to share usernames and passwords.
Security policy and regulation.	5. Organizations do not pay attention to updating the document, the policy. 6. Lack of the process documentation to evaluate and ensure compliance with security policies, laws and rules of use, and assurance requirements.
Network and system management.	7. The absence of documentation and test plans keamanaan to maintain systems and networks. 8. Tools and mechanisms for security and network administration system is used, rarely be regularly reviewed and updated or replaced even though it is not feasible to use.

Table 2 above describes the threat that exist in the company, it is linked to the aspect priorities of security practices, the threats are taken from the items that cannot be fullfil by the company, beside the items get from the 15 OCTAVE-S security practices. When the threats that exist in the company is taken, then the next step is to develop mitigation of risk. Lack of OCTAVE-S is when the company risk mitigation makes its own desire of the person whose doing the analysis based on that reason ISO / EIC 27001 that is used as a control standard and it is recognized as International best practices in formulating risk mitigation for the company.

Table 3 Threat That Apear in The Company Link to The ISO 27001 Controls

THREAT	ISO 27001/2005 CONTROLS
1. Organization does not make security awareness training to new staff as activities to do.	1. All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.(A.8.2.2)
2. Lack of corporate information security policy documentation.	2. Operating procedures shall be documented, maintained, and made available to all users who need them. (A.10.1.1)
3. Employees do not understand the responsibility and security policy.	3. Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy. (A.8.1.1).
4. Employees still like to share usernames and passwords.	4. Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. (A.8.2.1) 5. There shall be a formal disciplinary process for employees who have committed a security breach. (A.8.2.3) 6. The allocation of passwords shall be controlled through a formal management process. (A.11.2.3). 7. Manajemen harus meninjau hak akses pengguna secara teratur yang menggunakan proses formal. 8. Users shall be required to follow good security practices in the selection and use of passwords. (A.11.3.1)

5. Organizations do not pay attention to updating the document, the policy.	9. There shall be a formal disciplinary process for employees who have committed a security breach. (A.8.2.3) 10. Operating procedures shall be documented, maintained, and made available to all users who need them. (A.10.1.1)
6. Lack of the process documentation to evaluate and ensure compliance with security policies, laws and rules of use, and assurance requirements.	11. The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. (A.5.1.2)
7. The absence of documentation and test plans keamanaan to maintain systems and networks.	8. Operating procedures shall be documented, maintained, and made available to all users who need them. (A.10.1.1)
8. Tools and mechanisms for security and network administration system is used, rarely be regularly reviewed and updated or replaced even though it is not feasible to use.	9. Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. (A.10.6.1) 10. Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. (A.10.6.2)

Table 4 above describe the controls of threat that was identified in the table 3, the controls is from the ISO 27001 control and objective. In order to align between threat and the control, they should be aligned with the ISO 27001 objective as well.

CONCLUSION

From the results of analysis and research, there are few things could be drawn from the use of the OCTAVE-S as a baseline to evaluate the risk and ISO 27001 that used as a control for the threats of the selected security aspects of information system: (1) By evaluating the company’s risk using the OCTAVE-S then the company can map the risks and weaknesses of corporate information systems. (2) With risk management information system the company can find out how big the impact of risks, threats and weaknesses that appear on the company's business continuity. (3) The level of risk management of the company currently is known.

By using the existing controls in ISO 27001, it is expected to assist companies in making preparations to implement the ISO standard, especially for corporate information technology division.

REFERENCES

Alberts, C., Dorofee, A., Stevens, J., Woody, C. (2005). OCTAVE®-S Implementation Guide, Version 1.0. USA: Carnegie Mellon University.

Backhouse, J., Hsu, C. W., Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. MIS Quarterly , 413-438.

Barlette, Y. (2006). Les comportements sécuritares des acteurs dans les systémes d'information des pme. Université de Montpellier I .

Bornman, W., Labuschagne, L. (2004). A Comparative framework for evaluating information security risk management methods. Standard Bank Academy for Information Technology.

Coleman, J. (2004). Assessing Information Security Risk in Healthcare Organizations of Different Scale. Proceedings of the 18th International Congress and Exhibition, 125-130, Elsevier.

ENISA. (2006). Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. USA: ENISA.

Humfreys, T. (2005). State-of-the-art information security management system with ISO/IEC 27001:2005. ISO Management Systems, 15-18.

ISO, & EIC. (2005). International Standard, Information Technology - Security Techniques - Information Security Management System - Requirements. London: British Standard Institution.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal, IV, 60-66.

Stoneburner, G., Goguen, A., Feringa, A. (2002). Risk Management Guide for Information Technology Systems. USA: National Institute of Standards and Technology.