Information Technology Risk Measurement: Octave-S Method

Rudy M. Harahap

Abstract - The purpose of this research are to identify the risk of IT in the company and make some recommendation to solve any risk happened in the company, and also to give the reference in measure the risk of IT in the company. Research Method used are book studies, field studies, and analysis techniques. Book studies by collecting the information from books and journal. Then, for field studies, it done by interview, and observation to the company. Analysis techniques done by qualitative approach and using the Octave-S (Operational Threat Asset and Vulnerability Evaluation) – S as the method to measure the risk of IT in the company. The result of this research will be a description of Information Technology in the company and give any risk happened in IT and mitigation activity through the risk in the company. Conclusion of the research are looking for three critical areas, such the awareness and security training, security strategy, security management, and disaster recovery.

Index Terms - Risk Management, Information Technology, Octave-S method

1. Introduction

In this globalization area, IT roles become an important things in developing of business area especially for the company performance. Using IT in the company will help the company to get the valid information and help the management to make a right decision. Many company didn't realize the risk happened because of IT implementation in the company, so company have to take some action to control the risk happened that causing any loss of the company.

According to Papaioannou [8], measuring the risk can help the company to reduce the vulnerability which affected the profit margin. There's some principles in taking the best decision on risk management, first it need to identified the type or exchange rate risk , then develop the exchange rate risk management strategy, creation a centralized entity in the firm's treasure to deal with the practical aspects of the execution of exchange rate, next develop a set of control to monitor a firm's exchange rate risk and last to establish a risk oversight committee. In managing currency risk, company utilize a different hedging strategies depends on the specific type of currency risk.

This research will be in the TIS. Ltd, which in this company still many risk happened and to control it, we use the Octave-S method to measure any risk happened and give some recommendation as a problem solving.

2. Research Method

To achieve the purpose of the company, this research will used book studies, field studies, and analysis techniques. In the book studies, collecting information from literature books and journal. Then for field studies done by interview to the IT department in the company about data IT in the company according to the question about the Octave S method and done by observation directly to the company. Last, for analysis techniques done by using the qualitative approach and based on Octave-S method to measure the risk in the company which divided into three phases, such determine the threat profile according to the asset, identify the employee infrastructure, and develop the security strategy and planning.

3. Literature Review

According to Anghelache et al. [2], operational risk as a direct or indirect risk that resulted from the inadequate internal process, people, and system from external area, and it also become a risk of income, direct loss that connect to the important error or illegal behavior because the error of system and process inadequation and it can be interpreted as a vulnerability of financial institution and need to be eliminate though an increased control.

According to Moteff [6], risk assessment will involve the integration of threat, and vulnerability but it also will involve on deciding which measure will take the based on risk reduction strategy. To assess risk it implies uncertain consequences, the impact can be categorized in number of ways. The impact or consequence may be measured more accurately at the point of process.

According to Nekrasov, et.all [7], risk measurement is the most difficult single task in valuation of security, it is done to estimate the risk from return and obtain an expected discount payoff. Value in risk are created by the operating, investing, an financing activities, and directed link to the process.To validate a risk measures result, it can be done in a different approach. First, it have to emphasized the price level creation to evaluate the method by compared it with the observed price. Second, to assess the accuracy of average value estimate, it have to examine the relation between the fundamental based and the cost of equity by the current price. Third, it have to evaluate the realibility of alternative to implied the cost of equity by examine the association with know proxies from several information.

According to Branger and Schlag [3], model risk consider to the case where it need to be increased the uncertainty continuosly and it also arises when there are a class of model but not which model from this class is the true one. Solving the problem of model risk done by going the data in order to identify the process. Some probability distribution according the model risk. First, model risk seem to be quite similar to the market incompleteness that didn't include the model risk, the number of risk factor just too high relative to the number of linearly. Model risk also didn't imply if the candidate model are incomplete. It is important to clear the notation about the risk measures. First, risk measure in case of model risk that used to measure overall amount,

Second, there are model risk measure that capture the risk model itself.

According to Chang et al. [4], managing the portfolio risk are necessary to be a concept of risk management and it is important to consider what the consequences of risk were not well managed. Risk is an essentially standard deviation of return on asset portfolio. To have a risk measure, it need some improvement of the risk management model that will qualify the risk on the moneter scale,large losis, and encourage diversification.

On this measurement, we will use the Octave-S approach. According to Alberts et al. [1], Octave is an approach who will manage the risk of information system and it presents an interview of the approach that developed in the Software engineering Institute (SEI).Octave targeted at organizational risk and focused on strategic, it also driven by two of aspect : operational risk and security practice. The main keys of Octave approach are:

- Identify information related to assets that are important to the organization
- Focus risk analysis activities on those asset judged to be the most critical to organization
- Consider the relationship among the critical assets.
- Evaluate risk in the operational context.
- Create a practice based on protections strategy of organization.

There are three phases in octave, first build asset-based threat profiles, second identify infrastructure vulnerabilities, last to develop security strategy and plan. Octave-S requires some knowledge of an actor and it interest to see the type of data should be collecting to establish a reasonably measurement of security risk. Some of Octave-S materials such:

- Volume 1 : introduction to Octave-S. it provide a basic description of Octave-S
- Volume 2: preparation guidelines- - contain a background to conduct the Octave-S
- Volume 3: Method guidelines – includes detailed guidance of every activity
- Volume 4: Organizational worksheet – contains all worksheet in the company
- Volume 5: Critical Asset worksheet for information –provide worksheet to document related to critical asset
- Volume 6: Critical Asset Worksheets for Systems –provides worksheets to document related to critical assets categorized as systems.
- Volume 7: Critical Asset Worksheets for Applications –provides worksheets to document related to critical assets categorized as applications.
- Volume 8: Critical Asset Worksheets for People –provides worksheets to document related to critical assets categorized as people.
- Volume 9: Strategy and Plans Worksheets –contains worksheets to record the current and desired strategy and the risk mitigation plans.
- Volume 10: Example Scenario –contains a detailed scenario illustrating a completed set of worksheets.

According to Panda [5], Octave approach is one of the framework that enables to understand, assess and get their information of security risk perspective. Octave will help the organization to: (1) develop qualitative risk evaluation criteria based on operational risk tolerance, (2) identify assets that are critical to the mission of organization (3) Identify vulnerabilities and threats to the critical assets, (4) Determine and evaluate potential consequences to the organisation if threats are realized, and (5) Initiate corrective actions to mitigate risks and create practice-based protection strategy.

4. Risk management in the company

Implementation of Information Technology in the company will support the business process in the company, but there's still any problem happened where the company haven't do the risk management of the company since they implement the IT into the system. So the company needs to measure the risk to know how far the risk will impact to the business process of the company. Information Technology Risk measurement will use the Octave-S (the Operational Critical Threat Asset and Vulnerability Evaluation –S). Octave S is a various approach that develop to company needed in the smaller scope.

Criteria Evaluation was the first step done by the company to determine the level of impact in every criteria where this research just took 3 criteria, such : First, Reputation / customer trustworthy , in this criteria there will be three levels of impact, such low, medium, and high impact. Customer gets a little loss and didn't need any changing of loss that customer receive. Second, Financial. There's three impact from the financial criteria, such operational and revenue losing cost, in this criteria, there will be operational and revenue losing cost which if the operational cost increase less than 2%, so it will low impact, then if the operational cost increase from 2%-15% , it will in medium impact, and if the operational cost increase more than 15% it will cause high impact. Risk of using the Information Technology will cause the revenue losing, it will be low impact if the loss less than 5% in a year, then will be in medium impact if the los 5%-20% a year, and will be high impact if the los more than 20% per year. Third, Productivity, this thing seen from the working hour of every employee, which if the working hour increase less than 10% for 2 days, it will be a low impact, then if it increase between 10%-30% in 2 days, it will be a medium impact, and last id it increase more than 30% for 2 days, it will show the high impact.

Asset Identification was the second step on this Octave-S framework. This step will identify the information system application and service in the supply IS, and also to identify the importance persons in the company who has a skill and knowledge. System, Information, Service, and asset that related to the supply process. System will the system using in the process, information about the product stock, Application and service about database application using SQL 2005, and the other asset related to the system such Delivery Order form, Invoice form, and Stock Report. Then for person will be the employee who has any skill and special knowledge that will be difficult to replace.

Security Practice was the last step on Octave-S framework. It identified into 15 aspects of security practices to evaluate how far the security practice has been implemented into the company. It will assess in three colors, Red when

the company didn't do anything in security practices. Yellow when the company rarely did the security steps and need to improve the effort of the company, and green when the company did well the security steps and didn't need any improvement.

Choosing the critical asset could be the step of Octave-S needs to be identified by the company. According to the scope of research, it necessary to know the total of product stock. User from this system are logistic and finance department, and to maintain the system will give to the IT staff. The other asset related to this system : Information, the information needed are master product, initial product cost, sales production cost with FIFO method, the other aseet will be a computer and LAN network.

5. Conclusion

From this research we can took some conclusion about the risk happened in the IT from the critical areas:

- Awareness and security training. In this area, company hasn't prepare the security awareness training to the employee related to the information system supply in the company and will done in periodically.
- Security strategy, this company didn't know and understand how the strategy and security procedure will be in the IT department to the IS supply because there's no time to make any procedure .
- Security Management. In this area, procedure to take care all the company with the IT hasn't been documentation so it need more activity to reduce it in the security management
- Disaster recovery. Company didn't have any plan about the disaster happen, and it caused if it happened will give a big loss to the company.

Reference

[1] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," PA 15213-3890, Carnegie Mellon Institute, Aug. 2003, from: http://www.itgovernanceusa.com/files/Octave.pdf

[2] G. Anghelache, A. O. Puiu, and A. Radu, "Operational Risk Measurement," in *European Research Studies*, vol 13, iss. 1, XIII, Issue (1), pp 215-223.

[3] N. Branger and C. Schlag, "Model Risk: A Conceptual Framework for Risk Measurement and Hedging," Working Paper, Jan. 15, 2004 from: http://www.finance.uni-frankfurt.de/wp/685.pdf

[4] K. J. Chang, C. Lin, and T. Zhu, "Risk Measurement and Management," Student Project, from http://www.stat.berkeley.edu/~aldous/157/Old_Projects/chang_lin_zhu.pdf

[5] P. Panda, "The OCTAVE® Approach to Information Security Risk Assessment," *ISACA Journal*, vol. 4, pp 37-41, Aug. 2009, from http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Pages/The-OCTAVE-Approach-to-Information-Security-Risk-Assessment1.aspx.

[6] J. Moteff, "Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences," CRS Report for Congress Order Code RL32561, Sep. 2, 2004, from: http://www.fas.org/sgp/crs/RL32561.pdf.

[7] A. Nekrasov and P. K. Shroff, "Fundamentals-Based Risk Measurement in Valuation" in *The Accounting Review*, vol. 84, no. 6, pp. 1983–2011.

[8] M. G. Papaioannou, "Exchange Rate Risk Measurement and Management: Issues and Approaches for Firms," in South-Eastern Europe Journal of Economics, vol. 2, pp. 129-146.