International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

The Designing of Measurement Instrument for Information Technology Risk Assessment as a Risk Management Strategy Recommendation at SBUPE Bandung

Yudi Priyadi[1], Suhardi[2]

[1]Departement of Telecommunication and Informatics Business Management,
School of Business and Economics, Telkom University, Bandung 40257, Indonesia

[2]School of Electrical Engineering and Informatics, Bandung Institute of Technology Bandung, Indonesia

Abstract: ***Portal Express Strategic Business Unit, furthermore called SBUPE. In carry out its services, SBUPE is using Barcode at tracing and tracking system to identify and as media in data storage relate to delivered packets. Barcode is using to track and trace system at SBUPE, is used in logistic and currier services. So that obtained features at Barcode, also has adopted to that unit work pattern. SBUPE is faced to local courier service competition with global companies, which had successful to use goods shipment tracing technology with calculate the risk from its services treatment application. Until now, the track and trace system at SBUPE is not having instrument to do an information technology risk management, that is conducted process by IT managers to adjust operational activity and finance cost spending, in reach the profit with protect the IT system and data which support its organization mission. In this report has carried out a designing as tool, for provide a recommendation at that unit management level with to do risk mitigation, is directed to an incident handling. SBUPE can be applied the strategy based four quadrant that are: to do risk transfer to other (quadrant IV), to avoid a risk (quadrant III), to less negative effect of risk (quadrant II), to receive some or all of risk consequences (quadrant I). From designing results, has suggested doing incident handling process and information technology audit, in based data sources of reconciliation result among written documentation with situation when field study, as condition validity to do risk mitigation strategy.***

Keywords: Information Technology Risk Management (ITRM), Risk Mitigation, Risk Assesment, Audit.

1. Introduction

Information technology roles in business world is having important role for a company and its business managers. In strategic decision-making, information technology will affect the operational continuity, where it will be bring changes to that organization. The company and its manager are not having the same way to face an information technology risk. First difference, that risks are not considered openly. Second, just some tools or instruments to handle of appeared risk. Third, processes are obtained in organization has not reacted toward risk. [3].

In general, to prepare a safeguard toward every threat possibility, it is not economically activity. Therefore, an IT security programme, must be provided a process to estimate threat and to decision the choice would be made, what to choice or ignore a threat or to give reduction its safeguard. Its control measure installation based on a balance among cost of control and necessary to reduce or to lose a threats. Basically, as risk analysis is a risk-management approach, to help to identify a threat and to choice a security measure criteria which has resulted cost-effective. [12].

Using a centralized data table, have contents data reference and estimating technique, with some key variables to do determining risk and its loss, it can be used of management in security improvement. The assessment method for tangible and intangible assets will help to measure an information security, by to do risk calculating and measurement is using quantitatively risk analysis. [1].

Postal service industry (postal service, including courier service, express delivery, financial, and logistic) is a business will never loss a player, even continue to increase in along with economic growing. Delivering service business which has conducted by players in post service industry is very prospective due to its very wide scope, unlimited to specific commodity only. Logistic and courier services are needed to support trading and industry sectors activity, mainly for document and goods delivering. The necessary toward logistic and courier service is linear proportionate to industry growing. At present, logistic market potential in Indonesia is reaching 10% from gross national product. [14].

In according to Vice-president the Indonesia Express Service Company Association of West Java, just in Bandung the average courier operator number is growing about 5%-10%. [15]. Following the document of Universal Postal Union (UPU, World Post Organization), the number of letter volume increasing in 1995 to 2000 in Asia Pacific about 1.4%, while the growing among 2000 to 2005 has estimated about 4.1% [16]. In communication market case in physically letter, communication service for domestic scope is still dominated by government post operator. But, otherwise for international market or across nation, at present a communication service in physically letter has dominated by private operator (70%) [17]. Therefore, government post

service ability to maintain its market share toward that competition condition is very important.

This complexity emerge is not business uniformity only, but also because some business kinds that is embraced have different characteristics. For example, in communication service field, PT. Portalindo has faced with competitor as Titipan Kilat, Pandu Siwi Sentosa and other local couriers or world class companies as DHL, TNT, FedEx and UPS, had successful to use a good shipment technology tracing and tracking with calculate risk from that service application. Pos Express strategy Business Unit, furthermore called SBUPE. In carry out its services, SBUPE is using Barcode at tracing and tracking system to identify and as media in data storage relate to delivered packets. Barcode is using to track and trace system at SBUPE, is used in logistic and currier services. So that obtained features at Barcode, also has adopted to that unit work pattern. Until now, the track and trace system at SBUPE is not having instrument to do risk management, that is conducted process by IT managers for adjust operational activity and finance cost spending, in reach the profit with protect the IT system and data which support its organization mission.

2. Literature Review

2.1 Risk Management of Information technology

Risk management is conducted process by IT managers for adjust operational activity and finance cost spending; in reach the profit with protect the IT system and data which support its organization mission. [2]. Risk management is covering three processes, which are: Risk Assessment, Risk Mitigation, and Evaluation and Assessment.

Risk assessment is first process in risk management methodology. Organization is using risk assessment to determine potential threat and risk levels related with an IT system whole it's SDLC (System Development Life Cycle). This process output is helping to appropriated control identify direction to decrease or lose a risk as long as risk mitigation process. To determine the possibility a bad event in future, threats on IT system must be analyzed in together with potential vulnerability and control in place for IT system.

Generally, to lose the all of risks at scenario may be is not conducted, this case is responsibility to senior managements and their functional and business managers to use least-cost, to make an approach and apply more appropriate control to organization mission, so that its impact can be accepted or adjusted with organization human resources and its mission. Risk mitigation is used systematic methodology by senior managers to reduce risk from has been made mission. This thing can be reached by some choices, as Risk Assumption, Risk Avoidance, Risk Limitation, Risk Planning, Research and Acknowledgement, Risk Transference. The objective and mission of an organization has to balance in to choice whatever risk mitigations. If difficulty is occur to know the all risk, then priority must be given to threat and vulnerability which is having potential impact to mission. This thing, also conducted to protect an organization mission and its IT system, because every situation/surrounding and organization object, have uniqueness, used choice to reduce a risk and its implementation method can be adjusted.

2.2 Qualitative Risk Analysis

The measure of risk derived from combination among exposure rating, vulnerability level, and safeguard affectivity level. Simply, qualitatively risk measurement has conducted with give the high, medium and low scales. Risk measurement with that scale is having the shortage, which is high valued for risk with exposure, vulnerability, and safeguard, will have same results with risk to exposure, vulnerability, and safeguard in low valued. Therefore, to risk measurement level has given five scales that are: [8]

- High = 5
- Moderately high = 4
- Medium = 3
- Low = 2
- Very low = 1.

Safeguard is using to identify mechanism, service, or procedure can to prevent or reduce threat occurs which can exposure vulnerability. Functionally, safeguard related with confidentiality, integrity, and available areas. Safeguard level is measured based for categories that are: [8]

- Level 3 = high, if possibility a vulnerability had exposure by threat, with high can be reduced.
- Level 2 = medium, if possibility a vulnerability had exposure by threat, can be reduced moderately
- Level 1 = low, if possibility a vulnerability had exposure by threat, it can be a little reduced only.
- Level 0 = none, nothing safeguard

2.3 Quantitative Risk Analysis

The steps to do quantitative risk analysis as follow. [1]

1. Risk estimating study is doing to determine risk factors.
2. Based risk factors in above, determine a value from which have asset risk (Tangible and Intangible Assets).
3. Determine an approach based available procedure at company, in report of loss when to do security assessment in company. As its reference, can to use a data about ownership information in making adjustment from quantitatively estimating for risk analysis.
4. Estimating of Annualized rate of Occurrence (ARO) for every risk factor.
5. Determine necessary countermeasures to anticipate each risk factors.
6. Determine Annualized Loss Expectancy (ALE) to every risk factor. With note that: ARO for ALE after countermeasures implementations, have possibility is not always equal with zero.
7. To do analysis safeguard cost-benefit with calculate difference among ALE, before apply of countermeasures with ALE after apply of countermeasures.
8. Based analysis on f and g steps, determine Return On Investment with use Internal rate of Return (IRR). To explanation IRR, can be seen at subchapter about quantitatively risk analysis counting.

9. The result is a brief serve at management for review. Used methodology can be same with request characteristic to engineering project capital.

3. Risk Analysis of Information Technology

From some manners could be used to analysis of risk, two basic methods can be applied to SBUPE, that are qualitatively and quantitatively evaluations. Qualitatively evaluation is conducted based intuition, so that risk analysis approach is conducted very subjective, relatively. This method is not resulted the measurement which can be to calculate the bigger specification of its impact, therefore making cost benefit analysis about control recommendation is difficult to apply. So this basic method is needed much, for initial step of quantitatively risk analysis.

Together with this, is serving a conducted flow at SBUPE organization to know qualitatively risk level.

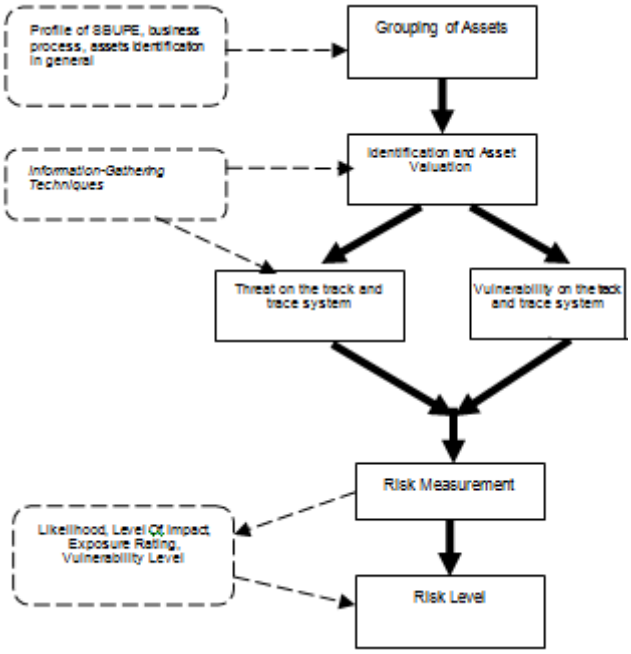

Figure 1: Flow of Qualitative Method Application

To do quantitatively risk analysis, it is need to determine a potential losses value with postponed process, property damage, or data. Then, it is also need carried out the estimating of occurrence possibility form risk failure, so that eventually it can be calculated the annual loss estimating. [10].

Study about identification, valuation asset (subjectively), threat, and vulnerability assessment has conducted at qualitatively risk analysis procedure. Further, at quantitative procedure has conducted the counting which dealt to cost-benefit analysis with use value like a currency unit bigger.

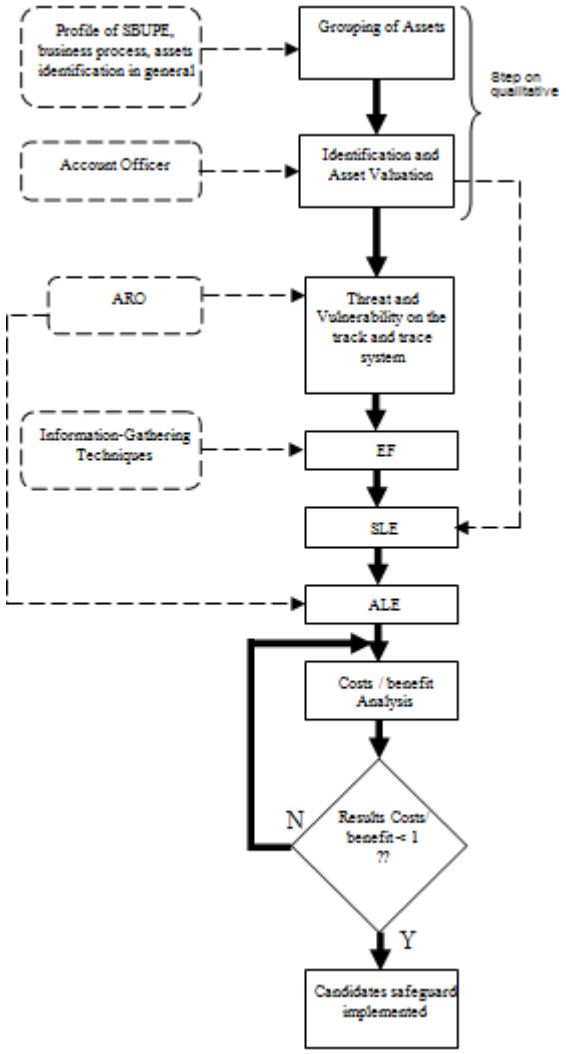

Figure 2: Flow of Quantitative Method Application

4. Risk Mitigation Strategy

The SBUPE purpose and mission must be considered to choice whatever risk mitigation. If difficulty is happened to know the all of risks, so priority must be given to threat and vulnerability is having impact on mission. This case, also conducted in safeguard an organization mission and its IT system, because an organization object and situation/surrounding, have uniqueness, used choice to reduce risk and its implementation method can be adjusted.

In this report has conducted a designing like a tool, to serve recommendation to that unit management level with to do risk mitigation, dealt to incident handling.

4.1 Instrument Designing Flow

In this instrument plan making, has conducted of asset classifying related directly to Track and Trace system operational at SBUPE, which has resulted some tables of asset. To this asset classifying its data derived from field study and Service regulation documents about accountancy which had become tangible asset by that unit. Then, has conducted quantitatively and qualitatively risk analysis constituted risk evaluation activity part. The result of this plan is as template of format could be created for risk

management strategy supporting recommendation. While for its plan testing, this report is serving the suggested for its test steps that is with adopted audit methodology at CISA Review Manual.

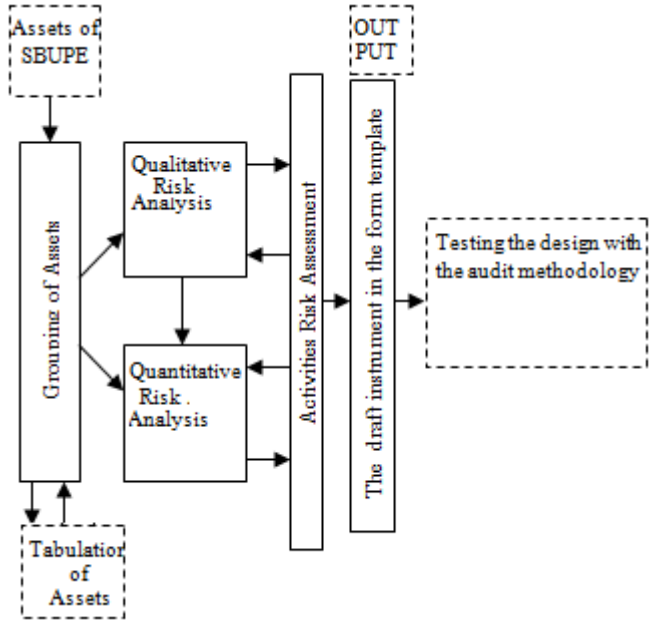

Figure 3: Flow of Designing Process

4.2 Risk Mitigation Strategy at SBUPE

SBUPE can be applied a strategy based four quadrants as follows:

- To do risk transfer to others (Quadrant IV) that is to move risk with use a choice, to replace a loss, as insurance purchase.
- To avoid a risk (Quadrant III) that is to avoid a risk with to making lose risk cause and its consequence. For example, to cancel specific function at system and to close its system, when obtained known risk.
- To decrease negative effect from risk (quadrant II) that is to organize risk with develops a risk mitigation plan, its implementation is prioritized and control in it's maintained.
- To accept a part or all of risk consequences (Quadrant I) that is to accept risk potential and to continue IT system operational or to apply a control to reduce a risk to be acceptable risk.

Together with this is tabulation (Table 1) from risk mitigation strategy with to do classifying based that four quadrants above.

Table 1: Risk Mitigation Strategy

NO	RISK		QUADRANT
	THREAT	VULNERABILITY	
1	Unauthorized access	No implementation of reconciliation financial at any operational units that relate directly between the receipt with accounting process	III
2	Malicious code (virus, logic bomb, Trojan horse)	Antivirus that have been installed on the computer, not be updated or renewed for version of the latest database	II
3	Administration failure	Insights into the development of courier services are not performed on all personnel	II
4	Fraudulent act (replay, impersonation, interception)	The procedures are not able to anticipate the current conditions that occur in the organization.	II
5	Fraud and theft	The lack of sustainability and its revisions to the guidelines documentation	III
6	Computer abuse	Standard operating procedure is not implemented or procedures can not anticipate the current conditions that occur in the APE.	II
7	Theft of laptop/PC	For general strategic location in carrying out operational functions, is not equipped with a TV camera for monitoring.	II
8	Unauthorized system access (access to classified, proprietary, and/or technology-related information)	This unit does not have specialized personnel who handle technical issues of hardware / software / networking, is still handled by the IT division Portal building Bandung	II
9	Earthquake	Cooperation with the insurance that exist in this unit, not refurbished / no cover for the current resource conditions.	IV
10	Client/ server failure	The procedures and results of the procurement decision is not in accordance with operational requirements specifications	I
11	Power failure	UPS which is already installed on this unit, maintenance is not carried out.	I

4.3 Plan Testing Suggest

In this report, to its plan testing stage has served in a steps suggest would be conducted to do audit, based a standard methodology from CobiT. [13].

Audit process must be planned prior before it is applied. Audit planning has to clearly to explain the audit purpose, auditor authority, presence top-management approval, and audit method.

Based audit methodology as Control Objectives for Information and related Technology (CobiT), so to occur condition at SBUPE can adopt audit steps as in Table 2.

Table 2: Plan Testing Risk Management Strategy at SBUPE

No.	Audit phase	Description
1.	Audit subject	The results of designing of measurement instrument for information technology risk assessment as a risk management strategy recommendation at SBUPE
2.	Audit objective	Make adjustments recommendations design with the condition that occurs in SBUPE
3.	Audit scope	Risk management strategies undertaken by SBUPE based on the draft recommendations made
4.	Pre audit planning	•Identify assets SBUPE directly involved with the system design that

		will be audited •Human resources directly involved is the employees SBUPE, while the auditors from the unit of internal control •The necessary document: operational guidelines, accounting reports •Location audited is SBUPE to track and trace system on the package
5.	Audit procedures and steps for data gathering	•Reconcile with the unit that does bookkeeping accounting and administrative operations •Interviews conducted in sub unit Processing, Account Office, Supervisor, and Branch Manager
6.	Evaluation of the test results and examination	Evaluation of the specifically that occurs in SBUPE
7.	Communication procedures with the management	Procedures of the specifically that occurs in SBUPE
8.	Audit report preparation	•Determine how to review the audit results •Evaluation of the validity documents, procedure, and policies of organization audited

5. Conclusion

Based written discussion at this report, so has obtained some conclusions as follow:

- In this instrument plan making, has conducted asset classifying related directly with Track and Trace system operational, so that it is resulted some tables of asset, had become as reference to do risk assessment.
- To classifying that asset above, its data derived from field study and organization regulation documentation, where it is needed to do qualitatively and quantitatively risk analysis, with result a occur safeguard at SBUPE to cost benefit analysis table.
- The result of plan to risk mitigation as format template to be recommendation in carry out of risk reducing, with divide to be four quadrant, so that threat and vulnerability classifying in carry out a risk mitigation strategy to be directed.
- While for plan testing, this report has served suggest as steps, with adopt audit methodology from COBIT (Control Objectives for Information and related technology) at CISA Review Manual.

6. Development Suggest

Based discussion and conclusion, it is obtained some necessary suggest in its development as follows:

- In furthermore research, has conducted the review to do incident handling process.
- In furthermore research, has conducted implementation to do information technology audit based Control Objectives for Information and related technology.
- It is needed data sources of reconciliation result among written documentation with situation when field study.
- To make software application with reference a database can be used by company in generally, in to do risk management strategy.

References

[1] Ding Tan, "Quantitative Risk Analysis Step-By-Step", December 2002 SANS Institute 2003.
[2] G. Stoneburner, A. Goguen and A. Feringa, "Risk Management Guide for Information Technology System", Recommedation of National Institute of Standards and Technology Special Publication 800-30, July, 2002.
[3] Ernie Jordan and Luke Silcock, "Beating IT Risks", 2005 Published in 2005 by John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester.
[4] C.Alberts, A.Dorofee, "Managing Information Security Risks: The Octavesm Approach", Addison Wesley, USA, July 09, 2002.
[5] Turban Efraim, McLean Ephraim, and Wetherbe James, "Information Technology for Management: transforming organizations in the digital economy", John Wiley & Sons, Inc., 4th Edition, 2004.
[6] Marchewka Jack T. "IT Project Management: providing measurable organizational value" Published by John Wiley & Sons Ltd, 2003.
[7] Muhammad Mahreza Maulana, Suhono Harso Supangkat, "Pemodelan Framework Manajemen Resiko Teknologi Informasi Untuk Perusahaan Di Negara Berkembang", Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia 3-4 Mei 2006, Institut Teknologi Bandung.
[8] Muhlis Muhamad, Suhardi (Pembimbing T.A.), "Analisis Resiko Keamanan Jaringan Voip dengan Metode Kualitatif dan Kuantitatif", Laporan Tugas Akhir, STEI-ITB, 2007.
[9] ____(2005), Information Technology Security Risk Management (ITS-RM) Program, University of Virginia, URL:http://www.itc.virginia.edu/security/ riskmanagement (15 Agustus 2007).
[10] Miller, Jean. "Risk Management for Your Web Site." International Risk Management Institute Expert Commentary, September 2000. URL: http:// www. irmi.com/ expert/ articles/ schoenfeld003.asp (1 November 2007).
[11] Indriantoro Nur, "Metodologi penelitian bisnis", edisi pertama, 1999, BPFE Yogyakarta.
[12] Hiles, A., "Enterprise Risk Assessment and Business Impact Analysis", Rothstein Assoc., 2002.
[13] CISA Review Manual, Information Systems Audit & Control Association, 2002, http://www.isaca.org/ ContentManagement/, diakses tanggal 31 Januari 2008.
[14] Investor Daily (2007). Berebut Bisnis Kargo Rp 330 Triliun. Investor Daily, edisi 14 Maret 2007.
[15] Kompas (2006), "Peluang Bisnis Kurir Masih Menjanjikan", www.kompas.com/ kompas-cetak/0605/18/Jabar/, diakses tanggal 2 Agustus 2007.
[16] Universal Postal Union (2003). The Postal Industry at October 2002. Universal Postal Union (UPU), Berne.

[17] Universal Postal Union (2002). The Postal Market in the Age of Globalization. Universal Postal Union (UPU), Berne.
[18] Dowson, John M., Edward E. Horgan and T. Wood Parker (1997). Postal Performance: The Transformation of A Global Industry. Coopers & Lybrand L.L.P., Arlington.
[19] Wikimedia Foundation, Inc (2007), Information Security, url=(0038), http://en. wikipedia.org/wiki/ CIA_triad, (15 Agustus 2007).
[20] _____(2007). Petunjuk Pelaksanaan Layanan Portal Express, Strategic Business Portal Express, PT Portalindo (Persero).
[21] _____(2007). Peraturan Dinas No.6 (Akuntansi), Strategic Business Portal Express, PT Portalindo (Persero).

Author Profile

Yudi Priyadi. Currently active as a lecturer at Departement of Telecommunication and Informatics Business Management, Telkom University. He has competence of teaching and practitioners in the field of data management, WEB development, information system modeling, multimedia action script, information technology risk management.

Dr. Ing. Ir. Suhardi. Currently working at School of Electrical Engineering and Informatics, Bandung Institute of Technology Bandung, Indonesia.