RISK MANAGEMENT FRAMEWORK AND SECURITY READINESS IN INFORMATION AND COMMUNICATION TECHNOLOGY OF PUBLIC ORGANIZATIONS IN THAILAND

Yuthtapon Pichainarong

Project Office for Consortium on Doctor of Philosophy Programs, Phrai .non Rajabhat University,Bangkhen Bangkok, Thailand

E-mail: yuthtapon@dede.go.th

Prasong Praneetpolgrang

Master of Science program in Information Technology, Graduate School, Sripatum University, 61 Phaholyothin Rd, Jatujak, Bangkok, Thailand

E-mail: prasong.pr@spu.ac.th

Abstract

The objectives of this research was 1) to study security readiness in ICT of public organizations. 2) to study risk impacts level and likelihood in ICT. 3) to study relationship between risk impacts level and likelihood in ICT. 4) to propose risk management framework and to modify ICT security management framework in public organizations based on ISO 17799 / ISO 27001, ITIL and COBIT, as well as OCTAVE to set evaluation risk. The researcher study from 20 ministries. The research methodologies were both qualitative and quantitative research. The qualitative is represented by content analysis from documents, literature review and interviews CIOs Also, the quantitative is represented by data collected in analyzing from questionnaires.

The research discovery that risk impacts level and likelihood in management of ICT is in the middle-level but the potential impacts of less of all 4 categories, which are computer network systems, database management, information project systems, management and planning, are risk impacts in the high-level. The research also discovery that the overall security readiness of public organizations is risk likelihood in the middle-level which the cofactor like Human resources, equipments, management, vision and environment that also have the effect to the risk and security readiness in ICT.

Index Terms– Risk Management, Security, ICT

1. Introduction

Currently, ICT becomes important for an organization in many aspects including management, information collection, and operating evaluation especially for computer network systems, database system, information project systems and managing and planning as well as information systems. The functions in an organization are more efficient and effective by implementing ICT. However, there are some risks associated with the ICT management and security which lead to the mistakes, slow processes, information loss or leak out, undesirable consequences, failure, and the damage to the relevant sections as well.

As mention earlier, I realize the significant of information technology management and the risk assessment particular in public organizations. The reasons behind that are because the computer network, information database management, project system development, and also managing and planning in the public organization need to be monitored and controlled. To make sure that all information and assets are secure, it is necessary to design the problem prevention as well as find the solutions for both weaknesses and threats which can affect the ICT implementation in the public organization. Hence, Researcher would like to study the *"Risk Assessment."* for controlling the risks resulted from ICT to be acceptable and manageable.

2. Research Objectives

1) To study the security readiness in information and communication technologies (ICT) of Thai public organizations

2) To Analysis the risk assessment for risk impacts level and likelihood in information and communication technologies (ICT) of Thai public organizations.

3) To investigate the relation between risk impacts level and likelihood in information and communication technologies (ICT) of Thai public organizations.

4) To propose ICT risk management framework in Thai public organizations.

3. Theories and Related Research

3.1 Risk Management

Risk can be defined as "the threat or likelihood that an action or event, will adversely or beneficially affect an organization's ability to achieve its objectives"

3.1.1 Risk Analysis

There are three main elements for risk analysis. The first one is *Risk Impact* which is consideration about how the risks of deficiency have impact on the organization. The second element is *Problem*. The risk of a problem can be ranked from 0 to 1 depending on the likelihood of occurrences of the problem. The last one is *Risk Control*, the capability to control the risk, such as the protection from computer virus.

3.1.2 Risk Assessment

I would like to apply the seven steps of OCTAVE methods of risk assessment for this research including: 1) Preparation and planning 2) Survey and identify significant things relating to the objective, vision, status, or success of the organization 3) Identify all relevant hazards 4) Explore the weak points of the significant things 5) Assess the risks from the identified hazards 6) Plan and execute the appropriate actions to handle the risks 7) Monitor and revise the risk assessment processes regularly.

Risk assessment is a management procedu're for determining and analyzing risks related to the goal of organization which concerns about the likelihood of occurrences as well as severity impacting on the organization.

3.2 Security Readiness

Security Readiness is the readiness of service, operation and threat handling based on the security standard for acknowledging the security condition of ICT.

3.2.1 Security Standard

Computer security together with security management standard is considered for developing the Information Security Management (ISO27001), TIL, and COBIT to define the information security framework with the acceptable level.

1. ISO 17799

ISO 17799 (BS7799) is an international information security standard directly related to the information. The information security, an important factor for the effective management in an organization, is composed of the three parts which are *Confidentiality, Integrity*, and *Availability*.

ISO 17799 in Thailand is different from the original one in two terms. Firstly, there are some additional criteria suitable for practice as well as the adaptation of technology appropriated with the computer network users in Thailand. This issue can be separated into 44 points which are added to the Thai version ISO 17799 from the 127 points of the original one. Secondly, the standard is classified into 0-3 levels for applying in each organization.

2. COBIT (Control Objective for Information and Related Technology)

COBIT is an international information security standard developed by ISACA and IT Governance Institute. COBIT is a widespread framework especially for the financial and banking businesses in terms of the effective internal control and best practice; additionally, it can be modified in order to suit for every organization. The COBIT designing is based on the business processes which can be categorized into four domains: Planning and Organization (PO), Acquisition and Implementation (AI), Delivery and Support (DS), and Monitoring (M). COBIT contains the 34 High-level Control Objectives, 318 Detailed Control Objectives, and the verify procedures as well.

COBIT contains the 34 High-level Control Objectives, 318 Detailed Control Objectives, and the verify procedures as well.

3. ITIL (IT Infrastructure Library)

ITIL is originally from England and developed by OGC (Office of Government Commerce) and BST (British Standard Institute). The purpose is to establish "Best Practice" for IT Service Management such as Service Support, Service Delivery, and also Service Level Agreement (SLA).

At present, ICT is rapidly increasing. Due to the importance of the standard of service quality management, an organization needs to specify the minimum standard of IT service for the outsource company to make sure that the service is efficient and effective which will lead to the customers' satisfaction as well as good image to the organization.

3.3 Information and Commutation Technology (ICT)

3.3.1 The Meaning of ICT

Information Technology is to bring all technologies together into the storing procedures, processing, and IT media which include the information transaction such as recording, collecting, processing, retrieving, sending and receiving information, the equipments and tools used in those transactions like a computer, and the monitoring system e.g. computer operating system, communication system.

3.3.2 The Elements of ICT

According to the functions of the Information Technology, ICT consists of the four elements- computer network systems, database management, information project systems, and planning and managing ICT which can be applied for risk management, analyzing, and assessment based on the international standard criteria.

The five major factors affecting ICT are 1) Man 2) Machine 3) Management 4) Vision and Vision 5) Environment.

3.4 Relevant Researches

Ms. Suvaree Yaipuak [1] researched the topic "Information Technology Security Assessment". She was successful in the security assessment system, computing the weak points from risk factors, determining threats, defining the standard procedures to correct the weaknesses, and demonstrating the results by comparing graphs.

Ms. Varaporn Arsalaprakit,[2] a researcher, studied for "Risk Management of Information Technology consulting and installing". She found that risk factors must be ranked and evaluated by the specialists, project managers, and operators of the project. Then, she used the analytical techniques to generate a risk control plan. Refer to her project, four risk control plans were executed out of the total 14. Furthermore, the specialists were able to reduce the severity of the external risk factors from level 3 to become level 1.

3.5 Research Conceptual Framework

Conception of research can explain as follows be The Impacts factors that exist in 5 factors such as Man, Machine, Management, Vision, Environment. To effect risk and security in information and communication technology for public Organizations. from that time Risk Identification to Analysis and
assessment form collecting the data documents analyzed and questionnaire bring risk analysis and assessment to use risk assessment based on OCTAVE in international standard of risk assessment. result is risk assessment model in Figure 1

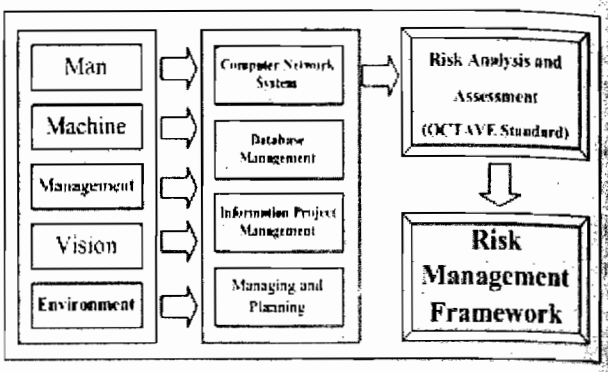

Fig.1 : Research Conceptual Framework

3.6 Research Hypotheses

In this research, we try to test the main hypothesis that relates to study relationship between risk impacts level and likelihood as follow:

1. Risk likelihood in ICT of Thai public organizations in the high-level.
2. Risk impacts in ICT of Thai public organizations in the high-level.
3. Risk likelihood correlate with risk impacts of computer network in the high-level.
4. Risk likelihood correlate with risk impacts of Database management in the high-level.
5. Risk likelihood correlate with risk impacts of Information project system in the high-level.
6. Risk likelihood correlate with risk Impacts of Management and Planning in the high-level.

4. Research Methodology

The research to study technical, principle, document and risk management model in ICT of public Organizations. The research methodologies were both qualitative and quantitative research.

4.1 Population and Sampling Groups

The population are 20 ministries in Thailand. The sampling group were divided into three groups as follows: 1) Chief Information Officers (CIOs) 2) ICT Administrator in state organizations. 3) ICT Users in state organizations.

As the mention, we use both qualitative and quantitative research.

1. The qualitative is represented by content analysis from documents and interviews CIOs amount 20 persons.

2. The quantitative is represented by data collected in analyzing questionnaires from ICT Administrator in state organizations amount 60 persons and ICT Users in state organizations amount 60 persons.

4.2 Research tool and Collecting Data

In this research, questionnaire was used as a tool for collecting the data amount 120 questionnaires to respond 90 questionnaires. the sampling group 2 and 3. To built up the questionnaire, quantitative data from documents were analyzed and collecting the data structure interviews group 1

4.3 Data Analysis

In this research based on qualitative and quantitative research, it can be divided into 2 steps and briefly explained as follow:

1. Based on qualitative research, collecting data the qualitative is represented by documentary analysis and content analysis were used for analyzed the document and literature review. Interview CIOs.
2. Based on quantitative research, collecting data , the quantitative is represented by data that collected in analyzing from questionnaires By analyzing State value ass follow Mean, Standard Deviation : S.D., Correlation Coefficient and t-test

5. Research Results

After I analyzed the three samples, Research Results findings as follow.

5.1 ICT Security Readiness in ICT of public organization

Refer to the interviews from the 20 CIOs and document analyzing, I realized the ICT Security Readiness of the public organization below.

5.1.1 Computer Network System Readiness

1. Network infrastructure is not ready.
2. Network architecture does not get along with the standards and is too various to manage.
3. Unskillful network maintainers require the outsource company.

5.1.2 Database Management Readiness

1. Databases in the organization are numerous.
2. The users are incapable to use the standard Information Technology effectively.

5.1.3 Information Project Development Readiness

1. Lack of qualified staffs to develop the Information Technology
2. Lack of Data Dictionary to reduce the information redundancy

5.1.4 Information Technology Management and Planning Readiness

1. Unsystematic and uncertain direction management
2. Unclear operation plan
3. Insufficient budget for executing the whole planned project

5.2 Results Level of Risk Analysis and Risk likelihood

By analyzing all information, the next section is the result from studying the Impacts and likelihood of risks affecting ICT security in the public organization.

1) Level of Risk Impact and ICT Security Readiness are shown in the table1.

Table 1 : Show Level of Impacts of Risk

Impacts of Risk	Risk Statistic Calculation		
	$\bar{x}$	S.D.	Level
computer network systems	3.4811	0.73431	High
database management	3.4267	0.77249	High
information project systems	3.4133	0.78699	High
managing and planning	3.4100	0.68275	High
Total	**3.4328**	**0.67085**	**High**

As you can see from the table1, Risk Impacts has the significant effect on the ICT security for the public organization. ($\bar{x}$ = 3.4328). After seeing the calculation results, I found that the Risk Impacts of each aspect is pretty high. That of computer network systems is the high ($\bar{x}$ =3.4811). The next are database management is the high ($\bar{x}$ = 3.4267), information project system is the high ($\bar{x}$ = 3.4133), and managing and planning is the high ($\bar{x}$ = 3.4100), respectively.

2) Likelihood of Risk Occurrence and ICT Security Readiness are shown in the table2.

Table 2 : Show likelihood of Risk

Likelihood of Risk	Risk Statistic Calculation		
	$\bar{x}$	S.D.	Level
computer network systems	3.2722	0.71616	middle
database management	3.2822	0.70931	middle
information project systems	3.2889	0.71112	middle
managing and planning	3.2440	0.71802	middle
Total	**3.2669**	**0.65796**	**middle**

As you can see from the table2, Risk likelihood has the significant effect on the ICT security for the public organization. ($\bar{x}$ = 3.2669). After seeing the calculation results, I found that the Risk likelihood of each aspect is the middle-level. That of computer network systems is the middle-level ($\bar{x}$ =3.2722). The next are database management is the middle-level ($\bar{x}$ = 3.2822), information project system is the middle-level. ($\bar{x}$ = 3.2889), and managing and planning is the middle-level ($\bar{x}$ = 3.2440), respectively.

Table 3: Show Testing hypothesis of Risk Impacts

Risk Impacts Level	Test Value = 3.41					
	t	df	Sig. (2-tail)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
computer network systems	.929	89	.355	.0711	-.0809	.2232
database management	.207	89	.836	.0167	-.1433	.1766
information project systems	.041	89	.968	.0033	-.1596	.1663
managing and planning	.000	89	1.000	.0000	-.1414	.1414
Totol	.326	89	.745	.0228	-.1161	.1617

As you can see from the table3, Results from this testing hypothesis of Risk Impacts discovery. That of computer network systems (Sig = 0.1775). The next are database management (Sig = 0.418), information project systems (Sig = 0.484), and managing and planning (Sig = 0.500), respectively. Risk Impacts has the high. Significant of statistics effect on the confidence level 0.05

Table 4 : Show Testing hypothesis of Risk likelihood

Risk likelihood	Test Value = 3.41					
	t	df	Sig. (2-tail)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
computer network systems	-1.846	89	.068	-.1378	-.2861	.0105
database management	-1.729	89	.087	-.1278	-.2747	.0191
information project systems	-1.634	89	.106	-.1211	-.2684	.0261
managing and planning	-2.480	89	.015	-.1856	-.3342	-.0369
Total	-2.086	89	.040	-.1431	-.2793	-.0068

As you can see from the table3, Results from this testing hypothesis of Risk likelihood discovery deny hypothesis. That of computer network systems (Sig = 0.034). The next are database management (Sig = 0.435), and managing and planning (Sig = 0.0075), respectively. Risk likelihood has the deny hypothesis. Information project systems (Sig = 0.0075) Accept hypothesis, Risk likelihood has the high. Significant of statistics effect on the confidence level 0.05

5.3 Show Correlation between Level of Risk likelihood and Risk Impacts.

Form Study and Analyzing discovery, Conception of research can explain as follows be The Impacts factors that exist in 5 factors such as Man, Machine, Management, Vision, Environment. To effect risk and security in information and communication technology for public Organizations.

Table 5 : Show value Correlation risk management in ICT for computer network.

Table Correlation		Risk likelihood				
		Man	Machine	Management	Mission	Environment
Risk Impacts Level	Man	0.729	-	-	-	-
	Machine	-	0.604	-	-	-
	Management	-	-	0.567	-	-
	Vision	-	-	-	0.604	-
	Environment	-	-	-	-	0.076

As you can see from the table5, Correlation risk management in ICT, computer network systems between risk impact and risk likelihood By consider from 5 factors for example
Man: Correlation value is the highest (Sig. = 0.729),
Machine: Correlation value is the high (Sig. = 0.604), Management: Correlation value is the high (Sig. = 0.567), Vision: Correlation value is the high (Sig. = 0.604) and Environment: Correlation value is the Low (Sig. = 0.076).

Table 6: Show value Correlation risk management in ICT for database management.

Table Correlation		Risk likelihood				
		Man	Machine	Management	Mission	Environment
Risk Impacts Level	Man	0.53	-	-	-	-
	Machine	-	0.609	-	-	-
	Management	-	-	0.623	-	-
	Vision	-	-	-	0.626	-
	Environment	-	-	-	-	0.438

As you can see from the table6, Correlation risk management in ICT, database management between risk impact and risk likelihood By consider from 5 factors for example
Man: Correlation value is the high (Sig. = 0.53),
Machine: Correlation value is the high (Sig. = 0.6), Management: Correlation value is the high (Sig. = 0.623), Vision: Correlation value is the high (Sig. = 0.626) and Environment: Correlation value is the middle (Sig. = 0.438).

Table 7: Show value Correlation risk management in ICT for information project management.

Table Correlation		Risk likelihood				
		Man	Machine	Management	Mission	Environment
Risk Impacts Level	Man	0.298	-	-	-	-
	Machine	-	0.607	-	-	-
	Management	-	-	0.726	-	-
	Vision	-	-	-	0.549	-
	Environment	-	-	-	-	0.453

As you can see from the table7, Correlation risk management in ICT, information project management between risk impact and risk likelihood By consider from 5 factors for example
Management: Correlation value is the highest (Sig. = 0.726),
Machine: Correlation value is the high (Sig. = 0.607),
Vision: Correlation value is the high (Sig. = 0.549),
Environment: Correlation value is the middle (Sig. = 0.435) and
Man : Correlation value is the low (Sig. = 0.298)

Table 8: Show value Correlation risk management in ICT for managing and planning

Table Correlation		Risk likelihood				
		Man	Machine	Management	Mission	Environment
Risk Impacts Level	Man	0.785	-	-	-	-
	Machine	-	0.656	-	-	-
	Management	-	-	0.842	-	-
	Vision	-	-	-	0.811	-
	Environment	-	-	-	-	0.277

As you can see from the table8, Correlation risk management in ICT, managing and planning between risk impact and risk likelihood By consider from 5 factors for example
Man: Correlation value is the highest (Sig. = 0.785),
Machine: Correlation value is the high (Sig. = 0.656), Management: Correlation value is the high (Sig. = 0.842), Vision: Correlation value is the high (Sig. = 0.811) and Environment: Correlation value is the low (Sig. = 0.277).

Form table 5 to table 8 Accept hypothesis discovery, Risk likelihood in ICT and Risk Impacts has Correlation is the high And Has Correlation go to in same direction.

6. Conclusion

To emphasize the research findings, ICT has high risk impacts and moderate likelihood of risk occurrence which are directly inter-relation. As ICT is comprised of four elements- computer network systems, database management, information project systems, and planning and managing of which concern about Man, Machine, Management, Vision, and Environment, it brings about the improvement of Risk Management Framework and Security Readiness in ICT of public organizations.

7. Discussion and Suggestion

This research is not only provide the Risk Management Framework and Security Readiness in ICT for public organizations in Thailand, but also can be utilized for the subsequent research related to Risk Assessment and ICT Security Architecture Design which can be applied by using *Delphi Technique* to the public organization implementing ICT.

8. References

[1] Suvaree Yaipuak, (2547). "Information Technology Security Assessment" Master of King Mongkut's University of Technology North Bangkok.

[2] Varaporn Arsalaprakita, (2547). "Risk Management of Information Technology consulting and installing". Master of Chulalongkorn University

[3] International Standards for Business Government and Society.(2550) Information Security Management Requirements ISO/IEC 27001. Switzerland: ISO Office

[4] International Standards for Business Government and Society. (2550) Code of practice for Information Security Management ISO/IEC FDIS 17799:2005 .Switzerland: ISO Office

[5] Lawrence Millerand Peter Gregory.(2007). CISSP For Dummies (2nd Edition). United States: John Wiley & Sons

[6] Suphannika Thamnithatsana. (2550). Development the Risk Management Standard for Manufacturing Industries. Master of Engineering in Industrial Engineering Department of Industrial Engineering Faculty of Engineering Chulalongkorn University.

[7] Varaporn Asanprakit.(2547). Risk Management For The Project of Advisability and Information System. Master of Engineering in Industrial Engineering Department of Industrial Engineering Faculty of Engineering Chulalongkorn University.

[8] Buewbunjong A. (1995). Problems and Safety Management in Rajamangala Institute of Technology's Workshops M.S. Thesis Chiang Mai University Thailand.

[9] Chaisaeng W. (1999). Feasibility Study of Modern Safety Management in Large Contractor Companies. M.S. Thesis King Mongkut University of Technology Thonburi Thailand.

[10] Harold F. Tipton and Micki Krause (2007).Information Security Management (Sixth Edition). United States: Auerbach Publications

[11] ASIS International Advance Security (2007).Chief Security Officer (CSO) Guideline. United States: ASIA International

[12] Harold F. Tipton and Micki Krause, (2007). Information Security Management, (Sixth Edition). United States: Auerbach Publications

[13] International Standards for Business, Government and Society.(2550) Information Security Management Requirements ISO/IEC 27001. Switzerland: ISO Office

[14] International Standards for Business, Government and Society. (2550) Code of practice for Information Security Management ISO/IEC FDIS 17799:2005 .Switzerland: ISO Office

[15] Lawrence Millerand Peter Gregory.(2007). CISSP For Dummies, (2nd Edition). United States: John Wiley & Sons

[16] Suphannika Thamnithatsana. (2550). Development the Risk Management Standard for Manufacturing Industries. Master of Engineering in Industrial Engineering, Department of Industrial Engineering Faculty of Engineering, Chulalongkorn University.

[17] Varaporn Asanprakit.(2547). Risk Management For The Project of Advisability and Information System. Master of Engineering in Industrial Engineering, Department of Industrial Engineering Faculty of Engineering, Chulalongkorn University.

[18] Buewbunjong, A. 1995. Problems and Safety Management in Rajamangala Institute of Technology's Workshops, M.S. Thesis, Chiang Mai University, Thailand.

[19] Chaisaeng, W. 1999. Feasibility Study of Modern Safety Management in Large Contractor Companies. M.S. Thesis, King Mongkut University of Technology Thonburi, Thailand.

[20] Natee Kerdssri (2003): Risk Assessment for Maintenance Work of High Voltage Substation Equipment. Master of Engineering (Safety Engineering), Major Field: Safety Engineering. Interdisciplinary Graduate Program, Kasetsart Universitty.

[21] Pongson SookMark. (1989). Development for Security: Royal Thai Armed forces Scenario. Engineering Management UMI.

[22] Huseyin Cavusoglu B.Sc in I.E. (2003). The Economic of Information Technology Security. A Doctoral Thesis in Management Science, The University of Texas at Dallas.

[23] Sudsanguan Ngmsuriyaroj. (2002).Performance Aspects of Security-Aware Database Systems. A Doctoral Thesis in Management Science, The Pennsylvania State University.

[24] Thomas Arthur Marbach. (2003).Detecting Risk in Information technology Projects. A Doctoral Thesis in Management Science, The University of Texas at Arlington.

[25] Borislav H. Simov. (2003). Algorithms for Security in robotics and networks. A Doctoral Thesis in Computer Science, Iowa State University.

[26] Craig Hunt, (2002). TCP/IP Network Administration. 3rd Edition, USA: O'Reilly & Associates,

[27] William Stallings (2000). Data & Computer Communications. 6th Edition, USA: Prentice Hall International,.

[28] Coffee, P. Dyck, T. Sturdevant, C. and Rapoza, J. 5 Steps to Enterprise Security, eWeek White Paper.

[29] McCabe, B., and Ford, D. Using Belief Networks To Assess Risk. Proceeding of the 2001 Winter Simulation Conference.

[30] Goseva-Popstojanova.(2003)., K., Hassan, A., and Guedem. An Architectural-Level Risk Analysis Using UML. IEEE Transaction on Software Engineering Vol.29, No.10.,

[31] Larry, J. H. Jr. Actually Useful Internet Security Technique. ISBN 1-56205-508-9. New Riders Publishing, Indianapolis, Indiana. 1995.

[32] Pfleeger, P. C., and Pfleeger, L. S. Security in Computing Third Edition. ISBN 0-13-120199-9. Pearson Education International., 2003.

[33] Gourley D. Totty B. HTTP : The Definitive Gide. ISBN 1-56592-509-2. O'Reilly &Associates,Inc , 2002.

[34] Mcclure, Stuart. Shah, Saumil. Shah, Shreeraj. Web Hacking: Attacks And Defense.,Pearson Education, Inc., 2003.

[35] Mirza Ahmad, David R. Dubrawsky, Ido. Flynn, Hal. Grand, Joseph. Graham, Robert.Johnson Jr.,Norris L. Kaminsky, Dan. Lynch, F. William. Manzuil, Steve W.Permeh, Ryan. Pfeil, Ken. Puppy, Rain Forest. Hack Proofing Your Network Second Edition., Syngress Publishing, Inc., 2002.

[36] Bodeau, J.D. A Conceptual Model for Computer Security Risk Analysis. IEEE. 1992.

[37] Geoff Huston. Internet Performance Survival Guide. Canada: John Wiley & Sons, 2000.

[38] Olson, M. H., *Information technology and where and when of office work : Electronic cottages of flexible organizational: Managing Information technology's Organization Impact,* ACS, 1991.

[39] Christopher Alberts, Audrey Dorofee. (2002) Managing Information Security Risks: The OCTAVE[SM] Approach.