

ปีที่ 35 ฉบับที่ 135 กรกฎาคม-กันยายน 2555

Krongras Tiatsin

Graduate Student of Master of Science Program
in Management Information Systems,
Thammasat Business School.

Dr.Siriluck Rotchanakitumnui

Professor of Department of Management Information Systems,
Thammasat Business School.

IT Risk Management for E-Government Implementation Success

การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ
เพื่อก่อให้เกิดความสำเร็จในระบบรัฐบาลอิเล็กทรอนิกส์

ABSTRACT

E-Government is a multidimensional concept which requires an understanding and management in order to implement successfully. Information technology (IT) risk management is one of the important issues of e-Government implementation success. This research presents the factors of IT risk management for e-Government implementation success. A survey was conducted with Thai government officers who are involved in e-Government implementation. There are five IT risk management factors which are IT infrastructure risk, economic risk, legal and regulation risk, change management risk and performance risk. The Thai government can apply the research framework to prevent implementation failure.

Keywords: E-Government, IT risk management

บทคัดย่อ

ส รัฐบาลอิเล็กทรอนิกส์เป็นแนวคิดที่มีหลายมิติ ซึ่งต้องใช้ความเข้าใจและการบริหารจัดการเพื่อก่อให้เกิดความสำเร็จใน
ดำเนินการ การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นหนึ่งในปัญหาสำคัญของการดำเนินการ
รัฐบาลอิเล็กทรอนิกส์ให้ประสบความสำเร็จ งานวิจัยนี้แสดงปัจจัยต่าง ๆ ของการบริหารความเสี่ยงทางด้าน
เทคโนโลยีสารสนเทศเพื่อให้เกิดความสำเร็จและดำเนินการสำรวจกับเจ้าหน้าที่ภาครัฐในประเทศไทย ที่มีส่วน
เกี่ยวข้องในการดำเนินงานอิเล็กทรอนิกส์ภาครัฐ ในการดำเนินการรัฐบาลอิเล็กทรอนิกส์ประกอบด้วยห้าปัจจัยเสี่ยง คือ ความเสี่ยง
ทางด้านโครงสร้างพื้นฐานของเทคโนโลยี ความเสี่ยงทางด้านเศรษฐกิจการเงิน ความเสี่ยงทางด้านกฎหมายและระเบียบ
ความเสี่ยงทางด้านจัดการการเปลี่ยนแปลง และความเสี่ยงทางด้านประสิทธิภาพ รัฐบาลไทยสามารถใช้กรอบการวิจัยนี้เพื่อ
ป้องกันไม่ให้เกิดความล้มเหลวการดำเนินงานรัฐบาลอิเล็กทรอนิกส์

คำสำคัญ : รัฐบาลอิเล็กทรอนิกส์ การบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

1. INTRODUCTION

Many organizations have adopted information technology (IT) to enhance operational efficiency, cost reduction, quality of services, convenience, innovation and learning (Reffat, 2003). In government sector, e-Government has been implemented to transform the traditional processes of providing information and services to citizens and businesses (Orgeron, 2008). As spending on IT increases sharply, technology is increasingly taken part in organizations, for this reason, they become highly vulnerable to the risks of IT failure (Bandyopadhyay et al., 1999). Risk factors are conditions that can cause a serious threat to implementation e-Government successfully (Bradley and Pratt, 2011). In the past ten years, Thai government has implemented e-Government to encourage the web usage of citizens interacting with the government agencies (Rotchanakitumnuai, 2007). However, e-Government in Thailand is still ineffective and inefficient in present. Moreover, an investment for the e-Government is not critical issues in the Thai government agencies (Vathanophas et al., 2008). E-Government contains several risks of implementing failure, e.g. IT infrastructure risk, change management risk, performance risk (Kim et al., 2007). Information technology risk management plays an important role in e-Government implementation success (White, 1995; Woods, 2009). Therefore, we focus on study in field of e-Government success in Thailand as a guide to solve a problem of IT risk management. This research aims to develop the systematic framework of IT risk management framework to achieve e-Government implementation success.

2. THEORETICAL BACKGROUND

E-government has been conceptualized as the use of information technologies in government for the public services, and managerial effectiveness (Guo et al., 2009). Because of the increased complication, IT management of government agencies is confronted with risks (Walser et al., 2009). E-Government implementation in some countries has faced problems to develop a basic infrastructure to take advantage of new technologies tools. Many developing countries do not have the infrastructure necessary to implement e-Government infrastructure and services throughout their country (Reffat, 2003). Therefore, IT risk management plays an important role to solve the problem for IT implementation success. Simultaneously, government practitioners have worked to improve their chances for success by reducing IT risk management for responding to challenges to their IT initiatives (Gil-Garcia and Pardo, 2005). Prior study used constraints in identifying factors for successful e-government implementation. These include laws, regulations and policies; technical capabilities; and user feasibility (Belanger and Hiller, 2006). Specific to this study e-Government, government agencies have to concern of IT risk management, such as IT infrastructure risk, economic risk, legal and regulation risk, change management risk, and performance risk. Risk factors are conditions that can pose a serious threat to the successful completion or accomplishment of e-Government (Bradley and Pratt, 2011).

IT Infrastructure Risk

IT infrastructure is defined as a set of shared IT resources which is a foundation for both communication across the organization and the implementation of present/future business applications. IT Infrastructure composes of computer, communicating technology, database, shared technology platform and so

IT Risk Management for E-Government Implementation Success

on. IT infrastructure more precisely is through the qualities of scalability, connectivity, compatibility, modularity, rapidity, modularity, facility, modernity. Briefly, IT infrastructure is the ability of the hardware and software to make internal and external electronic linkages (Chanopas et al., 2006). In the e-Government domain, the fundamental IT infrastructure must be integrated with the front-end applications that are implemented for users (Esteves and Joseph, 2007). Therefore, IT infrastructure becomes an increasingly important factor that affects organization competitiveness (Weill and Broadbent, 1998). All countries implementing e-Government have struggled to develop a basic infrastructure to take advantage of new technologies tools. Many developing countries do not have the infrastructure necessary to implement e-Government services throughout their country (Reffat, 2003).

Economic Risk

Prior research shown that there were risks emerging from the financial operations and management of the business. From an internal perspective on operating costs were reduced by carrying out assessments while agencies could optimize operating and maintenance costs (Pollard et al., 2004). Economic risk is defined as risk related to economic issues, e.g. financial issues cause to supply interruptions and possibly insolvency, failure to comply with legal regulations, and strategic issues that ensure competition and strategy implementation (Matook et al., 2009). Financial risk is the potential loss of benefit or money because a product or service does not satisfy the customer's expectation (Rotchanakitumnuai, 2007). The transaction sectors must endure a certain level of risk. There may be a number of fraud and unreliable service. It seems that wrong decisions may result in transaction failure, and cause some economic losses (Ruizhong et al., 2010). The current financial services research context expands this facet to include the recurring potential for financial loss due to fraud (Featherman and Pavlou, 2003).

Legal and Regulation Risk

There are the importance of changing relationship between government and its stakeholders and the difference of new structure of communication and interaction between traditional government and e-Government. One of the major differences of e-Government includes the legal structure of the activities in government from the need of the compliance of the constitution and other laws in order to assure social performance (Montagna, 2005). Previously developing laws and regulations or in ignorance of technologies related to e-Government have an impact on the success of projects. Investing in changes of the regulatory is one of responses for these challenges that consider or enable for adoption of technologies (Gil-Garcia and Pardo, 2005). The legal risk refers to the likelihood of loss owing to violation of the rights of citizens through the use of IT (Bandyopadhyay et al., 1999). When reviewing of risk management, it can be considered between risk analysis and techniques used by law enforcement. The potential for lawsuits or other legal action in the information leaks can also be considered an important barrier or challenges that must be overcome (Schneider, 2010). The law and policy limitation requests the action conducts with relevant laws, regulations, and policies within the power of government. Regulations may limit government powers to institute and complete e-Government projects (Chen and Perry, 2003; Belanger and Hiller, 2006).

Change Management Risk

E-Government consists of various problems from technical aspects to organizational problems such as implementation, process change. Deeper changes cause larger resistance. Governmental activities require changes through information technology. Change management involves effectively balancing forces in a change of resistance (Montagna, 2005). The organization is arranged to manage the change and its cultural impact. Moreover, it plans to reduce the general opposition to change and facilitate the use and consolidation of new technologies and systems (Iribarren et al., 2008). Risk is a relatively new facet to be explored within the scope of IT change management (Bannister and Connolly, 2011). Prior researches considered that change management concerns all human and social related to changes and cultural improvement techniques required by management to the impletion of newly-designed processes and structures into working practice and to cope effectively with a resistance (Al-Mashari and Zairi, 1999). For the level of organizational and official competences required for an effective and efficient e-Government implementation, it shows how the organization is arranged to manage the change and its cultural impact. Moreover, it plans to reduce the general opposition to change and facilitate the use and consolidation of new technologies and systems (Iribarren et al., 2008).

Performance Risk

The term “performance risk” is used to consider for the possibility and consequences. Performance risk is defined as the possibility of the product malfunctioning and not performing. It was designed and failed to deliver the desired benefits (Featherman and Pavlou, 2003). It is the possibility that a product or service will not work as expected by the customer (Rotchanakitumnuai, 2007). Therefore, performance risk has to do with failure of the performance objectives (Ratnasingham, 1999). The performance is considered in the process performance by operational efficiency, responsiveness and flexibility. When environmental uncertainty is high, it seem to occur from likely adverse government regulations, market volatility and a lack of stakeholder competence, thus managers will perceive that performance risk is high. However, when performance risk is low, output controls will monitor overall performance (Langfield-Smith, 2008).

Risk management is a systematic process of identifying and assessing company risks to protect agencies. However, agencies need risk management to analyze risks for balancing potential gains against potential losses and avoid mistakes. It is the best use as a preventive measure rather than as a reactive measure. In this study, we present the IT risk management regarding systematic process in five dimensions. We use this process systematic approach in order to manage and reduce all five factors risks in electronically government service. (Figure 1)

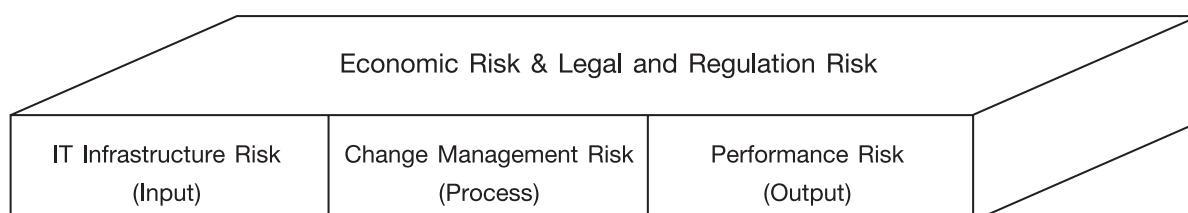


Figure 1: IT risk management for e-Government implementation success

3. RESEARCH METHODOLOGY

The survey research was conducted with e-Government officers who have involved in e-Government implementation. Most systems of government agencies in Thailand that respondents have participated to implement are e-Customs, e-Revenue, GFMS, TCL, Online Registration System and etc. Judgment sampling was used to select the respondents. Measurement items of the questionnaire measured by a five-point Likert type scales, ranging from 1=strongly disagree to 5=strongly agree. Respondent profile is shown in Table 1.

Table 1: Respondent profile

Characteristic	Frequency	Percent
Age		
21 - 30	79	37.6
31 - 40	67	31.9
41 - 50	51	24.3
More than 50	13	6.2
Total	210	100
Gender		
Male	61	29
Female	149	71
Total	210	100
Level of education		
Less than bachelor degree	16	7.6
Bachelor degree	121	57.6
Master degree	72	34.3
PhD	1	0.5
Total	210	100

4. DATA ANALYSIS

An exploratory factor analysis with varimax rotation was conducted to determine the five IT risk management factors including change management risk, IT infrastructure risk, performance risk, legal and regulation risk and economic risk. Three measurement items with factor loading lower than 0.5 are dropped. All constructs of IT risk management factors have the high level of reliability with the value of Cronbach Alpha from 0.682 – 0.813. (Table 2)

Firstly, change management risk factor includes the items: No reform processes by simplifying regulations and procedures, No plans to reduce opposition to change the use of new systems, No responsibility to change effort, No analysis impact of change program, and No benet from changing traditional process to e-

Government. These items had the average mean between 2.99 and 3.34. The lowest mean score was 2.99 on 'No benefit from changing traditional process to -Government'; while item 'Lower performance-to-price ratio' had the highest mean score of 3.34.

Secondly, IT infrastructure risk factor comprises the items: No security from using database management systems, No electronic linkages among departments or external, No design IT infrastructure to handle an increase in users, workload and transactions, and User-unfriendly applications. These items had the average mean between 2.99 and 3.12. The lowest mean score was 2.99 on 'No securities from using database management systems', while item 'No design IT infrastructure to handle an increase in users, workload and transactions' had the highest mean score of 3.12.

Thirdly, performance risk factor is composed of the items: Slow response time, Difficult to access service, No security to protect privacy, and No accuracy information. These items had the average mean between 2.98 and 3.27. The lowest mean score was 2.98 on 'Difficult to access service', while item 'Slow response time' had the highest mean score of 3.27.

Fourthly, legal and regulation risk factor includes the items: No procedure to enforce law and regulation, Lower compliance level with internal and external law and procedure, and No legal structure to protect from problems on internet. These items had the average mean between 3.00 and 3.12. The lowest mean score was 3.00 on 'Lower compliance levels with internal and external law and procedure', while item 'No legal structure to protect from problems on internet' had the highest mean score of 3.12

Finally, economic risk factor constitutes the items: Over maintenance costs, Uncertainty of future funding to sustainability, and No control of IT costs and cost predictability. These items had the average mean between 3.24 and 3.42. The lowest mean score was 3.24 on 'No control of IT costs and cost predictability', while item 'Over maintenance costs' had the highest mean score of 3.42.

Table 2: IT risk management factors

Items	Factor Loading	Mean	SD	Cronbach Alpha
Factor 1: Change Management risk				.813
No reform processes by simplifying regulations and procedures	.714	3.10	1.137	
No plans to reduce opposition to change the use of new systems	.709	3.20	1.072	
No responsibility to change effort	.693	3.24	1.082	
No analysisimpact of change program	.691	3.26	1.026	
No benet from changing traditional process to e-Government	.622	2.99	1.151	
Inadequate network capacity or bandwidth	.467*	3.22	1.058	
Lower performance-to-price ratio	.453*	3.34	1.066	
No quality of interactions with the users	.417*	3.02	1.053	
Factor 2: IT Infrastructure Risk				.807
No security from using databasemanagement systems	.765	2.99	1.159	
No electronic linkages among departments or external	.723	3.03	1.252	
No design IT infrastructure tohandle an increase in users, workload and transactions	.717	3.12	1.121	
User-unfriendly applications	.557	3.01	1.058	
Factor 3: Performance Risk				.778
Slow response time	.811	3.27	1.043	
Difficult to access service	.755	2.98	1.035	
No security to protect privacy	.655	3.07	1.019	
No accuracy information	.510	3.04	1.006	
Factor 4: Legal and Regulation Risk				.793
No procedure to enforce law and regulation	.743	3.02	1.194	
Lower compliance level with internal and external law and procedure	.722	3.00	1.222	
No legal structure to protect from problems on internet	.702	3.12	1.014	
Factor 5: Economic Risk				.682
Over maintenance costs	.762	3.42	1.034	
Uncertainty of future funding to sustainability	.549	3.26	1.098	
No control of IT costs and cost predictability	.517	3.24	1.049	

* Item is dropped

For prioritizing the ranks of all areas in IT risk management to be useful in operation for e-Government in government agencies in Thailand.

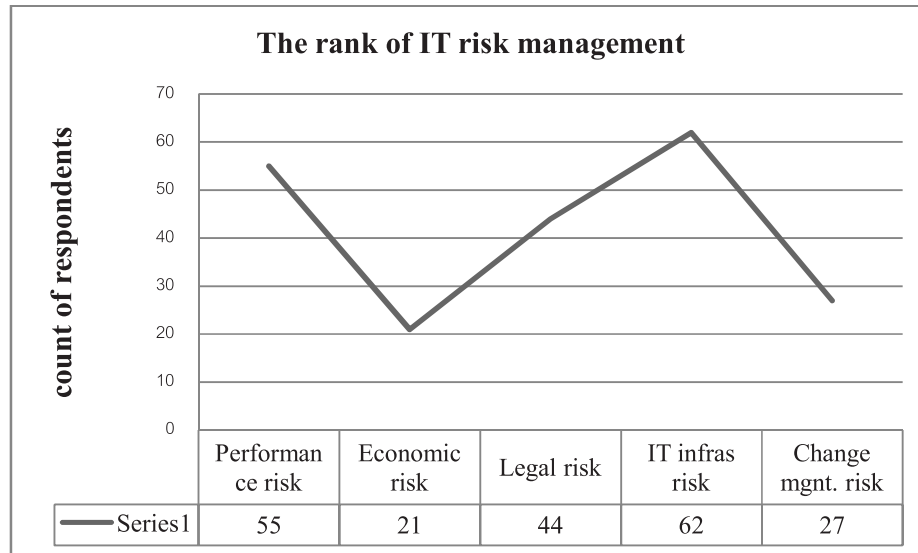


Figure2: The rank of IT risk management

The results make government agencies aware of the importance of IT risk management. Government agencies can take the result of this study applied in the implementation of IT risk management. The result found that IT infrastructure risk is highest rank of risk among the five factors. Thai government officers see that IT infrastructure risk that is input of the system is highest rank risk to manage in Thai government agencies. Performance risk, legal and regulation risk, change management, and economic risk will be managed respectively in e-Government system.

5. CONCLUSIONS

This study presents IT risk management as a determinant of e-Government implementation success. The components of IT risk management consist of change management risk, IT infrastructure risk, performance risk, legal and regulation risk and economic risk. The result of five variables is assessed by mean scores. Firstly, change management risk factor shows that item on 'no analysis impact of change program' is ranked as first. This suggested that respondents viewed the analysis impact of change program as most important impact on change management risk. Secondly, IT infrastructure risk factor presents that item on 'no design IT infrastructure to handle an increase in users, workload and transactions' is ranked as first. This suggested that respondents viewed the design IT infrastructure to handle an increase in users, workload and transactions as most essential impact on IT infrastructure risk. Thirdly, performance risk factor explains that item on 'slow response time' is ranked as first. This suggested that respondents viewed the slow response time as most significant impact on performance risk. Fourthly, legal and regulation risk factor shows that item on 'no legal structure to protect from problems on internet' is ranked as first. This suggested that respondents viewed the legal structure to protect from problems on internet as most important impact on legal and regulation risk. Finally, economic risk factor

IT Risk Management for E-Government Implementation Success

explains that item on 'over maintenance costs' is ranked as first. This suggested that respondents viewed the over maintenance costs as most significant impact on economic risk. This study gives the conclusion as various areas of risk and the rank of various fields of IT risk management in e-Government. Implementation problems of e-Government are resolved by managing IT risk in all factors. Moreover, this study can assist government agencies to prioritize important risk factors for achieving e-Government implementation success.

According to the result of all factors of IT risk management in systematic process, it could be recommended that if government agencies conduct to manage IT risk in systematic process, e-Government implementation will be success. IT infrastructure risk as input in systematic process should be improve about the design of IT infrastructure for increasing in transactions, the electronic linkages among departments, the user-friendly applications, the security of data from applications using database management systems and also adequate network capacity or bandwidth. Change management risk as process should be concerned about analysis of work processes by the change program, reducing the natural opposition to change the use of new systems, contributing and accountable to the agencies' change effort and any interests from changing traditional process to e-Government. Performance risk as output should be considered to improve about quality of interactions with the users, the response time to access service, security to protect privacy and accuracy information. Economic risk as overall process in systematic process should be recognize about higher control and maintenance costs, certainty of future funding to sustainability, and control of IT costs and cost predictability. In addition, legal and regulation risk also as overall process should be concerned about procedure to enforce law and regulation, compliance level with internal and external law and procedure, legal structure to protect from problems on internet and reform processes by simplifying regulations and procedures. The limitation of the research is that it focused on the government agencies involved with government to citizen (G2C) and government to business (G2B). Future research can expand to other group of respondents such as government to government (G2G) for analyzing the full range of Thai government agencies.

REFERENCES

- Al-Mashari, M. and Zairi, M. 1999, 'BPR implementation process: an analysis of key success and failure factors', *Journal*, Vol. 5, No. 1, pp. 87-112.
- Bandyopadhyay, K., Mykytyn, P. P. and Mykytyn, K. 1999, 'A framework for integrated risk management in information technology', *Management Decision* 37/5, pp. 437- 444.
- Bannister, F. and Connolly, R. 2011, 'Trust and transformational government: A proposed framework for research', *Government Information Quarterly*, Vol.28, pp. 137-147.
- Belanger, F. and Hiller, J. S. 2006, 'A framework for e-government: privacy implications', *Business Process Management Journal*, Vol. 12, No. 1, pp. 48-60.

- Bradley, V. and Pratt, R. 2011, ' Exploring the Relationships Among Corporate Entrepreneurship, IT Governance, and Risk Management', *Proceedings of the 44th Hawaii International Conference on System Sciences*.
- Chanopas, A., Krairit, D. and Khang, D.B. 2006, 'Managing information technology infrastructure: a new flexibility framework', *Management Research News*, Vol. 29, No. 10, pp. 632-651.
- Chen, Y. and Perry, J. 2003, 'Outsourcing for e-government', *Public Performance & Management Review*, Vol. 26, No. 4, pp. 404-21.
- Esteves J. and Joseph R. C. 2008, 'A comprehensive framework for the assessment of e-Government projects', *Government Information Quarterly*, Vol.25, pp. 118–132.
- Featherman, M. and Pavlou, P. 2003, 'Predicting e-services adoption: a perceived risk facets perspective', *Int. J. Human -Computer Studies*, Vol.59, pp. 451–474.
- Gil-Garcia, R., and Pardo, T. 2005, 'E-government success factors: Mapping practical tools to theoretical foundations', *Government Information Quarterly*, Vol. 22, pp. 187–216.
- Guo Y., Fang D., and Chen, J. 2009, 'Effect of IT Capability on IT Project Risk', *International Conference on Management and Service Science*.
- Iribarren, M., Concha, G., Valdes, G., Solar, M., Villarroel, M.T., Guti"rrez, P. and Vsquez, . 2008, ' Capability Maturity Framework for e-Government: A Multi-dimensional Model and Assessing Tool', *EGOV 2008, LNCS*, Vol.5184, pp. 136–147.
- Kim, H. J., Pan, G., and Pan, S. L. 2007, 'Managing IT-enabled transformation in the public sector: A case study on e-government in South Korea', *Government Information Quarterly*, Vol.24, pp. 338–352.
- Langfield-Smith, K. 2008, 'The relations between transactional characteristics, trust and risk in the start-up phase of a collaborative alliance', *Management Accounting Research*, Vol.19, pp. 344–364.
- Matook, S., Lasch, R., and Tamaschke, R. 2009, 'Supplier development with benchmarking as part of a comprehensive supplier risk management framework', *International Journal of Operations & Production Management*, Vol.29, No.3, pp. 241-267.
- Montagna, J. M. 2005, 'A framework for the assessment and analysis of electronic government proposals', *Electronic Commerce Research and Applications*, Vol.4, pp. 204–219.
- Orgeron, C. P. 2008, 'Evaluating citizen adoption and satisfaction of e-government', *ProQuest Information and Learning Company*.

IT Risk Management for E-Government Implementation Success

- Pollard, S.J.T., Strutt, J. E., Macgillivray, B. H., Hamilton, P. D., and Hrudey, S. E. 2004, 'RISK ANALYSIS AND MANAGEMENT IN THE WATER UTILITY SECTOR', *Process Safety and Environmental Protection*, Vol.82(B6), pp. 453–462.
- Ratnasingham, P. 1999, 'Risks in Low Trust Among Trading Partners in Electronic Commerce', *Computers & Security*, Vol.18, pp. 587-592.
- Reffat, R. M. 2003, ' Developing a Successful e-Government', *in the proceedings of the Symposium on e-Government: Opportunities and Challenge*, Muscat Municipality, Oman, IV1-IV13.
- Rotchanakitumnuai, S. 2007, ' The important risk factors of e-government service adoption', *International Conference on Wireless Communications, Networking and Mobile Computing*, 2007.
- Ruizhong, D., Xiaoxue, M., and Zixian, W. 2010, ' Dynamic Trust Model based on Perceived Risk', *International Conference on E-Business and E-Government*.
- Schneider, R. 2010, ' A Comparison of Information Security Risk Analysis in the Context of e-Government to Criminological Threat Assessment Techniques', *InfoSecCD' 10*, Kennesaw, GA, USA.
- Vathanophas, V., Krittayaphongphun, N., and Klomsiri, C. 2008, ' Technology acceptance toward e-government initiative in Royal Thai Navy', *Transforming Government: People, Process and Policy*, Vol. 2, No. 4, pp. 256-282.
- Walser, K., Khn, A., and Riedl, R. 2009, ' Risk management in e-government from the perspective of IT governance', *The Proceedings of the 10th International Digital Government Research Conference*.
- Weill, P. and Broadbent, M. 1998, 'Leveraging the New Infrastructure - How Market Leaders Capitalize on Information Technology', *Harvard Business School Press*, Boston, Massachusetts.
- White, D. 1995, ' Application of systems thinking to risk management: a review of the literature', *Management Decision*, Vol. 33, No. 10, pp. 35-45.
- Woods, M. 2009, ' A contingency theory perspective on the risk management control system within Birmingham City Council', *Management Accounting Research*, Vol.20, pp. 69–81.