The Journal of Applied Science **Vol. 19 No. 1: 13-24 [2020]**
วารสารวิทยาศาสตร์ประยุกต์ doi: 10.14416/j.appsci.2020.01.002
ISSN 1513-7805 Printed in Thailand ISSN 2586-9663 (Online)

Research Article

A Study of Information Technology Risk Management of Government and Business Organizations in Thailand using COSO-ERM based on the COBIT 5 Framework

Sakchai Tangprasert

Department of Mathematics, Faculty of Applied Science, King Mongkut's University of Technology North Bangkok
1518 Pracharat 1 Road, Wongsawang, Bangsue, Bangkok, 10800, Thailand
E-mail: Sakchai.t@sci.kmutnb.ac.th
Received: 20/01/2020; Revised: 03/06/2020; Accepted: 15/06/2020

Abstract

Information technology (IT) risk management plays an important role in controlling security and building confidence in using IT system services. Many organizations have focused on risk management for IT security. In this study the committee of sponsoring organizations of the treadway commission (COSO) enterprise risk management (ERM) was used in risk management by identifying risk factors in accordance with the requirements of COBIT 5 areas that need to be controlled. In addition, 2 experiments were conducted with 3 government organizations and 3 business organizations in order to evaluate the performance of IT security control. The first experiment identified the risk levels with risk assessment, which provided the risk levels that need risk response in accordance with COBIT 5 framework implementation life cycle. From the second experiment, it was found that the risk management using all 7 phases of the COBIT 5 implementation life cycle decreased the risk levels for both government and business organizations. However, moderate and low risk levels were still observed which need to be managed in order to keep them at a very low level. In addition, it was found that the risks of government and Business organizations were different, which was a result of differences in obstacles and the context of the problems encountered in risk management. The findings of this study provide the guidelines for developing a framework for IT risk management in the future.

Keywords: IT Risk Management, COSO-ERM, COBIT 5 framework

Introduction

In a globalized world, business competition due to both domestic and international factors affects the changes and drives the workflow of both government and business organizations. In order to speed up the operations of the organizations, reduce workloads and increase operational performance (Tangprasert, 2019), IT systems have been used for data storage, communication, operations including providing services to outsiders. In addition to the benefits, on the other hand, there are many risks (Prasetyo & Sucahyo, 2014) affecting the operations, information, and services of the organization. In order to gain confidence and acceptance of IT services, it is necessary to manage the risks (Wijanarka, 2014), such as risks from human error, employee compliance violation, losing important data and IT system

disruption and so on. The risks mentioned above negatively affect the image and also result in loss of budget and

business opportunity. This study therefore adopted the COSO-ERM (COSO, 2004) principle to define the risk criteria for risk assessment and risk response. This research applied COBIT 5 areas for determining guidelines and topics in risk assessment (Su & Zhao, 2011) which is applicable and consistent with information technology risk management of both government and Business organizations (Khrisna & Harlili, 2014). This research has been experimental with 3 government organizations and 3 Business organizations with experimental twice. The 1st experimental for risk assessment of information technology in accordance with the framework of COBIT 5 areas. After the organization was reported the risk of information technology and risk management in accordance with the principles of risk response, then performed the 2nd experimental to assess the result of risk change. The aim of this study to determine the valuation of issues, effects and solutions to be a guideline for indicating the conclusions from this research to continue developing the technology risk prevention framework for government and Business organizations.

IT risk management

IT risk management is a risk management process that involves the use of IT systems to identify threats, find the guidelines for preventing the impact of system errors, data retention, and securing and getting the organization ready to deal with the problems all the time whether it is hardware, software, or data problems (Tangprasert, 2019). These problems are related to personnel at all levels in the organization, from operators, managers to top executives. Everyone must be involved in the organization's operations to ensure standardized processes in order to achieve work performance and the objectives of the organization (Foley, 2009). The important risk management principles of COSO-ERM (COSO, 2004) are as follows (Fang, 2005):

Risk identification

Risk identification or event identification is a process of identifying events in which the organization considered that they may hold potential risks (Islam & Dong, 2008) and may affect the strategic plans and work processes and cause damage to the organization. In risk identification, both external risk factors (Zhu etal., 2012) such as technological changes, competitive conditions, customers, trading partners, economic conditions, inflation, politics and law and internal risk factors such as management policies, employee performance, work processes and IT systems used must be analyzed.

Risk assessment

Risk assessment or risk analysis is an assessment or analysis of the likelihood and impact of the potential events in the organization's operations. Each event affects the organization at a different level and with a different probability of occurrence (Roberts, 2017). Therefore, the risk matrix consists of 2 dimensions (Xiaosong etal., 2009). Dimension 1 is likelihood which considers the probability level of occurrence. Dimension 2 is impact which involves an analysis of the lvel of impact of an event. The risk matrix in this study is shown in Figure 1.

Impact

Likelihood	1 = Negligible	2 = Minor	3 = Moderate	4 = Significant	5. Severe
5 = Very Likely	Moderate 5 x 1 = 5	Moderate 5 x 2 = 10	High 5 x 3 = 15	Extreme 5 x 4 = 20	Extreme 5 x 5 = 25
4 = Likely	Low 4 x 1 = 4	Moderate 4 x 2 = 8	High 4 x 3 = 12	High 4 x 4 = 16	Extreme 4 x 5 = 20
3 = Possible	Low 3 x 1 = 3	Low 3 x 2 = 6	Moderate 3 x 3 = 9	High 3 x 4 = 12	High 3 x 5 = 15
2 = Unlikely	Very Low 2 x 1 = 2	Low 2 x 2 = 4	Low 2 x 3 = 6	Moderate 2 x 4 = 8	High 2 x 5 = 10
1 = Rare	Very Low 1 x 1 = 1	Very Low 1 x 2 = 2	Low 1 x 3 = 3	Low 1 x 4 = 4	Moderate 1 x 5 = 5

Figure 1. Risk Matrix

Dimension 1 Likelihood: level 1 = rare, the event has almost no chance of occurring or the event likely to occur once in 1-2 years; level 2 = unlikely, the event can occur at some time or likely to occur once in 6-12 months; level 3 = possible, the event might occur several times or likely to once in 3-6 months, level 4 = likely, the event will probably occur on a monthly basis and level 5 = very likely, the event is likely to occur on a daily or weekly basis.

Dimension 2 Impact: level 1 = negligible, very small damage, the impact may not be observed, or affects or only results in unreasonable waste of resources; level 2 = minor, minor damage causing slight delay in minutes in work or little budget damage; level 3 = moderate, moderate damage causing 1-2 hour delay in work and damage to the budget at an extent that need to be acknowledge or approved by the management; level 4 = major, critical damage causing delays in work for more than 1-2 hours or a day or more or causing damage to the budget at an extent that needed to be acknowledged or approved by the management, or the organization loses business opportunities and potential benefits; level 5 = severe or catastrophic, disaster, damage is very high causing system disruption for many days or permanent disruption which is unable to continue or very difficult for recover.

From the risk matrix, the risk can be classified into 5 levels, consisting of 1 - 3 = very low, 4 - 6 = low, 7 - 10 = moderate, 11 - 16 = high and 17 - 25 = extreme to provide a basis for risk identification and further organization's risk response.

Risk response

In risk response and management, the actions that should be taken to manage the risks are chosen according to the risk assessment results (Jing etal., 2014), considering the level of risk occurring and the value of risk management to the risk tolerance level (Jung & Kim, 2015). There are 4 risk response strategies (Gonen, 2011) as follows:

1) Risk avoidance involves managing an extremely high-level risk that is unacceptable and decision must be made in the operations, such as canceling the project or activity, purchasing new materials as replacement and using other alternative processes and so on.

2) Risk sharing involves distributing or transferring the risk to others in order to share responsibility.

3) Risk Reduction involves improving work systems or designing the new working methods in order to reduce the chance of occurrence or the impact to an acceptable level of the organization.

4) Risk acceptance involves accepting the risk because it is not worthwhile to manage, control or prevent the risk, since it is likely to happen less and has little effect (Dhukaram etal., 2011).

COBIT 5 areas

The Cobit 5 Framework is an internationally accepted guideline for control and IT organization management to achive organization objectives that help enterprises optimum value from IT management by balancing of risk and benefit to make the most of resource. (ISACA, 2012) The benefit of Cobit 5 Framework are applicable to almost every organization including government and business organization that different in process and business scale.

The COBIT 5 framework is the business framework for IT governance that aims to supervise and manage the organization's IT systems and to reduce the potential risks of IT Systems (Susanti & Sucahyo, 2016). It can facilitate the IT security management and increase performance to maximize benefits (Wolden etal., 2015). The COBIT 5 framework defines the scope of control with COBIT 5 areas as follows (ISACA, 2012):

Area 1 align, planning and organize (APO): Corporate planning and management allows corporate executives to align IT and business strategies, encourages workers to gain knowledge and understanding of IT risks and management strategies for potential IT risks in the organization.

Area 2 build, acquire and implement (BAI): The provision and installation of IT projects to be developed or implemented which can be used to solve problems or support the operations of the organization on time according to the specified budget.

Area 3 deliver, service and support (DSS): Delivery and maintenance of the new information system to be used so that they can work efficiently and meet the organization's needs and to effectively control changes that may affect the operations of the organization.

Area 4 monitor, evaluate and assess (MEA): Monitoring of IT services can support operations in accordance with the goals and mission of the organization so that IT systems can be used in the operations of the organization for better performance and safety, including confidentiality, integrity and availability.

Area 5 evaluate, direct and monitor (EDM): The evaluation of IT system performance can detect potential problems before occurrence and can support the organization’s mission. Control, compliance, and performance risks are monitored and reported to the top executives.

All COBIT 5 areas allows the organization to assess their operations, supervision and management of IT systems in order to identify the risks that need to be controlled to keep them at the risk tolerance (Jung & Kim, 2015). This results in effective and safe use of IT systems for the benefit of all stakeholders and organization (ISACA, 2012).

Experimental design

This study is an experimental research for assessing the risks of information security management system in order to ensure the reliable and comprehensive survey results. The tools used in this study included interview, observation and record to find facts according to

predetermined objectives (Park et al., 2007). For the diversity of risk assessment and for the purposes of comparison to find the guidelines for risk management, 6 organizations including 3 government organizations and 3 business organizations. To show the various the organization culture and different processes in both of government and business including the number of staff that effect the organization risk and problem solving. In addition, period of time and budget are the important factors on risk management in the different employee scale that selected in range 1) 100 people 2) 100-500 people 3) 500 people respectively from 1) office level, 2) division level and 3) department level of ministry respectively. This study conducted the same method in government and business organization namely 1) limited partnership, 2) company limited (DBD, 2019) and 3) the public limited company (PLC) (SET, 2019) respectively. They were selected in this study using purposive sampling. Interview and data collection were performed with 5 people from each of these 6 organizations, a total of 30 people.

The sample consisted of personnel who were involved in the management and supervision of IT systems at different levels such as chief information officer (CIO), IT consultant, IT manager, system engineer, system administrator and IT support. Two experiments were conducted, the fist experiment was conducted in the second quarter of 2018 and the second experiment was conducted in the second quarter of 2019. The experiments were conducted using 3 methods: 1) interview, 2) observation and 3) survey based on empirical evidence as an experimental framework for this study. Risk assessment was conducted by 3 people; researcher, IT external auditor and IT manager of each organization.

The implementation life cycle (Youssfi etal., 2014)

In the first experiment, COBIT 5 areas were used for risk identification in order to cover the scopes of COBIT 5 areas and risk assessment was also performed to determine risk level of the organization and to manage the risk response using appropriate strategies. COBIT 5 implementation life cycle was used in order to apply the risk response strategies to control existing risks. After completion of the first experiment, the second experiment was carried out with the same experimental process as the first experiment. COBIT 5 implementation life cycle consists of 7 phases (ISACA, 2012) as shown in Figure 2.

Figure 2. COBIT 5 framework implementation life cycle (ISACA, 2012)

Phase 1: The starting point for raising awareness and building a consensus in the need to solve problems at both the management and the operator levels.

Phase 2: Defining the scope of operations as a framework for achieving organizational goals and IT goals.

Phase 3: Setting targets for improvement, specify details that can be used as a comprehensive and rapid solution to problems

Phase 4: Planning an integrated problem-solving process to put into action by defining the projects that are in line with the organization' business, as well as having backup plans for dealing with changes.

Phase 5: The comprehensive resolution process after consideration is established as a daily operation.

Phase 6: For sustainable operations, measures, evaluations and monitoring of operations must be defined in accordance with the organization' business.

Phase 7: Review of the overall success of the implementation initiative, specify the supervision and management of IT systems that should be added and promoted for continuous development.

The multiple iterations of the processes in this cycle will lead to effective IT governance and management.

Experimental results

Risk assessment was conducted by 3 risk management experts without the personnel of the organization in order to prevent prejudice and bias which might affect the assessment. The average risk levels of each organization and the overall average risk levels across these 3 organizations were also determined using the results from all 3 experts. Risk assessment in the first experiment provided the risk levels of each organization. The risk levels of these organization were calculated by average risk from researcher, IT external auditor and IT manager as shown in table 1.

Table 1. The risk assessment results in the first experiment

COBIT 5 areas	Government organizations						Business organizations					
	A	B	C	$\overline{X}$	S.D.	Risk	D	E	F	$\overline{X}$	S.D.	Risk
1: APO	9.3	7.7	10.3	9.1	1.7	Moderate	15.7	15.7	20.3	17.2	3.1	Extreme
2. BAI	9.0	8.7	8.3	8.7	0.7	Moderate	20.0	23.3	20.3	21.2	3.8	Extreme
3. DSS	14.3	12.3	10.7	12.4	2.2	High	13.3	15.7	18.7	15.9	2.8	High
4. MEA	20.3	21.7	23.3	21.8	3.1	Extreme	9.3	9.3	9.0	9.2	2.5	Moderate
5. EDM	21.7	23.3	25.0	23.3	2.4	Extreme	14.3	12.3	15.7	14.1	2.4	High

According to the risk assessment in the first experiment, government and business organizations had different risk levels in each area due to many factors and difference in operating processes as follows:

Area 1 align, planning and organize (APO): The government organizations in this study had distinct organization chart and IT master plan defining development plans, problem prevention, or the use of IT systems over the long term of 3-5 years. However, they still lack concrete implementation and there was no an annual IT action plan in accordance with such long-term policy plan. In addition, there was an IT security plan which could identify the risks

affecting IT systems but there was no business continuity management (BCM) operation to prevent risks and to provide a framework for operations in case of system errors or disruptions. In addition, it was found these organizations had no IT policies that specify rules, regulations, including penalties for the use of IT systems, resulting in the moderate level of risk with an average of 9.1. For business organizations, it was found that the risk level was higher than to those of the government organizations because most of them had organization charts, but they had not been updated, making it difficult to determine the chain of command and there was no policy related to complete IT systems. In addition, the policies were not complete, including the IT master plan, IT action plan, IT security plan, BCM and IT Policy, resulting in the extreme level of risk with an average of 17.2.

Area 2 build, acquire and implement (BAI): According to the results, the government organizations had drafted the terms of reference (TOR), procurement of IT projects and specifications and installation procedures were clearly defined in the TOR. However, budget requests and TOR assignments were often delayed and unable to keep up with rapidly changing IT systems, resulting in the moderate level of risk with an average of 8.7. As for the business organizations, the risk observed was a result of procurement due to unclear specifications and some projects did not have an agreement covering the services of vendor. As a result, the installation of IT Systems was not in line with the objectives, additional costs and longer installation time than scheduled. This resulted in the extreme level of risk with an average of 21.2.

Area 3 deliver, service and support (DSS): For the government organizations in this study, the deliveries were inspected by the commission under the terms of the TOR, making them met the specifications. However, personnel and budgets were inadequate to maintain the system and the maintenance contracts for many systems expired and the contract has not been renewed. This resulted in the high level of risk with an average of 12.4. However, the opposite findings were observed for the business organizations. As there was no specific delivery committee appointed, and there was no documentation for inspecting the completeness of the delivery. However, with the use of this system, the person responsible for monitoring, problem solving and maintenance were appointed so that IT Systems could meet the operational needs of the organization. This resulted in the high level of risk with an average of 15.9.

Area 4 monitor, evaluate and assess (MEA): It was found that in the government organizations in this study, IT services were not monitored and evaluated. In addition, these organizations used the file sharing system but there was no data classification policy specifying the type and priority of the data etc. This resulted in an extreme level of risk with an average of 21.8. On the other hand, as for the business organizations, key performance indicators (KPI) or objectives and key results (OKR) were defined for assessing the information services. However, there was still a problem with data classification policy as the government organizations. This resulted in the moderate level of risk with an average of 9.2.

Area 5 evaluate, direct and monitor (EDM): The government organizations in this study did not periodically monitor the IT systems to ensure their availability. In addition, the established IT security plan had not been used to control the risks in concrete, and there was no BCM plan including business continuity plan (BCP) testing which led to lack of confidence that the system will work when problems or errors actually occur. This resulted in the extreme level of risk with an average of 2 3 . 3 . For private sector organizations, IT systems were monitored regularly and there was also the preventive maintenance (PM). Risk management and BCM were also the problems as government organizations. This resulted in the high level of risk with an average of 14.1.

The first risk assessment was performed with the real situation to show the problem issue and risk in these organizations. Before assessment, baseline study was recored and applied COBIT 5 areas as a guideline of IT software management. After the risk assessment in the first experiment, the organization managed their risk response by selecting the appropriate strategies in each area using the COBIT 5 implementation life cycle in order to apply such risk response strategies in controlling the existing risks. After the completion of all operations, the second experiment was conducted and the results by the risk levels of these organization were calculated by average risk from researcher, IT external auditor and IT manager as shown in table 2.

Table 2. The risk assessment results in the second experiment

COBIT 5 areas	Government organization						Business organization					
	A	B	C	$\bar{X}$	S.D.	Risk	D	E	F	$\bar{X}$	S.D.	Risk
1: APO	4.3	2.3	2.3	3.0	1.2	Very Low	5.3	4.7	5.7	5.2	0.9	Low
2. BAI	2.3	2.3	2.7	2.4	1.2	Very Low	10.7	8.7	9.7	9.7	1.5	Moderate
3. DSS	5.7	7.7	4.3	5.9	1.7	Low	5.7	4.7	5.3	5.2	0.6	Low
4. MEA	7.7	9.3	11.3	9.4	1.8	Moderate	2.7	3.3	2.3	2.8	0.9	Very Low
5. EDM	8.3	6.7	7.7	7.6	1.7	Moderate	4.3	2.7	4.7	3.9	1.2	Low

Area 1 align, planning and organize (APO): For the government organizations, the annual IT action plan was prepared and implemented in accordance with the IT master plan. BCM was also implemented and IT policy was established. An average risk level of the government organizations decreased by 3.0 and was at very low level. For the business organizations, it was found that the organization chart was reviewed and updated and with various IT policies. However, some policies were incomplete and did not comply with actual operations. An average risk level of the business organizations decreased by 5.2 and was at a low level.

Area 2 build, acquire and implement (BAI): For the government organizations, after an annual IT action plan was established and in line with the IT master plan, each organization could plan its budget requests and establish TOR in time. An average risk level of the government organizations decreased by 2.4 and was at a very low level. For the business organizations, it was found that the contract with the vendors was entered into but there was still a clear specification as well as the output from the operation in accordance with the organization's objectives. An average risk level of the business organizations decreased by 9.7 and was at a moderate level.

Area 3 deliver, service and support (DSS): For the government organizations, it was found that the workload was assigned to the personnel for the maintenance of information systems. However, it did not cover all existing systems. An average risk level decreased of the government organizations by 5.9 and was at a low level. The business organizations defined the clear delivery criteria and the inspection committees were assigned for the high-value projects. An average risk level of the business organizations decreased by 5.2 and was at a low level.

Area 4 monitor, evaluate and assess (MEA): The government organizations defined the IT service assessment criteria and data classification policies. However, in the implementation, the lack of cooperation from management and the lack of enforcement with

the operators were observed. An average risk level of the government organizations decreased by 9.4 and was at a moderate level. The similar results were observed for the business organizations in this study. It was found that the business organizations defined the data classification polity, but the management gave priority to this policy and instructed the operators to strictly comply with the new policy. An average risk level of the business organizations decreased by 2.8 and was at a very low level.

Area 5 Evaluate, Direct and Monitor (EDM): It was found that the government organizations in this study assigned the person responsible for periodic system monitoring. However, the lack of cooperation and implementation were observed in risk control according to IT security plan and business continuity plan. An average risk level of the government organizations decreased by 7.6 and was at a moderate level. The business organizations monitored their IT system and risk prevention and BCM has been implemented but not yet complete. An average risk level the business organizations decreased by 3.9 and was at a low level.

Discussions and conclusions

From both experiments, before and after using COBIT 5 framework implementation life cycle according to the requirements of the COBIT 5 framework in all 5 areas, the comparison of risk assessment results between government and business organizations is shown in figure 3.

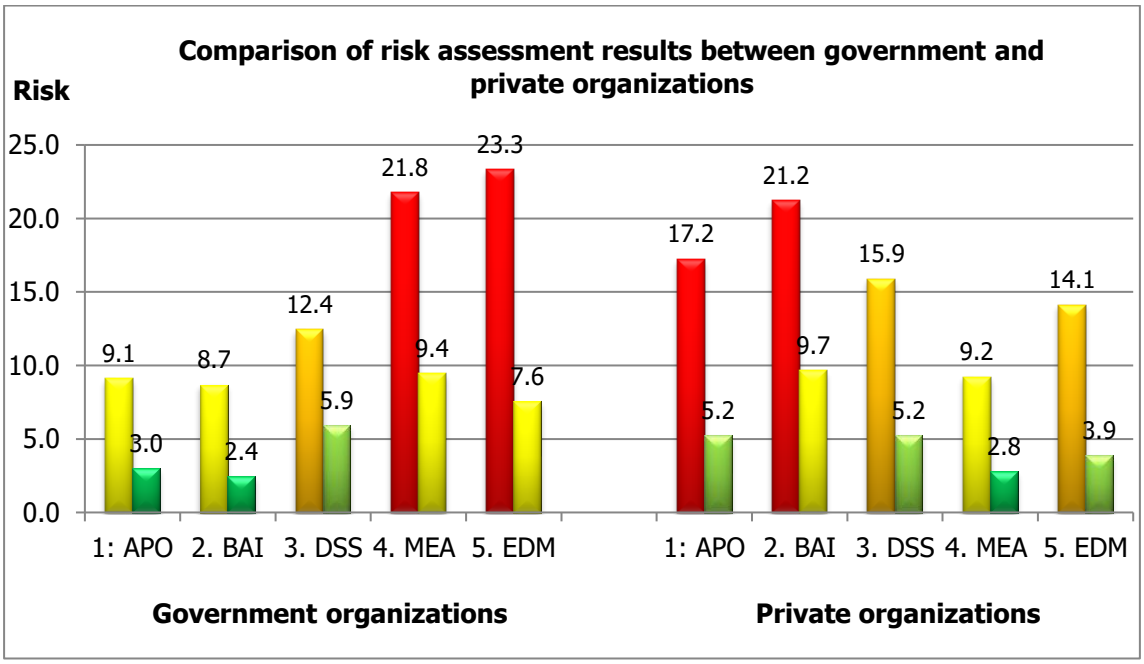

Figure 3 the comparison of risk assessment results between government and business organizations

The study of IT risk management in government and business organizations in Thailand using COSO-ERM based on COBIT 5 framework showed that the use of COBIT 5 implementation life cycle in risk control reduced organizational risks. In the first experiment, the

author observed that management and personnel in all 6 organizations recognized the importance of IT risk management. However, they lacked knowledge and understanding of IT system risk management in order to prevent the potential risks caused by errors or omissions of IT governance and to enhance the organization's business performance. After COBIT 5 areas were used to determine the extent of control along with the risk assessment in the first experiment, the government organizations showed a lower risk level in area 1 APO than that of the business organization. This is because government policies require government organizations to establish and prepare regulations, policies and plans, unlike business organizations that do not focus on policies, resulting in an extreme level of risk. For area 2 BAI, it was found that the government organization defined TOR with the qualifications and delivery, while the business organization did not define a clear TOR and scope of IT system development, resulting in an extreme level of risk and higher than that of the government organization. For area 3 DSS, both government and business organizations showed a high level of risk. The government organizations had IT delivery inspection, but the system administrator was not assigned. While the business organization did not have IT delivery inspection, but the system administrator was assigned. For area 4 MEA, it was found that IT service in the government organizations was monitored and evaluated, however there was no data classification police, resulting in an extreme level of risk. On the other hand, the business organizations focused on evaluation of performance of personnel at all levels and IT service with clear measures using KPI or OKR. For area 5 EDM, it was found that the government and business organizations had different levels of risk. The government organizations showed extreme level of risk because IT systems in these organization were not evaluated and there was no periodic system monitoring. In addition, the BCM was not given priority and awareness. While the business organizations gave priority to IT system monitoring and preventive maintenance (PM) and took regular actions.

From the second experiment, it was found that, the risk management using all 7 phases of the COBIT 5 implementation life cycle decreased the risk levels of both government and business organizations. However, it can be seen that there are still moderate and low levels of risk that need to be managed and controlled. The risk tolerance of all these 6 organizations should be at very low level for all areas or at low level for some areas. In this study, the differences in problems encountered by the government organizations were observed. In the initial stage of IT system development, the moderate level of risk was observed in area 1 APO and area 2 BAI. After the development of IT systems, there was no maintenance management, raising awareness of cooperation in the inspection and audit and surveillance for potential problems, resulting in an extreme level of risk in area 4 MEA and area 5 EDM. This is different from the business organizations which encountered problems in the initial stage of IT system procurement and development project. However, person in charge was assigned and the IT system maintenance was performed periodically, as can be seen from the extreme risk levels in area 1 APO and area 2 BAI. At the completion of IT system development, the risk levels in area 3 DSS, area 4 MEA and area 5 EDM decreased. The related factors consist of personnel who are ready to solve problems and sufficient time and budget for risk management. These 3 factors are very important factors allowing the organization to decide in risk response to keep the level of risk at its risk tolerance.

From risk identification in risk management indicated the different of organization scale has effected on the different risk management results which appeared on the cooperation and risk management acceptance especially small organization could manage and solve easier than large organization because of the good employee communication in a smaller group. The benefit of organization after applied risk management brought IT security system in that

organization. IT General Control was controlled by IT Governance who implement IT policy especially the confidence of director staff and other institutions related IT problem and business continuity management.

Future work

Risk assessment of government and business organizations reveals obstacles and context of the problems encountered in risk management and also provides the guidelines for developing the framework to be used in risk management in the future.

References

COSO. (2004). *Enterprise risk management – integrated framework (Executive summary and framework) The committee of sponsoring organizations of the treadway commission (COSO)*

DBD. (2019). DBD data warehouse+ The source of thailand's business information: department of business development, ministry of commerce. *Department of business development, ministry of commerce.* Department of business development, ministry of commerce. Retrieved June 26, 2019, 2019, from https://www.dbd.go.th

Dhukaram, A. V., Baber, C., Elloumi, L., Beijnum, B. van & Stefanis, P. De. (2011). *End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust.* Proceedings of the 2011 5th International conference on pervasive computing technologies for healthcare (Pervasive health) and workshops.

Fang H. (2005). *IC research about the AIS under the environment of the networks*. Proceedings of the 7th international conference on Electronic commerce, Xi'an, China.

Foley, S.N. (2009). *Security risk management using internal controls*. Proceedings of the first ACM workshop on Information security governance, Chicago, Illinois, USA.

Gonen, A. (2011). *Optimal risk response plan of project risk management.* Proceedings of the 2011 IEEE International conference on industrial engineering and engineering management.

ISACA. (2012). *Cobit 5 a business framework for the governance and management of enterprise IT*. United states of america: ISACA knowledge center.

Islam, Shareeful & Dong, Wei. (2008). *Human factors in software security risk management*. Proceedings of the first international workshop on Leadership and management in software architecture, Leipzig, Germany.

Jing, Z., Zhao, Y., Qiang, H, & Tian, W. (2014). *Risk response strategy research of water and sediment regulation system running schemes in the yellow river.* Proceedings of the 26th Chinese control and decision conference (2014 CCDC).

Jung, Yoonhyuk & Kim, Seongcheol. (2015). Response to potential information technology risk: Users' valuation of electromagnetic field from mobile phones. *Telematics and informatics, 32*(1), 57-66. doi: https://doi.org/10.1016/j.tele.2014.03.002

Khrisna, A, & Harlili. (2014). *Risk management framework with COBIT 5 and risk management framework for cloud computing integration.* Proceedings of the 2014 International conference of advanced informatics: Concept, theory and application (ICAICTA).

Park, J., MacRae, H., Musselman, L.J., Rossos, P., Hamstra, S.J., Wolman, S., & R.K., Richard K. (2007). Randomized controlled trial of virtual reality simulator training: transfer to live patients. *The American Journal of Surgery, 194*(2), 205-211. doi: http://dx.doi.org/10.1016/j.amjsurg.2006.11.032

Prasetyo, S., & Sucahyo, Y. G. (2014). *Information security risk management planning: A case study at application module of state asset directorate general of state asset ministry of finance.* Proceedings of the 2014 International conference on advanced computer science and information system.

Roberts, D. T. (2017). *Applying risk assessment at the worker level.* Proceedings of the 2017 Petroleum and chemical industry technical conference (PCIC).

Tangprasert, S. (2019, 13 - 15 December 2019). *Internal control for information technology security controls with COBIT 5 framework in enterprises.* Proceedings of the International conference robotics, informatics, and intelligence control technology (RIIT) 2019, Bangkok, Thailand.

SET. (2019). Companies or securities in focus. Retrieved on June 6, 2019, from https://www.set.or.th

Su, X., & Zhao, X. (2011). *Analysis on effects of risk management level on internal control.* Proceedings of the 2011 IEEE 18th International conference on industrial engineering and engineering management.

Susanti, R. Y. & Sucahyo, Y. G. (2016). *Information technology governance evaluation and processes improvement prioritization based on COBIT 5 framework at secretariat general of the Indonesian house of representatives.* Proceedings of the 2016 4th International conference on information and communication technology (ICoICT).

Wijanarka, H. (2014). *IT risk management to support the realization of IT value in public organizations.* Proceedings of the 2014 International conference on ICT for smart society (ICISS).

Wolden, Mark, Valverde, Raul & Talla, Malleswara. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine, 48*(3), 1846-1852. doi: https://doi.org/10.1016/j.ifacol.2015.06.355

Xiaosong, L., Shushi, L., Wenjun, C. & Songjiang, F. (2009). *The application of risk matrix to software project risk management.* Proceedings of the 2009 International forum on information technology and applications.

Youssfi, K., Boutahar, J. & Elghazi, S. (2014). *IT Governance implementation: A tool design of COBIT 5 roadmap.* Proceedings of the 2014 Second world conference on complex systems (WCCS).

Zhu, Y., Shi, L. & Hipel, K. W. (2012). *The identification of risk factors in brownfield redevelopment: An empirical study.* Proceedings of the 2012 IEEE International conference on systems, man, and cybernetics (SMC).