2010

Determinants of Successful ICT Risk Management in Thai Organisations

Siridech Kumsuprom
RMIT University, siridech.kumsuprom@rmit.edu.au

Brian Corbitt
RMIT University, brian.corbitt@rmit.edu.au

Siddhi Pittayachawan
RMIT University, siddhi.pittayachawan@rmit.edu.au

Phoommhiphat Mingmalairaks
RMIT University, phommhiphat.mingmalairaks@rmit.edu.au

DETERMINANTS OF SUCCESSFUL ICT RISK MANAGEMENT IN THAI ORGANISATIONS

Siridech Kumsuprom, School of Business Information Technology and Logistics, RMIT University, Australia, siridech.kumsuprom@rmit.edu.au

Brian Corbitt, School of Business Information Technology and Logistics, RMIT University, Australia, brian.corbitt@rmit.edu.au

Siddhi Pittayachawan, School of Business Information Technology and Logistics, RMIT University, Australia, siddhi.pittayachawan@rmit.edu.au

Phoommhiphat Mingmalairaks, School of Business Information Technology and Logistics, RMIT University, Australia, phommhiphat.mingmalairaks@rmit.edu.au

Abstract

This paper reports a study of the key factors that affect ICT risk management using Thai businesses as the data sources. Three hundred and two respondents from listed organisations on the Stock Exchange of Thailand (SET) were surveyed and the data analysed to establish the strength of relationships in a model derived from extant literature and the application of the two most commonly used governance standards for information and communication technology (ICT), COBIT and ISO/IEC 17799. The research shows that a small number of key factors have the most effect on successful ICT risk management, namely organisational policy, human resource management planning, organisational security and management of ICT. The focus of the research is to propose the successful ICT risk management model to organisations.

Keywords: ICT, Risk, Management, Planning and SEM.

1 INTRODUCTION

This paper reports a study of an integrated approach to organisational ICT risk management using a study of listed companies in Thailand. The adoption of ICT applications has brought risks to organisations. To effectively minimize and control risks, ICT governance framework are developed and implemented in organisations. ICT governance helps deal with risk management to aid achieving risk mitigation, risk prevention and risk avoidance (Stoneburner et al. 2002). This paper extends the work of Kumsuprom et al. (2008) who reported the imperative issues (see the conceptual model) of using the COBIT framework and the ISO/IEC 17799 standard (renumbered to ISO/IEC 27002) reflecting the key factors for dealing with ICT risk management in Thai organisations. This research highlights success factors based on the COBIT framework and the ISO/IEC 17799 standard in organisations for planning ICT risk management. Siponen and Willison (2009) argue that there is little research that proposes how the two standards can fit together in the context of an integrated approach to ICT risk management.

2 LITERATURE REVIEW

In the extant research literature there are a number of themes that emerge as factors impacting on ICT risk management in organisations. Ciborra (2006) argued that risk management emerged from people in organisations having a lack of knowledge, from the role of biased data when assessing risk in organisations and from the influence of internal politics. Levine (2004) and Hughes (2006) added that a lack of clarity of the roles and responsibilities of people impacted on successful risk management. Straub and Welke (1998) argued that human resource management is considered significant whilst dealing with ICT risk management. The reason is that the organisation needs senior management support in order to gain a thorough understanding of organisational vulnerability and of the resources required in securing organisational systems. It is necessary that senior management understand the security actions required and for them to integrate security planning into information security policy through adoption of organisational standards, and that users are trained and educated about security awareness in order that organisational standards can be reviewed and updated. Staff at all levels can help reduce risks; therefore, training programs, clarification of roles and responsibilities, and the identification of specific authority for specific roles must be provided for all staff (Hughes 2006) to ensure success risk management.

Smith and Eloff (2002) argued for a different emphasis, that ICT risk management was defined in terms of information and communication technology (ICT) and information security (IS) components. Specifically the ICT component is used to describe the scope of the ICT domain where ICT produces data throughout input, processing and output (IPO) and disseminates information to internal and external parties (Smith & Eloff 2002). This is used to control the ability of ICT used in IPO processes particularly in relation to ICT risks. Byrd et al. (1995) further suggested that effective ICT related architecture helped organisations define the strategy to drive, shape and control its architecture when dealing with ICT risk management. ICT architectures are specified by what types of hardware and software are employed; where personnel, equipment, data and facilities are located; the levels of applications, data and procedural compatibility that exist across locations (e.g. department to department, business unit to business unit); and how locations are connected, coordinated, and controlled (e.g. telecommunications networking) (Byrd et al. 1995).

Smith and Eloff (2002) also argued that another component of ICT risk management was information security (IS). Schultz (2007) provided guidance on how to mitigate ICT risks with regard to information security through proper management of physical security systems such as devices, process control systems and ICT infrastructure. Schultz (2007) further explained that for successful ICT risk management in organisations that senior management are responsible for understanding the configuration of networks, systems and ICT infrastructure, use of penetration tests, for supporting to management and audit functions, and for developing organisational information security policies (e.g. a corporate plan and an operational plan−a technical means). However, ‘many senior managers are

unaware that ICT security in their organizations is inadequate what the consequences of vulnerability may be' (Byrd et al. 1995, p41). Information security is used to describe the security domain where data and information is protected and rendered with 'identification and authentication, authorization, confidentiality, integrity and non-repudiation' (Smith & Eloff 2002, p. 268).

3 HYPOTHESIS DEVELOPMENT

This research built of those previously identified factors with reference to the most commonly accepted and used standards. From a different perspective the two standards addressing governance of ICT in business organisations focus on other factors as being more influential on successful ICT risk management. The COBIT framework is recognised as a top-down or high-level framework for governance and control over ICT risk (Khan 2006; Smith & McKeen 2006). The main purpose of the COBIT framework is to clarify business-focused, process-oriented, control-based and measurement-driven objectives and requirements through business process and ICT systems in organisations (ITGI 2007). The COBIT framework was established as ICT control practices to help senior management direct their responsibility with regard to an organisation's assets by aligning the requirements in terms of business risk, control needs, and technical issues (Bodnar 2006). The COBIT framework also describes the information process requirements that match the broader classes of ICT control used by organisations to achieve its objectives and goals (Bae et al. 2003).

The COBIT framework assists senior management to build ICT processes and controls which are appropriate for implementing and developing ICT governance and management for dealing with strategic and operational risks in ICT risk management (Smith & McKeen 2006). The COBIT framework provides senior management with management strategies for ICT resources in four domains: planning and organising; acquiring and implementing; deliver of services and support; and monitoring and evaluating (ITGI 2007). Within these four domains, the standard defines how ICT infrastructure and systems can be managed and controlled to support ICT functions for users and how ICT infrastructure and systems can be maintained to ensure that ICT performance meets business objectives and goals (ITGI 2007). As a result, the COBIT framework emphasises the policy for and management of ICT infrastructure and systems when dealing with ICT risk management (ITGI 2007). Policy is considered in the COBIT framework to provide the clear direction of the role and responsibility of executives and the Board of Directors to manage ICT related risks (ITGI 2007). In addition, management of ICT risk management is considered in the COBIT framework to assure that ICT processes and controls can maintain the value of ICT, and ensure that the enterprise's ICT supports business objectives.

The ISO/IEC 17799 standard provides a focus on the details of organisational information security practices (ISO/IEC 2005). This standard is used more as a set of lower-level guideline that details the specifics of how information security must be done for dealing with strategic, operational and technical risks in ICT risk management (Solms 2005). Furthermore, this standard is the focus of information security control at the operational level and helps the operational manager define precisely how control objectives can be used to achieve business objectives and goals in terms of their technical directions (Solms 2005).

The ISO/IEC 17799 standard helps organisations manage information security in defining asset management, physical security mechanisms and access control; in documenting information security policy and operational procedures; in reporting security incidents and in business continuity management (Myler & Broadbent 2006). Information systems security refers to the protection of all information system elements and the safeguarding of information integrity, that is, confidentiality, integrity and availability (Theoharidou et al 2005).

The ISO/IEC 17799 standard helps the operational manager assign information security roles and responsibilities (Groves 2003). By doing so, staff at different levels are responsible for different perspectives of the standard. For example, senior management is concerned with creating information security guidelines, the organisation of information security, human resource security, business continuity management and for compliance. Furthermore, at the operational level managers are concerned with taking action on technical matters such as setting access control policy, data and

information integrity management, data protection and for dealing with privacy. Theoharidou et al. (2005) mentioned that implementing the ISO/IEC 17799 standard can help organisations deal with insider threats by providing the control objectives regarding job descriptions of security staff, personnel screening, confidentiality agreements, security responsibility in the terms and condition of employment, and information security and training. Therefore, the ISO/IEC 17799 standard mainly focuses on technical or security policy, information security management and human resource management as supporting successful ICT risk management. Technical or security policy is considered to supplement the setting of ICT policy for the executives and the Board of Directors in the organisation to deal with ICT risk management. Human resource management is considered important in the ISO/IEC 17799 standard to provide information security during employment and for associated ICT risk management.

In summary, the extant literature, and both of the standards uses in ICT risk management from a governance perspective, have highlighted separate and sometime overlapping factors that have a significant influence on organisations being successful with ICT risk management. These are summarised in Table 1.

Research Literature	The COBIT framework focused on at the highest appropriate organisational level	The ISO/IEC 17799 standard focused on at the operational level
- Relevant policy in place	- Establishment of ICT policy regarding defining a strategic ICT plan and determining technological direction	- Establishment of an information security policy regarding information security policy document and review of the information security policy.
- Policy and mechanisms in place to protect ICT resources such as information assets, ICT infrastructures and ICT architecture	- Establishment of ICT resource management with regard to ICT infrastructure, ICT performance, ICT project.	- Not clearly defined
- Policy and mechanisms in place to manage human resources and defining roles and responsibilities	- Establishment of management of ICT human resources including training and educating programs.	- Establishment of human resources security for employment, during employment and termination or change of employment
- Policy and mechanisms in place to manage access control in physical and logical systems	- Establishment of a process for managing the physical environment	- Establishment of secure areas, equipment security, user access management, user responsibilities, network access control, operating system access control and application and information access control.
- Policy and mechanisms in place to manage business continuity planning	- Establishment of a continuous services plan	- Establishment of business continuity management and information security incident planning and management
- Implementation of control mechanisms to secure information, information systems and assets	- Establishment of an ICT security plan (an overall ICT security plan) regarding the ICT infrastructure and for developing of a security culture	- Establishment in the organisation of information security and asset management
- Implementation of control mechanisms to protect information integrity such as input, processing and output	- Establishment of ICT processes, technology infrastructure, and data management	- Establishment of information systems development and maintenance

(IPO) processes		
- Implementation of control mechanisms to protect threats and vulnerabilities of assets	- Not clearly defined	- Establishment in organisation of information security; internal organisation focusing on vulnerability of assets and external environment focusing on threats.
- Operationalisation of ICT management control	- Establishment of ICT processes by providing the control objectives for ICT management	- Not clearly defined
- Operationalisation of information security control	- Not clearly defined	- Establishment of information security processes by providing the control objectives for information security management

Table 1. A summary of key factors of successful ICT risk management in previous research, in the COBIT framework and in the ISO/IEC 17799 standard

From this table of factors, it became evident in the interviews (Kumsuprom et al. 2008) and from the classification used in COBIT and in ISO/IEC 17799 that 4 key areas appear to be, in combination, key indicators of successful ICT risk management. These are policy (POLICY), the management of people and their behaviour in organisations (HRMP), organisational information security management (OS), management of ICT infrastructure (IT) and the various plans that are created and used in organisations both at the corporate (CLP) and operational (OLP) levels for achieving successful ICT risk management (SICTRM). Successful ICT risk management can be achieved by senior management and operational managers perceive that organisations can achieve risk mitigation, risk prevention and risk avoidance (Stoneburner et al. 2002). The hypothesis used in this study, that 'the conceptual model of successful ICT risk management positively influences success factors of ICT risk management in Thai businesses,' concerns the whole model not parts of it because this model represents the whole system of successful ICT risk management (each key factor affects successful ICT risk management) rather than each path or each relationship in the model (Figure 1).

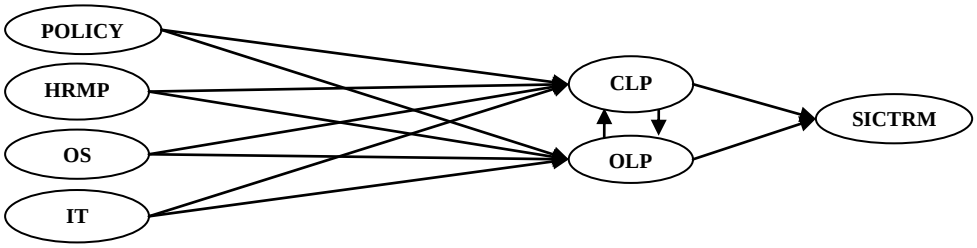

Figure 1. The conceptual model

The testing of the model is described below.

4 RESEARCH METHOD

This research used a stratified sample from the listed organisations on the Stock Exchange of Thailand (SET), because a stratified sample helps the researcher focuses on only the organisations that are familiar with managing ICT risks in organisations. The stratified sample exemplars were selected from an analysis of organisational structure regarding ICT infrastructure in combination with organisational reports to the SET. The samples chosen were from the bank, telecommunication and insurance industries. Several researchers have identified that the position levels which influence the planning of ICT risk management include the management level (Bodnar 2006; Damianides 2005; Smith & McKeen 2006) and the operational level (Gordon et al. 2006; Myler & Broadbent 2006). This means that the planning of ICT risk management in organisations involves staff members from these two position levels. Moreover, ICT risk management mainly relates to ICT control and audit, which involve the accounting, internal audits, information technology, information security and risk

management departments (Leung et al. 2003; Pickett 2005; Hardy 2006). As a result, three indicators—type of business, position level, and department—were factors in the researcher's choice of sample for the survey.

The organisational characteristics are also based on the assumption that these groups of people are representative of practitioners who are familiar with ICT risk management in an organisational context. Therefore, 11 banking, 25 technology and 17 insurance organisations comprised the sample in this research. Firstly, 11 banking organisations, each consists of five departments, and each department comprise three management and three operational levels (SET 2008). Secondly, 25 technology organisations, 18 of which have three departments, while the remaining seven organisations have four departments; each department has three management levels and three operational levels. Lastly, 17 insurance organisations, each consists of three departments, each with three management levels and three operational levels. The rationale for defining three samples in the management level and three samples in the operational level is that fixed samples would have the same chance of being chosen for the stratified random sampling by the researcher (Neuman 2006). Therefore, a group of management level staff was chosen to represent the position above assistant head of the department in each organisation; and a group of operational level staff representing the operational staff of each department in each organisation was selected.

A questionnaire was constructed from the research findings of Kumsuprom et al. (2008) in conjunction with the control objectives of both the COBIT framework and the ISO 17799 standard. A seven-point Likert scale ranged from Strongly Disagree (1) to Strongly Agree (7) was used to evaluate the hypothesis depending upon construct relationships. Prior to lunching the survey, a questionnaire was pilot-tested to validate content validity and was generated in an English version first and then in Thai. Two researchers were involved to validate the items representing sense and meaning clearly. Ten experts were used to validate each particular question in the questionnaire. After validating the questionnaire, the surveys were sent out by mail to organisations during a period from June to August 2008. A total of 302 respondents (53 out of 497 listed organisations) were returned back from 1,000 disseminated surveys (response rate=30.20%). The data was collated into SPSS 16 for data analysis.

5 DATA ANALYSIS

The constructs were validated with confirmatory factor analysis (CFA) to examine construct validity due to the latent variables and items were constructed based on the literature, previous research (Kumsuprom et al 2008), the COBIT framework, and the ISO/IEC 17799 standard. CFA was followed in AMOS 16 to calculate the reliability coefficients (i.e. coefficient H) of each factor. Coefficient H of POLICY, HRMP, OS, IT, CLP, OLP and SICTRM are 0.87, 0.83, 0.92, 0.86, 0.89, 0.92 and 0.89 respectively (Table 2). As a result, all factors hold good levels of reliability (H > 0.80).

Factor	Indicator	Coefficient H
POLICY	policy1-4	0.87
HRMP	hrmp1-4	0.83
OS	os1-4	0.92
IT	it1-4	0.86
CLP	clp1-4	0.89
OLP	olp1-4	0.92
SICTRM	sictrm1-3	0.89

Table 2. A summary of the reliability test

Discriminant validity was then followed to estimate the difference amongst constructs. This validity was performed on a pair of factors until the whole model had discriminant validity. Hair et al (2006) and Kline (1998) suggest that high correlation values (e.g. greater than 0.85) mean the two constructs lack discriminant validity. In this process, two groups of constructs were identified to lack

discriminant validity: the first group is HRMP and OS, and the second group is CLP, OLP and OSM. The correlation coefficients among these constructs are greater than 0.85, suggesting that they measure the same things. As a result, these factors were merged into two factors. The constructs HRMP and OS were merged and renamed to organisational information security management (OSM). According to ISO/IEC 17799 standard, organisation information security management (OSM) includes information security in itself and information security in people and their behaviour (ISO/IEC 2005). Thus, the researcher combined the two dimensions OS and HRMP to form a new factor called organisation information security management (OSM) (ISO/IEC 2005). Secondly, the constructs CLP and OLP, organisation theory was used to name the enterprise level plan (ELP), based on the claim of Christensen et al. (2007, p. 27) that 'reforming public organizations through restructuring does not necessarily lead to either centralization (or the corporate level plan) or decentralization (or the operational plan), but may involve both simultaneously'. Lastly, OSM and ELP were merged and renamed to enterprise security plan (ESP). The combination of OSM and ELP implies that the samples manage ICT risks by using information security at both the corporate level (i.e. a top-down approach) and the operational level (i.e. a bottom-up approach) (Solms 2005). Consequently, the new name ESP represents the data more clearly. After validating all constructs in the model again, AVE values of all constructs are greater than the squared correlations amongst constructs as shown in Table 3. Thus, all constructs in the revised model hold discriminant validity.

Factor			AVE			ρ^2
POLICY	<--->	IT	0.650	<--->	0.647	0.370
POLICY	<--->	ESP	0.658	<--->	0.751	0.612
POLICY	<--->	SICTRM	0.648	<--->	0.835	0.260
IT	<--->	ESP	0.647	<--->	0.750	0.632
IT	<--->	SICTRM	0.653	<--->	0.835	0.420
ESP	<--->	SICTRM	0.751	<--->	0.834	0.432

Table 3. AVE measures summary

The measurement model was then conducted to determine validity of the instrument. Hair et al. (2006) suggest that validity of an instrument is indicated by the factor loading of all indicators, standardized residual, critical ratio and modification indices. Four measures were applied to modify the measurement model to fit with the data. The factor loadings of all indicators were greater than 0.7, which means that all items represent the constructs well. The standardized residuals among the indicators were less than |2.5|, and critical ratios (CR) of all indicators were greater than |2|; as a result, only items that performed poorly were dropped from the analysis based on modification indices (MI) (Hair et al 2006). The results of indices represented the good fit measurement model as the values of $\chi 2$/df (113.762/59)= 1.928, p=.218, TLI=.982 CFI=.987, RMSEA=.056, SRMR= .029 and HOELTER (P=0.05)=207 (Table 4).

Indicator		Factor	λ	R^2	Model Fit	
					Indices	After Rectification
policy1	<---	POLICY	0.885	0.783	χ^2/df (113.762/59)	1.928
policy2	<---	POLICY	0.933	0.871	P-value	0.218
policy3	<---	POLICY	0.843	0.711	IFI	0.987
it1	<---	IT	0.826	0.682	TLI	0.982
it3	<---	IT	0.922	0.849	CFI	0.987
it4	<---	IT	0.881	0.777	RMSEA	0.056
esp1	<---	ESP	0.900	0.810	SRMR	0.029
esp2	<---	ESP	0.950	0.903	HOELTER ($p < 0.05$)	207
esp3	<---	ESP	0.932	0.869		
esp4	<---	ESP	0.890	0.792		
sictrm1	<---	SICTRM	0.919	0.845		
sictrm2	<---	SICTRM	0.943	0.890		
sictrm3	<---	SICTRM	0.887	0.787		

Table 4. The measurement model indices

The structural model (Figure 2) was used to show that all factors represented relevant dimensions. An analysis of SEM was performed with the maximum likelihood estimation (MLE) in combination with bootstrapping method to measure the relationship amongst dimensions in order to confirm or reject the research hypothesis. The outputs of the SEM indicated an overall good fit, with the values of χ^2/df (113.762/60)= 1.896, p=.251, TLI=.983 CFI=.987, RMSEA=.055, SRMR= .029 and HOELTER (P=0.05)=210.

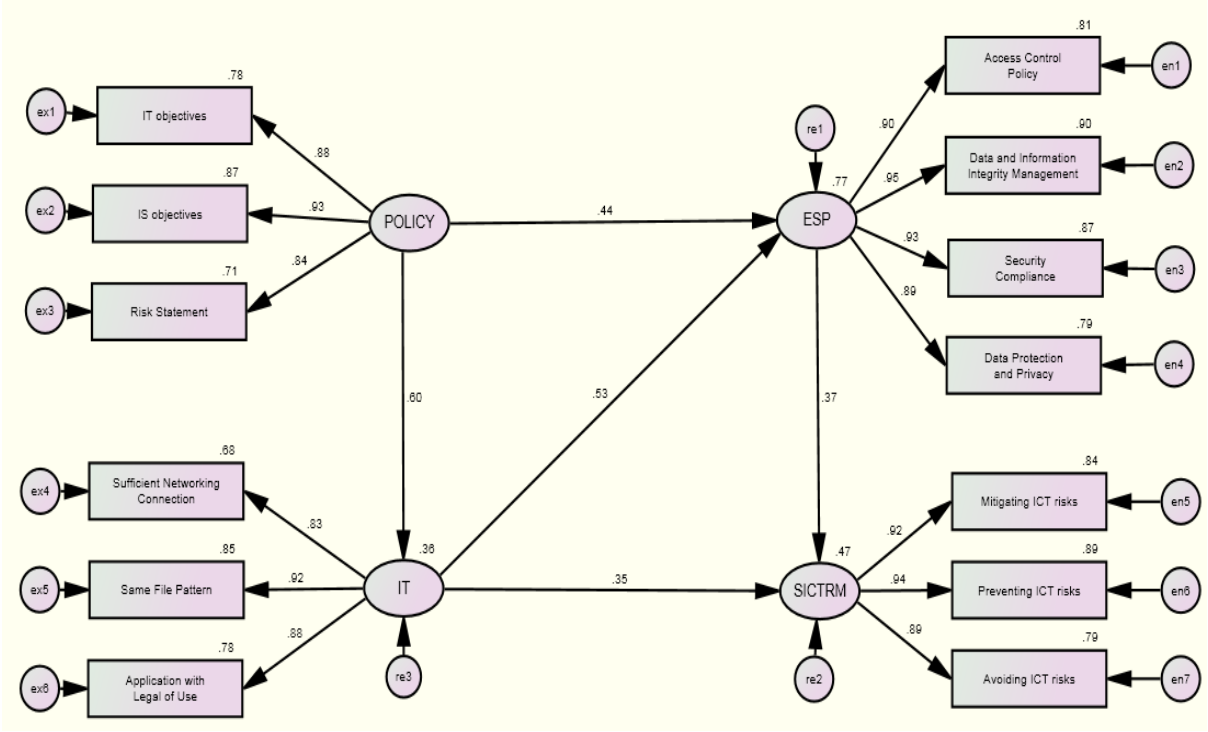

Figure 2: Successful ICT risk management based on the COBIT framework and the ISO/IEC 17799 standard

All indices met the requirements, which suggest that the structural model explains the data well. Moreover, the squared multiple correlations (R^2) for the structural model, which represent the amount of variance in each endogenous variable predicted by exogenous variables, were estimated. This research of ICT risk management using the COBIT framework and the ISO/IEC 17799 standard justified in Thai organisations identifies that organisational policy and management or ICT resources values of enterprise security plan, in combination with the corporate level plan, the operational level plan, human resource management planning, and organisational security, have a positive effect on successful ICT risk management. The estimation values of the structural model are χ^2=113.762, df=60, χ^2/df=1.896 and p=0.251. These measures indicate that the structural model has a good fit, which then leads to the conceptual model being rejected. The R^2 of the enterprise security plan is .77, which indicates that one exogenous variable (Organisational Policy) and one endogenous variable (Management of ICT Resources) explained 77% of the variance in the enterprise security plan (Figure 2). Likewise, the R^2 of the model was .47, which indicated that three latent variables (organisational policy, management of ICT resources and the enterprise security plan) explained 47% of the variance in successful ICT risk management. In contrast, 53% of unexplained variance in the successful ICT risk management model is also considered in terms of the optimisation of the model. Unexplained variances might result from the types of sample which derive from both the qualitative (Kumsuprom et al. 2008) and quantitative methods. The types of sample in the qualitative method include the banking and software development sectors that may affect the validation in the quantitative method. Both the banking and software development sectors might consider service management as other success factors, related to other standards (i.e. the ITIL framework and the Basel II accord), to deal with ICT risk management (ITGI 2007; Basel 2005).

6 DISCUSSION

This research then proposes that the success factors for ICT risk management in organisations are more likely to be organisational policy, management of ICT resources, and the enterprise level plan. Three success factors were therefore validated in the SEM in order to confirm the relationship and significance amongst factor for establishing successful ICT risk management in Thai organisations. SEM was further utilised along with maximum likelihood estimation (MLE) and bootstrapping (due to the small sample size and to boost accurate data) to further analyse the data. In bootstrapping, both the biased-corrected p-value (pbc) and the percentile p-value (ppc) were used with a 95% confidence level, as recommended by Byrne (2001), to ensure that results would not occur by chance.

The two p-values for the relationships between organisational policy and the enterprise security plan to establish successful ICT risk management are 0.002 (pbc) and 0.004 (ppc) respectively. It can be then argued that organisational policy has a positive effect (.441) on the enterprise security plan in establishing successful ICT risk management. Furthermore, organisational policy also has an indirect effect (0.323) through management of ICT resources on the enterprise security plan with the two p-values; 0.000 (pbc) and 0.000 (ppc) respectively. To apply organisational policy, information security (IS) objectives must be clearly defined in dealing with ICT risk management. In addition, it is necessary to formulate a risk statement to scope information security definitions so that Thai business organisations focus on the policy regarding information security management. These relationships then indicate that Thai organisations delineate organisational policy in terms of an enterprise security plan in IS strategy within its policy statements. This outcome will enable organisations to achieve its goals in dealing with ICT risks in both directions.

The two p-values for the relationships between organisational policy and management of ICT resources to establish the enterprise security plan and successful ICT risk management are 0.004 (pbc) and 0.004 (ppc) respectively. It can be argued then that organisational policy has a positive effect (.604) on management of ICT resources in establishing the enterprise security plan and successful ICT risk management. Moreover, organisational policy also has an indirect effect (.496) through management of ICT resources and the enterprise security plan on successful ICT risk management with the two p-values; 0.000 (pbc) and 0.000 (ppc) respectively. To apply this latent variable (organisational policy), information and communication technology objectives must be clearly defined in dealing with ICT risk management. In addition, it is necessary to formulate a risk statement to scope ICT resources definitions so that Thai organisations focus on the policy regarding management of ICT resources. These relationships then indicate that Thai organisations delineate ICT strategy as ICT objectives within its policy statements. This outcome will enable Thai organisations to achieve its goals in dealing with ICT risks in both directions.

The two p-values for the relationships between management of ICT resources and the enterprise security plan to establish successful ICT risk management are 0.006 (pbc) and 0.004 (ppc) respectively. This indicates that management of ICT resources has a positive effect (0.535) on the enterprise security plan in achieving successful ICT risk management. When reflecting on management of ICT resources, Thai organisations appear to ensure that database management (same data and file pattern) are considered when planning ICT risk management. Software license or applications with license can also assist Thai organisations to mitigate, prevent and avoid ICT risks. These relationships show that management of ICT resources and information security are distinct from each other. Management of ICT resources focuses on providing ICT facilities to all staff in Thai organisations. In contrast, the enterprise security plan focuses on information security control and audit instead.

The relationships between management of ICT resources and successful ICT risk management are revealed by two p-values of 0.004 (pbc) and 0.005 (ppc) respectively. This signifies that management of ICT resources has a positive effect (0.354) on successful ICT risk management in organisations. Furthermore, management of ICT resources also has an indirect effect (0.197) through the enterprise security plan on successful ICT risk management with the two p-value 0.018 (pbc) and 0.015 (ppc) respectively. This indicates that management of ICT resources (i.e. providing sufficient networking connection, maintaining the same data and information patterns in the same database system, software

licence or applications with license) are significant to help Thai organisations mitigate, prevent and avoid ICT risks. Focusing on only management of ICT resources, organisations can achieve successful ICT risk management.

Lastly, the relationships between the enterprise security plan and successful ICT risk management are revealed by two p-values of 0.026 (pbc) and 0.024 (ppc) respectively. This signifies that the enterprise security plan has a positive effect (0.369) on successful ICT risk management in organisations, although this factor is generated from the combination of human resource management planning, organisational security, corporate level planning and operational level planning. However, this does not mean that the indicators amongst the four factors are similar in content, but are in structure. In other words, all indicators are considered as one factor by combining two plans (at the corporate and the operational levels) to one plan, as per organisation theory (Christensen et al. 2007). Also, this combination of four factors is supported by the suggestion of Solms (2005), who claims that information security governance as in the ISO/IEC 17799 standard (including human resource protection and management, and organisational information security) needs to be considered at both the corporate and the operational levels. Consequently, the enterprise security plan plays a vital role successfully dealing with ICT risk management.

7 CONCLUSION

This research sought to identify and then model the success elements of ICT risk management in a sample of Thai business organisations. This research supported and confirmed previous research (Kumsuprom et al. 2008) that argues that policy must be structured, first at the board of directors and then at the levels of senior management and operational management, who together must delineate the procedures and practices for dealing with ICT risk management. In dealing with ICT risk management, several frameworks and standards have been introduced but ICT risks still persist, therefore, the implication of this research was that we can learn from the Thai organisations that organisations needed to consider the success factors when managing ICT risk management. This research proposed that three main success factors affect ICT risk management in Thai organisations. Firstly, the effective organisational policy helped the Thai organisations to plan the effective management of ICT resources and the effective planning of enterprise information security. Secondly, the effective management of ICT resources facilitated the planning of enterprise information security to achieve successful ICT risk management planning. In addition, the survey results have shown that effective organisational policy was the main influence on the management of ICT resources and the planning of enterprise information security. All three success factors complement each other and were significant together in terms of strategic development (i.e. policy) and strategic implementation (i.e. management direction). Lastly, the effective planning of enterprise information security was shown to be a critical factor that helped an organisation mitigate, prevent and avoid operational, technical and strategic risks related to ICT. All three success factors were initially drawn from both the COBIT framework and the ISO/IEC 17799 standard and were found to positively contribute to successful ICT risk management.

References

Bae, B. Epps, R.W. and Gwathmey, S.S. (2003). Internal control issues: The case of changes to information processes. Information Systems Control Journal, 4, 44-46.

Bank for International Settlements, Basel (2005). International Convergence of Capital Measurement and Capital Standards, Basel, Switzerland.

Bodnar, G.H. (2003). IT Governance. Internal Auditing, 18 (3), 27-32.

Byrd, T.A. and Sankar, C.S. and McCreary, J.D. (1995). The strategic risks of implementing global information technology. Information Strategy, 12 (1), 39-43.

Byrne, B.M. (2001). Structural Equation Modeling with AMOS : Basic Concepts, Applications, and Programming, Multivariate applications book series: Lawrence Erlbaum Associates, Mahwah, New Jersy.

Christensen, T., Lægreid, P., Roness, G.P. and Røvik, K.R. (2007). Organization Theory and the Public Sector: Instrument, Culture and Myth. Routledge, New York, USA.
Ciborra, C. (2006). Imbrication of representations: Risk and digital technologies. Journal of Management Studies, 43 (6), 1339-1356.
Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance, Information Systems Management, 22 (1), 77-85.
Gordon, L. A., Loeb, M.P., Lucyshyn, W. and Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities, Journal of Accounting and Public Policy, 25 (5), 503-30.
Groves, S. (2003). The unlikely heroes of cyber security. Information Management Journal, 37 (3), 34-42.
Hair, J., Black, W., Babin, A. and Tatham, R. (2006). Multivariate Data Analysis. 2nd Edition. Prentice-Hall, New Jersey.
Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges, Information Security Technical Report, 11 (1), 55-61.
Hughes, G. (2006). Five steps to IT risk management best practices. Risk Management, 53 (7), p. 34-37.
Kline R.B. (1988). Principles and Practice of Structural Equation Modelling. Guilford Press, New York.
Khan, K. (2006). How IT governance is changing. Journal of Corporate Accounting & Finance, 17 (5), 21-25.
Kumsuprom, S. Corbitt, B. and Pittayachawan, S. (2008). ICT risk management in organizations: Case studies in Thai business. In Proceeding of the 19th Australasian Conference on Information system, New Zealand.
Leung, P., Cooper, B.J., and Robertson, P.T. (2003). The role of internal audit in corporate governance & management, School of Accounting and Law, RMIT University, Institute of Internal Auditors (Australia), Melbourne.
Levine, R. (2004). Risk management systems: Understanding the need. EDPACS, 32 (2), 1-13.
Myler, E. and Broadbent, G. (2006). ISO/IEC 17799: standard for security. Information Management Journal, 40 (6), 43-52.
Neuman, W. (2006). Social research methods: Qualitative and quantitative approaches, 6th Edition, Pearson, Boston.
Pickett, K. (2005). The essential handbook of internal auditing, John Wiley & Son Ltd, Hoboken, New Jersey.
Schultz, E.E. (2007). Risks due to convergence of physical security systems and information technology environments. Information Security Technical Report, 12 (2), 80-84.
Siponen, M. and Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46 (5), 267-70.
Smith, E. and Eloff, J.H.P. (2002). A prototype for assessing information technology risks in health care. Computers & Security, 21 (3), 266-84.
Smith, H.A. and McKeen, J.D. (2006). Developments in practice XXI: IT in the new world of corporate governance reforms. Communications of the Association for Information Systems, 17 (1), Article 32.
Solms, B. V. (2005). Information Security governance: COBIT or ISO 17799 or both?. Computers & Security, 24 (2), 99-104.
Stoneburner, G. Geguen, A. and Feringa, A. (2002). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. National Institue of Standard and Technology (NIST), Publication SP 800-30.
Straub, D.W. and Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 20 (4), 441-469.
The Internaltional Organization for Standardization and the International Electrotechnical Commission, ISO/IEC (2005). Information Technology Security Techniques-Code of Practice ISO/IEC 17799:2005. ISO/IEC, Switzerland.
The IT Governance Institute, ITGI (2007). COBIT 4.1 Framework: Control Objectives Management Guidelines Maturity Models. ITGI, Illinois, USA.

Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799, Computers & Security, 24 (6), 472-484.