International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 13, Issue 6, 2020

Factors Influencing Process Structuring in IT Risk Management

Urairat Maneerattanasak[a*], Nitaya Wongpinunwatana[b], Chainarong Kaeowaranonchai[c], Metha Suvanasarn[d], [a]Thammasat Business School, Thammasat University, Bangkok, Thailand, [b]Department of Business Administration (Management Information Systems) Thammasat University, Bangkok, Thailand, [c]Freelance IT Auditor, Bangkok, Thailand, [d]IT GRC consultant, Bangkok, Thailand, Email: [a*]urairat-man59@tbs.tu.ac.th, [b]wongpinn5@gmail.com, [c]Ckaeowaranonchai@gmail.com, [d]suvanasarn@gmail.com

Information technology risk management (ITRM) is being enforced by regulators on strategic and complex organisations such as financial institutions. This research paper investigates risk management problems uncovered while doing case study analysis with selected organisations. This study revealed that factors most impacted by organisation size are tools, interdependence and expertise of the three lines of defence. The findings imply that risk management tools need development to fit with the interdependent working of the three lines of defence structure. Also, people in the organisation need training to improve risk management expertise and to drive the three lines of defence to work effectively. Size of an organisation also impacts ITRM practice. Furthermore, the results of this research reveal problems different from previous ITRM research as most of the prior research suggested improving ITRM processes and models. The theoretical contribution of this research is the framework of principles and practice fit focusing on process structuring.

Key words: *IT risk management, principle and practice fit, case study analysis.*

Introduction

Information technology (IT) risks can be identified, analysed and controlled by IT risk management processes. Even though IT risk management (ITRM) has been implemented in organisations for a number of years, and is enforced by regulators such as the central bank of Thailand, threats and vulnerabilities still cause great losses to organisations, including to financial institutions. IT risks are part of operational risks because organisations very often design their business operations to be dependent on IT. Operational risk failures may lead to severe damage to a company. Thus, management of operational risks is as important to an entity as ITRM.

ITRM consists of several processes as a cycle. There are several widely-accepted frameworks, principles and guidelines developed by professional associations and organisations which are designed to be applied by organisations. Organisations of any size can apply them depending on the level of their resources and risk needs. The frameworks, principles and guidelines after being applied by an organisation are assessed if they meet the maturity model. The maturity model measures the state of implementation of risk management tools, risk culture, and level of controls.

A literature review was conducted on prior academic research. Some academic research focusing on risk management frameworks (Agrawal, 2016; Bandyopadhyay et al, 1999; Pereira et al, 2012; Shameli-Sendi et al, 2015; Suh et al, 2003) found that estimation methods are difficult to apply. Additionally, some studies (Gelbstein, 2016; Kouns et al, 2010) claimed that experts hired by organisation often incorrectly identify risks and that incorrect identification leads to incorrect treatment. Also, academic research (Kouns et al, 2010; Schmittling et al, 2010) also strongly suggests that robust ITRM processes be established in an organisation.

This research paper investigates the present status of ITRM practice of leading financial institutions in Thailand, including successes and obstacles, and the issues these organisations face. The institutions studied were selected from a list of commercial banks registered in Thailand (The Bank of Thailand, 2016). The research method utilised was interviewing relevant key persons in ITRM of the selected institutions. The case study analysis was conducted by reviewing the content of the interview transcripts.

The remainder of this paper consists of a theoretical background, including general risk management frameworks and principles (principles), the three lines of defence (people), and ITRM processes (processes). The research methodology is described in Section 3. Case study analysis and interpretation is explained in Section 4. The discussion of the results is presented in Section 5. Finally, research limitations and any potential future work issuggested.

ITRM Principles, People and Processes

The theoretical background of this research is the task-technology fit (TTF). The well-known TTF theory was proposed by Goodhue and Thompson and published in MIS Quarterly in 1995 (Goodhue et al, 1995). TTF theory provides factors for measuring individual users' performance on their tasks. Performance of individuals utilising several systems of technology which was tested by researchers (Smith et al, 2010; El Said, 2015; Kilmon et al, 2008). TTF also was applied to other models and theories such as task-individual-technology fit (TITF) (Liu et al, 2011; Parkes, 2013), technology acceptance model (TAM) (Wu et al, 2017) and post-acceptance model (PAM) (Larsen et al, 2009).

Additionally, this concept was extended by applying it at the group level (Zigurs et al, 1998). Early TTF research aimed to demonstrate that the implementation of technology raises users' performance in completing tasks and decision making. Tasks matched with appropriate technology increase performance on those tasks. Process structuring is a part of technology implementation. For example, the process structuring of a group decision support system is built to facilitate managing group discussions and interaction (Zigurs et al, 1998). Nevertheless, most research still focuses on technology rather than process structuring.

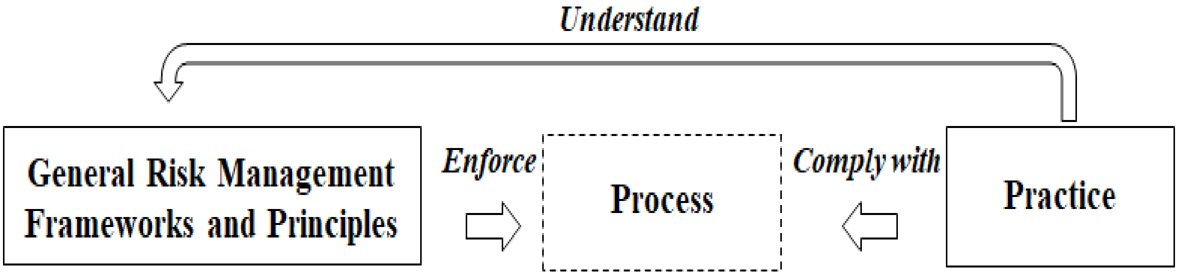
In the ITRM environment, people interact following general risk management frameworks and principles to facilitate the process and group discussions and decisions. Researchers are interested in the process structuring of ITRM and tend to investigate issues in depth to determine significant factors for further measuring performance. Therefore, researchers' interest is not only in technology, but also the structuring of relevant components such as principles, processes and people. The fit theory is still applied to the proposed framework. From the literature review, principle and practice theories are studied and chosen to be the primary constructs of the proposed framework in this research.

Principle theory is a guideline for productivity in management and governance. An organisation's practice is designed from principles to achieve its objectives. The understanding, compliance and enforcement of principles are considered success factors in principle theory. The finding of this study (Caldwell et al, 2006) showed that the signal of success is management support and enforcement, as well as practitioners understanding and complying with the principles. This concept is similar to applying general risk management frameworks and principles to design the ITRM process for an organisation.

An organisation's practices were studied (Feldman et al, 2011) using three approaches - empirical, theoretical, and philosophical. Practice theory, by examining it using an empirical approach, gives significance to people's actions in an operation that increases performance. The practice theory applies to ITRM practice. The people in an organisation must concentrate on tasks at hand in the ITRM process. The ITRM process needs expertise to identify critical operations, assets, threats, and vulnerabilities. Each process needs diverse sources of data and produces sufficient and necessary information to management for making effective decisions (Kouns et al, 2010). The ITRM outcomes are the efficiency and effectiveness in asset protection, detection and correction. Individual characteristics and expertise assist in doing tasks proficiently (DeSanctis et al, 1994; Parkes, 2013).

Accordingly, the proposed framework of principle and practice fit of risk management has components. These are general risk management frameworks and principles (principles), the three lines of defence (people), and ITRM processes (processes). Tools and technologies are classified as part of ITRM processes. Figure 1 shows the relationship of components in principles and practice fit framework

Figure 1. Relationship of components in principles and practice fit framework

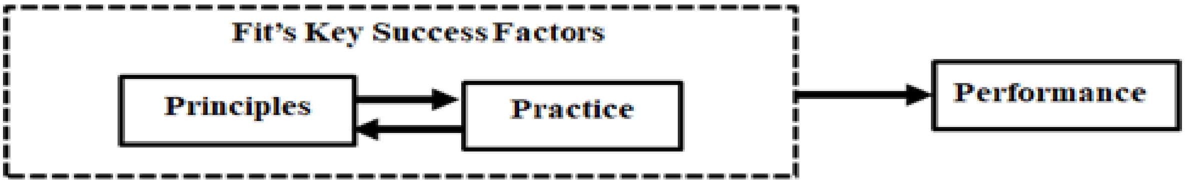


This study started with "ITRM principles" general risk management frameworks and principles and how well the organisations implement them in the case studies. There were two criteria used in selecting ITRM principles. The first criterion is the source of principles. General risk management frameworks and principles were selected from organisations such as the Committee of Sponsoring Organisations of the Treadway Commission (COSO), Information Systems Audit and Control Association (ISACA), International Organisation for Standardisation (ISO) and Basel Committee on Banking Supervision (BCBS). The second criterion is the type of risk management: enterprise risk management, operational risk management and IT risk management. Five general risk management frameworks and principles were selected to review: ISO 31000 and COSO ERM are enterprise risk management guidelines; Basel committee's principles are for operational risk management; ISO/IEC 27005 and Cobit□5 for Risk are IT risk management tools.

The key success factors (Maneerattanasak et al, 2017) were obtained from these principles (BCBS, 2011; ISACA, 2013; ISO, 2009, 2011; COSO, 2004) using content analysis. The key success factors are significant for the successful practice of ITRM. The obtained key success factors consist of understanding the organisation's context; the three lines of defence structure; the team's expertise, training and culture; ITRM process design; and communication. These factors are further used to investigate ITRM practice as well.

ITRM practice was investigated by using case study analysis from selected Thai financial institutions. The principles and practice fit is the proposed framework of this research. Results of the investigation are presented in Section 4, Key success factors of ITRM practice. Figure 2 shows the overall framework of principles and practice fit.

Figure 2. Overall framework of principles and practice fit



Research methodology

Case Selection

Matching case (Nielsen, 2016), balancing case, and randomisation (Bruhn et al, 2009) are three criteria for choosing the cases to study.

Matching case criterion considers cases that have a similar business environment so they can be validly compared with each other (Nielsen, 2016). The unit of analysis for choosing case studies in this research is organisations that use information systems and technology (IST) and ITRM functions as part of operational risk management and enterprise risk management (Gerring et al, 2016; Yin, 2003). The case studies selected in this research are financial institutions which are substantial users of ISTs and always are facing new cyber threats. The people in the case studies are directly involved in ITRM processes as part of the first and second lines of defence, and can, therefore, share current processes, current situations, successful experiences, and failures learned during implementation and current practice. The third line of defence is not a focus of this study, since it does not directly conduct the ITRM process. This research emphasises the significant factors affecting ITRM processes from the fit between principles and practice.

Balancing case criterion relates to properly grouping case studies (Bruhn et al, 2009). This research used multiple case studies in designing data collection. Three main criteria for classifying the selected case studies are from the classification used by the central bank of Thailand (BOT). First, commercial banks registered in Thailand according to the definition of the BOT are “Financial businesses under the Bank of Thailand’s supervision and examination”. Second, commercial banks are allowed to provide electronic banking services. Finally, the classification of bank size depends on the market share of total Thailand bank assets. Two banks from the large bank group, two banks from the medium bank group, and three banks from the small bank group were chosen for the case study analysis.

Randomisation criterion reduces bias from selection and classification of the case studies (Bruhn et al, 2009). There are two datasets with seven actual case studies. Each dataset contains a mix of sizes which are large, medium and small banks.

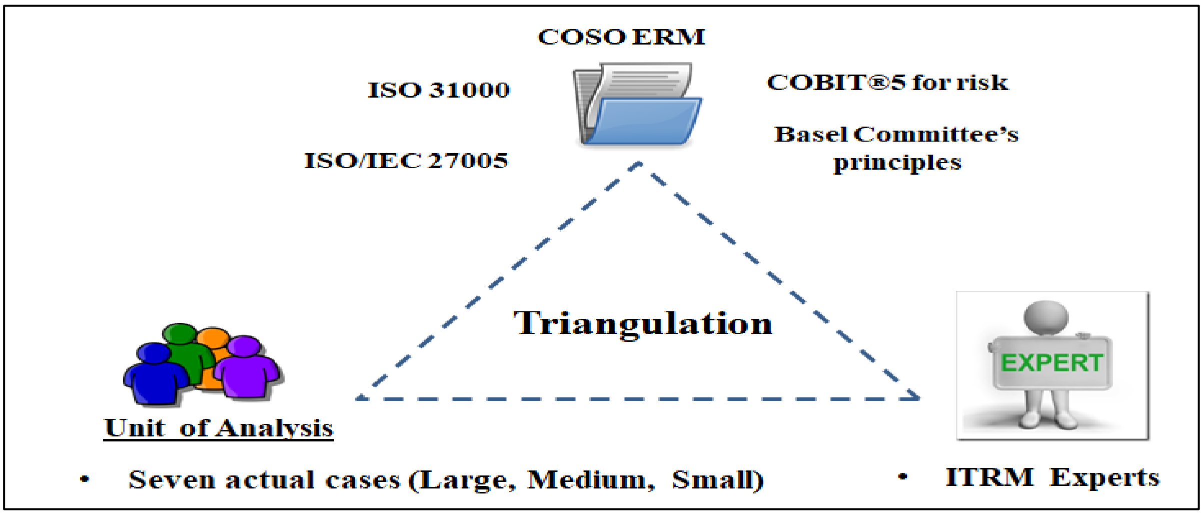
Case Study Analysis Approach

The case study analysis process consists of coding and interpreting by content analysis, translation, revision by ITRM experts and language editing by a native speaker. The data was evaluated by content analysis. Content analysis is a method to describe a message from interviewee to the audience, who in this study is the researcher (Neuendorf, 2002). The definition of content analysis matches the purpose of this research "a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns" (Hsieh et al, 2005). The case study interpretation aimed to investigate the fit and unfit factors between principles and practice constructs. In other words, the data was analysed to test the consistency of key success factors and to draw the fit patterns between data from the literature review and data from the case study interviews. Process tracing is a technique to trace the causal mechanism of the individual case study to determine the outcome. The tracing of causal path comes from statements given by the interviewee following sequential questioning about the ITRM practice in their organisation. The answers were compared to the content analysis from the general risk management frameworks and principles. The key success factors were used as the causal factors to make a causal inference as suggested by this study (George et al, 2005).

Quality of Research Method

The three methods used to check the validity of the qualitative research were researcher, participants and reviewer (Creswell et al, 2000). The researcher should be familiar with IT risk and control. The participants were interviewees. The reviewer was an external person, such as a domain expert, who can comment on the researcher's interpretation and classification.

Figure 3. Triangulation of qualitative research



The trustworthiness of case study analysis is typically tested to ensure validity (Riege, 2003; Yin, 2003), of constructs such as principle, practice and key success factors. The constructs can be tested using multiple sources of data, such as academic literature and general risk management frameworks and principles; participants involved in ITRM processes; ITRM experts; and experience of the researcher which normally called a triangulation of qualitative research as illustrated in Figure 3. Furthermore, financial institutions are leading organisations that use IST, and this infrastructure drives their business; at the same time, regulators enforce the implementation of ITRM processes. ITRM practices of financial institutions are expected to set an example to other non-financial organisations (Anney, 2014). Recently, ITRM processes of leading financial institutions were studied by organisations in other industries. That study was designed systematically - well-prepared case study protocols and the research were conducted strictly following relevant procedures to ensure the reliability of the research. The protocol that was developed contained questions, theoretical framework, letter of permission for an interview, collection of case study details and the outline of the case study report.

Key Success Factors of ITRM Practice

Key success factors of ITRM practice from the case studies were ranked using the number of counted quotations, as explained in Section 3.2, Case study analysis approach. First ranked is ITRM process design, second ranked is understanding organisation's context, third ranked is team's expertise and training, fourth ranked is the three lines of defence structure, and fifth ranked is communication.

ITRM Process Design Ranking

The three methods used to check the validity of the qualitative research were researcher, participants and reviewer (Creswell et al, 2000). The researcher should be familiar with IT risk and control. The participants were interviewees. The reviewer was an external person, such as a domain expert, who can comment on the researcher's interpretation and classification.

Rank First: Tools and Techniques

As determined in this research, GRC tools have been implemented in some of the organisations studied, and these tools are not suitably fitted to ITRM practice. Other organisations studied have not yet implemented GRC tools at all. Nevertheless, the case studies share specific tools and techniques which are in use currently. The content from interviewing the organisations presents that (1) tools and techniques for risk identification are brainstorming workshops, process mapping, penetration testing and vulnerability scanning, and risk and control self-assessment templates. (2) Tools and techniques for risk analysis are root cause analysis, most-likely worst case, ranking identified risks by voting, business impact analysis, and risk matrix representation. (3) Tools and techniques for risk evaluation are risk matrix and risk acceptance. (4) Tools and techniques for risk monitoring are risk monitoring indicators and dashboards. (5) Other tools and techniques have been implemented, such as GRC integration tools, analyses using Microsoft Excel, monitoring systems, and key performance indicator systems. The problems shared in the case studies are lacking effective tools and incorrect data input in the system.

Ranked Second: Risk Identification

First significance in risk identification found in the case studies is the accountability of risk owner and experience of the first and second lines of defence. The second most significant is to identify potential risks from various sources such as incident records, management concerns and lessons learned from organisations in the same industry. Experience gained from the second line of defence can help in identifying risks. Problems of risk identification revealed in the case studies are neglect of the first line of defence, the conflict between business units and IT (the first line of defence), underestimation of potential risks, the inexperience of the second line of defence, and management ignoring the concerns.

Ranked Third: Risk Analysis and Risk Evaluation

For risk analysis, the case studies emphasised impact, likelihood, existing controls and risk monitoring indicators. One organisation studied focused on the capability of the second line of defence in risk aggregation and validation. Another case study warned about incorrect analysis from hidden risks. For risk evaluation, the case studies emphasised the authority of decision-makers for rating risks, and treatment method or risk acceptance.

Rank Fourth: Risk Monitoring

The case studies discussed the period of monitoring of potential risks from uncertain events. The proactiveness of the second line of defence to timely alert the risk monitoring process of issues also was shared in one case study. Finally, all case studies focused on monitoring potential risks rather than monitoring the efficiency and effectiveness of risk management processes.

Ranked Fifth: Risk Treatment

The case studies focused on controls implemented during system development.

Understanding Organisation's Context Ranking

Understanding an organisation's context consists of six indicators, which also were ranked. The indicator ranked first is policies, standards and procedures. Interdependence is the second ranked indicator. The third ranked is internal and external environments. The fourth ranked is end-to-end process, and the fifth ranked is objectives, strategic direction and current risk. Data criticality ranked sixth.

Ranked First: Policies, Standards and Procedures

All organisations studied comply with government regulations, internal policies and processes, and are responsive to their stakeholders. Policies, standards, and procedures have been adopted from various sources such as general risk management frameworks and principles. Organisation size does not affect this indicator.

Ranked Second: Interdependence

Effective risk assessment depends on (1) judgement and decisions of the first line of defence, (2) senior participants' involvement and support, and (3) collaboration and good relationships between the business units and IT department. The characteristics of the second line of defence, such as proactiveness and intensive action when required, are as significant as the expertise and experience of the first line of defence in risk management processes. An effective design of the three lines of defence helps to reduce shortcomings in risk management and increases cooperation and connectivity of each line of defence. Three case studies specified the significance of the three lines of defence's interdependence. Furthermore, the case studies also confirmed that organisation size is a significant factor in the interdependence of risk management processes. A problem of large organisations, due to their department-based working arrangements, is a lack of attention and involvement of people in the three lines of defence. It can be difficult to obtain cooperation from the first line of defence with the second and third lines. Negative attitudes and lack of time in the first line of defence, as well as getting the attention of senior management when issues arise, are as significant as a deficiency of expertise in the second line of defence. Inappropriate action of the third line of defence's role is an obstacle of the risk management process.

Ranked: Internal and External Environments

Regarding the external environment, all organisation studied emphasised the importance of complying with government regulations. Also noted was using existing data and information effectively and outsourcing some processes to external experts. Internal environment concerns obtained from the case studies are attention, awareness and experience of people. Data and information of applicants gathered in the recruitment process are useful for determining where they may fit in the first line of defence. Three case studies stressed this indicator.

Ranked Fourth: End-To-End Process

Effective end-to-end designs of a business process incorporate appropriate risk identification systems, also end-to-end. Data and information from an end-to-end business process provided by the first line of defence and obtained from historical incidents increase effective risk assessment. The second line of defence should understand the end-to-end business process and the related end-to-end risk management process. This indicator is stressed by one case study and supported by others.

Ranked Fifth: Objectives, Strategic Direction and Current Risks

All organisations studied stressed IT risks. Senior-level staff interviewed focused on strategic direction and risks that impact business operations.

Ranked Sixth: Data Criticality

Only two case studies emphasise this indicator. Data criticality is important for indicating the control level required to mitigate risk and for estimating the valuation and severity level of data and systems.

Team's Expertise and Training Ranking

There are two indicators in this category expertise of the three lines of defence (first ranked), and risk awareness culture and training of the three lines of defence (second ranked).

First Ranked: Expertise of the Three Lines of Defence

The accumulated experience in business concepts and operations, and risk management processes are required skills of the first and second lines of defence. Internal characteristics and soft skills such as proactiveness, interpersonal skills, and adaptation are necessary. However, employees often lack sufficient expertise in the first and second lines of defence. The organisation can either provide training for important skills and expertise or implement knowledge-based systems to enhance risk. Three case studies stressed expertise and the skills of the second line of defence which enhances the effectiveness of risk management processes.

Second Ranked: Risk Awareness Culture and Training of the Three Lines of Defence

Six of the seven case studies provide employee training to educate them about the roles of the three lines of defence, products and services, risk management processes, and security and privacy. Strictly enforcing internal control policies, testing internal controls, escorting risk assessments from the second line of defence to the first, and getting strong support of risk management processes from management, are methods applied by four case studies to build risk awareness. The case studies recommended that formal training be held once a year, as well as frequent informal training, to enhance the risk awareness culture. One case study emphasised the importance of two-way communication.

Three Lines of Defence Structure

All case studies stated that the attention of the first line of defence is significant to effective risk management. Time management for routine tasks and risk management tasks is essential for driving successful risk management processes. Current problems in the first line of defence are lack of expertise in identifying risks, lack of attention to risk management processes, and lack of risk awareness. The changing role of the second line of defence from only designing policy to be a facilitator in risk assessment pushes the risk management practice to be more proactive. This change of role was supported by six of the seven case studies.

The design of three lines of defence structure and management support were two other success factors identified by three case studies. One case study shared that the concept of three lines of defence should be observed even in a small organisation. Another case study shared that the second line of defence of IT risks should be separated from other risks. Finally, three case studies the emphasised the role of the third line of defence, which assists in monitoring and assessing that internal controls are adequate. In summary, problems identified in the first line of defence are lack of knowledge and experience in assessing and prioritising risks, and lack of responsibility. In the second line of defence, the problem identified is lack of expertise; and in the third line of defence, interference in the function of the first line of defence by the third line was brought up.

Communication

All case studies communicate risk management in various ways such as meetings, during training and through reporting. One case study raised the benefits of informal and two-way communication between the first and second lines of defence. Another case study emphasised reporting to the board of directors and relevant committees. Social media is an effective communication tool. The problem of communication is that it is sometimes an additional workload on top of routine tasks.

Key Success Factors of ITRM Practice

Discussion

The case study analysis found the following concerns:

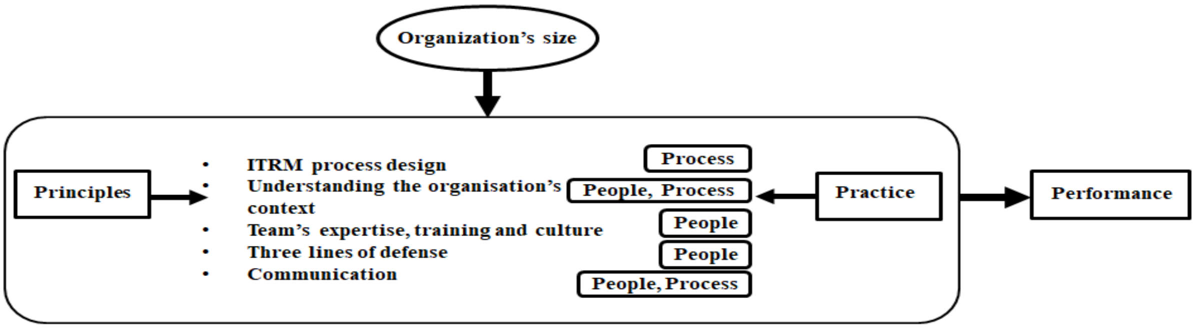
First, *tools* are a significant issue. Current tools do not integrate well with the three lines of defence functions. Other problems about tools are unfriendly user interfaces and tools that are not a good fit with ITRM tasks. As shared by the case studies, spreadsheet software is still used for risk and control self-assessments, risk monitoring indicators, and monitoring dashboards. The problems identified in *ITRM process design* are (1) risk owner – the first line of defence – does not recognise risks when they arise (2) poor attitude and lack of involvement within the first line of defence. The problems are consistent with understanding the organisation's context: internal environment regarding people, business processes, data and information, and the team's expertise. Some solutions to these issues suggested by the case studies are (1) fully understanding management's concerns and appropriate workshops should be utilised for risk identification. (2) Process mapping and root cause analysis should be applied to risk analysis processes to derive thinking systematic thinking.

Second, the concept of *three lines of defence* has been maintained in the case studies to fit the principles for risk management. However, people who are in the three lines of defence and involved interdependently in ITRM processes often are currently lacking sufficient expertise and experience in product lines, risk management processes, and information systems. The case studies recommend that training programs be implemented to help organisations develop staff to understand business and IT risks, to build risk awareness and develop appropriate personal characteristics.

Third, relevant to people, the enforcement to comply with principles is consistent with the *external environment*, such as regulation. This, in turn, makes it important to understand the organisation's context, including policies, standards and procedures. Some case studies where the interviewees are in a management role gave significance to *understanding the organisation's context*: objectives, strategic direction and current risks. Other interviewees focused on threats of IT risk, which affect the operations. The *criticality of data* is concerned with analysing risk; however, some case studies have not implemented suitable processes.
Fourth, *communications* affect how messaging is made, such as sharing concerns and smoothing over conflicts. Social media is used for informal and fast communication for consulting, solving problems and updating information.

The theoretical contribution of this research is the principle and practice fit framework of ITRM. The factors influencing the fit were obtained from the general risk management frameworks and principles (ITRM principle framework) and confirmed by interviews from case studies (ITRM practice). Five key success factors in ITRM practice were investigated. The investigation was conducted using qualitative research to obtain and to confirm the existence of factors. These factors can be further measured in future work, such as level of compliance with existing processes. These processes include internal policies, standards and procedures; perceptions toward tools and technologies implemented; understanding of organisation objectives; strategic direction and current risk; acknowledgement of external environment (regulatory, economic factors, crises, competitors, technology, innovation, suppliers, customers, public interest, etc.); readiness of internal environment (people, processes and culture) and classification of critical data. Additionally, preparation of team structure, level of expertise, the development plan of employees, interdependence level among team members, level of interaction through communication channels, can be studied and assessed in future work. Figure 4 illustrates the key success factors that affect the principles and practice fit framework.

Figure 4. Principle key success factors that affect the fit with ITRM practice Ordered from the most to least important



Conclusion

This research aims to examine current problems and solutions from seven leading information systems technology organisations which have implemented ITRM processes. This research found problems and proposed solutions different from other academic research through principles and practice fit and introduced a proposed framework. This research focused on the roles of the first and second lines of defence, which are directly involved in ITRM processes.

The case study analysis of ITRM processes was conducted to investigate factors of success in the practice, current problems and the recommendations of the case studies. The research was conducted following case study protocol which was carefully designed to achieve the research objective. Verification of the validity of the research was proven by multiple sources, such as general risk management frameworks and principles, review from ITRM experts, the experience of the researcher and the information shared by the seven case studies, all in the commercial banking industry. The case studies were selected from the criteria of case selection as described previously.

What is stated the most by the case studies for successful ITRM practice is effective tools which can be used as a substitute for lack of expertise in the three lines of defence. Currently, implemented tools are not a good fit for the interdependent working among the three lines of defence. The development of skills, competency and internal characteristics of people involved in the process should be conducted by training or brainstorming about potential risks, impacts and likelihood of risk occurrence, understanding product lines and services, business processes, and risk management processes. Additionally, the case studies disclosed a greater concern regarding understanding risk and risk management processes, more than using complicated risk management techniques. The policies, standards and procedures are adopted from regulations and general risk management frameworks and principles which are enforced by the organisation. Other important factors are the internal and external environments emphasising the use of data and information because various sources of information help to identify risk effectively. Furthermore, relevant communication, such as social media, workshops and meetings, increase risk management performance. Additionally, this developed framework can be applied if the research area is process structuring rather than a technological emphasis. The obtained factors can affirm the success or failure of tasks.

Limitations and Future Work

Limitations

This research selected for study was seven banks from the fourteen commercial banks registered in Thailand. The seven banks were selected to get a mix of bank sizes. As this research is concerned only with the seven commercial banks studied, generalisation of the results may not be valid at banks not studied.

Future Work

The results of this study suggest several areas for future work. First, ITRM tasks and tools should be measured and whether they fit ITRM practice and increase performance. The task-technology fit theory can be applied for these measurements such as the effect of ITRM tools and decision tasks and the effect of characteristics and attitudes of the three lines of defence to technology on the task to the effect of acceptance from social motivation to use technology, etc. Second, to build risk awareness of people in the three lines of defence, action research is suggested to enhance and to change the self-conception of people. For example, applying gamification functions to systems activities to improve the risk awareness culture in an organisation.

REFERENCES

Agrawal, V. (2016). Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard. Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016). 101-111.

Anney, V. N. (2014). Ensuring the Quality of the Findings of Qualitative Research:Looking at Trustworthiness Criteria. *Journal of Emerging Trends in Educational Research and Policy Studies*, 5(2):272-281.

Bandyopadhyay K.; Mykytyn, P. & Mykytyn, K. (1999). A Framework for Integrated Risk Management in Information Technology. MCB University Press: *Management Decision*, 37(5):437-444.

Basel Committee on Banking Supervision (BCBS). (2011). *Principles for the Sound Management of Operational Risk*, Bank for International Settlements. Retrieved at April 16, 2017, from the website https://www.bis.org/publ/bcbs195.pdf.

Bruhn, M. & McKenzie, D. (2009). In Pursuit of Balance: Randomization in Practice in Development Field Experiments. *American Economic Journal: Applied Economics*, 1(4):200-232.

Caldwell, C., Karri, R. & Vollmar, P. (2006). Principal Theory and Principle Theory: Ethical Governance from the Follower's Perspective. *Journal of Business Ethics*, 66, 207-223.

Creswell, J. W. & Miller, D. L. (2000). Determining Validity in Qualitative Inquiry. *Theory into Practice*, 39(3):124-130, DOI: 10.1207/s15430421tip3903_2.

DeSanctis, G. & Poole, M. S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organisation Science*, 5(2), 121-147.

El Said, G. R. (2015). Understanding Knowledge Management System Antecedents of Performance Impact: Extending the Task-Technology Fit Model with Intention to Share Knowledge Construct. *ScienceDirect: Future Business Journal*, 1, 75-87.

Feldman, M.S. & Orlikowski, W. J. (2011). Theorizing Practice and Practicing Theory. *OrganisationScience*, 22(5), 1240-1253.

Gelbstein, E. (2016). Auditing IS/IT Risk Management, Part 1. *ISACA Journal*, 2:1-3.

George, A. L. & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Gerring, J. & Cojocaru, L. (2016). Selecting Cases for Intensive Analysis: A Diversity of Goals and Methods. *Sociological Methods & Research*, 1-32.

Goodhue, D. L. & Thompson, R. L. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, 19(2), 213-236.

Hsieh, H.-F. & Shannon, S.E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9):1277-1288.

Information Systems Audit and Control Association (ISACA). (2013). *Cobit5 for Risk*. IL: ISACA.

International Organisation for Standardization (ISO). (2009). *ISO 31000: Risk Management-Principles and Guideline*. Geneva, Switzerland: ISO.

International Organisation for Standardization (ISO). (2011). *ISO/IEC 27005:2011 Information Technology – Security Techniques - Information Security Risk Management*. London, UK: BSI.

Kilmon, C. A., Fagan, M. H., Pandey, V. & Belt, T. (2008). Using the Task Technology Fit Model As a Diagnostic Tool for Electronic Medical Records Systems Evaluation. *Issues in Information Systems*, 9(2), 196-203.

Kouns, J. & Minoli, D. (2010). *Information Technology Risk Management in Enterprise Environments: A Review of Industry practices and a practical guide to risk*. NJ: John Wiley & Sons, Inc.

Larsen, T. J., Sorebo, A. M. & Sorebo, O. (2009). The Role of Task-Technology Fit as Users' Motivation to Continue Information System Use. *Computers in Human Behavior*, 25, 778-784.

Liu, Y., Lee, Y. & Chen, A. N. K. (2011). Evaluating the Effects of Task-Individual-Technology Fit in Multi-DSS Models Contexts: A Two-Phase View. *Decision Support Systems*, 51(3), 688-700.

Maneerattanasak, U. & Wongpinunwatana, N. (2017). A Proposed Framework: An Appropriation for Principle and Practice in Information Technology Risk Management, *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, Langkawi, Malaysia, 1-6.

Neuendorf, K. A. (2002). *The content analysis guidebook*. LA: SAGE. 1st edition.

Nielsen, R. A. (2016). Case Selection via Matching, *Sociological Methods & Research*, 45(3):569-597.

Parkes, A. (2013). The Effect of Task-Individual-Technology Fit on User Attitude and Performance: An Experimental Investigation. *Decision Support Systems*, 54, 997-1009.

Pereira, T. & Santos, H. (2012). An Ontology Approach in Designing Security Information Systems to Support Organisational Security Risk Knowledge. *International Conference on Knowledge Engineering and Ontology Development (KEOD 2012)* 461-466.

Riege, A. M. (2003). Validity and Reliability Tests in Case Study Research: A Literature Review with "Hands-on" Applications for Each Research Phase. *Qualitative Market Research: An International Journal*, 6(2):75-86.

Schmittling, R. & Munns, A. (2010). Performing a Security Risk Assessment. *ISACA Journal*, 1:1-7.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2015). Taxonomy of Information Security Risk Assessment (ISRA). *ScienceDirect: Computers and Security*, 57:14-30.

Smith, C. D. & Mentzet, J. T. (2010). Forecasting Task-Technology Fit: The Influence of Individuals, Systems and Procedures on Forecast Performance. *ScienceDirect: International Journal of Forecasting*, 26, 144-161.

Suh, B. & Han, I. (2003). The IS Risk Analysis Based on a Business Model. *ScienceDirect: Information & Management*, 41:149-158.

The Committee of Sponsoring Organisations of the Treadway Commission (COSO). (2004). *Enterprise Risk Management - Integrated Framework: Executive Summary*. Available on http://www.coso.org/documents/coso_erm_executivesummary.pdf.

The Bank of Thailand. (2016). *Average of Assets and Liabilities of Thai Commercial Banks (Peer Group)*. [Data file]. Retrieved from http://www2.bot.or.th/statistics/BOTWEBSTAT.aspx?reportID=677&language=TH.

Wu, B. & Chen, X. (2017). Continuance Intention to Use MOOCs: Integrating the Technology Acceptance Model (TAM) and Task Technology Fit (TTF) Model.*Computers in Human Behaviour*, 67, 221-232.

Yin, R. K. (2003). *Case Study Research: Design and Methods*. CA: SAGE Publication, Inc. 3rd edition. 3.

Zigurs, I. & Buckland, B. K. (1998). A Theory of Task/Technology Fit and Group Support Systems Effectiveness. *MIS Quarterly*, 22(3), 313-334.