DOI: 10.20472/IAC.2017.032.027

URAIRAT MANEERATTANASAK
Thammasat University , Thailand

NITAYA WONGPINUNWATANA
Thammasat University , Thailand

A STUDY OF SUCCESS FACTORS OF PRINCIPLE AND PRACTICE IN INFORMATION TECHNOLOGY RISK MANAGEMENT

Abstract:

The purpose of studying the success factors of principle and practice in Information Technology Risk Management (ITRM) is initiated from the proposition that appropriate ITRM principle and practice can mitigate IT risks and losses which is a result of security threats. The literature showed that various general principles and frameworks are widely published but the established principle cannot be put into the practice. Additionally, there is a research study regarding the difficulty to maintain independent in identifying, reviewing and reporting tasks of IT risk and internal audit functions.
The methodology consisted of the review of general principles and frameworks' documents and the interview from case studies. The general principles and frameworks in this research collected from the question "Which principles and frameworks are applied to ITRM in your organization?". The question was asked to people in IT risk and IT internal audit functions from banking organizations and other industries which advanced information technologies are critical to the organizations. The content from first five applied principles and frameworks from the survey are Basel, COBIT 5 framework, COSO Enterprise Risk Management, ISO 31000 and ISO/IEC 27005 were reviewed. In addition, the interviews were conducted to the people in both functions from banking organizations regarding the success factors of principle and practice in ITRM in their opinions without guiding from the interviewer.
The findings from the review of documents are eleven success factors that are general principle and framework selection, principle establishment, process design, structure of risk team, team's expertise, complex level of task, interdependent level, risk culture, communication in organization, training and risk management's tools and techniques. Meanwhile, the in-depth interviews' results showed that nine success factors that are adoption of ITRM principle, appropriate Process from ITRM Principle, task, interaction, adaptability, outsourcing, management support, conflict management and culture transformation. In conclusion, the success factors from both resources were compared and discussed as triangulation.
The practical contribution of the research is that the success factors can be used as a primary check for the appropriation of current principle and practice, the exploration an intrinsic problem in both principle and practice on ITRM or the development stage. For the theoretical contribution, the researcher recommends studying various success case studies applying the principle and practices from various industries and classified the patterns by organization types which the information technologies are significant to their operation.

Keywords:

Information Technology Risk Management; Principle and Practice; Success Factors

JEL Classification: M15

Introduction

Nowadays the financial institutions have obviously adopted the advantage of the internet or other electronic channels to provide accurate and reliable services (Omariba et al., 2012; Malami et al., 2012; Khrais, 2015). Nevertheless, there has been frequently updated news regarding various patterns of cybercrime causing abundant individual or financial institution's losses. Security threats are events that damage the information system resources or reduce the confidentiality, integrity and availability of information (Geriè and Hutinski, 2007). The proposition in the study is an appropriate Information Technology Risk Management (ITRM) principle and practice can mitigate IT risks and losses which is a result of security threats.

From our review, several ITRM principles and frameworks have been developed and updated by various well-known professional associations and organizations. Nevertheless, there were some issues in the adoption of those principles and frameworks into the practice (Bandyopadhyay et al., 1999; Suh and Han, 2003; Pereira and Santos, 2012; Shameli-Sendi et al., 2015; Agrawal, 2016). Furthermore, another issue was that the fast developed principles and frameworks cannot be effectively practiced in real circumstances (Gelbstein, 2016).

As a result, the study of ITRM practice seems to be essential and contributed to an organization to acknowledge the success factors for appropriation in the ITRM principle and practice. The organization of this paper starts with introduction. The theoretical background is explained followed by the research methodology. Subsequently, the research results are explained. The success factors from reviewing documents and the interviews were compared as a triangulation in analysis and interpretation. Finally, the conclusion and suggestion for future work are described.

Theoretical Background

According to the review of relevant documents, there are several ITRM principle and framework documents from professional associations and organizations such as the Basel Committee on Banking Supervision (BCBS), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Information Systems Audit and Control Association (ISACA), International Standards Organization (ISO) and etc. The principle and framework documents in this study from the primary survey are Basel Principles, COBIT 5 for risk, COSO ERM, ISO 31000 and ISO/IEC 27005. Considerably, they are classified by the developers into two levels which are framework and organization levels. The principle and framework documents in the framework level are developed by professional associations such as COSO ERM and COBIT 5 for risk and supervisory authority such as Basel Principles whereas those in the organization level are

developed by technical committees who are representatives from various industries[1] impulsively established from industries or stakeholders' requirement such as ISO 31000 and ISO/IEC 27005. Furthermore, the objective of development in the framework level can be separated into two types for governance, risk management and compliance (GRC) and for regulation. Examples for GRC are COSO ERM and COBIT 5 for risk whereas example for regulation is Basel Principles. The objective of development in the organization level can be adopted as principle and standard such as ISO 31000 and ISO/IEC 27005, respectively. Moreover, the target groups of the documents' adoption are general organizations except Basel Principles that are specific to the financial institutions. Additionally, if divided by scope of the context in those documents, most principle and framework documents are developed focusing on enterprise management such as COSO ERM, Basel Principles and ISO 31000. Meanwhile, others are developed focusing on information technology (IT) management such as COBIT 5 for risk and ISO/IEC 27005. The classification is summarized in Table 1.

Agreeably to previous research studies (Ekelhart at el., 2007; and AIRMIC, Alarm and IRM, 2010), several principles and frameworks must be elaborately customized and properly applied to the organizations depending on their size, nature and complexity. The difficulty to select an appropriate principle found in the study of Shameli-Sendi et al. (2015). Additionally, there was inappropriateness in ITRM adoptions such as the integration of the ITRM process to build the overall ITRM system (Bandyopadhyay et al., 1999), the insufficient models (Pereira and Santos, 2012), the improper estimation of loss by considering the value of IT assets (Suh and Han, 2003) and misunderstanding the concepts of ISO/IEC 27005:2011 by various stakeholders (Agrawal, 2016). From these issues the authors brought about developing taxonomy, ontology and concept in ITRM. Nonetheless, not only the appropriation of principle but also the appropriation of the practice is significant in driving the efficiency and effectiveness of the ITRM.

Table 1: Classification of ITRM principles and frameworks[2]

Level	Objective	Target	Scope	
			Enterprise	Focusing on IT
Framework	Governance, Risk Management, Compliance (GRC)	General Organization	COSO ERM	COBIT 5 for risk
	Regulation	Specific (Financial Institution)	Basel Principles	

[1] Public information from ISO official website

[2] Adopted and adapted from the paper accepted to present in ICRIIS 2017 and will be published in IEEE conference proceeding.

Level	Objective	Target	Scope	
			Enterprise	Focusing on IT
Organization	Principle	General Organization	ISO 31000	
	Standard	General Organization		ISO/IEC 27005

Practically, ITRM is a complex task because it consists of many processes in a dynamic cycle and involvement from several divisions known as three lines of defense. The Basel Committee defines three lines of defense in risk management which consists of business line, corporate risk and independent review functions (Basel Committee, 2011). Additionally, task experience is significant to perform a quality ITRM task. Level of experience brings about expertise that increases confidence in doing tasks complying with principle and process (Parkes, 2013). Nevertheless, a research study which classified risk management and internal audit function based on organization structure, responsibility and reporting found that it was difficult to maintain independence in identifying risk, reviewing and reporting tasks of both functions. Those functions have gaps and overlaps in their roles and responsibilities (Crawford and Stein, 2002). In addition, most organizations hired a consultant team for a concise risk management workshop and fast developed risk management documents in order to present that they have the formal documents (Gelbstein, 2016) but the documents cannot be put into the practice.

Research Methodology

We designed the methods to select the general principle and framework documents for context review and interviewed the case studies in order to obtain the success factors as follows.

The methodology consists of reviewing the contexts of general principle and framework documents and interviewing two case studies from IT risk and IT internal audit personnel in banking organizations The interview question is “Which principles and frameworks are applied to ITRM in your organization?”. The first five principles and frameworks which are most applied from the survey were COBIT 5 for risk, COSO ERM, ISO 31000, ISO/IEC 27005 and Basel Principles.

For the interview section, this research is conducted based on multiple-case studies to answer a research question which is appropriate for collecting and analyzing empirical evidence focusing on contemporary events (Yin, 2003). On the complex situations of individual’s accountability, operational and managerial processes and social relation, case study research is suggested to understand and to describe the phenomenon in a qualitative manner (Yin, 2003).

Due to the fact that ITRM in an organization is practiced by several divisions such as business, risk management, IT and IT internal audit, and several levels such as board committee, senior

management, supervisor and officer. Nonetheless, this study focused on the ITRM in perspectives of the IT risk officer who is responsible for implementing ITRM and the IT internal auditor who is responsible for reasonable assurance on the ITRM process. Two case studies were chosen as purposive sampling. One informant is an IT risk manager from a large-sized bank and another is an IT internal audit director from a mid-sized bank which both having experience in ITRM and IT internal audit for more than 15 years. The method used in data collection is in-depth interview. After semi-structure interview questions had been prepared, the informants were contacted for interview appointment. The interview was conducted in a private area where the informant was able to answer questions via telephone without interruption from telephone calls or their colleagues. As giving a reason for the advantages of telephone interview by Betteridge, it was a personal channel of communication and the dialogue was easy to unfold (Betteridge, 1997). The researcher compiled the information by using field note and recording template without losing any significant issues. Each issue of interview was summarized by the researcher and confirmed with informants after each question. Each interview session took an hour. The interview summary report was created to record all interview details of both case studies in a comparative manner.

Research Results

The results from the review of general principle and framework documents and from the interviews are presented in Table 2 and Table 3, respectively.

The Success Factors from the General Principles and Frameworks

From our review, the contexts in document were interpreted by researchers to obtain keywords. These keywords are categorized as success factors which are general principle and framework selection, principle establishment, process design, team structure, team's expertise, complexity of task and interdependence level. In addition, risk culture, communication in organization, training, and risk management's tools and techniques are also supportive success factors that have been extracted from the review. All factors are presented in Table 2.

Table 2: The Success Factors from General Principles and Frameworks[3]

Reference of the Reviewed General Principle and Framework Documents	Keyword	Success Factor
▪ Basel Principles (Basel Committee, 2011): Principle 1, Principle 2, Principle 3 (p.5)	Principle Policy	General principle and framework

[3] Adopted and adapted from the paper accepted to present in ICRIIS 2017 and will be published in IEEE conference proceeding.

Reference of the Reviewed General Principle and Framework Documents	Keyword	Success Factor
▪ COBIT®5 for risk (ISACA, 2013):Enabler: Principles, Policies and Frameworks (p.29) ▪ ISO 31000:2009 (ISO, 2009): 4.3.2 Risk management policy (p.10) ▪ ISO/IEC 27005:2011(ISO, 2011): Annex A (p.29) ▪ COSO ERM (ISACA, 2013): Internal environment (p.93)	Philosophy Guidance Develop Establish	selection Principle establishment
▪ Basel Principles (Basel Committee, 2011): Principle 3, Principle 5, Principle 6, Principle 7, Principle 10 (p.5-6) ▪ COBIT®5 for risk (ISACA, 2013): Enabler: Processes (p.33) ▪ ISO 31000:2009 (ISO, 2009): 4.3.4 Integration into organizational processes (p.11) ▪ ISO/IEC 27005:2011(ISO, 2011): Process overview (p.7) and 7.4 Organization of information security risk management (p.12) ▪ COSO ERM (ISACA, 2013): Eight components (p.93)	Process Operation	Process design
▪ Basel Principles (Basel Committee, 2011): Principle 1 (No.22, p.7), Principle 5 (p. 6) ▪ COBIT®5 for risk (ISACA, 2013): Enabler: People, Skills and Competencies (p.55) ▪ ISO 31000:2009 (ISO, 2009): 4.3.3 Accountability (p.11) ▪ ISO/IEC 27005:2011(ISO, 2011): 7.4 Organization of information security risk management (p.12) ▪ COSO ERM (ISACA, 2013): Authority and responsibility of people (p.93)	Accountability Role Responsibility Authority Structure	Team Structure
▪ Basel Principles (Basel Committee, 2011): Principles for operational risk management (No. 15, p.4) ▪ COBIT®5 for risk (ISACA, 2013): Skill and Competencies stated (p.55) ▪ ISO 31000:2009 (ISO, 2009): 4.3.5 Resources (p.11) ▪ ISO/IEC 27005:2011(ISO, 2011): Expertise and Skill for testing (D.2, p.48) ▪ COSO ERM (ISACA, 2013): Competencies (p.93)	Expertise Experience Skill Competency	Team's Expertise
▪ Basel Principles (Basel Committee, 2011): principle 8, principle 9 (p.6) ▪ COBIT®5 for risk (ISACA, 2013): Skill and competencies (p.56) ▪ ISO 31000:2009 (ISO, 2009): A.3.2 Variety of tasks and activities in risk management (p.22) ▪ ISO/IEC 27005:2011(ISO, 2011): 8.3.1 Complex methods in risk analysis (p.17), difficulties (Annex A, p.28) ▪ COSO ERM (ISACA, 2013): tasks in components (p.94)	Complex Vary	Complexity of Task
▪ Basel Principles (Basel Committee, 2011): principle 5 (No.34, p.10), principle 11 (p.6), supervisors' role (No. 7, p.2) ▪ COBIT®5 for risk (ISACA, 2013): Culture and behavior (p.42) ▪ ISO 31000:2009 (ISO, 2009): Involvement (p.8) ▪ ISO/IEC 27005:2011(ISO, 2011): Annex A (p.28) ▪ COSO ERM (COSO, 2004): Entity's units is one of three dimensions (p.5)	Incorporate Cooperation Involvement	Interdependence Level
▪ Basel Principles (Basel Committee, 2011): Principle 1 (p.5) ▪ COBIT®5 for risk (ISACA, 2013): Enabler: Culture, Ethics and	Culture	Risk culture

Reference of the Reviewed General Principle and Framework Documents	Keyword	Success Factor
Behavior (p.41) ▪ ISO 31000:2009 (ISO, 2009): Culture and practice (p.10) ▪ ISO/IEC 27005:2011(ISO, 2011): A.1 (p.28) ▪ COSO ERM (COSO, 2004): Components of ERM (p.3)	Environment Ethic Behavior Practice	
▪ Basel Principles (Basel Committee, 2011): Principle 5 (No.34, p.10) ▪ COBIT®5 for risk (ISACA, 2013): Governance and Management (p.30) ▪ ISO 31000:2009 (ISO, 2009): 4.3.6 (p.12) ▪ ISO/IEC 27005:2011(ISO, 2011): Risk communication (p.24) ▪ COSO ERM (ISACA, 2013): Information and communication (p.95)	Communicate	Communication in Organization
▪ Basel Principles (Basel Committee, 2011): Principle 1 (No.23, p.7) ▪ COBIT®5 for risk (ISACA, 2013): Skill (p.55) ▪ ISO 31000:2009 (ISO, 2009): Training program (p.11, p.12, p.22) ▪ ISO/IEC 27005:2011(ISO, 2011): Annex A (p.32) ▪ COSO ERM (ISACA, 2013): Internal environment (p.93)	Training Education Awareness	Training
▪ Basel Principles (Basel Committee, 2011): Supervisors' role (No.8, p.2), Principle 9 (No.51, No.52, p.15) ▪ COBIT®5 for risk (ISACA, 2013): Service tools (p.52) ▪ ISO 31000:2009 (ISO, 2009): 5.4.2 (p.17) ▪ ISO/IEC 27005:2011(ISO, 2011): Tools and techniques (p.32, p. 48-49) ▪ COSO ERM (ISACA, 2013): Information systems (p.95)	Tool Technology Implementation Technique	Risk Management's Tools and Techniques

The Success Factors from the Interviews

Data from the case studies were collected from the question "What are the success factors to the ITRM in your opinion?" This section shows the interview contexts and keywords categorized by defined success factors presented in Table 3.

Table 3: The Success Factors from the Interviews

Interview Context	Keyword	Success Factor
Case Study A: "Various global standards such ISO 31000 and ISO 27005 are applied." *Case Study B:* "The same ITRM concept is applied even derived from different standards such as ISO, ERM and COBIT."	Applied	Adoption of ITRM principle

Interview Context	Keyword	Success Factor
Case Study A: "Common question to risk management team is have those risks been completely identified? First step, the team focuses on service area and considers business risk and IT-related risk covering facility and Equipment." Many pain points are hidden. Risk and control template should be updated to monitor the ranked risk. Currently, there are many separated tools. Each tool has capability individually. The organization has considered the compatibility, usefulness and lifetime of those selected tools. Process is more important than tools." *Case Study B:* "As we know the recent cyber threat that occurred to a financial institution, It was caused by misunderstanding the symptom of issue and using the wrong treatment method. The existing processes, even well-designed, such as identification, assessment, treatment and monitoring are not effective when it is carelessly put into practice."	Process Compatibility Well-designed	Appropriation of the ITRM Process
Case Study A: "IT risk beginning with identification of IT-related risk from the internal and external source of information. The internal sources are risk registration and incident. Meanwhile, the external sources are general accepted standard, news, repository, regulator and consultant. Subsequently, possible scenarios/events are created. Those scenarios are ranked after they are assessed impact and likelihood." *Case Study B:* "IT Auditor is used as a check-up center in the organization which investigates the deficiency of overall IT tasks upon risk-based method. Monitor performance of people or divisions who are relevant to the governance and management of IT. Role of IT auditor has to comply with the professional ethic." *Case Study A:* "The designed internal templates are customized from those principles by both professional organizations and regulation proper by an experienced IT risk team and practically used." *Case Study B:* "A team is responsible for designing ITRM processes familiar with those standards and possesses certification on risk and information system control."	Identification Assess Investigate Check-up Comply Experience Responsible Familiar Ethic	Task Characteristic
Case Study A: "IT risk team cooperate with business unit and bank's risk management team verifying overall risk (re-assessment) and matching relation between business risks and IT-related risks to final critical key risks of bank and minor risks for close monitoring."	Cooperate Relation Cross-functional	Interaction

Interview Context	Keyword	Success Factor
Case Study B: "Due to the fact that IT organization has currently owned IT risk management division and Quality Assurance itself. IT auditors don't detail in testing but select samples to test control over IT-related operational management."		
Case Study A: "Not only cyber threats but also cyber resilience is the new technical issues in concern and challenge ISRM team. The cyber resilience is more important than response that is well-prepared and has good governance to self-protective, fast monitoring, detection and correction. At present, there is enormous data ready to be analyzed by efficient tools. The integrated overview of the organization will help to scrutinize root cause of those related problems and develop effective controls that are a cost-effective method to the governance as well." *Case Study B:* "Cyber activities raise role of IT auditor becomes more important. Recently, the world needs specialists. Additionally, other concerns in ITRM are readiness to the emergent change from the advanced information technologies and the update of new business patterns to replace old-fashioned methods. Traditional risk-based upon only documents should be changed. Three things that should be changed. Role that people should be more concerned with cyber activities; methodology that people should concern Big Data, cyber/internet banking, challenge to try new bank's product to understand process and threats; and learning in new process, follow cybercrime news, dynamic marketing such as positioning of the bank is digital banking."	Resilience Change Learning	Adaptability
Case Study A: "There is a requirement from PCI DSS to audit the ATM machine but it depends on audit extent, team and time. Anyway, nowadays that Fintech startup has being popular. Some enterprises provide ATM assessor services and take risks instead of the bank. Other Fintech provides analytic tools to the bank."	Fintech	Outsourcing
Case Study B: "The IT projects increase in number but size of IT audit team is limited both by vision of governance and management team and welfare for team members. Working under pressure due to limited team size makes it difficult to discover any complicated significant issues."	Vision of governance and management	Management Support
Case Study B: "Work upon risk management and echo from internal resistance and external concern. There is some resistance against IS auditor's working such as threatening demands from income-making unit. The perception of users to the audit concept and IT	Internal/External Resistance	Conflict Management

Interview Context	Keyword	Success Factor
security is not good from past history. Allusions of mistake from business unit and risk management lead to a hazardous operation and a possible time bomb."		
Case Study A: "The informant said most information comes from lessons learned. The success of risk management depends on consistent process, personnel quality and philosophy of management. Thai culture differs from foreigner such as Europe and America in sharing pain points. There are many oversea forums held up to share problems and solutions. However, what information would be shared has been considered. At this moment, there are central units to collect some useful information that can be shared with each other. Each bank can contact to request useful information for analysis."	Lesson learned Culture Sharing	Culture Transformation

In conclusion, the in-depth interviews gave nine success factors which are adoption of ITRM principle, appropriation of the ITRM process, task characteristic, interaction, adaptability, outsourcing, management support, conflict management and culture transformation.

Analysis and Interpretation

The success factors from reviewing documents and interviews were matched as triangulation from different sources. In triangulation process, the eleven success factors from reviewing documents which are *general principle and framework selection, principle establishment, process design, team structure, team's expertise, complexity of task, interdependence level, risk culture, communication in organization, training, and risk management's tools and techniques* are matched to the nine success factors from interview which are *adoption of ITRM principle, appropriation of the ITRM process, task characteristic, interaction, adaptability, outsourcing, management support, conflict management and culture transformation* by researchers' analysis and interpretation from keywords in Table 2 and Table 3 as presented in Table 4. Matching results shows a relationship between success factors from principle (reviewing general principle and framework documents) and practice (interviewing two case studies) in ITRM.

Table 4: Success Factors from Two Sources Matching

Success Factors from Reviewing document	Keyword	Success Factors from Interview	Keyword
General principle and framework selection *Principle establishment*	Principle Policy Philosophy Guidance Develop	*Adoption of ITRM principle*	Applied

Success Factors from Reviewing document	Keyword	Success Factors from Interview	Keyword
	Establish		
Process design	Process Operation	*Appropriation of the ITRM process*	Process Compatibility Well-designed
		Outsourcing	Fintech
Team structure	Accountability Role Responsibility Authority Structure	*Task characteristic*	Identification Assess Investigate Check-up Comply Responsible
		Management support	Vision of governance and management
Team's expertise	Expertise Experience Skill Competency	*Task characteristic*	Experience Familiar
Complexity of task	Complex Vary	*Task characteristic*	Identification Assess Investigate Check-up Comply
Interdependence level	Incorporate Cooperation Involvement	*Interaction*	Cooperate Relation Cross-function
		Conflict management	Internal/External Resistance
Risk culture	Culture Environment Ethic Behavior Practice	*Task characteristic*	Ethic
		Conflict management	Internal/External Resistance
		Culture Transformation	Lesson learned Culture Sharing
Communication	Communicate	*Conflict management*	Internal/External Resistance
Training	Training Education Awareness	*Adaptability*	Resilience Change Learning
Risk management's tools and techniques	Tool Technology Implementation Technique	*Appropriation of the ITRM process*	Process Compatibility Well-designed
		Adaptability	Resilience Change Learning
		Outsourcing	Fintech

Additionally, the triangulation is plotted in Table 5. The success factors from reviewing documents are in row whereas the success factors from interview are in column.

Table 5: Triangulation of the Success Factors' Matching

Success	Success Factors from Interview

Factors from Reviewing General Principles and Frameworks	Adoption of ITRM principle	Appropriation of ITRM Process	Task Characteristic	Interaction	Adaptability	Outsourcing	Management Support	Conflict Management	Culture Transformation
General principle and framework selection	●								
Principle establishment	●								
Process design		●				●			
Team structure			●				●		
Team's expertise			●						
Complexity of task			●						
Interdependence level				●				●	
Risk culture			●					●	●
Communication in organization								●	
Training					●				
Risk management's tools and techniques		●			●	●			

Conclusion and Suggestion for Future Research

In conclusion, the success factors from both resources were compared and discussed as a triangulation. The contribution of the research in practice is the success factors can be used as a primary check for the appropriation of current principle and practice and the exploration of an intrinsic problem in current process or the early stage of ITRM implementation. The theoretical contribution of this research is to fulfill the ITRM research in IT governance perspective. The keywords and derived success factors can be used as a dictionary and baseline in seeking for the success factors in principle and practice in any domains.

Nevertheless, the limitation of this research is a sample size. Because of purposive sampling, the two case studies in different roles from different organizations were chosen to investigate primary success factors.

For the future work, the researcher continues studying success case studies for the appropriation of principle and practice from various industries and classifying the patterns by organization types and sizes which the information technologies are significant to their operations. This process is conducted repeatedly as an experiment to find out other factors by increasing sample sizes. Moreover, different methodology can be applied to replicate the research. Additionally, the case studies in this research are financial institutions. It could be expanded to other industries which

have been facing threats and risks from the advanced information technologies such as telecommunication, online service and etc.

Reference

THE ASSOCIATION OF INSURANCE AND RISK MANAGERS (AIRMIC), THE PUBLIC RISK MANAGEMENT ASSOCIATION (ALARM) and THE INSTITUTE OF RISK MANAGEMENT (IRM). (2010). "A Structured Approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000", Available on https://www.theirm.org/media/886062/ISO3100_doc.pdf.

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), pp. 101-111.

BANDYOPADHYAY, K.; MYKYTYN, P.; and MYKYTYN, K. (1999). A Framework for Integrated Risk Management in Information Technology". Management Decision, vol. 37, No. 5, pp. 437-444.

BASEL COMMITTEE. (2011). Principles for the Sound Management of Operational Risk, Basel: Bank for International Settlements, 2011.

BETTERIDGE, J. (1997). Answering back: The Telephone, Modernity and Everyday life. Media, Culture & Society, vol. 19, pp. 585-603.

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

CRAWFORD, M. and STEIN, W. (2002). “Auditing Risk Management Fine in Theory but who can do it in Practice?”. International Journal of Auditing, 6, 199-131.

EKELHART, A.; FENZ, S.; KLEMEN, M.; and WEIPPL, E. (2007). "Security Ontologies: Improving Quantitative Risk Analysis". 2014 47th Hawaii International Conference on System Sciences, 156a.

GELBSTEIN, E. (2016). Auditing IS/IT Risk Management, Part 1. ISACA Journal, vol. 2, pp. 1-3.

GERIÈ, S. and HUTINSKI, Z. (2007). Information System Security Threats Classifications. Journal of Information and organizational sciences, vol. 31, pp. 51-61.

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

ISO (International Standards Organization). (2009). ISO 31000: Risk Management-Principles and Guideline, Geneva, Switzerland: ISO.

ISO (International Standards Organization). (2011). ISO/IEC 27005:2011 Information Technology – Security Techniques - Information Security Risk Management, London, UK: BSI.

KHRAIS, L. T. (2015). Highlighting the Vulnerabilities of Online Banking System. Journal of Internet Banking and Commerce, vol.20, no.3, pp. 1-10.

MALAMI, A. B.; ZAINOL, Z.; and NELSON, S. P. (2012). Security Threats of Computerized Banking Systems (CBS): The Managers’ Perception in Malaysia, International Journal of Economics and Finance studies, vol.49, no.1, pp. 21-30.

OMARIBA, Z. B.; MASESE, N. B.; and WANYEMBI, G. W. (2012). Security and Privacy of Electronic Banking. IJCSI International Journal of Computer Science, vol.9, no.4, pp. 432-446.

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

PEREIRA, T. and SANTOS, H. (2012). An Ontology Approach in Designing Security Information Systems to Support Organizational Security Risk Knowledge, in Proceeding of the International Conference on Knowledge Engineering and Ontology Development (KEOD 2012), pp. 461-466.

SUH, B., and HAN, I. (2003). The IS Risk Analysis Based on a Business Model, ScienceDirect: Information & Management, vol.41, pp. 149-158.

SHAMELI-SENDI, A., AGHABABAEI-BARZEGAR, R., and CHERIET, M. (2015). Taxonomy of Information Security Risk Assessment (ISRA), ScienceDirect: Computers and Security, vol.57, pp. 14-30.

YIN, R. K. (2003). Case Study Research: Design and Methods. CA: SAGE Publication, Inc.

ZIGURS, I., and BUCKLAND, B. K. (1998). A Theory of Task/Technology Fit and Group Support Systems Effectiveness. MIS Quarterly, vol.22, no.3, pp. 313-334.