RISK ASSESSMENT OF IT GOVERNANCE: A SYSTEMATIC LITERATURE REVIEW

[1]NORAINI CHE PA, [2]BOKOLO ANTHONY JNR, [3]ROZI NOR HAIZAN NOR AND [4]MASRAH AZRIFAH AZMI MURAD

[1,2,3,4]Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia.

E-mail: [1]norainip@upm.edu.my , [2]result4real@yahoo.com , [3]rozinor@upm.upm.edu.my , [4]masrah@upm.edu.my

ABSTRACT

Risk assessment (RA) is one of the main activities in risk management of IT governance. Basically, IT governance is a process or a procedure that involves evaluating and directing the plans for the use of ICT to support the organization and monitoring the achievement of these plans. The risks that may emerge during the implementation of IT governance must be properly assessed to ensure its success. In general, risk assessment in IT governance is focusing on the essential process to aid all relevant parties involved in IT implementation from both the technical and services aspects. Many studies related to IT risk assessment and risk assessments of IT governance have been reviewed based on a systematic method which is called Systematic Literature Review (SLR). Based on this approach, all previous studies related to this title can be analyzed systematically. Based on the same framework, this paper presents the results of the systematic reviews on the concept, process, framework, model and challenges of risk assessment of IT governance. In general, the findings from this review indicate that RA requires a more holistic consideration on numerous limitations and issues.

Keywords: *Risk Assessment, IT Governance, Systematic Literature Review.*

1. INTRODUCTION

Risk is considered as something that might go wrong in an establishing process. Risk is also a combination of the likelihood of an event and its effects. According to [1] there are three categories of risks: projects risks, product risks and business risks. Organizations must learn to stabilize the possible negative effects of risk against the possible gains of its related opportunity.

Risk Assessment (RA) is one of the main activities in risk management stages [2]. RA involves five phases; identification, analysis, evaluation, control and mitigation, and documentation. In general, IT risk assessment is referred to as the essential process to aid enterprise in implementing new business changes and where appropriate, invest in information systems to accommodate these changes. However, the adoption of IT applications has also exposed organizations to IT related risks such as strategic risk, financial risk, operational risk and technological risk [3]. In order to minimize and control these risks successfully, IT risk assessment policies and strategies have been developed and implemented in organizations.

IT enables organizations to move accordingly with development trends and acquire a competitive advantage over their competitors. This motivates them to improve IT service performance within their organization. This can be achieved by setting up ICT mission and vision that is in accordance with their organization's mission and vision. This very much depends on smoothness of coordination, effective monitoring and continuous action that will only be accessible through steady governance aspects for IT services [4]. In practice, IT Governance supports business operations, adding plus value through IT component and IT risks minimisation. IT governance is a very important issue at present as an integral component of any corporation or organisation. The purpose of IT governance is to direct IT endeavours to ensure that IT performance meets the objectives set out in its strategy [5]. With effective governance, the return of IT investment can be optimized to support business strategies and goal.

According to [6], IT Governance is faced with different challenges and issues such as part of much broader notion of Governance. Lining up in this order the two concepts, IT governance should follow the principles of corporate governance e.g. effective, transparent and accountable without which IT Governance cannot be properly implemented in an organisation. IT Governance reflects broader corporate governance principles while focusing on the management and use of IT to achieve corporate performance goals. Because IT outcomes are often difficult to measure, firms must assign responsibility for desired outcomes and assess how well they achieve them. IT Governance shouldn't be considered in isolation because IT is linked with other key enterprise assets.

Thus, IT Governance might share mechanisms (such as executive committees and budget processes) with other asset governance processes thereby coordinating enterprise wide decision making processes [7]. [6] expands on this definition by adding that IT governance is the delivery of IT, while balancing risks. Risks can be minimized with the correct organizational decision-making structures and the assignment of roles and responsibilities. For example, strategic risks are lack of investment, different understanding of the business process, lack of support by the management and unresolved conflicts between business and IT management. Effective risk management makes it easier to cope with problems and to ensure that these do no lead to unacceptable situation through identifying, controlling, and minimizing the impact of threats. RA needs to be integrated into the business process in a way that provides timely and relevant risk information to the management. Many researchers state that RA is one of the main activities in risk management of IT governance.

However, the need for this work is to carry out a comprehensive review and synthesis of the current studies, practices, issues and challenges of Risk Assessment based on the prior work done by many researchers. Though, all previous studies agree on the importance of Risk Assessment but there is no consensus on the framework, model and processes involved in their implementation. For this reason this paper aims to review previous studies on Risk Assessment from 2005 until 2014 including their framework, models, processes, and challenges. The structure of this paper is organized as follows: section 2 presents the method applied in this study which is Systematic Literature Review (SLR). Section 3 describes the findings of the study regarding the current approaches and issues related to challenges of RA. Finally, the study is concluded and implications of the review are identified in the last section.

2. METHOD OF STUDY

The Systematic Literature Review (SLR) is "a means of evaluating and interpreting all available research relevant to a particular research question or topic area or phenomenon of interest" [8]. It has been considered as the leading method in collecting and analysing existing research work. SLR also provides methodological advantages and applicability to our research questions. It involves three main phases namely planning, conducting and reporting [9]. These main phases are illustrated in Figure 1.

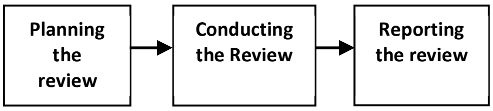

Figure 1: SLR Research Phases

The study started with identifying the needs for a literature review, formulating the review research questions and review protocol. The review was performed by defining the initial protocol. The actual gathering process was performed and the results were evaluated using subsequent gathering steps. Then data was extracted from the selected studies. Finally, the data was synthesized and analysed.

A systematic literature review evaluates and interprets all available research relevant to a particular question or topic area. It was not easy to locate articles about this subject as there is very little existing literature and descriptive framework. Consequently, the best method to achieve the research purpose is by assigning a common framework or uniform description to conduct this review. We summarized this evidence in order to investigate risk assessment in IT governance. We conduct the SLR by following the guidelines by [8]. We looked at the literature to answer these research questions:

- Question 1: What is the relationship between risk assessment and IT governance?
- Question 2: What are the existing frameworks, models and challenges for risk assessment in IT governance?

A review protocol is essential to any systematic literature review. Driven by the research questions, the protocol defines inclusion/exclusion criteria to select primary studies as shown in Table

Table 1: Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
IT risk, risk assessment, risk management, IT Governance.	not described in detail or a structured template is lacking
conference or journal or technical reports or books (2005-2014)	new and similar study exists
abstract and content are written in English.	review or evaluation of existing practices for risk assessment.
Reported SLRs or meta-analyses in risk assessment and IT Governance.	

2.1 Search Process

We design a SLR protocol to guide the search process [8]. Relevant papers were retrieved automatically from the databases as well as manually from target journals, conferences, and workshops as a supplementary source to the database search. The SLR guidelines suggested that the creditability of a study is based on the type of experiment [8]. In order to make this SLR credible, the studies without any validation were intentionally excluded according to the evidence levels. In the end, studies that passed this screening process were finally selected to be further analysed in this SLR. This review covers previous studies within the time period from Jan. 2005 to March. 2014. We discovered that there is an obvious lack of survey on risk assessment in IT governance.

2.2 Data Sources

The following databases as per (Table 2) are selected as the primary study sources. This selection based on the previous study by [10] is chosen as it is the most promising. In order to ensure that we did not overlook any important material, additional searches were performed directly on key conference proceedings, journals and authors. Furthermore we conducted secondary searches based on references found in our primary sources.

Table 2: Electronic databases included in this SLR

Electronic databases
IEEE Xplore
ACM Digital library
ScienceDirect
SpringerLink
Wiley InterScience
Google Scholar

The availability of many data sources that can be accessed through electronic libraries give a reasonable confidence of covering all relevant publications. These sources include journals and conference proceedings (refer to Table 3 and Table 4).

Table 3:List of Journals

Journals
IEEE Transactions on Software Engineering (TSE)
Empirical Software Engineering (ESE)
IEEE Software (IEEE SW)
International Journal of Software Engineering and Knowledge Engineering (IJSEKE)
Journal of Systems and Software (JSS)
Information and Software Technology (IST)
The Knowledge Engineering Review (KER)
International journal of project management
Knowledge based systems
Journal of Information Systems

Table 4:List of Conferences

Conferences
International Conference on Software Engineering and Knowledge Engineering (SEKE)
International Conference on Software Engineering (ICSE)
IEEE/ACM International Conference on Automated Software Engineering (ASE)
International Requirements Engineering Conference (RE)
ACM Symposium on Document Engineering (DocEng)

2.3 Search Terms

This section defines the search terms for database search. From our research questions, we derived the keywords. A search string was constructed using relevant terms based on the research questions. The first iteration included a manual search and an automatic search based on a list of keywords in the electronic databases. The following Boolean search strings were used:

"Risk assessment" or "Risk management" or "Knowledge risk" or "risk quantitative" or "risk quantification" or "IT governance"

Before selecting the papers to be used for the SLR, we checked for repetition of the same studies to ensure that there is no duplication; for example if the same study is published in two different journals with different first authors. In the event that we need to make a choice we include the most comprehensive study or the most recent study.

3. SLR FINDINGS

A total of 32 studies discuss the risk assessment methods in IT governance. Citations for the papers and other relevant papers are included in the reference for further reading. The inspected publications were classified according to the applied research method. Figure 2 shows that out of the 32 studies, 85% are empirical, 12%theoretical and, a small number of studies (3%) are either reviews of the literature or secondary studies, where empirical work is re-examined.

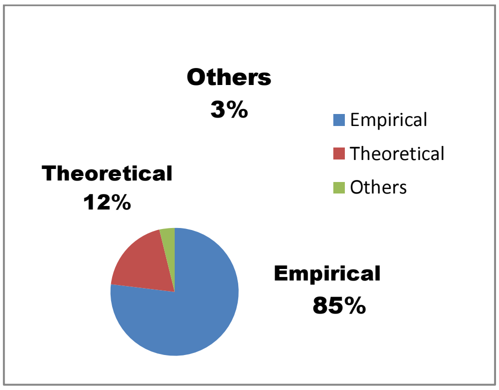

Figure 2: Research Method In Paper Study

Out of the 27 studies that are empirically based, only 4 studies do not include questionnaires. Figure 3 shows the breakdown of data collection methods for the empirical studies.

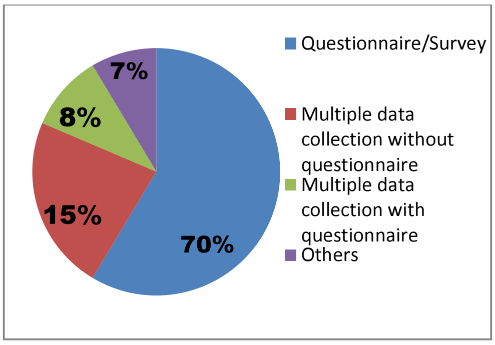

Figure3: Data Collection Methods Used in The Empirical Studies

The reviewed papers were published between 2005 and 2014. Fig. 4 shows that more papers on this subject were published in 2005 compared to more recent years.

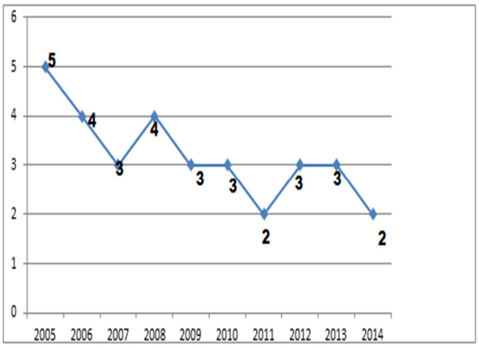

Figure 4: Data Collection Methods Used in The Empirical Studies

3.1 Risk Assessment Of IT Governance

By investigating the two research questions, we aim to gain a broad picture of what the literature is reporting on Risk assessment in IT governance. We collected information about the relationship between risk assessment and IT governance (RQ1); and what are the existing frameworks and models for risk assessment in IT governance (RQ2). 19 studies were identified in answering RQ1 as shown in Table 5. All the studies analysed gave the impression that many attempts have been made to define IT governance and give detailed explanations of how risk assessment relates to IT governance. Risk assessment is one of the main activities in risk management of IT governance [11].

IT governance is a very important issue at present as an integral component of any corporation or organisation. The purpose of IT governance is to direct IT endeavours to ensure that IT performance meets the objectives set out in its strategy [5]. With effective governance, the return of IT investment can be optimized to extend business strategies and goal. IT governance has focused on the domains of IT strategic alignment, IT resource management, risk management, performance measurement and IT value delivery. Risk management framework is put in place to ensure that risks have been adequately managed by the organisation. RA is one of the main activities in risk management of IT governance [2]. The phases in RA as identified by [2] are identification, analysis, evaluation, control and mitigation, and documentation. [2] revealed that most critical risk driver was the choice of methodology, customer involvement, use of formal project management practices, project complexity, and requirement volatility. [12] proposed a tool used to perform intuitive – if" "what – if" analyses to guide managers in determining how they can proactively reduce software project risk.

Risk assessment is a series of steps which the objectives are to identify, address, and eliminate software risk items before they become either threats to successful software operation or a major source of expensive rework[13]. In general, IT risk assessment is referred to as the essential process to aid enterprise achieving "the new business changes as well as decide on future investment in information and information system".

[3] recommends evaluating risk assessment in organisations by comparing the Control Objectives for the Information and related Technology (COBIT) framework and the ISO/IEC 17799 standard for dealing with IT risk assessment in IT Governance. The findings from three case studies indicate that successful IT risk management planning focuses on the collaboration between the management level activities and the operational level activities in order to cope with IT risks successfully. They further commented that the adoption of IT applications has also brought organizations risks related to IT such as strategic risk, financial risk, operational risk and technological risk. In order to minimize and control these risks successfully, IT risk assessment policies and strategies have been developed and implemented in organizations.

However, this management control emphasises both business control and technological control which support business requirement and governance. To be effective, risk assessment cannot be merely a checklist or a process that is disconnected from business decision making. When the risk assessment process is incorporated into ongoing business practices, risk can be managed as part of day-to-day decision making, in a manner consistent with the organization's risk appetite and tolerance [14].

Categories	Paper references	Frequency (studies)
Risk assessment and IT governance.	[13]), [6], [11], [5], [2] and [12]	6
The interaction between Risk assessment and IT governance.	[15], [16], [13], [17], [18],and [19].	6
An assessment of Risk in IT governance.	[20], [21], [22], [23], [24], [25] and[3].	7

Table 5:Risk Assessment in IT Governance Studies Categories.

3.2 Risk Assessment Frameworks of IT Governance

A total of 22 papers answered RQ2. There is general agreement about the need to find effective frameworks relating to Risk assessment in IT governance. We identified the three best risk assessment frameworks in the papers analysed (refer Table 6) based on literatures by [26], [18],[27], [3], [23]. [15] stated that COBIT is one of the preferred frameworks in IT Governance because it uses a classification which consists of five focus areas: strategic alignment, value delivery, resource management, risk management, and performance measurement. In COBIT 5.0 the concepts and ideas contained in these focus areas are maintained and built upon in the framework, but the focus areas themselves have not been literally maintained [25].

[18] find out in their research in IT Governance theory and practice that IT governance aims to align business and information technology strategies. IT governance frameworks, such as COBIT and ITIL, are internationally accepted and promote these benefits.

[3] identifies the current profile of IT risk management planning and investigates success in implementation in Thai organizations of both the Control Objectives for the Information and related Technology (COBIT) framework and the ISO/IEC 17799 standard for dealing with IT risk assessment. The findings from three case studies on successful IT risk assessment conclude that ITIL is considered the best practice and it is also recommended to supplement the COBIT and the ISO 17999 for dealing with IT risk assessment [3].

[27]in their case study in organizational challenges and barriers to implementing IT Governance presented both a COBIT and an ITIL assessment framework applied. The outcome of both the COBIT and ITIL assessments have shown that organisation is still not fully using all components of COBIT and at low level usage of ITIL tools, respectively [27].

[28] in their report started that COBIT provides a framework of processes and key controls that can be matched to identified key risks to which the enterprise has decided to respond to via mitigation. COBIT framework provides a reference model for the second line of defence because it defines IT activities in a generic process [28].

[23]stated that the COBIT distinguishes itself as a well-recognized framework for IT governance and auditing accounting IT systems. It is designed as an accessible guide for managers, users, auditors others who use the computer for their business in order to ensure the confidentiality, integrity and availability of data and information.

Table 6: Best Risk Assessment in IT Governance Framework and Models

Categories	Paper references	Frequency (studies)
COBIT framework	[29], [13], [30], [31], [21], [32].	6
ISO 27002 (ISO 17799)	[33], [34], [35], [36][37], [38], [21] and [39].	8
ITIL	[6], [26], [18]. [3], [27], [28], [23], [29]	8

3.3 Risk Assessment Model /Framework

There are numerous risk assessment models of Information Technology (IT) nowadays and many more emerging every day. They all have the same basic goal, but very different perspectives and addressing different problems. Some of them applied to all kinds of risk, while others are specific for particular risks. These papers compare and clarify the different activities, components, advantages and limitations required by each risk assessment model/ framework in IT. The risk assessment models in IT are shown in Table 7.

[5] proposed a risk assessment framework in supply chain (Information System)that addresses the problem of operational risk assessment in supply chain operations. The framework consists of four components: Value Modelling, Process Analysis, Uncertainty Estimation and Multi-Criteria Decision Making that used to assess the risk level on user, application and database architecture. In developing the framework a Value Based Method was used as a technique. The framework is representing a general conceptual road-map and serves as a guideline but not tested in real environment.

[38]designed a software risk assessment model (SRAM) in software engineering to access the level of risk in software project. The model includes three main components namely quality, schedule and cost. The model is able to predict a possible outcome of project risks. This model works as questionnaire to assess the risks. The SRAM is considering for risk in software development (software engineering). [39] proposed a software risk assessment identification and estimation model (SRAIEM) for software engineering process. SRAIEM is able to assess, identify, prioritize, estimate and predict the risks by using software metrics. [40] proposed Genetic Risk Assessment Model (GePRA) in programming logic domain(software engineering). The model uses vulnerability and asset value as technique to support risk assessment and decision making process for intrusion detection system. GePRA model performs quickly due to its utilisation of simple processes such as simulation and programming. GePRA concentrate on particular risks such as technical risk. [41] proposed risk-assessment model to assess the impact of cyber-attacks in software engineering. The model uses mathematical technique to aid different organizations to perform risk assessment of their control systems and facilitate cost-benefit analysis. The model considers technical and financial risks.[42] designed Quantitative Risk

Assessment Model in Project Management comprising Qualitative Rules, Risk Factors, Project Risk and Risk Taxonomy. The model applies a quantitative CMMI assessment as their technique for quantifying and monitoring risks. The model is automated and provides specific decision-making guidance.

[43]contributed a knowledge-based risk assessment framework in Knowledge management to capture, codify, store and distribute knowledge in Small Medium Businesses (SME). The model is being used as a template for evaluating the benefits and risks of application outsourcing of SME. The model components comprise of delivery and enablement; integration; management and operations; business transformation; and client/vendor relationships.[44] proposed a Fuzzy risk assessment model in information system. The model helps to integrate possible risk factors for decision making process to support the implementation of new information systems. The model uses a Fuzzy Algorithm as a technique. The model components include risk likelihood, risk severity, risk factor, risk, aggregation, fuzzy inference.

[45]developed a Fussy ExCOM risk assessment model for Information system to integrate the estimation and assessment of risk activities in software project. The model uses a fussy novel as a technique. The model component comprise of Software size, Project Risk, Contingency Allowance and Effort Estimation.[46] developed an architecture-oriented information security risk assessment model (AOISRAM) for Information system. The model components include risk monitoring, risk resolution, risk management planning, risk prioritization, risk analysis and risk identification. The model can be applied as a guideline in particular domains such as information security. The model was appraised to solves many difficulties caused by the process oriented approach in ISO 27001 of IS risk assessment such as irregular distribution of resources, poor safety performance and high risk.

4. CONCLUSION AND FURTHER RESEARCH

This paper presents a systematic literature review that investigates risk assessment of IT governance. The aim is to identify the process, frameworks, model and their challenges in implementing RA in IT governance. Risk assessment is one of the main activities in risk management of IT governance [11], [2]. The findings confirmed that The Information Technology Infrastructure Library (ITIL)is considered best practice for ICT, service management and it is also recommended to supplement the COBIT and the ISO 17999 for dealing with ICT risk management. Further research work could be conducted on the need of a tool for assisting RA process in IT governance. To date, there is no standard guideline to help managers in conducting main risks assessment consisting of operational, technical and strategic risks. As the final conclusion, findings obtained in this review, including an examination of the shortcomings found in this systematic literature review provides a strong evidence to encourage further research in the development of a new methodology to adequately perform Risk assessment in IT governance.

ACKNOWLEDGEMENTS

The authors gratefully acknowledged supports by the Faculty of Computer Science & Information Technology, Universiti Putra Malaysia and to our parents.

REFERENCES:

[1] I.Sommerville, “Software Engineering”, 9th Edition; Addison-Wesley Publishers, (USA), May 21-23, 2011.

[2] A. Tiwana and M. Keil, “The one-minute risk assessment tool”,*Communications of the ACM*, Vol. 47, No. 11, 2005, pp. 73-77**.**

[3] S.Kumsuprom, B.CorbittandS.Pittayachawan, “ICT Risk Management in Organizations: Case studies in Thai Business”, *19th Australasian Conference on Information System*,Dec 3-5 2008, pp.513-522.

[4] R. NHaizan, “ICT Service Quality Measurement Framework for the Context of Malaysian Universities”,*Doctor of Philosophy*, February 2013, UniversitiTeknologi Malaysia, Skudai Johor, Malaysia, 2013, pp. 1-343.

[5] L. Liu and H. Daniels, “Towards a Value-based Method for Risk Assessment in Supply Chain Operations”,*Journal of Economic Literature (JEL)*, May 2011, pp. 1-3.

[6] ITGI,"Board Briefing on IT Governance", IT Governance Institute, Retrieved from http://www.itgi.org, 2010, pp. 1-20.

[7] P. Weill and J. W. Ross, "IT Governance on One Page", *CISR Working Paper*, June 2005, pp. 1-349.

[8] B.A. Kitchenham, "Procedures for Performing Systematic Reviews",*Joint Technical Report Software Engineering Group*. Department of Computer Science Keele University (UK) and Empirical Software Engineering, National ICT Australia.Vol. 4, No. 2, 2005, pp. 45-56.

[9] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from Applying The Systematic Literature Review Process within The Software Engineering Domain",School of Computing and Mathematics Keele University Keele, Staffordshire, ST5 5BG UKVol. 80, No. 3, 2007, pp. 571–583.

[10] W. Ding, P. Liang, A. Tang and Van Vliet, "Knowledge-based Approaches in Software Documentation: A Systematic Literature Review", Information and Software Technology, *Journal of Information and Software Technology*18 January 2014, pp.1-51.

[11] P. Woods and R.Byrt, "Risk assessment, measurement and management", Book on Forensic, November 2006.

[12] M. A. Mustafa, and J.F. Al-Bahar,"Project risk assessment using analytical hierarchy process",*IEEE Transactions on Engineering Management*, Vol. 3, No. 2, 2010, pp. 1-11.

[13] G. H. Bodnar, "IT Governance", *Internal Auditing*, Vol. 18, No.3, May 2008, pp. 27-32

[14] R. McAdams and A. Galloway, "Enterprise Resource Planning and Organisational Innovation: A Management Perspective",*Industrial Management & Data Systems*, Vol. 105, No. 3, 2005, pp. 1-14.

[15] A.R. Rim, "A Risk Management Standard AIRMIC, ALARM, IRM", *Journal of Risk Management,*Febuary2005, pp.1-39.

[16] P.Coopers,IT Governance in Practice Insight from leading CIOs; PricewaterhouseCoopers International Limited,June 2007.

[17] D.Steuperaert, "The Risk IT Framework",*Excerpt ISACA Journal USA*, March 2009, pp. 234-343.

[18] E. Wessels and J.L .Van, "IT Governance: Theory and Practice",*Proceedings of the Conference on Information Technology in Tertiary Education*, Pretoria, South Africa, Vol. 1, No. 2, 20 September 2006, pp. 1-14.

[19] G. Stoneburner, A.Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems",*Recommendations of the National Institute of Standards and Technology*. February 2002, pp. 434-470.

[20] L. Jack and B. Junior, "Information Security Risk Assessment GAO Practices of Leading Organizations",*Accounting and Information Management DivisionJordan*, May 2009, pp. 1-12.

[21] E. Jordan, and Silcock L, "Beating IT risks. West Sussex, England: John Wiley & Sons Ltd, May 2005.

[22] Laurie Williams, "Risk Management",*IEEE Computer Society Press*, Vol. 5, No. 2, 2005, pp. 1-15.

[23] M. Gheorghe, "Risk Management in IT Governance Framework", The Bucharest Academy of Economic Studies, Romania. Vol. 14, No. 3, 2011, pp. 545-552.

[24] R. Beers, "Risk Management Fundamentals; Risk Management for Decision Making",*Homeland Security Risk Management Doctrine*, Vol. 1, No 3 2011, pp.1-31.

[25] R. Oyemade, "Effective IT Governance through the Three Lines of Defence, RiskIT and COBIT ISACA Journal Vol. 5, No. 4, 2012, pp. 10-21.

[26] W. D. Junior, "Assessing IT Governance Maturity: The Case of San Marcos, Texas". *Applied Research Projects*, Texas State University-San Marcos Luis, February 21-23, 2013, pp. 626-632.

[27] ISACA, 2013."Issues COBIT 5 Governance Framework". ISACA.org. retrievedonline, Vol. 5, No. 4, 2013, pp. 1-10.

[28] J. W.Lainhart, 2010. "Why IT governance is a top management issue", *The Journal of Corporate Accounting & Finance,*Vol. 11, No.5, July, pp. 33-40.

[29] S. B. Von, "Information Security governance: COBIT or ISO 17799 or both?", *Journal of Computers & Security,*Elsevier Advanced Technology Publishers, May 10-11, 2005 pp. 1-10.

[30] G.Sarens and I. De-Beelde, "The Relationship between Internal Audit and Senior Management: A Qualitative Analysis of Expectations and Perceptions".*International Journal of Auditing*, Febuary 8-9, 2007 pp. 10-21.

[31] G. R.Saint, "Information Security Management Best Practice Based on ISO/IEC 17799"', *Information Management Journal,*Vol. 39, No. 4, July 2005, pp. 60-66.

[32] K. Bilge and I.Sogukpinar., A quantitative method for ISO 17799 gap analysis. Computers & Security, Vol.25, No. 6, 2006, pp. 413-419

[33] D.Mellado and D. G. Rosado, "An Overview of Current Information Systems Security Challenges and Innovations", Journal*of Universal Computer Science*, February 21-23, 2007, pp. 234-241.

[34] J. Eloffand M.Eloff, "Information Security Management-A New Paradigm", *Proceedings of SAICSIT*, February 21-23, 2003, pp. 130-136.

[35] S. Groves, "The Unlikely Heroes of Cyber Security", *Information Management Journal*,Vol. 37, No. 3, May 2003, pp. 34-40.

[36] M.Theoharidou, S.Kokolakis, Karyda, M. and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799",*Computers & Security*, Vol. 24, No. 6, May2005, pp. 472-484.

[37] N.Robinson, "IT excellence starts with governance", *The Journal of Investment Compliance*, Vol. 6, No.3, April 2005, pp. 45-49.

[38] F. Say-weiand A.Muruganantham, "Software Risk Assessment Model; National University of Singapore",*IEEEinternational conference on management of innovation and technology*, May 21-23, 2005, pp. 536-544.

[39] B.Singh, D. S.Kapil and S. Chandra, "A New Model for Software Risk Management" *Inc. Computer Technology & Applications,* Vol. 3, No.3, 2012,pp. 953-956.

[40] A. Abraham and S. Y. Han, "Programming Risk Assessment Models for Online Security Evaluation Systems", International *Journal of Computer Trends and Technology (IJCTT*), Vol. 9, No 6,2009, pp.279-285

[41] S. Patel and J.Zaveri, "A Risk-Assessment Model for Cyber Attacks on Information Systems Department of Information Science & Systems", Morgan State University, Baltimore, *Journal Of Computers*, Vol. 5, No. 3, 2010, pp. 352-359

[42] M. ChoetkiertikulandT.Sunetnanta, "A Risk Assessment Model for Offshoring Using CMMI Quantitative Approach; Faculty of Information and Communication Technology Mahidol University Bangkok, Thailand", *Fifth International Conference on Software Engineering Advances*, February 10-11, 2010, pp 331-337

[43] W. L. Currie, "A Knowledge-Based Risk Assessment Framework for Evaluating Web-Enabled Application Outsourcing Projects", *International Journal of Project Management*, Vol. 21, No.2 2005, pp. 207-217

[44] G.Yucel, S. Cebi, B.Hoege and Ahmet F. Ozok, "A Fuzzy Risk Assessment Model for Hospital Information System Implementation"; Experts systems with applications Elsevier publishers, *Expert Systems with Applications*, Vol. 39,No.7, 2011 pp.1211–1218.

[45] E.Manalif, L. F. Capretz and H. Danny, "Software Project Risk Assessment and Effort Contingency Model based on COCOMO Cost Factors" *Journal of Computations & Modeling*, Vol.3, No.1, 2013, pp. 113-132.

[46] M. Wei-Ming, Study on Architecture-Oriented Information Security Risk Assessment Model Information Management Department, Cheng-Shiu University, Vol. 3, No.4, 2010, pp. 218–226,

Table 7: Risk Assessment Model/Framework of Information Technology

Model/Categories	Researchers	Components/ Technique	Limitation
Risk assessment framework in supply chain	[5]	Value Modeling, Process Analysis, Uncertainty Estimation & Multi-Criteria Decision Making Use Value based method as a technique	The framework is still a general conceptual Road-map, serving as a guideline for future research. Much work has to be done to make it practically applicable to real world business.
Software risk assessment model (SRAM)	[38]	Quality, Schedule & cost of a project risk Use questionnaire as a technique	addresses the development risk and does not assess the marketing risk.
(SRAIEM) software risk assessment identification and estimation model	[39]	Level of risk, prioritize the risk and categorize the risk. Use software metrics as a technique	Is not able to manage the risks in web distributed environment alone.
Genetic Risk Assessment Model (GePRA)	[40]	Threat level, vulnerability & Asset Value Simulations/ Programming based technique	Only able to assess technical risk in networks
Risk-assessment model to assess the impact of cyber attacks	[41]	Employees/Customers, Corporate network, Monitoring Interface, Media, Control Station & Internet Mathematical technique	Only able to assess risk loss in technical and financial damages
A Quantitative Risk Assessment Model	[42]	Qualitative Rules, Risk Factors, Project Risk & Risk Taxonomy Technique use is the quantitative CMMI assessment	No proof-of-concept prototype of this work. The validation of this model and its assessment rules will need to be further investigated
A knowledge-based risk assessment framework	[43]	delivery and enablement; integration; management and operations; business transformation; and client/vendor relationships Technique is Knowledge management	Risk assessment can only be carried on a web based.
A Fuzzy risk assessment model	[44]	Risk Likelihood, risk Severity, Risk factor, Risk, Aggregation, Fuzzy Inferencing & Deffuzification Technique is Fuzzy Algorithm	Can only assess risk for a hospital information system & has been developed to estimate risk for the implementation of new IS
A Fussy ExCOM risk assessment model	[45]	Software size, Project Risk, Contingency Allowance & Effort Estimation Technique is fuzzy novel	Model cannot be implemented thus needs learning ability and feasibility
Architecture-oriented information security risk assessment model (AOISRAM)	[46]	Risk monitoring, Risk resolution, Risk management planning, Risk prioritization, Risk analysis & Risk identification. Technique is a structure behaviour coalescence method	Research model is based on addressing security related risk