VOL. 10, NO. 23, DECEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

RISK ASSESSMENT MODEL FOR ORGANIZATIONAL INFORMATION SECURITY

Balla Moussa Dioubate[1], Nurul Nuha Abdul Molok[1], Shuhaili Talib[1] and Abu Osman Md. Tap[2]
[1]Department of Information System, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2] Department of Computer Sciences, International Islamic University Malaysia, Kuala Lumpur, Malaysia
E-Mail: ballamoussa2006@yahoo.fr

ABSTRACT

Information security risk assessment (RA) plays an important role in the organization's future strategic planning. Generally there are two types of RA approaches: quantitative RA and qualitative RA. The quantitative RA is an objective study of the risk that use numerical data. On the other hand, the qualitative RA is a subjective evaluation based on judgment and experiences which does not operate on numerical data. It is difficult to conduct a purely quantitative RA method, because of the difficulty to comprehend numerical data alone without a subjective explanation. However, the qualitative RA does not necessarily demand the objectivity of the risks, although it is possible to conduct RA that is purely qualitative in nature. If implemented in silos, the limitations of both quantitative and qualitative methods may increase the likelihood of direct and indirect losses of an organization. This paper suggests a combined RA model from both quantitative and qualitative RA methods to be used for assessing information security risks. In order to interpret and apply the model, a prototype of RA for information security risks will be developed. This prototype will be evaluated by information security risk management experts from the industry. Feedback from the experts will be used to improve the proposed RA model. The implementation of an appropriate model ensures a successful RA method and prevent the organization from the natural and causal risks that are related to securing information assets.

Keywords: Information Security Risk Assessment, Quantitative Risk Assessment, Qualitative Risk Assessment.

INTRODUCTION

Due to the advancement of interconnected networks, organizations are facing information security risks on a daily basis. Therefore, it is important for organization to manage the risks which can jeopardize the security of their valuable information [1, 2]. According to [3], information security risks can be defined as consequence of uncertainty on information security objectives [3], specifies the control as a measure from the international best security practices to modify information security risks. A control can decrease the risk by reducing the possibility of an event, the impact or both [4].

Information security risk management is very important for business, government, and also for individuals in order to protect their information. Since a decade ago, the organizations are paying more attention to their information assets against possible security threats [5]. This is important for the survival of organizations and to gain competitive advantage. However, due to the lack of proper security risk management, it has been reported that organizations are experiencing financial losses and reputational risks [6]. Hence, to manage the risks, organizations need to assess the security risks to their valuable assets and plan for mitigating control actions to address these risks.

Information security RA represents a process to ensure that the appropriate security measures are identified and applied to meet the management's expectations for a secure and trusted computing environment [7]. However, a principal challenge that many agencies are facing is identifying and evaluating the information security risks to their operations. Therefore, careful selection of RA methods can help organizations to identify, manage, and evaluate the risks to their assets. It informs organizations about information security threats that may affect the organizations' assets and exploit their vulnerabilities [5, 8, 9].

According to [10] some organizations practiced the quantitative approach to RA without proper judgment and understanding of the assessed risks. On the other hand, qualitative approaches are more subjective than quantitative methods, thus it can be used with or without any objectivities. According to [11], the difficulty in conducting the process and selection of appropriate methods of measures for information security systems. Therefore, it is important to develop a RA model in order to ensure that security risks are assessed properly.

Although RA model is important for the industry, research in this area is still limited. Thus, this paper attempts to fulfill this gap and proposes a combined method of qualitative and quantitative RA for information security that will lead to the development of a model and applying the model through the development of a prototype of RA application system. The proposed RA model will incorporate the use of numerical and non-numerical data in the assessment process.

BACKGROUND OF RESEARCH

The advancement of information technology (IT) requires an intelligent decision-making approaches when it comes to protection of information resources [5]. The use of digital data and the evolution of information systems expose business to threats that attack the organizational assets which can lead to economic losses. An effective risk management requires the probability analysis of events and the impact of the threats to the information assets [12].

Traditionally, information security RA tends to focus on risks in IT but, recently, it has been established that information security RA is more comprehensive than IT assets alone [13]. The estimation of the risks can be categorized into three methods such as: qualitative, semi-quantitative and quantitative, first of which is the most used even if not always provide an accurate mathematical model [14].

Information Security Risk Management

In recent years, information systems have been at risks from unintentional operator errors, and from natural and instrumental disaster. These are mostly caused by the interconnection of the computers and accessibility by many people [1, 15]. Consequently, the number of people with computer skills is increasing, and so as the hacking skills and techniques. Information security risk management is the precondition of information security management, it is perceived as a way to reduce uncertainty and its consequences. In turn, successful risk management meaningful understanding of the whole security profile of organizations [15]. A successful IT security requires an affective risk management process, which intend to provide an appropriate e-business atmosphere, as IT systems are challenged by high degrees of risks [1, 15]. Therefore, a security risk management process allow many enterprises to perform in the most cost efficient manner in order to mitigate business risks.

Information Security Risk Assessment

Information security RA plays an important role in the risk management of organizations especially when there is high dependency on IT [16]. Thus, organizations need to assess those risks to ensure that the appropriate security measures are identified and applied to meet management's expectations for a protected and trusted computing atmosphere [7]. RA is an important step of risk management, which define suitable controls methods for reducing or eliminating risks. It is categorized by the following four steps: 1) Threat identification, 2) Vulnerability identification, 3) Risk determination, and 4) Control recommendation [17]. Similarly, [18] mentioned that information security RA process includes preparation of RA, asset identification, threat identification, vulnerability identification, risk calculation and other stages. According to [18], information security RA process is categorized into six steps, Step 1: Determine the assessment of the objective, this step define information system data, the hardware and software assets. Step 2: Performance of assessment, to improve the evaluation plan, determine the process of assessment and select a proper assessment methods and tools. Step 3: Identification of risk to identify the assets within the scope of assessment, the threat, asset vulnerability and existing security measures. Step 4: Risk analysis, to analyze the possibility and consequences of threats and vulnerabilities. Step 5: Evaluation of the result, to make a risk assessment report evaluated by expert. Finally, step 6 Risk control, is to take effective measures either to transfer the risks, to avoid or to reduce risk in order to control the system. Figure-1 summarizes the procedures of RA for information security.

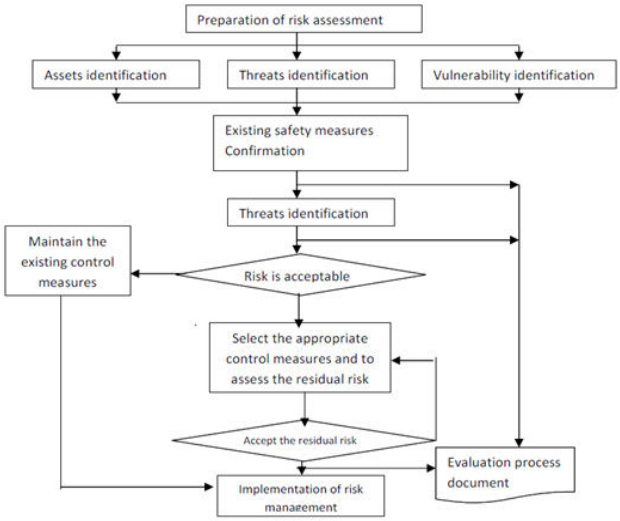

Figure-1. The process of the information security RA [18].

According to [13, 18, 22, 24, 26] there are two approaches of RA quantitative and qualitative methods, realizing both approaches have its own strengths and weaknesses, this study proposes to combine both methods and name it the combined risk assessment model (C-RAM) to manage some of the limitations of the current RA models.

Information Security Risk Assessment Quantitative Methods

Quantitative analysis assigned numerical values derived from a variety of sources to both impact and likelihood [19]. Although [20] mentioned that "*A quantitative risk analysis attempts to assign numeric values to the likelihood and the impact of the risk and to the costs and benefits related to the introduction of security controls and systems*" [20, p-218]. However, [21] stated that, the risk quantification consists of two main steps, risk analysis which provide input to the risk evaluation and treatment, and the risk evaluation that gives the synthetically expression of the risk level for each risk factor.

According to [16], the quantification methods of e-commerce security risk simply show the attributed value given for normal comparison which is different from the real probability of risk arrangement. In the same light, the earlier work of [22] defined the risk as the product of the probability (Pe) of the security threat event e and the potential impact (Ie):

$$Re = Pe.Ie \quad (1)$$

Where, Pe typically is a fraction less than 1 so it comprises between ($0 \leq Pe \leq 1$), whereas Ie may be

assigned a value on numerical scale, for example (Ie) can be LOW (1-5); MODERATE (6-10); HIGH (11-15). After the risk calculation, a group of experts shall discuss the results and agreed on the results. Once consensus is achieved, the resulting Ie will be assessed based on information security components: confidentiality, integrity, availability, multi-trust, auditability and usability (CIAMAU).

On the other hand, [18] extended the RA procedure by incorporating the economic idea, that consists of evaluating the probability of an event occurring and the loss that may incur, such as risk value, annual loss expectancy (ALE), safeguard value, and return on investment. Therefore, the risk is evaluated as follow:

$$R = p \times W \text{ and } p = F \times V \quad (2)$$

Where, R is Risk value; p is the predicted number of incident occurrence causing loss of assets value in defined period; W-- The value of loss of assets value on a single incident occurrence; F is frequency of threat occurrence; V is the measure of probability of usage of specified susceptibility by a given threat.

However, the quantitative model of information security RA evaluation can be difficult due to the limitation of the company‘s unsuccessful track of security incidents reports management [5]. This paper adopts the strengths of quantitative RA. It proposes a risk calculation formula derived from the earlier developed risks calculation methods.

Information Security Risk Assessment Qualitative Methods

The qualitative RA method analyzes the risks with the help of adjectives instead of using mathematics [9]. Therefore, it is used as a preliminary assessment to detect risks that will be assessed to have more details for analysis [23]. In the same way [24] revealed that most methods are used with qualitative measurements, and this statement is confirmed by the fact that most RA methods today are carried out in a qualitative way. Perhaps due to the difficulty the organization to assign and apply quantitative data or due to time constraints. Furthermore, qualitative models for RA are often preferred by professionals for several reasons such as the perception of speed and facility of application, the accessibility and easily understood by policy makers [24]. Thus, the qualitative assessment results satisfy a range of needs, although sometimes the assessment is not faster or easier to achieve [12, 24]. According to [10] qualitative RAs are more subjective than quantitative RAs and it may result in a better understanding of the business, as well as to ameliorate the communication between the different departments in charge of the RA. Similarly, [12] found that the qualitative risk analysis regularly provides assistance for additional investigation of quantitative RA method, but it can also provide information required for risk management. Therefore, by referring to the survey of RA published by [17] IT is more connected with the qualitative approach of RA because this approach is used in events where by it is difficult to express numerical measures of risks. Thus, this research, adopts the qualitative RA as the subjective study of the risk that used an interval scale to represent the likelihood, the impact and also the risk, in which each interval is typically represented by a non-numerical label such as Low, Medium and High.

Research Background Summary

In summary, the findings from the review of literature research show the gaps in both qualitative and quantitative methods of RA in the organization. Even though there are many industries that use quantitative RA methods, the use of quantitative RA in the IT industry is rare due to the lack of historical data and detailed explanation about the risks. The intensive quantitative measures in risks assessment methods are not common for information security risk analysis and they are not common for today’s organization. Therefore, this paper proposes the combination of qualitative and quantitative methods for information security RA.

RESEARCH METHODOLOGY

This study employs qualitative research approach of research methodology, but once it comes to the proposed RA model we adopt the hybrid of qualitative and quantitative risk assessment methods. The design of research is shown in Figure-2.

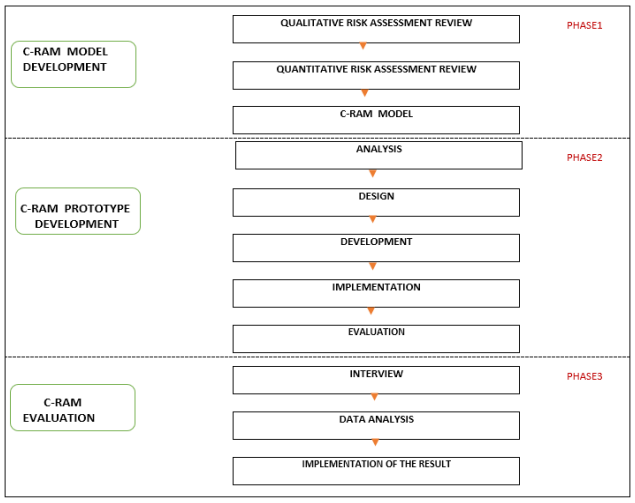

Figure-2. Research Methodology.

Based on Figure-2, the research study is divided into three phases:

Phase 1: Development of the RA model

The review of the literature from different papers highlighted the limitation of both qualitative and quantitative approach of RA if each method is

implemented separately. Therefore, we propose a model that combines both qualitative and quantitative which lead to the development of the combined RA model (C-RAM). (See Figure-3).

Phase 2: Development of the prototype

In order to interpret and apply the model, the development of a new prototype that will be done by using the ADDIE method which is an iterative instructional design process, where the outcome of each step forms an input for the rest procedure [25]. As the abbreviation, ADDIE method consists of five steps: analyze, design, development, implementation and evaluation.

Phase3: Evaluation of the model

The model will be evaluated and tested by experts in RA information security during an interview. This is done to improve the proposed model through the prototype. In order to get a really feedback about the developed C-RAM.

COMBINED RISK ASSESSMENT MODEL (C-RAM)

C-RAM is the combination of quantitative and qualitative methods for information security RA in order to manage some of the current limitations. The proposed C-RAM will incorporate a literal estimation of the identified risks through a RA checklist and the mathematic evaluation of the probability of risk appearance. The proposed C-RAM process is broken down into four steps: risk identification, risk rating, risk calculation, and result (Figure-3).

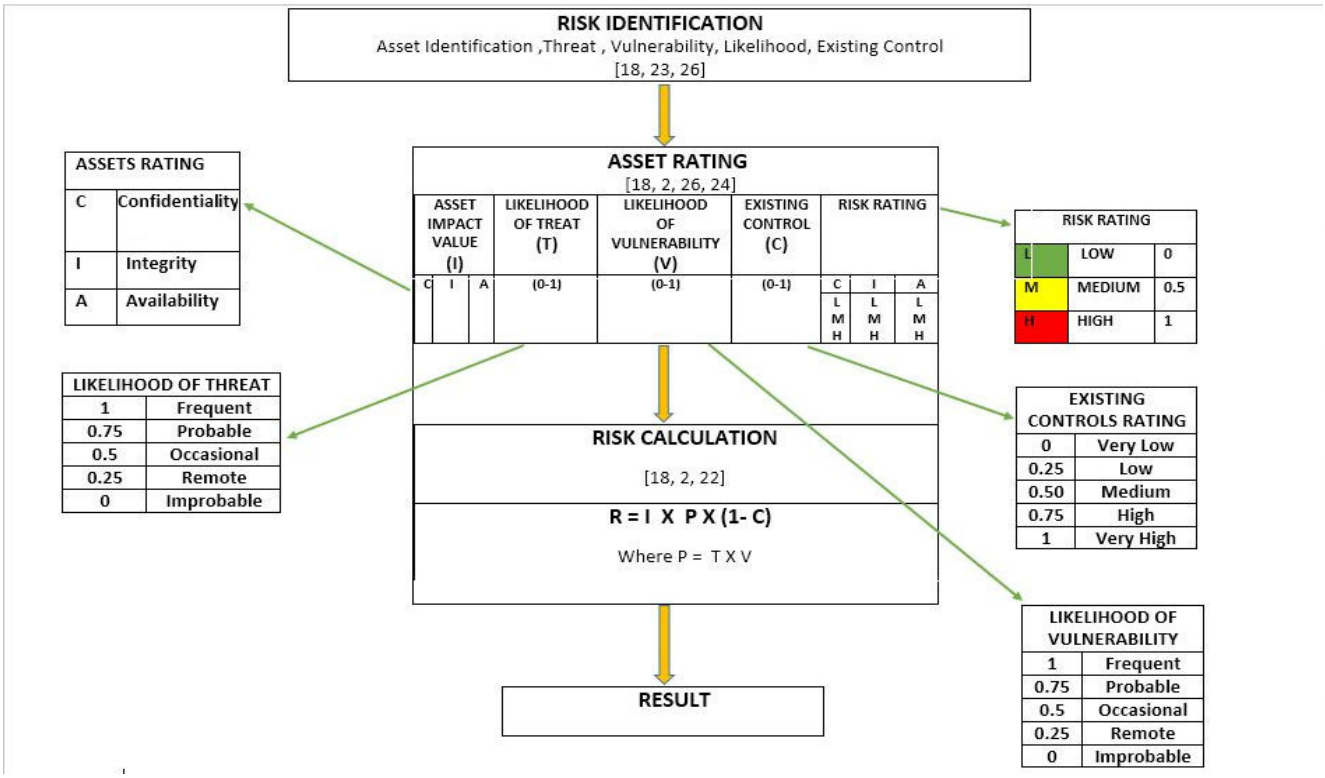

Figure-3. C-RAM Model Adapted from [2, 18, 22, 23, 24, 26].

Risk identification

Risk identification is the first step of the model. The selection of the components of risk identification is adapted from the authors [18, 19, 26]. This is to identify a comprehensive list of risks that may serve for risk rating. By referring to [19] the risk identification step is the phase where threats, vulnerabilities and the related risks are identified. In the same light, [18] identified the risk in the step3 of information security risk assessment process as follow: asset identification, threat identification, vulnerability identification and the existing security measures. However, [26] mentioned about the imperious need of identifying the correct information assets and the selection of the organization's critical assets from a complete list. Therefore, the method has to be methodical and inclusive enough to make sure that that no risk is omitted. However, based on the view of the above scholars, C-RAM risk identification phase comprised the identification of assets, threats, vulnerabilities, likelihoods and existing controls.

Risk Rating

The risk rating is adapted from the view of these authors [2, 18, 24, 26]. Following [26] asset impact value (I): the assets owner will be given an asset valuation form to be filled in for each asset and the rating is valued by referring to the confidentiality, integrity and availability (CIA).

Likelihood of threat (T): the threats are rated based on the probability of the occurrence. From the view of [25] the possibility to produce threats are evaluated on a scale from as shown in Table-1.

Table-1. Likelihood of threat

LIKELIHOOD OF THREAT	
1	Frequent
0.75	Probable
0.5	Occasional
0.25	Remote
0	Improbable

The same range applies for the likelihood of vulnerability (V): the likelihood of vulnerability is rated based on the probability of the threat to penetrate the organization assets (see Table-2).

Table-2. Likelihood of vulnerability

LIKELIHOOD OF VULNERABILITY	
1	Frequent
0.75	Probable
0.5	Occasional
0.25	Remote
0	Improbable

Existing control (C): According to [4] the control can diminish the risk by decreasing the likelihood of an event, the impact or both. Similarly, [18] stated that existing control requires effective measures to transfer, reduce or avoid risk. However, if there is an existing control the risk rate evaluated from C-RAM will be reduced according to the degree of the existing control. C-RAM existing control rating is as follow: (see Table-3).

Table-3. Existing control rating

EXISTING CONTROLS RATING	
0	Very Low
0.25	Low
0.50	Medium
0.75	High
1	Very High

Risk rating (R): From the view of [2], various scoring systems are possible; but the author suggested the use of the values none, low, moderate, high, very high. However, C-RAM risk rating will be based on CIA, the values generated have their corresponding interval scale from (0- Low, 0.5-Medium, 1-High). C-RAM risk rating is as follow: (see Table-4).

Table-4. An example of C-RAM Result.

RISK RATING	
1	High
0.5	Medium
0	Low

C-Ram Risk Calculation

After the risk rating, the corresponding value to each literal rate of the different component will be used as an input for C-RAM risk calculation formula. The risk calculation formula used in this model is adapted from [18, 2, 22]. From the view of [16], the risk value calculated determines whether a particular asset is in fact at 'high', 'medium', or 'low' risk for the risk classification. Following the work of [22] risk is defined as a product of the Probability (*Pe*) of a security compromise, i.e. a threat event, e, occurring and its potential Impact or Consequence (*Ie*). Similarly, [7] calculated the risk value as the product of the predicted number of incident (*P*) by the value of loss of assets value on single incident occurrence (*W*). Therefore C-RAM risk calculation formula determines the degree of risk that is pointing the asset. The risk rate may be reduce if there is an existing control implemented to the asset. This formula is incorporated into C-RAM prototype that is under development to interpret the model. However, C-RAM risk calculation uses the following formula to evaluate the risk rate.

$$R = I \times P \times (1-C) \quad (3)$$

Where: $P = T \times V$

R is Risk value; P is the value of incident based on threats and vulnerability; and C is existing control implemented.

C-RAM Result

C-RAM generates a result after the risk calculation, for the assets involved in risk assessment process. This result highlighted the particular information of the asset, the impact in term of CIA, the likelihood of threat and vulnerability, the existing control and also the risk based on CIA. This result serves the organization as a record that may contribute to the good decision making in assessing and managing risks. The report of the result can be directly printed from the C-RAM software as an excel file. Table-5 is an example of C-RAM Result for one particular asset.

Table-5. An example of C-RAM Result.

ASSET RISK ASSESSMENT RESULT												
Asset Id	Asset Name	Confidentiality	Integrity	Availability	Likelihood of Threat	Likelihood Of Vulnerability	Existing Control	Confidentiality Risk		Integrity Risk		Availability Risk	
001	LAP TOP	0.30	0.40	0.40	0.25	0.25	0.10	0.16	LOW	0.02	LOW	0.02	LOW

CONCLUSIONS

This paper presented a proposed model of RA for organizational information security. The proposed RA method combines both qualitative and quantitative assessment methods in order to adjust the weakness of both Approaches. The proposed model consists of both quantitative and qualitative RA methods. It is expected to address the weaknesses of the traditional RA methods and to give significant improvements in terms of information security RA practices. This proposed model may help organizations to manage and assess their operational information security. To ensure the RA model's practicality, the proposed model is translated into an RA prototype. This prototype will be evaluated by information security RA experts to seek valuable feedback in order to improve the RA model. This papers calls for more research in this area, to extend risk assessment to risk treatment, in order to complete the entire risk management lifecycle.

ACKNOWLEDGEMENTS

The authors wish to express our appreciation and thanks to the Kulliyah of Information and Communication Technology, International Islamic University Malaysia for providing financial support for this research paper.

REFERENCES

[1] Boltz, J. (1999). Informational Security Risk Assessment: Practices of Leading Organizations. DIANE Publishing.

[2] Mouw, E., van't Noordende, G., Louter, B., & Olabarriaga, S. D. (2013). A Model-based Information Security Risk Assessment Method for Science Gateways. In IWSG.

[3] International standard ISO/IEC. (2014). Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000:2014(E).

[4] Department of Internal affairs New Zealand government. (2014). Risk-Assessment-Process-Information-Security.pdf. Retrieved August 13, 2015, from https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf.

[5] Bojanc, R. (2012). Quantitative model for information security risk management (pp. 267–275).

[6] Bojanc, R. (2013). A Quantitative model for information-security risk management.

[7] Kleckner, M. (2001). Facilitating-qualitative-security-assessment-overview-process-defining-deliverin-431.pdf.

[8] Bojanc, R., & Jerman-Blažič, B. (2012). Quantitative Model for Economic Analyses of information Security investment in an Enterprise information System. Organizacija, 45(6), 276–288.

[9] Wawrzyniak, D. (2008). Information security risk assessment–the development of the standard approaches (pp. 759–764).

[10] Risk Assessment Special Interest Group (SIG), & Payment Card Industry (PCI) Security Standards Council.

[11] Rot, A. (2008). World Congress on Engineering and Computer Science, WCECS 2008, San Francisco, USA, 22 - 24 October, 2008. Hong Kong: IAENG International Association of Engineers.

[12] Iacob, V.-S. (2014). Risk management and Evaluation and qualitative method within the Projects. Ecoforum Journal, 3(1), 10.

[13] Saluja, U., & Idris, N. B. (2012). Information Risk Management: Qualitative or Quantitative? Cross industry lessons from medical and financial fields.

[14] Radu, L.-D. (2010). Discussions on qualitative assessment or risk quantification in adopting decisions concerning risk in financial auditing.

[15] Talet, A. N., Mat-Zin, R., & Houari, M. (2014). Risk management and information technology projects. International Journal of Digital Information and Wireless Communications (IJDIWC), 4(1), 1–9.

[16] Lao, G., & Wang, L. (2008). The Quantification Management of Information Security Risk. In Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on (pp. 1–4).

[17] Drissi, S., Houmani, H., & Medromi, H. (2013). Survey: Risk Assessment for Cloud Computing. International Journal of Advanced Computer Science and Applications, 4, 143–148.

[18] Chang Lee, M.-. (2014). Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. International Journal of Computer Science and Information Technology, 6(1), 29–45. http://doi.org/10.5121/ijcsit.2014.6103

[19] Iacob, V.-S. (2014). Risk management and Evaluation and qualitative method within the Projects. Ecoforum Journal, 3(1), 10.

[20] Bojanc, R., & Jerman-Blažič, B. (2008). Towards a standard approach for quantifying an ICT security investment. Computer Standards & Interfaces, 30(4), 216–222.

[21] Aloini, D., Dulmin, R., & Mininno, V. (2012). Risk assessment in ERP projects. Information Systems, 37(3), 183–199.

[22] Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security (pp. 280–288).

[23] Nasir, G. A., Yassir, A., & Ithnan, N. (2013). Enhancement of Dynamic Risk Assessment Model for Telecommunication Infrastructure. International Journal of Scientific and Research Publications.

[24] Radu, L.-D. (2010). Discussions on qualitative assessment or risk quantification in adopting decisions concerning risk in financial auditing.

[25] Dick, W., Carey, L., & Carey, J. O. (2001). The systematic design of instruction (5th ed). New York: Longman.

[26] Shedden, P., Smith, W., & Ahmad, A. (2010). Information security risk assessment: towards a business practice perspective. Retrieved from http://ro.ecu.edu.au/ism/98/