International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016
ISSN: 2395-3470
www.ijseas.com

Comparison of Information Security Risk Prioritizations in the Banking Industry
A Case Study of Private Banks

Shima Simsar [1], Alireza Poorebrahimi[2]
[1] Islamic Azad University Science and Research branch , Tehran, Iran
[2] Islamic Azad University,Karaj,Iran

Abstract
The identification and prioritization of key information security factors in banking will greatly contribute to their effective management. In this research, a comprehensive list of information security risks in banking was obtained through a review of relevant literature. Expert opinions were then employed in identifying bank-specific risk factors. Finally, the factors were prioritized through analytic hierarchy process. The research findings mainly served to identify and discuss private bank information security risks, the relative weight of each factor and sub-factor of private bank information security risks. The results indicated that "a lack of input data, internal processes, and output data verification", insecure software and information exchange processes inside/outside of banks, as well as " lack of backup information " were among the high-priority risks. Insufficient budget allocated on security plans was identified as a factor that needed lesser attention compared to other risks.
Keywords: *Information security, Private Banks, Risk factors, Analytic hierarchical process.*

1. Introduction
With the expansion of communication media and the exponential increase in the rate of electronic data storage and transmission, the need for information security has reached the highest level for both personal and organizational uses [1]. Given their practical expansion, one of the main missions of computer networks has been hardware and software resource sharing as well as quick and easy access to information. Shared-resource access and usage control are among the top priorities of any network security system. It is therefore necessary for any organization to pursue a specific strategy and implement a security strategy in line with protecting valuable information.
In order to protect organizational information, it is not merely enough to rely on a specific type of security or product. To expect that a particular product fulfills all security requirements of computer networks and network equipment is nothing but a dream [2].
In today's world, information is the most valuable asset and a basic commodity of any organization. Just as running a great deal of business affairs without electricity would encounter serious obstacles [3]. information is the most valuable asset of any organization and a critical factor for organizational success. Therefore, the highest level of management held accountable for organizational success is often assigned with the responsibility of protecting corporate information [4]. in order to maintain information and system security by minimizing security and business risks. Risk management is one of the most important functions of any information security management system that should be implemented in all organizations depending on their needs [5]. Risk management is the process of identifying and evaluating the impact probability of specified risks [6]. Risk ranking is a key part of risk evaluation in the process of risk management. The existing information security methodologies, e.g. COBRA, OCTAVE, and ISO 27005, only address general rules and instructions for the evaluation of information security risks without provide any information on the implementation details [7]. In this study, information security risks in private banks were first identified and then ranked using AHP fuzzy multiple attribute decision-making method. Finally, the identified risks were ranked through AHP and the results were compared.

2.Background:
This section explores the theoretical foundations, covering definitions and security issues.

2.1 Definition of risk:

Project risks are events or situations whose occurrence probability is undetermined and influence project goals in a positive or negative way if realized. There are specific causes behind each of these events or situations, but their consequences can be predicted [8].

2.2 Risk management:

Security risk management is a process by which the existing organizational risks are identified, prioritized and an acceptable way of managing them is arrived at. A systematic set of strategies for security risk management enables organizations to engage in identification and

prioritization of activities in an information technology (IT) environment and to maintain those procedures. Substituting prophylactic measures for passive ones is the most important achievement of security risk management which will definitely improve the organizational status [9]. Project risk management is one of the major concerns of project management that includes planning, organizing, monitoring, regulating all aspects of project, risk identification, risk measurement, risk response development, and risk response control [8]. Risk management is the process of risk identification and evaluation as well as making attempts to reduce risks to an acceptable level [10].

2.3 Organizational information security:

Information security refers to information protection and minimizing the risk of information disclosure to unauthorized sections. Information security denotes a set of tools used in preventing theft, attacks, felony, espionage, and sabotage. It is the science of studying data protection methods in computers and communication systems against unauthorized access or manipulation. Based on the above definitions, security is generally refers to a series of measures, methods, and tools employed to prevent unauthorized access to and manipulations in computer and communication systems [11]. Therefore, information security deals with information confidentiality, integrity, and accessibility. Other characteristics include originality, undeniable credibility, information accountability, and reliability [9].The purpose behind information security management in organizations is to maintain their assets (software, hardware, information, communication, and human resources) against any threat (including unauthorized access to information, environmental or systemic hazards, and user-created dangers), the attainment of which needs a systematic plan. The information security management system is not limited to a period of action in the management system; rather, it is achieved through a permanent security building process consisting of four steps as follows [12]:

1- Planning: creating the initial settings of the information security management system;
2- Execution: implementing the information security management system;
3- Evaluation and control: taking regulatory measures or investigating the conducted activities; and
4- Improvement and modification: maintenance activities and continuous improvement of the management system.

2.4 Information security management standards

Information security is part of the overall management system of an organization which is based on the business risk approach and aims at establishing, implementing, utilizing, supervising, reviewing, maintaining, and enhancing information security [9]. Several systems have been developed and recommended in many countries for establishing organizational information security. The US National Institute of Standards and Technology (NIST) has proposed a number of standards for establishing security in various domains [13]. The document taken as a reference point in this study is ISO/IEC 27002 information security management instruction which was introduced in 2007 by an amendment in BS 7799 standards developed in 1987 by the Computer Commerce and Technology Center (CCSC) [11]. The related regulations and regulatory goals to this standard are implemented for meeting input identification requirements through the implementation of risk evaluation. Employed as a guideline for the implementation of organizational security standards development, effective security management practices, and aiding the process of trust building in intra-organizational activities, this standard entails a comprehensible list of security controls in 11 items (the Standards and Industrial Research Institute of Iran, 2008) including: 1- security policy, 2- organization of information security, 3- asset management, 4- human resources security, 5- physical and environmental security, 6- communications and operations management, 7- access control, 8- information systems acquisition, development, and maintenance, 9- information security incident management, 10- business continuity management, and 11- compliance with law. This standard incorporates 11 control sets including 39 control objectives, 136 primary controls and more than 500 secondary controls [9].

2.5 Analytic Hierarchical Process

In any instance of decision-making, the decision-maker may deal with various criteria. In such circumstances, he has to resort to well-known methods of decision-making. One such method is the analytic hierarchy process (AHP), which is one of the most well-known multipurpose decision-making techniques developed by Thomas Saaty in 1980. This method can be employed when decision-making hinges on several competing options and criteria. AHP is based on the pairwise comparison of decision-making criteria and options. To make such a comparison, it is necessary to collect information about decision-makers who are then enabled to solely focus on two criteria or options [14]. To solve decision-making problems using AHP, a hierarchical structure chart should first be drawn. AHP is based on the following three principles: a) drawing a hierarchical tree chart, b) determining priorities, and c) logical consistency of judgments.

Now, we will analyze the problem using AHP. In doing so, we will divide it into a number of simpler problems. After determining options and measures, we will draw pairwise comparisons between the measures. In the next step, we will draw paired comparisons between options for each measure. Then, the following algorithm is employed:
a) Normalizing the pairwise comparison matrices,
b) Calculating the arithmetic mean of each normalized pairwise comparison matrix's row (relative weights),
c) Multiplying relative weights of measures by arithmetic mean of options,
d) Ranking the options.
After this step, we will begin measuring the compatibility index through the following steps:
Step 1- Calculating the Weighted Sum Vector (WSV): multiplying the pairwise comparison matrix (D) by the relative weights vector (W); the resulting vector is called WSV.

$$WSV = D \times W \qquad (1)$$

Step 2- Calculating the compatibility vector (CV): dividing WSV components by the relative weights vector; the resulting vector is called CV.
Step 3- Calculating the maximum eigenvalue of the pairwise comparison matrix (λ_{max}): to measure the maximum eigenvalue of the pairwise comparison matrix, the mean of CV components is calculated.
Step 4- Calculating incompatibility index (II).

$$II = \frac{\lambda_{max} - n}{n - 1} \qquad (2)$$

Step 5- calculating incompatibility rate (IR).
If IR≤0.1, there is compatibility in pairwise comparisons; otherwise, they need to be modified.

$$IR = \frac{II}{IRI} \qquad (3)$$

3. Literature review

The increasing prevalence of information security risks has compelled many researchers to identify and prioritize such risks in the business-related fields. What follows are some of the studies conducted in this regard.
Zhiwei and Zhongyuan (2012) proposed a model for better evaluation of information systems security risks based on a process approach [15]. Honghui and Yanling (2010) used a combination of radial basis function (RBF), neural networks and fuzzy particle swarm optimization evaluation methods to assess information security risks [16]. Ekelhart et al. (2009) proposed a method of information security risk management that completely covers the NIST [17]. Using economic modeling, Bojanc and Blajick (2008) analyzed and ranked information security risks[18]. Hung and Chen (2009) measured and ranked information security risks using the technique for order of preference by similarity to ideal solution (TOPSIS) and fuzzy theory[19]. Smojver (2011) presented a model for optimal selection of information security risk management method based on AHP [20]. To evaluate information security risks, Wang and Zeng (2010) integrated AHP, fuzzy mathematics, and artificial neural networks [21]. Shamely et al., (2010) used a combination of ISO 27001 security standard, fuzzy TOPSIS, and expert systems to evaluate information security risks[7].
Feng et al., (2014) proposed a model for the analysis of information system security risks using a Bayesian network and ant colony optimization [22]. Yang et al., (2013) presented a model for evaluation of information security risks, capable of enhancing information for organizations. This is a decision model that offers a combination of ANP, VIKOR, and DEMATEL methods for solving problems with paradoxical criteria[23].
Khajouyi (2011) investigated information security controls based on international standards[24]. Iesavi (2011) studied operational risks pertaining to information security in the modern banking system[25]. Biglarian (2012) examined the information security evaluation measures of the Tehran Stock Exchange [26]. Avalincharsooghi et al. (2013) investigated the utilization of artificial neural networks in information security risk evaluation and proposed new strategies for determining the probability of threats and degrees of vulnerability as well as their combination with the consequences of incidents[27].

4.Methodology

This was an applied, descriptive research. In addition, it was a survey-based research in terms of methodology, where the most important advantage is that the results can be generalized. This study sought to offer a framework that could be utilized by private banks in the effective implementation of information security.

4.1 Data collection tools

To examine information security risks, the factors posing such risks were first identified through desk reviews of previous articles and studies on information security risks. In-depth interviews with 6 experts who had more than 10 years of experience in banks were then conducted on risk factors and their ranking including a series of predetermined questions about specific topics, which enabled the interviewee to provide more inclusive answers to the interviewer. The purpose behind conducting this interview was to match the extracted risk factors from the literature with those of banks. By taking expert opinions into account, and combining and eliminating a number of factors, 6 primary factors and 17 sub-factors were ultimately identified, about which a general consensus was arrived at by experts. Table 1 illustrates the risk factors of private banks.

Table 1 .Risk Factors

Security Factor	Security sub-factor
1.Absence of a policy on organizational security	1-1Ambiguous definitions of information security responsibility in banks 1-2 lack of an inclusive, reviewable and up to date policy for all bank sections 1-3 mismatch between security activities and bank requirements
2.Management irresponsibility	2-1 Lack of information security support on the part of management; 2-2 insufficient budget for security plans; 2-3 lack of supervision and inspection by managers
3.Insecurity of human resources	3-1 Unawareness and lack of education on the part of employees with respect to information security; 3-2 Lack of commitment and regard on the part of employees with respect to information security;
4.Lack of security on the part of physical systems and equipment	4-1 Equipment insecurity in face of natural and manmade disasters (emergency power) 4-2 damage from unauthorized access and the halting of organizational activity
5.Insecure network and E-commerce	5-1 Insecurity of information exchange processes and software inside/outside banks 5-2 insecurity of E-commerce services including online transactions 5-3 lack of backup information

6.Inadequate control system	6-1 Lack of input data accuracy, internal processes, and output data verification 6-2 outsourced software development without monitoring and supervision 6-3 not reporting security events and weaknesses 6-4 not adopting prophylactic security measures

4.2 Statistical population

The statistical population of this study consisted of private banks in Urmia, Iran. An overall 30 pairwise comparison questionnaires were devised for the previously described risk factors and were handed to private bank IT experts. The risks were then ranked through AHP by Expert Choice software.

5.Results and analysis

In this article, bank risk factors were identified and their levels of importance were determined. Managers should not overlook information security risks. Therefore, risk management is an important matter. According to Boehm, risk management is a process comprising two main phases: risk estimation phase (including identification, analysis, and prioritization) and risk control phase (including risk management planning, risk monitoring planning, and corrective measures). This paper attempted to cover the first phase and offer an adequate framework for banks. AHP was used to rank the related risks to information security in banks by exploiting the opinions of 30 IT experts and managers in Urmia private banks. The new framework can offer a good understanding of the related risks to bank information security, their importance and prioritization manners. Additionally, this research helps banks guarantee data confidentiality, integration, and accessibility through risk identification and management. Using the hierarchical structure of Table 1, pairwise comparison matrices were first aggregated by expert opinions. Moreover, the compatibility index of each matrix was calculated followed by the weight of each sub-criterion. Questionnaires were used to obtain expert opinions in pairwise comparison matrices. The questionnaires were devised in a way that enable respondents to determine the relative importance of each criterion and sub-criterion through separate pairwise comparisons. The results of these comparisons were calculated by Expert Choice and illustrated in Table 2. Since the total incompatibility rate of factors was 0.07 that was less than 0.1, it is therefore concluded that the matrix is compatible and acceptable. Table 2 illustrates the factor and sub-factor weights and IR rate.

Table 2: Factor and sub-factor weights and IR rate

Security Factor,W,IR	**Security sub-factor , W**
1.Absence of a policy on organizational security W=0.028 IR=0.0035	1-1Ambiguous definitions of information security responsibility in banks (W=0.648), (W_T= 0.017) 1-2 lack of an inclusive, reviewable and up to date policy for all bank sections(W=0.122), (W_T= 0.003) 1-3 mismatch between security activities and bank requirements(W=0.230), (W_T= 0.006)
2.Management irresponsibility W=0.109 IR=0.05	2-1 Lack of information security support on the part of management(W=0.578) , (W_T= 0.068) 2-2 insufficient budget for security plans(W=0.057) (W_T= 0.007) 2-3 lack of supervision and inspection by managers (W=0.364), (W_T= 0.043)

3.Insecurity of human resources W=0.137 IR=0.00	3-1 Unawareness and lack of education on the part of employees with respect to information security(W=0.333), (W_T= 0.042) 3-2 Lack of commitment and regard on the part of employees with respect to information security(W=0.667), (W_T = 0.085)
4.Lack of security on the part of physical systems & equipment W=0.141 IR=0.00	4-1 Equipment insecurity in face of natural & manmade disasters(W=0.087) 4-2 damage from unauthorized access & the halting of organizational activity (W=0.167), (W_T= 0.017)
5.Insecure network and E-commerce W=0.276 IR=0.05	5-1 Insecurity of information exchange processes and software inside/outside banks(W=0.499), (W_T= 0.171) 5-2 insecurity of E-commerce services including online transactions(W=0.105) (W_T = 0.036) 5-3 lack of backup information(W=0.396), (W_T = 0.136)
6.Inadequate control system W=0.310 IR=0.009	6-1 Lack of input data accuracy, internal processes, and output data verification(W=0.679) (W_T= 0.192) 6-2 outsourced software development without monitoring and supervision(W=0.050), (W_T= 0.014) 6-3 not reporting security events and weaknesses(W=0.179) (W_T= 0.050) 6-4 not adopting prophylactic security measures(W=0.093) (W_T= 0.026)

6. Conclusion

In their effort to prevent any unforeseen and undesirable risks through identification of information security risks, private banks need to develop a proper governance structure so as to monitor the risk management plan. Such stated plan can manage the adopted policies to reduce information security risks. The framework proposed in this study was risk prioritization based on ISO standard by which bank information security risks were prioritized through AHP. The present research was carried out in two steps:

Step 1: information security risk identification of private banks

Step 2: determining the relative weights of private banks' information security risk factors and sub-factors using AHP and considering the results of private banks' information security risk prioritization. "Insufficient input data, internal processes, and output data verification", "insecurity of information exchange processes and software inside/outside banks", and " lack of backup information " have been identified as high-priority risks. Therefore, appropriate controlling strategies need to be formulated. On the other hand, allocating inadequate budget for security concerns requires to be paid less attention compared to other risks. Consequently, it would not be accurate to attribute the inefficacy of private banks' information security to the inadequate budget allocated. The present study helps soon-to-be-established private banks in identifying relevant risks before setting up their system and managing potential risks based on prioritization in order to guarantee the main factors of

information security in data confidentiality, integration, and accessibility. The incorporation of bank expert opinions in addition to the reviewed literature made this study even more practical.

References

[1] Dodge, C. R., Carver, C., & Ferguson, J. A. (2007). Phishing for user security awareness. Computer & Science, 26(1), 73.

[2] Maiwald , E. (2004): Computer Network Security. Translated by Ahmad Safaee, first edition. Tehran: Danesh Parvar Publications.

[3] Niekerk, J.F. & Solms, R. (2010). Information security culture: A management perspective . Computers & security, 29(4): 476-486.

[4] Ozkan, S. & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. International Journal of Information Management, 30: 567-572.

[5] Almunawar Mohammad Nabil,Susanto Heru,Tuan Yong Chee,"Information Security Management System Standards : A Comparative Study the Big Five ,"International Journal of Electrical & Computer Sciences IJECS-IJENS,2011 ,Vol.11,PP.23-27.

[6] Talabis Mark Rayan,Martin Jason,"Information Security Rick Assessment Toolkit,"1at ed.:Syngress,2013.

[7] Shameli-Sendi Alireza,Jabbarifar Masoume,Shajari Mehdi and Dagenais Michel,"FEMRA: Fuzzy Expery Model for Risk Assessment,"The Fifth International Conference on Internet Monitoring and Protection,2010.

[8] Jafarnejad, A. & yousefizenouz, R. (2008). The risk Ranking fuzzy Model in the drilling project of Petropars. Journal of Industrial Management of Tehran University, 1(1): 21-38. (in Persian)

[9] Madaholhosseini,M & Rasoulian,M."Information Security Mnagement System",2nd ed:Naghoos,2012. (in Persian)

[10] Lo, Ch. & Chen, W. (2012). Hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications, 39: 247-257.

[11] Malekalkalami, M. (2013). Evaluating the performance of information security management at the central libraries of public universities in Tehran, according to the international standard-ISO / IEC. Journal of Information Processing and Management, 28 (4): 895-916. (in Persian)

[12].Standard Institute and Industrial Research of Iran. (2008). IT- security technologies and information security management procedures. (in Persian).

[13] Mireskandari, M. (2010). Information Security Management System and the necessity of its use in organizations. Processor magazine. 11(107): 30-39. (in Persian)

[14] Saaty, T. L. 1989. Group decision making and the AHP. New York: Springer

[15]Zhiwei Yu,Zhongyuan Ji,"A Survey on the Evolution of Risk Evaluation for Information System Security ,"International Conference on Future Electrical Power and Energy System,2012,vol.17,pp.1288-1294.

[16]Yanling Shang,Honghui Niu,"Research on risk assessment model of information Security based on particle swarm algorithm-RBF neural network,"Second Pacific – Asia Conference on Circuits,Communications and System(PACCS),2010.

[17] Ekelhart Andreas,Fenz Stefan,Neubauer Thomas,"AURUM:A Framework for Information Security Risk Management,"42nd Hawaii International Conference on System Science-2009,2009.

[18] Bojanc Rok,Jerman-Blazic Borka,"An Economic Modeling Approach to Information Security Risk Management ,"International Journal of Information Management ,2008,vol.28,no.5,pp.413-422.

[19] Hung Chia-Chang,Chen Liang-Hsuan,"A Fuzzy TOPSIS Decision Making Model with Entropy Weight under Intuitionistic Fuzzy Environment,in International Multi Conference of Engineers and Computer scientists (IMECS),Hong Kong,2009,vol,1.

[20] Smojver Slave,"Selection of Information security Risk Management Method Using Analytic Hierarchy Process(AHP),"in 22nd Central European Conference on Information and Intelligence Systems,september 2011.

[21] Wang Zhihu,Zeng Haiwen,"Study on the Risk Assessment Quantitative Method of Information Security,"3rd International Conference on Advanced Computer Theory and Ingineering (ICACTE),2010,pp.V6-529-V6-533.

[22] Feng, N., Jiannan Wang, H. & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences, 256(2014): 57-73.

[23] Yu-Ping Ou Yang,How-Ming Shieh,Gwo-Hshiuung Tzeng,"A VIKOR technique based on DEMATEL and ANP for information security risk control assessment,"information Science Journal,2013,vol.232,pp.482-500.

[24] H. Khajouyi, "Research on Information Security Governance based on International Standards", M.S.thesis, Information Technology Management, Sistan Balouchestan, Sistan Balouchestan , Iran, 2011 .(in Persian).

[25] Iesavi, H. (2011). Evaluation of operational risks related to information security in the modern banking system. Master Thesis, Gilan, Iran. (in Persian).
[26] Biglarian, P. (2012). Compilation of information security evaluation criteria's (Case Study: Exchange Organization of Tehran). Master Thesis, Azahra, Iran. (in Persian)
[27] Avalincharsooghi, S. Doostari, M. Yazdianvarjani, A. & Mahdaviardestani, A. (2013). Use of artificial neural networks in the information security risk assessment. Journal of Electronic & Cyber Defense, 1(1): 1-14. (in Persian)