I J A B E R, Vol. 14, No. 2 (2016): 951-960

WEB-BASED ANALYTIC HIERARCHY PROCESS(AHP) ASSESSMENT MODEL FOR INFORMATION SECURITY POLICY OF COMMERCIAL BANKS

Shiann Ming Wu[1], Dongqiang Guo[1], Wen Tsann Lin[2], and Meng-Hua Li[3]

Abstract: *This study proposed a Web-based AHP risk assessment model according to the characteristics of mutual dependence among the assessment indices of the information security policy of commercial banks. To maintain information security of commercial banks, this study included the 14 fields of ISO27001:2013 into the 5 parts of the organizational information security architecture(Tudor, 2001), and used an expert questionnaire and Web-based AHP to perform a pairwise comparison on the various factors, under the condition where correlation among factors was taken into account in order to perform consistency test, obtain the overall weight and weights of various factors, verify the information security risks of commercial banks, and reflect the reliability of the assessment results of this model.*

Keywords: *Commercial Bank; Information Security; AHP; ISO27001*

1. INTRODUCTION

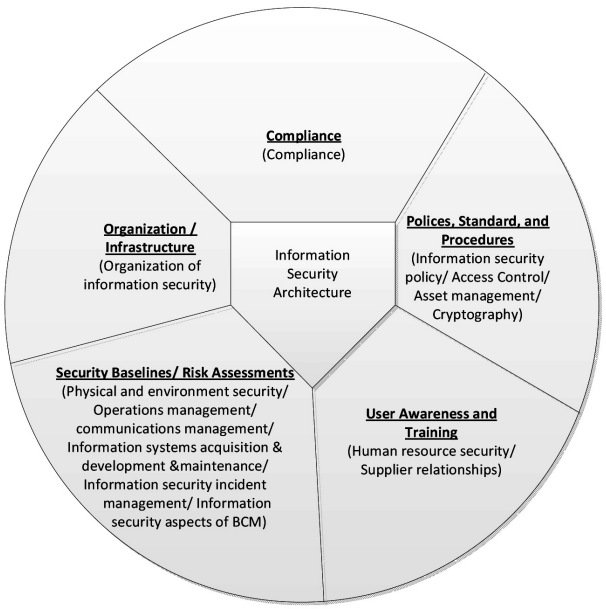
Information security expert Bruce Schneier said "Complexity is the enemy of security". For various enterprise applications, such as e-commerce, ERP, CRM, and flourishing Cloud Computing and Big Data, the network architecture, operating system, applications, database management system, and data processing are increasingly complex. ISO27001/ISMS is the international standard most universally used by Taiwan's commercial banks to promote their information security management system. In the PDCA (Plan-Do-Check-Act) cycle architecture, the risk evaluation method is determined, and the information security system and management system are built, in order to meet the goals of commercial bank organizations. ISO/IEC 27001:2013 has three aims, (1) to meet ISO Annex SL requirements for integration with other management systems; (2) to cite ISO 31000 risk management requirements to evaluate potential unknown risks; (3) to set goals, monitoring performance, and the measurement index,

1. College of Business Administration, National Huaqiao University, Fujian, China.
2. Department of Industrial Engineering & Management, NCUT, Taichung, Taiwan.
3. Department of Industrial Management, National Formosa University,Yunlin, Taiwan.

which emphasizes performance: the information security goal shall be consistent with the information security policy, shall be quantifiable and measurable, and the implementation results of risk evaluation and risk handling plans shall be considered, if necessary.

Tudor (2006) divided the organizational information security architecture into five frameworks. This study puts 14 domains of ISO27001:2013 in the five frameworks of the TUDOR (2006) organizational information security architecture according to the characteristics, and uses the AHP analysis method to validate the enforcement of commercial bank information security principles on the thinking principle of NIST SP800-30 for information security risk management. (see Figure 1), (1)**Compliance** (Compliance), (2)**Organization / Infrastructure** (Organization of information security), (3)**Security Baselines/ Risk Assessments**(Physical and environment security/ Operations management/ communications management/ Information systems acquisition & development &maintenance/ Information security incident management/ Information security aspects of BCM), (4) **User Awareness and Training** (Human resource security/ Supplier relationships), (5) **Polices, Standard, and Procedures** (Information security policy/ Access Control/ Asset management/ Cryptography).

Figure 1: Information Security architecture Components



Source: This study.

According to practical observations and literature review, the organizations of different industries have different information security requirements, as well as different opinions and practices for establishing information security principles (King, 1994). In terms of the information security of commercial banks, the competent authorities of various countries have increasingly strict requirements, e.g. the requirement of U.S. FFIEC (2015) for domestic bank information security about cyber security. This study analyzes 14 domains of ISO27001:2013, and lists 14 key factors that enhance information security. The information security policy is the top reference and guideline for organizational information security and the infrastructure of information security.

2. LITERATURE REVIEW

While the information security problem is multilayered and diversified, it can be reduced to Security=Information+Technology+People, (Hinde, 2001). The general objective of information security must protect the Confidentiality, Integrity, and Availability of data, i.e. the so-called CIA, (Smith, 1989; ISO/IEC17799, 2000; Dhillon & Backhouse, 2000; Anderson, 2003). According to Von Solms et al. (1994), the category of information security covers the information security policy, risk analysis, risk management, contingency planning, and disaster recovery. Information security is to protect all affairs related to computers, and to use a supervisory program and security technology in hardware, software, and data (Huang, 1992; Rusell & Gangemi, 1992). For an organization, information is a valuable commercial asset, and it shall be properly protected against various threats, in order to maintain the constancy of organizational operations, and minimize probable loss (ISO/IEC 17799, 2000). The factors in information security include secure and reliable electronic data transmission, providing an effective information security protection system, providing authenticated and confidential efficient methods to ensure all users are authorized, and knowing how to protect the information system and data users (Wu, 1999). This strategy is a comprehensive policy and plan that can be adopted to attain organizational objectives (Griffin). While the policy tells the manager how to make decisions in certain cases, the content is sometimes abstract and sometimes quite specific, thus, there is always a need for decision makers. For example, "the applicants must be examined in the open"; however, how and when the examination is implemented, and how open the examination is, are not specified. The policy and strategy are sometimes difficult to be distinguished, as many policies are a sort of strategy. For example, "a distributor with advanced image is preferred", is a policy, as well as a strategy (Hsu, Shih-Chun). In terms of creating an information security strategy, many scholars have proposed many methods to systematically assist organizations to establish feasible information security policies (Siponen, 2002; Eloff & von

Solms, 2000). NII (Taiwan) validates guidance services for ISO 27001 enterprises from the angle of enterprise or organizational operations, assists business organizations to build a management system that meets international standards, and establishes customized information security principles to meet the demands of business organizations in Business, Legal, Risk Management, and Cost Effective dimensions. The factors influencing an organizational information strategy are derived from four parts of the organizational information environment; the existing information resources of the organization, organization characteristics, rising science and technology, and organizational industry status (Smits, 1999). Tryfonas et al. (2001) indicated that organizational information security actions are different from the organization level, meaning that information security management activities are identical to the levels of management planning and control activities within the organization. Ezingeard and Birchall (2002) found that competitive advantage is the first factor impelling an enterprise to actively adopt information security standards, and suggested an important drive factor for international standards that implement the optimal model of information security management, in order to promote communication between external and internal stakeholders. The regulatory requirements, the push of information security groups, government, and trade organizations are not significant drive factors, as they are different from general cognition. Tseng (2002) found that Taiwan's banks and foreign banks pay the closest attention to three key points of information security; "access control", "entity and environmental security", and "system development and maintenance", and the application of "secure organization", "follow up", and "security policy" shall be enhanced. Li (2008) found that, the all-out support and participation of senior executives, who are specifically responsible for information security management units, as well as experienced consultants, who provide imported empirical rules, are important in all phases, while other factors are key success factors only in select phases. In addition, the study showed that the technical factors of perfect information security equipment and information security personnel with information security expertise are not the key factors imported into an information security management system.

3. METHODOLOGY

The organization shall build and maintain a documental information security management system, which shall emphasize the information assets to be protected, and adopt a risk management method, control objectives, control methods, and the required guarantee procedures, in order to promote the organization to attain the goal of information security. ISO27001:2013 specifies the goals of information security in 14 domains, which are divided into six major steps: define policy, define

range, risk assessment, risk management, select the control objectives and control methods to be implemented, and prepare a statement of applicability.

This study uses a questionnaire to construct a multicriterion evaluation model for information security as the tool for assessing organizational information security. To construct this model, the hierarchical structure of the evaluation criteria must be built first, and then the Analytic Hierarchy Process is used, where the weights of evaluation criteria are determined by pairwise comparison. The evaluation model is built according to theoretical basis, and the steps are briefly described, as follows:

1. Build hierarchical structure relationships for evaluating key factors, if there are n experts for evaluation criteria, there are n schemes of the hierarchical structure for decision analysis;
2. Build a pairwise comparison matrix, where each respondent uses linguistic variables to express the relatively important evaluation values for two schemes; data matrix:

$$A=[a_{ij}]=\begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_n \end{array}\begin{array}{c} \begin{array}{cccc} A_1 & A_2 & \cdots & A_n \end{array} \\ \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 1/a_{12} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & 1 & \vdots \\ 1/a_{1n} & \vdots & \vdots & 1 \end{bmatrix} \end{array} \qquad a_{ii}=1,\ a_{ji}=1/a_{ij};\ I,j=1,2,\ldots,n \circ$$

3. Calculate eigenvalue, Formula of Consistency Vector:

$$V_i = \frac{\sum_{j=1}^{n} W_j a_{ij}}{W_i} \quad I,j = 1,2,\ldots,n$$

So we will be able to obtain the eigenvalues. If it is consistent matrix, feature vector X is obtained by the following formula.

$$\lambda = \frac{\sum_{i=1}^{n} V_i}{n} \quad i=1,2,\ldots,n$$

4. Consistency testing of the consistency index (C.I.) and consistency ratio (C.R.) are determined, where the information is filtered to ensure the results reflect the actual conditions. Consistency refers to whether the decision

maker's judgment in the evaluation process is reasonable. The definition of consistency index formula is as follows:

$$C.\ I. = \frac{\lambda - n}{n - 1},\ C.\ R. = \frac{\text{C.I.}}{R.\ 1.}, \text{ R.I.(Random index)}$$

If C.I. = 0, the judgment is completely consistent; C.I.>0.1 means the judgment is inconsistent. Saaty (1980) recommended C.I.<=0.1 as the acceptable error range. C.R.<=0.1 means consistency is satisfactory; C.R.>0.1 means consistency is unsatisfactory.

Table 1
Random indexes

Hierarchy	1	2	3	4	5	6	7	8	9	10	11
R.I.	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49	1.51

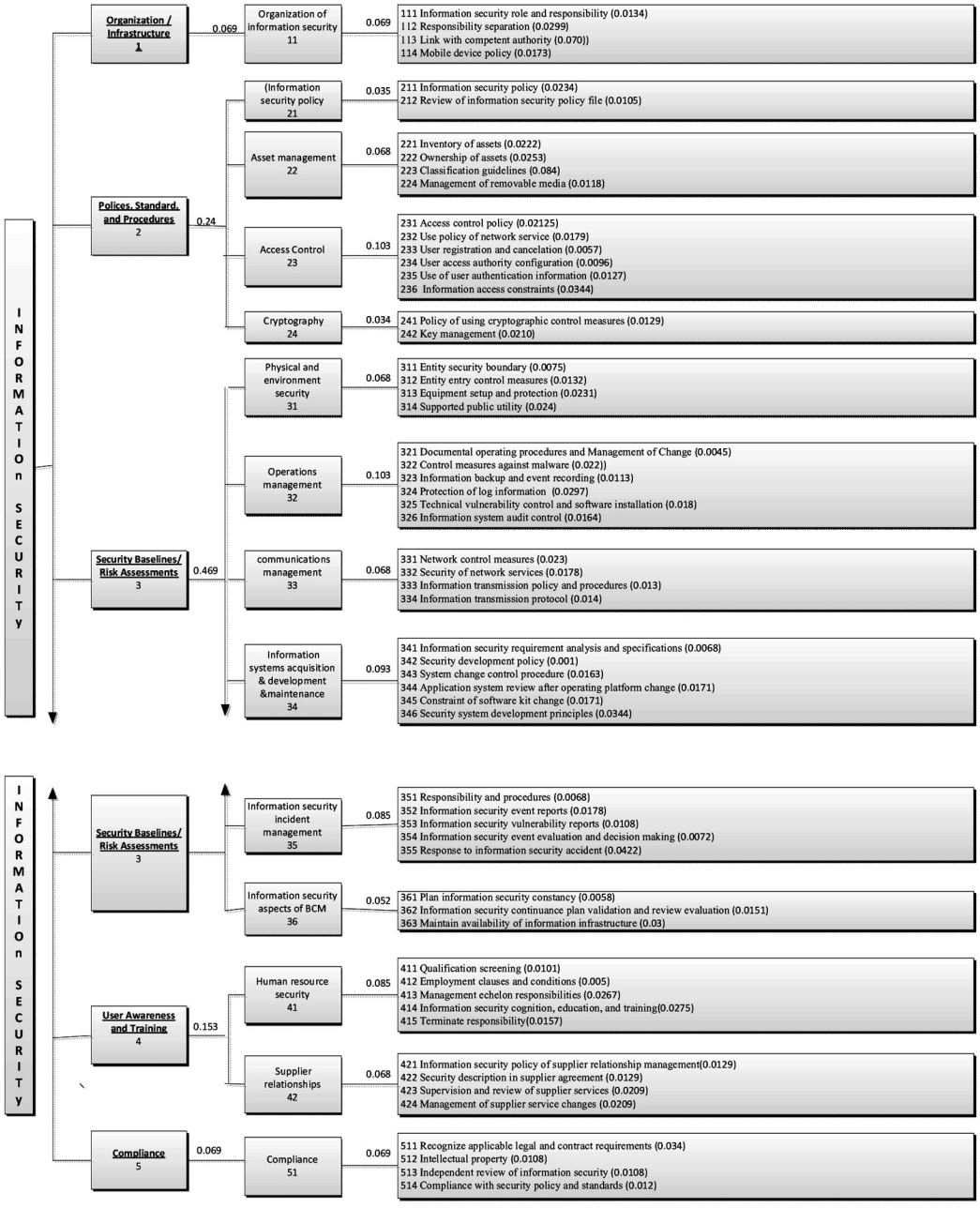
Source: Saaty(1980)

4. RESULTS

The levels of evaluation criteria of the evaluation model for information security can be divided into three levels and four sub-levels (Hong, 2003). The evaluation criteria used in this study have four levels. After literature the review and integration of ISO27001:2013 commercial bank information security review items (163 items), this study imports 5 major criteria (aspects), 14 sub-criteria (aspects) and 59 influencing factors that influence bank information security. After the expert questionnaire, pairwise comparison of importance, feature vectors (value), and consistency testing, the consistency ratio (C.R.) is analyzed by referring to Table 1 (random indices), in order to calculate the overall weight. The weight sum of all criteria is 1, the weight sum of various elements is 1, and the overall weight sum is 1. The analysis results are shown, as follows:

Generally speaking, most respondents have positive opinions regarding the import of ISO27001/ISMS, and affirm that the system helps to enhance the organizational information security to some extent. The organizational members must pay close attention regarding how to enhance information security competency and response capability in training, in order to reduce the risk occurrence rate and enhance the cognition of information security. Employee training and information security policy advocacy can be enhanced by importing ISO27001/ISMS into banking organizations, as there is a certain effect on the information security maintenance of banking organizations.

Figure 2: Information Security Evaluation Model (Four Classes)



5. DISCUSSION & CONCLUSION

Information security risk management is a continuous management process, including risk definition, recognition, analysis, evaluation, and processing strategy, which aims to conform to cost benefits, reduce risk probability, and minimize loss, while meeting the operating objectives and tasks. A good and continuous risk management system will be key to the success of the information security management of business organizations. Due to the rapid development of information technology, the era of all-encompassing information security has arrived, and the aspects of management, procedures, and technology must be highly considered, including the in-depth defense of anterior, middle, and posterior levels of the time axis of the technology aspect, network security, system security, website security, and data security can be used as information security measures. Management and procedure aspects can be enhanced by the ISO 27001 information security management system, and when assisted by information security training and information security check-up examinations, it can perfect information security.

This study focuses on the information security strategy through the application of information technology, the implementation of information security, and management of information security, as based on the information security of commercial banks, which are concluded, as follows: hypothesis (H21): efficient organization and infrastructure can influence the enhancement of information security. Hypothesis (H22): a consistent policy, with standard and program control, can influence the enhancement of information security. Hypothesis (H23): making information security references and appropriate information operating risk evaluations can help to enhance information security. Hypothesis (H24): organizational employees and related contractors shall receive appropriate cognitive education and training, and periodically update organizational policies and procedures related to their work, which is helpful to enhance information security. Hypothesis (H25): all related statutory, legal, and contract requirements, as well as the organization's practice for meeting the requirements, shall be recognized, documented, and updated, and periodically check to determine whether the organizational information security policy and standards are complied with, can influence information security.

This study uses the Analytic Hierarchy Process to discuss the information security architecture of Tudor, where the preliminarily known key factors influencing the bank are resulted from importing ISO27001:2013. However, there are still deficiencies, and the limitations of this study are, as follows: (1) information security personnel are the minority in an organization, thus, what ratio is adequate to maintain sufficient information security of an organization?

(2) as limited by resources, units other than banking organizations have not been investigated. Hence, future research may consider research different industry levels and research ISO27001/ISMS effects evaluation and differences.

References

1. Alexandre veronese Bentes, et al. (2012), Multidimensional assessment of organizational performance: Integrating BSC and AHP, *Journal of Business Research* 65(2012) 1790-1799.
2. Awni Itradat, et al. (2014), Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study, *Jordan Journal of Mechanical and Industrial Engineering*, Volume 8 Number 2, April 2014.
3. Candiwan, (2014), Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia, Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security, Kuala Lumpur, Malaysia, 2014.
4. Dorado et al. (2014), An AHP application to select software for engineering education, *Computer Educations in Engineering Education*, Vol. 22, No. 2, pp. 200-208.
5. Fang, R.W. (2006), "A Study on the Certification of Information Security Management Systems", Doctoral Dissertation, National Chiao Tung University.
6. G. H. Gao, et al. (2011), "Information security risk assessment based on information measure and fuzzy clustering," *Journal of Software*, vol. 6, no. 11, pp. 2159-2166, 2011.
7. Global Technology Audit Guide GTAG. The Institute of Internal Auditors, ROC.2011.06
8. Hong, et al., Discussion about Information Security Management Theory. *MIS Review*: 12, 2003(6):17-47.
9. Huang, G.M. Analysis of Deep Development Strategy for Bank Information Security [J]. *Agricultural Development and Finence*, 2006, (1).
10. IT- Enabled Services Management Association (2013), *Government Agency Information Service Management (ITSM) Reference Guide*.
11. Li, P.C., Discussion about IT Control Architecture COBIT. Taiwan Stock Exchange, 2009 (09).
12. Li, R.H. (2008) "A Study of Key Success Factor in Importing Information Security Management System into Taiwan Finance Industry—Case Study of A Monetary Control".
13. Research, Development and Evaluation Commission, Executive Yuan, Risk Management Operating Manual Ver 3.0, http://www.rdec.gov.tw/DO/DownloadControllerNDO.asp, access time: 2013/12/31.
14. S. Fu and Y. Xiao,(2011), "An effective process of information security risk assessment," *International Conference on Computer and Automation Engineering*, vol. 3, pp. 124-128, 2011.

15. Tseng, S.H. (2002) "BS 7799-based Evaluation of Information Security Environment of Banking", analysis of current condition of Taiwan's banks and foreign banks in information security.
16. Zeynep Filiz Eren-Dogu and Can Cengiz Celikoglu (2012), Information Aecurity Risk Aaaessment: Bayesian prioritization for AHP group decision making, ICIC International ©2012 ISSN 1349-4198
17. Zne-Jung Lee and Li-Yun Chang,, (2014), Apply Fuzzy Decision Tree to Information Security Risk Assessment, *International Journal of Fuzzy Systems,* Vol. 16, No. 2, June 2014.
18. Z.Yu and Z. Ji. (2011), "A survey on the evolution of risk evaluation for information systems security," *Energy Procedia*, vol. 17, pp. 1288-1294, 2011.