Expert Systems with Applications 39 (2012) 247–257

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

A hybrid information security risk assessment procedure considering interdependences between controls

Chi-Chun Lo, Wan-Jia Chen *

Institute of Information Management, National Chiao-Tung University, 1001 University Road, Hsinchu, Taiwan 300, Taiwan, ROC

ARTICLE INFO

Keywords:
Information security
Risk assessment
Decision Making Trial and Evaluation Laboratory (DEMATEL)
Analytic Network Process (ANP)
Order Weighted Averaging (OWA) operator
Fuzzy linguistic quantifiers
Maximum entropy method

ABSTRACT

Risk assessment is the core process of information security risk management. Organizations use risk assessment to determine the risks within an information system and provide sufficient means to reduce these risks. In this paper, a hybrid procedure for evaluating risk levels of information security under various security controls is proposed. First, this procedure applies the Decision Making Trial and Evaluation Laboratory (DEMATEL) approach to construct interrelations among security control areas. Secondly, likelihood ratings are obtained through the Analytic Network Process (ANP) method; as a result, the proposed procedure can detect the interdependences and feedback between security control families and function in real world situations. Lastly, the Fuzzy Linguistic Quantifiers-guided Maximum Entropy Order-Weighted averaging (FLQ-MEOWA) operator is used to aggregate impact values assessed by experts, applied to diminish the influence of extreme evaluations such as personal views and drastic perspectives. A real world application in a branch office of the health insurance institute in Taiwan was examined to verify the proposed procedure. By analyzing the acquired data, we confirm the proposed procedure certainly detects the influential factors among security control areas. This procedure also evaluates risk levels more accurately by coping with the interdependencies among security control families and determines the information systems safeguards required for better security, therefore enabling organizations to accomplish their missions.

1. Introduction

In recent years, the issue of information security has become an increasing concern by organizations that have long used information systems to perform their day-to-day operations. According to the surveys conducted by the Computer Security Institute (Richardson, 2007, 2008), the percentage of US enterprises who allocated 3% or more of their IT budget for security increased from 40% in 2006 to 55% in 2008. Evidently, the importance of information security is apparent within organizations.

Due to the fact that application of information technology systems may also create risks, an effective risk management process will result in a successful security program (Blakley, McDermott, & Geer, 2001). Risk management is performed through the process of identifying risks, assessing risks, and taking steps to reduce risks to an acceptable level (Stoneburner, Goguen, & Feringa, 2002). The most important process of information risk management is risk assessment (Peltier, 2005). Risk assessment ascertains the threats associated with assets and prioritizes risks to assets. An effective risk assessment can protect organizations and maintain their abilities to carry out missions and activities against threats as well as helping to implement controls and safeguards that are actually needed.

Methodologies of risk assessment generally fit into two categories: quantitative and qualitative (Peltier, 2005). Difficulties exist in identifying and assigning a value to an information system. In addition, lack of statistical data makes the direct value assignment inaccurate. Therefore, numerous risk assessment methodologies for information systems are built on measurements of qualitative risks. Nevertheless, qualitative risk assessments for risk identification are somewhat subjective. Fuzzy methodology is therefore used to reduce the subjective nature of qualitative risk measurements in research. Although the subjective nature is lowered by the fuzzy method, there is still great difficulty in qualitative risk assessments for defining the likelihood and impact values especially in cases where interrelations exist between security controls. Despite of this, not much research has been done on the interdependent relationships among security controls for information systems.

The purpose of this paper is to develop a hybrid procedure enabling organizations to efficiently evaluate risk levels on information systems. It will help them deal with intertwined relationships between risk controls as well as dealing with evaluations of experts with diverse professional backgrounds and views. The proposed procedure helps analysts find the crucial risk elements even when

* Corresponding author.
E-mail address: cwj@cc.ncue.edu.tw (W.-J. Chen).

0957-4174/$ - see front matter Crown Copyright © 2011 Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2011.07.015

interdependencies among risk elements exist. The seventeen security control families defined in the core of the NIST security management structure (Ross et al., 2007) are employed to formulate the risk evaluation criteria. The evaluation of risk likelihood is associated with these security control families. As the 17 security control families are not completely independent, the Decision Making Trial and Evaluation Laboratory (DEMATEL) approach is used to detect relationships and map relation-structure of the security control areas. Next, the Analytic Network Process (ANP) method, proposed by Saaty (1996), is applied to drive likelihood rating of risks to overcome the problem of dependence and feedback among security control families. Then, to cope with the subjective nature of conclusions made by experts with different occupational standings and professional perspectives, the fuzzy linguistic quantifiers-guided maximum entropy order-weighted averaging (FLQ-MEOWA) operator (Dimitar Filev & Yager, 1995; O'Hagan, 1988; Yager, 1988, 1993; Zadeh, 1983) is used to aggregate impact values of risks associated with each information system. Finally, the risk level of each information system is derived. To examine our hybrid procedure a real world case study on the risk assessment for information systems in a branch office of the health insurance institute in Taiwan was conducted. In this case study, the effective factors of security controls were sorted out and risk levels of information systems were derived to help the task in prioritizing and selecting corrective actions for implementing safeguards.

The rest of this paper is organized as follows: Section 2 discusses the existing research related to risk assessment and relative methods, Section 3 presents the proposed hybrid information security risk assessment method, next, the conduct of a real world case study on the risk assessment for information systems in a branch office of the health insurance institute in Taiwan has is illustrated in Section 4 and conclusions are presented in Section 5.

2. Literature review

2.1. Risk assessment methodologies

Quantitative risk assessment methods, using mathematical and statistical tools, attempt to assign specific numbers to the costs of safeguards and the amount of damage that can take place. These methods require a large amount of preliminary work to collect precise values of all elements, including asset values, threat frequency, safeguard effectiveness, and safeguard costs. The lack of good quality data for estimating probabilities of occurrence or loss expectancies, such as the probability of rare threats, is be a problem when the assessments are performed. In contrast, qualitative risk assessment methods are based on judgment, intuition, and experience. In this case, using assessments to assign the probabilities and risk consequences is more flexible for dealing with different scenarios of risks (Blakley et al., 2001; Karabacak & Sogukpinar, 2005; Peltier, 2005). Therefore, much research and many methodologies performed on the study of risk assessment were based on qualitative methods (Alberts & Dorofee, 2002; C&A Systems Security Limited, 2005; Peltier, 2005; Stolen et al., 2002; United Kingdom Central Computer & Telecommunications Agency, 2001). However, qualitative measures are subjective in nature. The major disadvantage of qualitative methods is its nature in producing subjective results which rely heavily on the quality of the risk assessment team.

Much research has been done on fuzzy methods intended to diminish the subjective nature of qualitative risk assessments (Liu, Dai, Wang, & Ma, 2005; Wang, Chao, Lo, Huang, & Younas, 2007). These fuzzy methods provide the processes to estimate the risk elements, such as the probability of threats and impact resulted losses while under uncertain circumstances with incomplete information. Although the fuzzy-based method will diminish the influence of the subjective nature, the major characteristic in qualitative risk assessment method still exists – biased results based on judgment and professional views of analysts. Especially so, when the risk controls are linked to each other, it is difficult for analysts to clearly gauge the risk elements by intuitive judgment or direct experience. However, few studies have been done on the process of risk assessments providing methods for analysts to find the critical risk factors when security controls are interactive.

2.2. Security controls

Various security controls have been suggested by many international organizations. ISO/IEC 27001 presents a list of control objects and 133 controls (ISO, 2005). The seventeen security control families of the NIST security management structure are listed by Ross et al. (2007). Organizations require properly selected security controls in accordance with their needs. According to Ron Ross et al., there are three general areas of security controls: the Management control area, the Operation control area, and the Technique control area, together with their associated seventeen security control families. Each family contains security controls related to the security functionality of the family. Management controls are the security controls of an information system that focus on the management of risks and information system security. The Management control area has four security control families: risk assessment; planning; system and services acquisition; and certification, accreditation, and security assessments. Operation controls are the security controls for an information system that is primarily implemented and executed by people. There are nine security control families in the Operation control area, including personnel security, physical and environmental protection, contingency planning, configuration management, maintenance, system and information integrity, media protection, incident response, and awareness and training. Technical controls are the security controls of an information system that are primarily implemented and executed by the information system through actions carried out in the hardware, software, or firmware components of the system (FIPS, 2006). Four security control families, identification and authentications, access control, audit and accountability, and system and communications protection, are classified into the Technique control area. Table 1 shows the areas and families in the security control catalog and the associated family identifiers.

Table 1
Security control areas, families, and identifiers (Ross et al., 2007).

Security control areas	ID	Security control families
Management (M)	RA	Risk assessment
	PL	Planning
	SA	System and services acquisition
	CA	Certification, accreditation, and security assessments
Operation (O)	PS	Personnel security
	PE	Physical & environmental protection
	CP	Contingency planning
	CM	Configuration management
	MA	Maintenance
	SI	System and information integrity
	MP	Media protection
	IR	Incident response
	AT	Awareness and training
Technique (T)	IA	Identification and authentications
	AC	Access control
	AU	Audit and accountability
	SC	System & communications protection

2.3. The DEMATEL method

The DEMATEL method is a comprehensive approach for constructing and analyzing a network model involving causal relationships between complex factors (Fontela & Gabus, 1976; Gabus & Fontela, 1972, 1973). This method can analyse relationships between factors and convert these relationships into a comprehensible structure which can demonstrate the cause group and effect group of factors and show the numeral strength of influence (Tsai & Chou, 2009; Tzeng, Chiang, & Li, 2007). It has been successfully applied in many situations such as marketing strategy, control systems, airline safety, reliability evaluation, selection of management systems, e-learning evaluation, and knowledge management strategies (Chiu, Chen, Tzeng, & Shyu, 2006; Hori & Shimizu, 1999; Liou, Tzeng, & Chang, 2007; Seyed-Hosseini, Safaei, & Asgharpour, 2006; Tsai & Chou, 2009; Tzeng et al., 2007; Wu, 2008). Appendix A summarizes the process of the DEMATEL method.

2.4. The ANP method

The analytic hierarchy process (AHP) method (Saaty, 1980) used in multicriteria decision making is restricted to the hierarchical structure. The ANP method, a general form of the AHP method, was proposed by Saaty (1996) to break the limits of the AHP method and to be applied to network structures. The ANP method deals with the interdependences and feedback between criteria or alternatives. The ANP method has been effectively applied in different areas (Karsak, Sozer, & Alptekin, 2003; Lee & Kim, 2000; Lin, Chiu, & Tsai, 2008; Meade & Presley, 2002; Shang, Tjader, & Ding, 2004). In real world situations, the criteria or alternatives to be evaluated are often interdependent. The inner and outer dependences within a cluster and among different clusters can be handled by the ANP method to overcome the limitation in linear hierarchic structures. The network structure of the ANP method reveals the relationship and feedback to capture the complex effects of interplay in human society, especially when risks and uncertainties are involved (Saaty & Saaty, 2003).

Initially, a series of pairwise comparisons are conducted to compare the relative importance, preference, or likelihood between two of the criteria in the entire system with respect to another criterion. Comparisons of likelihood are used to compare the possibility of uncertain events or scenarios, such as in risk analysis (Saaty & Saaty, 2003). The results of a series of pairwise comparisons form a supermatrix. After forming the supermatrix, the weighted supermatrix is derived by transforming all columns sum to unity exactly. Finally, the weighted supermatrix can be raised to limiting powers to calculate the global priority vectors or otherwise referred to as weights (Huang, Tzeng, & Ong, 2005; Wu, 2008). Appendix B summarizes the process of the ANP method.

2.5. The FLQ-MEOWA operator

The FLQ-MEOWA operator is based on the Order-Weighted Averaging (OWA) operator defined by Yager (1988), on fuzzy linguistic quantifier suggested by Herrera, Herrera-Viedma, and Verdegay (1995), Yager (1993) and Zadeh (1983), and on maximum entropy method proposed by O'Hagan (1988, 1990), which is resolved by Filev and Yager (1995). The OWA operator provides a general class of parametric aggregation techniques that include the min, max, and average, for combined information to achieve a final value from the synthesis of preferences from the majority of experts. It has proven useful for modeling many different kinds of aggregation needs where problems exist such as decision making, expert systems, neural networks, fuzzy system and control (Dimitar Filev & Yager, 1995; Filev & Yager, 1998; Herrera, Herrera-Viedma, & Verdegay, 1996; Yager, 1993). A basic question in the definition of the OWA operator is how to obtain the associated weighting vector. Yager (1988, 1993) proposed using linguistic quantifiers to compute the weights of OWA operator. Zadeh (1983) defined the fuzzy linguistic quantifier. Some examples of non-decreasing proportional fuzzy linguistic quantifiers proposed by Herrera et al. (1995). The maximum entropy method OWA (MEOWA) operator suggested by O'Hagan (1988) and their analytic properties were explored by Filev and Yager (1995), is used to optimize the OWA operator. Entropy represents the measurement in amounts of information used in the arguments during an aggregation based on the weighting vector. The purpose of the MEOWA operator is to optimize the OWA operator into having maximal entropy of the OWA weights for a given level of orness degree. Appendix C provides a summary of the process of the FLQ-MEOWA operator.

3. A hybrid information security risk assessment procedure

Effective risk assessments assist in determining appropriate safeguards to meet the needs of the organizations, but in real world risk evaluation scenarios it is difficult for all analysts to work out the complex relationships between security controls. As risk assessments are made by analysts from diverse backgrounds, they will produce subjective assessments based on their specialized standing, duties, and job positions. It is critical to diminish the subjective nature of these assessments with aggregation. Therefore, we propose a hybrid procedure which is based on DEMATEL, ANP and FLQ-MEOWA to assess the security risk levels of information systems.

3.1. Risk assessment criteria

Security controls in information systems can be taken as the criteria for risk assessments. For analysts, it will be too difficult and complicated to conduct assessments with the criteria of entire 133 security controls listed in ISO/IEC 27001. In this paper, working with the data from expert consultations and the core of the NIST security management structure (Ross et al., 2007), we used three security control areas and their corresponding seventeen control families to formulate the risk evaluation criteria. The analysts who conducted the risk assessments derived likelihood ratings for vulnerabilities by threats with respect to three security control areas and seventeen security control families. Meanwhile, analysts also assessed the impacts that could result from a security failure and the possible losses of confidentiality, integrity and availability on information systems, in relation with these seventeen security control families. The risk assessment criteria adapted by the proposed procedure can be replaced with other security criteria depending on varying practice needs of each organization.

3.2. Risk assessment procedure

As shown in Fig. 1, the proposed risk assessment procedure adapts the well known studies, Stoneburner et al. (2002) and Peltier (2005), and is organized into the following six steps: (1) System Characterization, (2) Threat and Vulnerability Identification, (3) Likelihood Assessment, (4) Impact Analysis, (5) Risk Determination and (6) Control Recommendations. In the System Characterization step (1), the boundaries of the information system are defined, the scope of risk assessments is characterized, and the system-related information such as the security controls used for the information systems is identified. This characterization provides analysts who conduct risk assessments a clear understanding of the entire system in regards to evaluating the risks. Threats to information systems and the vulnerabilities that might be exploited by threats associated with existence and effectiveness of the seventeen security control families are identified in the

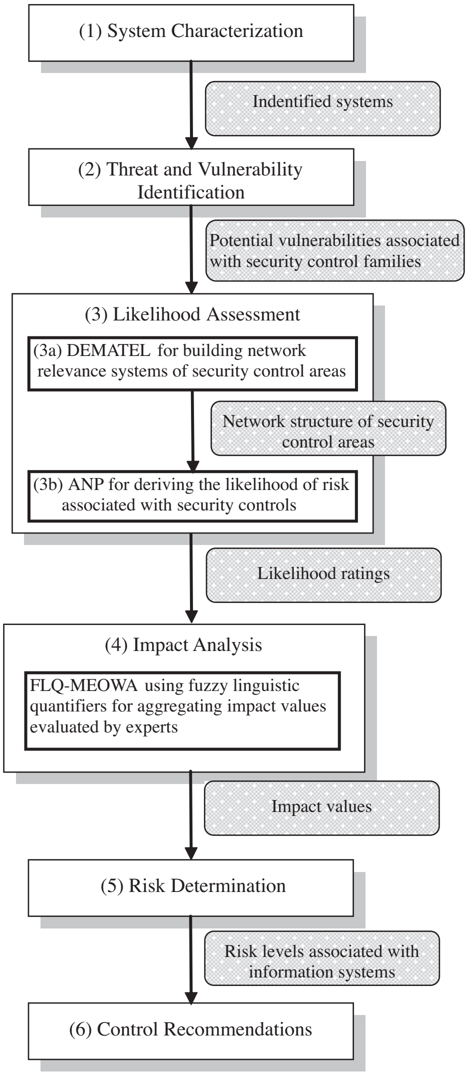
(1) System Characterization
Indentified systems
(2) Threat and Vulnerability Identification
Potential vulnerabilities associated with security control families
(3) Likelihood Assessment
(3a) DEMATEL for building network relevance systems of security control areas
Network structure of security control areas
(3b) ANP for deriving the likelihood of risk associated with security controls
Likelihood ratings
(4) Impact Analysis
FLQ-MEOWA using fuzzy linguistic quantifiers for aggregating impact values evaluated by experts
Impact values
(5) Risk Determination
Risk levels associated with information systems
(6) Control Recommendations

Fig. 1. An overview of the proposed hybrid risk assessment procedure.

Threat and Vulnerability Identification step (2). Although security controls have been implemented, potential threats and vulnerabilities can still exist due to the ineffective and inadequate implementation of these security controls. With respect to the seventeen security control families, the likelihoods of the occurrences of vulnerabilities exploited by threats will be determined in the Likelihood Assessment step (3). The Impact Analysis step (4) is to determine the magnitude of impacts resulting from successful threat exercises of vulnerabilities associated with the security control families. The purpose of Risk Determination step (5) is to assess the synthetic risk levels for each information system. We can rank the information systems by the derived risk levels and identify priorities for safeguard mechanisms. During the Control Recommendations step (6), security controls designed to mitigate the identified risks are recommended based on the ranking derived in step (5). Step (3) and (4) can be conducted reversely or in parallel with each other, as required to align with the practice in an organization. Detail discussions on steps (3a), (3b), (4) and (5) are shown in Sections 3.3, 3.4, 3.5 and 3.6 respectively.

3.3. Building network relevance systems between security control areas using the DEMATEL method

The three security control areas, the Management control area, the Operation control area, and the Technique control area, are not entirely independent. Implementation of one security control may influence the conduct of other security controls in the same or separate control areas. For example, the technology safeguards applied to the System and Communications Protection control in the Technique control area will affect the Awareness and Training of organization personnel control in the Operation control area in carrying out their assigned information security-related duties such as, to efficiently apply the encryption mechanism for important emails and attachment files and ensuring adequate training for individuals to apply these measures. For another example, the periodical conduct of the Risk Assessment control will affect the updating of security plans which is the mission of the Planning control. In this case, both of these security control families belong in the same security control area, the Management control area. This study applies the DEMATEL method to construct a network relevance structure in security control areas for detecting the potential interrelation between security control families. In the end, the relationships of a network structure and the degree of interdependences are determined. Subsequently, the ANP method is employed to obtain the likelihood ratings associated with these security control families.

3.4. Deriving the likelihood of risk associated with security control families using the ANP method

As security control areas are connected as a network and not a hierarchy structure, instead of the AHP method, the ANP method is applied to manage these interdependent relationships. First, a series of pairwise comparisons are conducted to compare the risk likelihoods between each two security control families with respect to another security control family. Pairwise studies are carried out by asking “With respect to one security control family, how likely will one other security control family lead to risks compared against another security control family?” For example, “With respect to the System and Services Acquisition control family how likely will the Personnel Security control family lead to risks compared against the Physical and Environmental Protection control family?”. The results from a series of pairwise comparisons form a supermatrix. Next, a weighted supermatrix is derived by transforming all column sums to unity exactly. Lastly, the weighted supermatrix can be raised to limiting powers in Eq. (B1) for calculating the likelihoods. The likelihood ratings for vector of occurrence in vulnerabilities exploited by threats associated with each security control families are thus determined for assessing the security risks.

3.5. Aggregating impact values using the FLQ-MEOWA operator

To eliminate the subjective nature of evaluations by different experts on the impact of risks, the FLQ-MEOWA (Dimitar Filev & Yager, 1995; O’Hagan, 1988; Yager, 1988, 1993; Zadeh, 1983) operator is used to aggregate impact values. With respect to seventeen security control families, the impacts from the occurrence of vulnerabilities associated with information systems are evaluated by experts. Experts who conduct the assessments may come from different professional backgrounds such as: technical, financial, engineering and management, with their own individual perceptions, attitudes, and motivations in determining the influence of risks. Since impact values of risks are endowed by the subjective cognition of each individual, the aggregation of the values is not suitable simply by directly taking classical averaging or constant weighted operators to derive a final impact value. Due to this reason, aggregating the risk impacts using the fuzzy linguistic quantifier is more realistic than using crisp weighted values.

Fuzzy linguistic quantifiers act as a medium for aggregating impact values diagnosed by different experts. To reduce the influence of extreme risk diagnosis and other relatively weak ones, we chose the linguistic quantifier "most" to emphasize the medium influence on the aggregated impact values (Herrera et al., 1995). Depending on the different risk management objectives and security requirements, appropriate linguistic quantifiers can be applied by organizations. Using the FLQ-MEOWA operator we can aggregate the impact values of risks submitted by different experts and cope with the subjective assessments to decrease the influence of extreme values.

3.6. Risk determination

As a result of deriving the likelihood of vulnerability occurrences associated with security control families and subsequently aggregating impact values of risks, risk levels for each information system can be obtained. If there are inadequate historical records or statistical analysis data, it will be better to find the risk level instead of determining the value of risk. The determination of risk levels can be expressed as a function of the vulnerability occurrence potential multiplied by the magnitude of the impact resulting from a successful threat exploitation (Peltier, 2005; Stoneburner et al., 2002). Hence, in this paper the risk levels formulate is defined in formula (1).

$$R_i = \sum_{j=1}^{n} l_j v_{ij} \tag{1}$$

where R_i denotes risk level of the ith information system, j denotes the jth security control family, l_j denotes the likelihood of occurrence in vulnerabilities of the jth security control family caused by threats, and v_{ij} denotes the impact value on information system i when vulnerabilities of the security control family j is exploited by threats. After evaluations on the risk levels of information systems, the results can be used for improving information security management processes, controls and safeguards to reduce the risks in the system.

4. Risk assessment of information systems in a branch office of the health insurance institute in Taiwan

In this section, risk assessment based on the proposed procedure is conducted on information systems of a branch office of the health insurance institute in Taiwan. Since overall operations of this office solely depend on information systems, information security management is crucial to the organization's business. This branch office has been required to implement Information Security Management System (ISMS) and acquire ISO27001 certificate. Risk assessment therefore is a critical process for them to determine risks associated within their existing information systems. The results of risk assessment can help to identify appropriate measures in reducing risks and to improve the information security of the branch office.

As for the selection of evaluators, both objectivity and correctness of risk evaluation need to be considered; thus, only those who have professional experience on administering management information system (MIS) and ISMS were selected. Three senior chiefs of the information center and two senior managers of two outer assessment and certification service providers had been selected for constructing the assessment. All experts had an average of 10.4 years with broad experiences in information system management and information security.

After discussions with the experts, five information systems – enrollment system of health insurance (ES), reimbursement and payment system of medical expenditure (RPS), the web site of the branch office (WEB), web-based workflow automation system (WFS), and issuance system of health insurance certificate (HICS) – were selected. ES provides the enrollment and withdrawal services to enroll qualified applicants and handles payments of premiums. RPS of medical expenditure processes the payments of expenses for medical services, claimed by designated hospitals, clinics, pharmacies and other organizations. WEB provides information and entrances for ordinary persons or insured organizations to access related insurance services of this branch office. WFS provides tools for individuals and groups in the branch office to execute business tasks which benefit from efficiency savings in avoiding duplicated work and reduced errors. HICS is referred to as the issuance system of the health insurance IC cards, it deals with the application, issuance, reissuance, and renewal procedures of the health insurance IC cards.

4.1. Constructing network relevance and structure of security control areas

The selected experts were consulted with a questionnaire to rank the security control areas using a 5-point scale ranking from 4 (extremely important) to 0 (no effect) (Chiu et al., 2006). These experts were asked to assess the importance of relationships between each pair of the three areas. First, the initial direct-relation 3 × 3 matrix was derived from pairwise comparisons in terms of influences and directions between security control families and is shown in Table 2. Secondly, on the basis of the direct-relation matrix, normalized direct-relation matrix could be obtained by formula (A1) and (A2), in which all principal diagonal elements are equaled to zero (Liu et al., 2005; O'Hagan, 1988). After the normalized direct-relation matrix was obtained, the total-relation matrix could be derived by using formula (A3). Table 3 shows the total-relation matrix. Next, a threshold value of 1.1 was chosen in consultation and discussion with the experts. The relationships with value less than 1.1 were not obvious and the value 1.1 was the most appropriate value to be used for acquiring a suitable relationship. Based on the threshold value and using formulas (A4)–(A6). the impact-relations-map is acquired by mapping a dataset of $(D+R, D-R)$ as shown in Fig. 2.

4.2. Deriving the likelihood of risks associated with security control families

After determining the relationship structure and producing the impact-relation-map, the ANP method is applied to derive the likelihood of threats to exercise potential vulnerabilities associated with security control families. The resolving process for likelihood is similar to the process in deciding the weights of evaluation criteria. First of all, the importance of relationships between each pair of security control families is compared. The experts were asked to respond to a series of questions such as: "With respect to the Risk assessment control family how likely will the Personnel Security family lead to risks compared against the Physical and Environmental Protection control family?" These pairwise comparisons are based on Saaty's 9-point scale which uses a score of 1 to indicate equal importance and 9 to indicate the extreme importance of one element over the other (Liou et al., 2007). Next, as the local weights of these criteria are obtained through the principal eigenvector of comparisons and the consistency ratio (CR) values appear acceptable, an unweighted supermatrix is generated as shown in

Table 2
The initial direction-relation matrix.

	Management	Operation	Technique
Management	0.0	4.0	3.8
Operation	2.8	0.0	2.2
Technique	3.0	3.0	0.0

Table 3
The total-relation matrix.

	Management	Operation	Technique	D	D + R	D − R
Management	**1.245**	**1.763**	**1.591**	4.599	12.246	0.861
Operation	**1.177**	1.046	**1.151**	3.374	7.648	−0.901
Technique	**1.316**	**1.465**	1.054	3.835	7.631	0.040
R	3.738	4.274	3.796			

Bolded numbers represent values that have reached the threshold of 1.1 for acquiring suitable relationship.

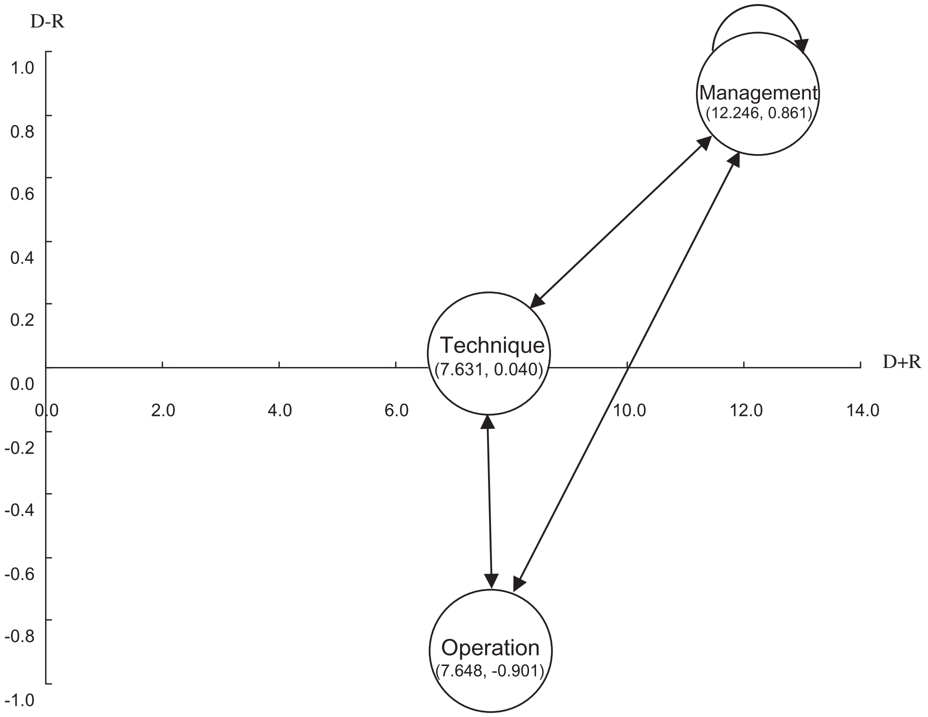

Fig. 2. The impact-relations-map of security control areas.

Table 4
The unweighted supermatrix.

	RA	PL	SA	CA	PS	PE	CP	CM	MA	SI	MP	IR	AT	IA	AC	AU	SC
RA	0.270	0.230	0.270	0.270	0.232	0.290	0.264	0.242	0.238	0.250	0.260	0.282	0.250	0.270	0.242	0.252	0.240
PL	0.200	0.260	0.190	0.190	0.190	0.220	0.272	0.190	0.202	0.222	0.220	0.252	0.212	0.200	0.198	0.198	0.190
SA	0.260	0.270	0.300	0.280	0.296	0.272	0.236	0.288	0.318	0.228	0.252	0.228	0.258	0.260	0.278	0.268	0.280
CA	0.270	0.240	0.240	0.260	0.282	0.218	0.228	0.280	0.242	0.300	0.268	0.238	0.280	0.270	0.282	0.282	0.290
PS	0.160	0.164	0.116	0.121	0	0	0	0	0	0	0	0	0	0.162	0.162	0.200	0.159
PE	0.102	0.090	0.146	0.109	0	0	0	0	0	0	0	0	0	0.136	0.132	0.126	0.129
CP	0.088	0.130	0.088	0.103	0	0	0	0	0	0	0	0	0	0.098	0.098	0.106	0.108
CM	0.120	0.110	0.120	0.140	0	0	0	0	0	0	0	0	0	0.136	0.126	0.102	0.119
MA	0.124	0.116	0.130	0.117	0	0	0	0	0	0	0	0	0	0.094	0.094	0.092	0.096
SI	0.076	0.080	0.098	0.123	0	0	0	0	0	0	0	0	0	0.100	0.090	0.084	0.096
MP	0.098	0.082	0.090	0.093	0	0	0	0	0	0	0	0	0	0.086	0.110	0.098	0.094
IR	0.120	0.124	0.108	0.097	0	0	0	0	0	0	0	0	0	0.098	0.098	0.090	0.094
AT	0.110	0.102	0.102	0.095	0	0	0	0	0	0	0	0	0	0.088	0.088	0.100	0.104
IA	0.272	0.280	0.278	0.280	0.282	0.222	0.232	0.292	0.244	0.250	0.212	0.200	0.220	0	0	0	0
AC	0.284	0.280	0.252	0.240	0.292	0.298	0.208	0.252	0.238	0.290	0.240	0.270	0.280	0	0	0	0
AU	0.202	0.210	0.200	0.210	0.212	0.222	0.288	0.208	0.248	0.240	0.268	0.258	0.250	0	0	0	0
SC	0.242	0.230	0.270	0.270	0.214	0.258	0.272	0.248	0.270	0.220	0.280	0.272	0.250	0	0	0	0

Table 4. Then, after forming the unweighted supermatrix, the weighted supermatrix is generated by transforming all column sums to unity exactly. Finally, by calculating the limiting powers of the weighted supermatrix, a steady-state condition is reached. Consequently, the limited supermatrix is derived as shown in Table 5 and each row represents the weights of the criterion. In this study, the weight vectors are the likelihood ratings of risk occurrence associated with security control families.

4.3. Impact analysis

In this phase, it is required to establish a set of linguistic terms for evaluating impacts. Through discussion with these senior experts, different degrees of "impact" are expressed with five linguistic terms: Very high impact, High impact, Medium impact, Low impact and Very low impact, and their corresponding linguistic values are 1.0, 0.75, 0.5, 0.25 and 0. The five senior experts generated impact

Table 5
The limited supermatrix.

	RA	PL	SA	CA	PS	PE	CP	CM	MA	SI	MP	IR	AT	IA	AC	AU	SC
RA	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101	0.101
PL	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082	0.082
SA	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107	0.107
CA	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105	0.105
PS	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051	0.051
PE	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041
CP	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035	0.035
CM	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042	0.042
MA	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038	0.038
SI	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032
MP	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032
IR	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036	0.036
AT	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034	0.034
IA	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067
AC	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070	0.070
AU	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060	0.060
SC	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067	0.067

values for each information system with respect to successful threats to exploit vulnerabilities in each control family. Subsequently, these impact values are aggregated by the FLQ-MEOWA operator described in Appendix C.

First, to diminish the influence of extreme evaluations from risk impact assessed by experts with varying personal views and perspectives, the fuzzy linguistic quantifier "most" was chosen to emphasize medium influence for aggregated impact values. After the computing process of the OWA operator with fuzzy linguistic quantifier "most" involving five experts, the initial weights, w_1, w_2, w_3, w_4 and w_5 were gained as 0, 0.2, 0.4, 0.4 and 0 respectively.

Next, the computing process for optimizing the aggregation operator is shown below and the new weights $w_1^*,\ w_2^*,\ w_3^*,\ w_4^*$ and w_5^* are derived as 0.1619, 0.1791, 0.1980, 0.2189 and 0.2421 respectively.

$$\begin{aligned} orness(W) &= \frac{1}{5-1}\sum_{j=1}^{5}(5-j)w_j = \frac{1}{4}(4w_1 + 3w_2 + 2w_3 + w_4) \\ &= 0.45 \sum_{j=1}^{5}\left(\frac{5-j}{5-1} - orness(W)\right)h^{5-j} = (1-0.45)h^4 \\ &\quad + \left(\frac{3}{4} - 0.45\right)h^3 + \left(\frac{2}{4} - 0.45\right)h^2 + \left(\frac{1}{4} - 0.45\right)h \\ &\quad - 0.45 = 0h = 0.9044\ w_j^* = \frac{h^{5-j}}{\sum_{j=1}^{5} h^{5-j}}, \quad j = 1, \ldots, 5 \end{aligned}$$

Finally, the impact values assessed by all experts can be aggregated by formula (C9) to generate the final single impact value for each information system with respect to vulnerabilities in each security control family. Table 6 shows the aggregated impact values of each information system.

Table 6
The aggregated impact values of each information system.

Security control families	Assets (5 information systems)				
	ES	RPS	WEBS	WFS	HICS
RA	0.425	0.520	0.331	0.385	0.750
PL	0.470	0.690	0.175	0.250	0.775
SA	0.470	0.585	0.175	0.335	0.775
CA	0.690	0.690	0.355	0.440	0.879
PS	0.675	0.791	0.256	0.250	0.885
PE	0.675	0.581	0.520	0.385	1.000
CP	0.585	0.585	0.175	0.421	0.775
CM	0.470	0.585	0.175	0.421	0.775
MA	0.585	0.585	0.291	0.500	0.690
SI	0.690	0.690	0.175	0.291	0.879
MP	0.541	0.635	0.310	0.335	0.940
IR	0.425	0.635	0.331	0.421	0.835
AT	0.331	0.635	0.216	0.250	0.635
IA	0.635	0.635	0.635	0.585	0.835
AC	0.750	0.635	0.425	0.470	0.835
AU	0.635	0.835	0.500	0.335	0.835
SC	0.635	0.750	0.541	0.470	0.940

Table 7
The risk level of each information system.

Information systems	ES	RPS	WEBS	WFS	HICS
Risk level	0.570 (3)	0.650 (2)	0.336 (5)	0.388 (4)	0.824 (1)

4.4. Deriving risk levels

Using the derived likelihood of risk (Table 5) and the aggregated impact values (Table 6) associated with security control families, the risk level of each information system can be calculated, using formula (1). The results are shown in Table 7.

4.5. Discussion

After obtaining the risk levels, the rationality of all results were reviewed and agreed by the experts from the branch office of the health insurance institute in Taiwan. The experts also agreed that the proposed procedure certainly provided an effective way to identify the crucial factors of security controls.

In this case study, results from constructing network relevance structure of security control areas shows that Management control area gets the highest values of $(D + R)$ and $(D - R)$. Highest value of $(D + R)$ in the Management control area shows it has the greatest importance compared with the other two security areas. On the other hand, the highest positive value of $(D - R)$ in the Management control area shows it is the key cause factor for impacting the other two areas. These findings conclude the Management control area as the most important security control area. In other words, an effective implementation of management controls plays a crucial factor that will lead to successful information security management.

The $(D - R)$ value of the Management control area and the Technique control area are both positive; however, the $(D - R)$ value of the Operation control area is negative. This is the result of the Operation control area being influenced by the other two areas. Hence, the security control measures chosen for the Management control area and the Technique control area will affect the choices of measures of the Operation control area.

As Table 4 presents, the sum of the weights from security control families in the same area with respect to a security control family equals one, and the weights of a security control area equals 0 if there are no influence from security control area. The weights between different security control areas can not be compared directly in the unwieghted supermatrix. Therefore, the steps of the ANP method synthesize and obtain the final likelihood ratings as shown in Table 5.

The likelihood ratings for the Management control area, including the Risk Assessment control family (0.101); the Planning control family (0.082); the System and Service Acquisition control family (0.107); the Certification, Accreditation, and Security Assessments control family (0.105), are greater than the ratings of the Operation control area and the Technique control area. This result is consistent with the findings of the DEMATEL method. The security safeguards or countermeasures in the Management control area are fundamental for all security controls and any negligence in this area will cause a strong probability for allowing a threat to occur. Therefore, we recommend the branch office to dedicate more efforts in implementing safeguards and controls to the Management control area.

The highest likelihood rating is from the System and Services Acquisition control family (0.107). The activities of the System and Services Acquisition control family allocate sufficient resources to protect organizational information systems and employ system development life cycle processes to incorporate information security considerations. The experts agree that security controls for the System and Service Acquisition control family is a very fundamental tactic as the incomplete and ineffective security controls in this control family can lead to serious vulnerabilities and prone to threat exploitations.

Each likelihood rating of the Technique control area is higher than the likelihood ratings of the Operation control area. This result is also consistent with the findings of the DEMATEL method. The $(D - R)$ value of the Technique control area is greater than the $(D - R)$ value of the Operation control area. Experts agree that in practice safeguards chosen for the Technique control area will derive the measures required for the Operation control area. Improperly chosen control measures in the Technique control area will cause a higher risk compared to the Operation control area.

In the Operation control area the likelihood rating for the Personnel Security control family is the greatest as assessed at 0.051. The controls in the Personnel Security control family will be more important than other controls of the Operation control area. The key security tasks for the Operation control area would be to ensure individuals occupying positions of responsibility within organizations are trustworthy and to protect organizational information and information systems during personnel change such as terminations and transfers. Based on this information, inadequate control of the Personnel Security control area will cause high potential for threats to occur.

From the assessments, the five information systems are ranked based on risk levels in the order of: HICS, RPS, ES, WFS, and WEB which were assessed at 0.824, 0.650, 0.57, 0.388, and 0.336 respectively. HICS was evaluated with the highest risk level, vulnerability is likely to be exposed if a given threat is exercised. As a result, there is an urgent need for corrective measures to be implemented. As the assessments from expert interviews revealed, the core techniques and operations areas of the HICS are mainly controlled by a third party which differs from other information systems. All other systems can be directly controlled by the health insurance institute as they possess all the source codes and security control measures can be implemented freely as needed. It is not the case with HICS. This lack of access in the third party information system results in branch office's inability to manage the security of HICS completely. This problem can be mitigated by obtaining a contract requiring higher security standards with the third party.

The RPS and the ES are rated at the second and the third risk levels and corrective actions are required within a reasonable period of time. The risk levels of the WFS and the WEB show less requirement for corrective actions and may be ignored if the authorities at the branch choose to accept the risks associated.

5. Conclusions

This study presents a hybrid information security risk assessment procedure which is based on the DEMATEL method, the ANP method and the FLQ-MEOWA operator. To adapt with real world situations the proposed procedure manages the interdependences and feedback among security control areas and derives risk ratings. As the subjective cognition of evaluators may skew the results in a desired neutral evaluation, an aggregation of the impact values from risks is applied to obtain the final risk levels and safeguard priorities for information systems. The derived results may be used to improve security capabilities and effectiveness for organizations.

A real world case was examined to illustrate the merits of the proposed procedure. In this case study, amongst complex interaction and feedback activities in security control areas, the proposed procedure identified security controls in the Management control area to be the key factor in information security management for the branch office of the health insurance institute. Consequently, proper design and implementation of security controls in this area will considerably enhance the effectiveness of information security measures. Moreover, the procedure also recognized the close relationship between the Technique control area and the Operation control areas which indicates the choices of security controls in the Technique control area to have an influence on the choices of security controls in the Operation control area. During the case study, we systematically evaluated the likelihood of risks instead of simply obtaining the ratings by using direct assessments. The proposed procedure also synthetically determined the risk levels for all of the examined information systems in the branch successfully and indicated HICS, RPS, and ES to be the most important systems for priority in protection needs. While corrective measures are essential to protect the information systems against threats, we conclude that HICS is of the highest priority in comparison to others. The security mission of the branch against threats critically depends on the effective security implementations of the above mentioned information systems as determined by the proposed hybrid information security risk assessment method in this paper. The proposed hybrid method is therefore proven to work and can be applied to other information systems with similar complexity of control relationships in reaching security missions.

Acknowledgement

The authors are very grateful to the anonymous experts and consultants for their participation in the case study of risk assessment used for this paper.

Appendix A. The process of the DEMATEL method

The DEMATEL method analyses relationships between factors and converts these relationships into a comprehensible structure model which can demonstrate cause group and effect group of factors and show the numeral strength of influence (Tsai & Chou, 2009; Tzeng et al., 2007). In this study, this DEMATEL method is applied to build network relevance system between security control areas. This method is summarized as follows:

Step 1: *Creating the initial direct-influence matrix*Experts compare each pair of security control areas in the light of influence of four levels shown in Table 2. Consequently, the result of these comparisons creates the initial direct-influence matrix that is a $n \times n$ matrix A, in which a_{ij} is denoted as the degree to which the security control area i affects the security control area j.

Step 2: *Obtaining the normalized direct-relation matrix*Secondly, the normalized direct-relation matrix X can be obtained through formulas (A1) and (A2) by the initial direct influence matrix A. All principal diagonal elements are equal to zero in X.

$$X = k \cdot A \tag{A1}$$

$$k = \frac{1}{\max\limits_{1 \leqslant i \leqslant n} \sum_{j=1}^{n} a_{ij}} \tag{A2}$$

Step 3: *Generating the total-relation matrix*Next, the total-relation matrix can be acquired through (A3), in which the I is denoted as the identity matrix (Huang, Shyu, & Tzeng, 2007).

$$T = X + X^2 + X^3 + \cdots = \sum_{i=1}^{\infty} X^i = X(I - X)^{-1} \tag{A3}$$

Step 4: *Building the impact-digraph map*After the total-relation matrix is obtained, the sum of rows and the sum of columns in matrix T can be computed and denoted as D and R, respectively, shown in formulas (A4)–(A6) (Hori & Shimizu, 1999; Tsai & Chou, 2009; Wu, 2008). The value of $(D + R)$ of each factor indicates how much importance the factor has. The larger the value of $(D + R)$ is, the more relationship between the factor and others is. On the other hand, the value of $(D - R)$ of each factor indicates the strength of influence on others. The factor having positive value of $(D - R)$ influences other factors and is assumed to be the cause element. On the contrary, the factor having negative value of $(D - R)$ receives influence from other factors and is assumed to be the effect element. Consequently, the impact-relations-map cab be built by mapping the dataset of $(D + R, D - R)$ (Seyed-Hosseini et al., 2006).

To build a simplified impact-digraph map, an appropriate threshold for value of t_{ij} should be determined by decision makers or experts through discussion. The influence whose value of t_{ij} is above the threshold will be selected as an edge in impact-digraph map (Liou et al., 2007; Tsai & Chou, 2009; Tzeng et al., 2007). Therefore, only the influences having higher importance will be displayed in impact-digraph map and the minor influences will be filtered. This simplification helps decision makers to clearly build a comprehensible structure of factors.

$$T = [t_{ij}]_{n \times n}, \quad i,j \in \{1, 2, ...n\} \tag{A4}$$

$$D = \sum_{j=1}^{n} t_{i,j} \tag{A5}$$

$$R = \sum_{i=1}^{n} t_{i,j} \tag{A6}$$

By the values of $(D + R, D - R)$ of factors and the impact-relation-map, the analysts can make decision in risk assessment to find the critical security control area which should have higher priority in risk management to mitigate the risk effectively. Moreover, the impact-relation-map can be the network relevance system of the ANP method to find the likelihood of occurrence in threats exercising potential vulnerability of each security control family.

$$W = \begin{array}{cc|cccc} & & C_1 & C_2 & \cdots & C_m \\ & & e_{11}\cdots e_{1n_1} & e_{21}\cdots e_{2n_2} & \cdots & e_{m1}\cdots e_{mn_m} \\ \hline C_1 & \begin{matrix} e_{11} \\ e_{12} \\ \vdots \\ e_{1n_1} \end{matrix} & W_{11} & W_{12} & \cdots & W_{1m} \\ C_2 & \begin{matrix} e_{21} \\ e_{22} \\ \vdots \\ e_{2n_2} \end{matrix} & W_{21} & W_{22} & \cdots & W_{2m} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ C_m & \begin{matrix} e_{m1} \\ e_{m2} \\ \vdots \\ e_{mn_m} \end{matrix} & W_{m1} & W_{m2} & \cdots & W_{mm} \end{array}$$

Fig. B1. Supermatrix.

Appendix B. The process of the ANP method

To handle the situation of interdependences among criteria or alternatives, Saaty (1996) proposed the ANP method. The ANP method can effectively deal with interplay relationship of network structure in real world, especially when risk and uncertainty are involved (Saaty & Saaty, 2003).

The first step of the ANP method is doing pairwise comparisons between each two the criteria of the whole system with respect to another criterion to establish priorities for the criteria being compared. This study pairwise compares the criteria by asking" With respect to one security control family how much likely is another security control family to lead risks compared to the other security control family?" These pairwise comparisons are based on the Saaty's nine-point scale of 1–9 representing equal likelihood to extreme likelihood (Huang et al., 2005).

The result of a series of pairwise comparisons will form a supermatrix in the generalized form shown in Fig. B1 where C_m denotes the mth cluster, e_{mn} denotes the nth element in the mth cluster, and matrix W_{ij} is the principal eigenvector of the influence of the elements compared in the jth cluster to the ith cluster (Saaty & Saaty, 2003).

After forming the supermatrix, the weighted supermatrix is derived by transforming each column of matrix sums to unity. Finally, the weighted supermatrix can be raised to limiting powers as formula (B1) to obtain the global priority vectors or called weights (Huang et al., 2005; Wu, 2008). Using the ANP method, the likelihood vector of potential threats associated with each security control families is determined.

$$\lim_{k \to \infty} W^k \tag{B1}$$

Appendix C. The process of the FLQ-MEOWA opertaor

The fuzzy linguistic quantifiers-guided maximum entropy order-weighted averaging (FLQ-MEOWA) operator can aggregate values assessed by different experts into a final evaluation value by various fuzzy linguistic quantifiers. Adopting different fuzzy linguistic quantifier produces different fuzzy majority to emphasize various influence of aggregation. This final value is between maximum and minimum of the origin assessment values. Consequently, FLQ-MEOWA operator can reduce the influence of the relatively extreme strong or weak assessment values. The FLQ-MEOWA operator, is based on order-weighted averaging (OWA) operator defined by Yager (1988), on fuzzy linguistic quantifier suggested by Yager (1993), Zadeh (1983) and Herrera et al. (1995), and on maximum entropy method proposed by O'Hagan

(1988, 1990) and resolved by Filev and Yager (1995). The steps of utilizing the FLQ-MEOWA operator in this study are shown as follows:

Step 1: *Meeting risk assessment objectives with fuzzy linguistic quantifier*A FLQ-MEOWA operator of dimension n is a mapping, F_Q: $R^n \to R$ where $R \in [0,1]$, that has an associated n vector $W = [w_1, w_2, \ldots, w_n]^T$ such that $\sum_{j=1}^{n} w_j = 1$ and $w_j \in [0,1]$. Furthermore,

$$F_Q(a) = F_Q(a_1, a_2, \ldots, a_n) = \sum_{j=1}^{n} w_j b_j \tag{C1}$$

where b_j denotes thejth largest elements of $a_1, a_2, \ldots, a_n$. Moreover, the aggregation weighted vector W is obtained by using a non-decreasing proportional fuzzy linguistic quantifier, Q, represented as formula (C2) and (C3).

$$w_j = Q\left(\frac{j}{n}\right) - Q\left(\frac{j-1}{n}\right), \quad j = 1, \ldots, n, \tag{C2}$$

$$Q(r) = \begin{cases} 0 & \text{if } r < a \\ \frac{r-a}{b-a} & \text{if } a \leqslant r \leqslant b, a, b, r \in [0,1] \\ 1 & \text{if } r > b \end{cases} \tag{C3}$$

The fuzzy linguistic quantifier Q generally represented the concept of fuzzy majority in the aggregation of elements (Kacprzyk, 1986). Some examples of non-decreasing proportional fuzzy linguistic quantifier are shown in Fig. C1, where the parameters, (a,b), are $(0.3, 0.8)$, $(0, 0.5)$, and $(0.5, 1)$ associated with "most", "at least half", and "as many as possible", respectively (Herrera et al., 1995). The quantifier "most" means that most of the elements are satisfied. This quantifier emphasizes the influence of the medium values of the re-ordered elements by means of giving small weights on higher and lower values. The quantifier "at least half" focuses on the first half of values after re-ordering them in descending order to emphasize the influence of the strong elements. The quantifier "as many as possible" focuses on the second half of values after reordering to emphasize the result of aggregation fulfils the essential elements. Depending on the different risk management objectives and security requirements of organizations, the appropriate linguistic quantifiers can be adopted. To decrease the influence of strong powerful evaluations of risk impact and other relatively weak ones, in this study the linguistic quantifier "most" was used for to emphasize the medium influence on aggregated impact value. Other linguistic quantifiers also can be used in our method depends on different objective of risk assessment.

Step 2: *Optimizing aggregation operator*After the weight vector is obtained by mapping to fuzzy linguistic quantifier, Q, MEOWA operator is used to optimize the aggregation operator. MEOWA operator developed by O'Hagan (1988) generates the OWA weights that have a maximal entropy for a given degree of *orness.Orness* measure and entropy measure are introduced by Yager to characterize the type of aggregation being performed for a particular value of the weighting vector. The *orness* measure of the aggregation is defined as

$$orness(w) = \frac{1}{n-1} \sum_{j=1}^{n} (n-j) w_j \tag{C4}$$

This measure, which lies in the unit interval [0, 1], characterizes the degree to which aggregation is like an *or* operation. The degree of *orness* can be 1, 0 and 0.5 meaning OWA operators equal the Max, Min and arithmetic mean operation, respectively. The second measure, entropy of the aggregation is defined as

$$entropy(w) = -\sum_{j=1}^{n} w_j \ln w_j \tag{C5}$$

Entropy measures the degree of how much of information in the arguments is taken into consideration during the aggregation based on the weighting vector. By these two measures, O'Hagan (1988) proposed a process to determined the OWA weights having maximal entropy based on a predefined degree of *orness*. The operators are called maximum entropy OWA (MEOWA) operators The approach based on the solution of a constrained optimized problem is illustrated as Maximize

$$-\sum_{j=1}^{n} w_j \ln w_j, \tag{C6}$$

subject to

$$orness(w) = \frac{1}{n-1} \sum_{j=1}^{n} (n-j) w_j \tag{C6a}$$

$$\sum_{j=1}^{n} w_j = 1, \quad w_j \in [0,1], \quad j = 1, \ldots, n. \tag{C6b}$$

Filev and Yager (1995) further presented the analytic properties of MEOWA operator, and proposed a method to generate MEOWA weights by transforming formulas (C6) into (C7) and (C8). A positive solution h can be obtained from formula (C7) by the numerical analysis approach. Next, w^* can be obtained by substitution h into formula (C8) (Chang, Wang, & Wang, 2006). The w^* derived from the constrained nonlinear optimization problem can be new associated weight of FLQ-MEOWA operator.

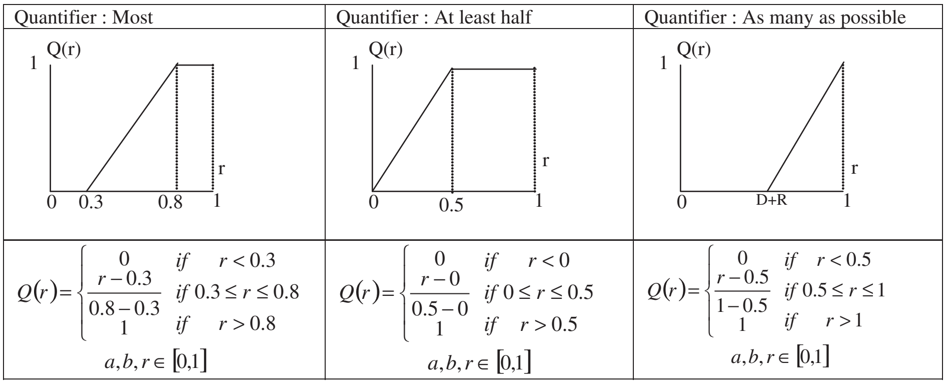

Fig. C1. Fuzzy linguistic quantifiers (Herrera et al., 1995).

$$\sum_{j=1}^{n}\left(\frac{n-j}{n-1} - orness(W)\right)h^{n-j} = 0 \tag{C7}$$

$$w_j^* = \frac{h^{n-j}}{\sum_{j=1}^{n} h^{n-j}}. \tag{C8}$$

Step 3: *Aggregating the impact values by optimal aggregation operator*Lastly, the impact values assessed by all experts, exploited by one threat can be aggregate by the optimal FLQ-MEOWA operator to generate the final one impact value. A FLQ-MEOWA operator of dimension p is a mapping, $FLQ - MEOWA_Q$: $R^p \to R$ where $R \in [0,1]$, that has an associated p vector $W^* = \left[w_1^*, w_2^*, \ldots, w_p^*\right]^T$ such that $\sum_{k=1}^{p} w_k^* = 1$ and $w_k \in [0,1]$. Furthermore, this FLQ-MEOWA operator can aggregate the impact value v_{ij} of asset i, assessed by p experts, with respect to vulnerability of security control family j exploited by threats. The aggregate formula is illustrated as following:

$$v_{ij} = FLQ - MEOWA_Q\left(v_{ij}^1, v_{ij}^2, \ldots, v_{ij}^p\right) = \sum_{k=1}^{p} w_k^* b_{ij}^k \tag{C9}$$

where b_{ij}^k is the k largest of the $v_{ij}^1, v_{ij}^2, \ldots, v_{ij}^p$

References

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms. Cloudcroft, New Mexico*: ACM.

C&A Systems Security Limited. (2005). Consultative, objective and bi-functional risk analysis: COBRA tools, ISO/IEC 17799 compliance and security risk analysis approach. In *C&A Systems Security Limited*.

Chang, S.-L., Wang, R.-C., & Wang, S.-Y. (2006). Applying fuzzy linguistic quantifier to select supply chain partners at different phases of product life cycle. *International Journal of Production Economics, 100*, 348–359.

Chiu, Y., Chen, H., Tzeng, G., & Shyu, J. (2006). Marketing strategy based on customer behaviour for the LCD-TV. *International Journal of Management and Decision Making, 7*, 143–165.

Filev, D., & Yager, R. R. (1995). Analytic properties of maximum entropy OWA operators. *Information Sciences, 85*, 11–27.

Filev, D., & Yager, R. R. (1998). On the issue of obtaining OWA operator weights. *Fuzzy Sets and Systems, 94*, 157–169.

FIPS. (2006). Federal Information processing standards publications 200 minimum security requirements for federal information and information systems. In *US National Institute of Standards and Technology*.

Fontela, E., & Gabus, A. (1976). *The DEMATEL observer*, DEMATEL 1976 report. Switzerland, Geneva: Battelle Geneva Research Center.

Gabus, A., & Fontela, E. (1972). *World problems, an invitation to further thought within the framework of DEMATEL*. Switzerland Geneva: Battelle Geneva Research Center.

Gabus, A., & Fontela, E. (1973). *Perceptions of the world problematique: Communication procedure, communicating with those bearing collective responsibility*. DEMATEL report. Vol. 1. Switzerland Geneva: Battelle Geneva Research Centre.

Herrera, F., Herrera-Viedma, E., & Verdegay, J. L. (1995). A sequential selection process in group decision making with a linguistic assessment approach. *Information Sciences, 85*, 223–239.

Herrera, F., Herrera-Viedma, E., & Verdegay, J. L. (1996). Direct approach processes in group decision making using linguistic OWA operators. *Fuzzy Sets and Systems, 79*, 175–190.

Hori, S., & Shimizu, Y. (1999). Designing methods of human interface for supervisory control systems. *Control Engineering Practice, 7*, 1413–1419.

Huang, C. Y., Shyu, J. Z., & Tzeng, G. H. (2007). Reconfiguring the innovation policy portfolios for Taiwan's SIP Mall industry. *Technovation, 27*, 744–765.

Huang, J. J., Tzeng, G. H., & Ong, C. S. (2005). Multidimensional data in multidimensional scaling using the analytic network process. *Pattern Recognition Letters, 26*, 755–767.

ISO. (2005). IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. In *International Organization for Standardization*.

Kacprzyk, J. (1986). Group decision making with a fuzzy linguistic majority. *Fuzzy Sets and Systems, 18*, 105–118.

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers & Security, 24*, 147–159.

Karsak, E. E., Sozer, S., & Alptekin, S. E. (2003). Product planning in quality function deployment using a combined analytic network process and goal programming approach. *Computers & industrial engineering, 44*, 171–190.

Lee, J. W., & Kim, S. H. (2000). Using analytic network process and goal programming for interdependent information system project selection. *Computers and Operations Research, 27*, 367–382.

Lin, Y.-H., Chiu, C.-C., & Tsai, C.-H. (2008). The study of applying ANP model to assess dispatching rules for wafer fabrication. *Expert Systems with Applications, 34*, 2148–2163.

Liou, J. J. H., Tzeng, G.-H., & Chang, H.-C. (2007). Airline safety measurement using a hybrid model. *Journal of Air Transport Management, 13*, 243–249.

Liu, F., Dai, K., Wang, Z., & Ma, J. (2005). Research on fuzzy group decision making in security risk assessment. In *Networking – ICN 2005* (pp. 1114–1121).

Meade, L. M., & Presley, A. (2002). R& D project selection using the analytic network process. *IEEE Transactions on Engineering Management, 49*, 59–66.

O'Hagan, M. (1988). Aggregating template rule antecedents in real-time expert systems with fuzzy set logic. In *The 22nd annual IEEE Asilomar conference on signals, systems and computers, Pacific Grove, CA* (pp. 681–689).

O'Hagan, M. (1990). *Using maximum entropy-ordered weighted averaging to construct a fuzzy neuron* (pp. 618–623).

Peltier, T. R. (2005). *Information security risk analysis*. Auerbach Pub.

Richardson, R. (2007). *CSI computer crime and security survey*. Available from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>.

Richardson, R. (2008). *CSI computer crime and security survey*. Available from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>.

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., & Rogers, G. (2007). Recommended security controls for federal information systems (Special Publication 800-53 Revision 2). In *National Institute of Standards and Technology*.

Saaty, T. L. (1980). *The analytic hierarchy process*. New York: McGraw-Hill.

Saaty, T. L. (1996). *Decision making with dependence and feedback: the analytic network process*. Pittsburgh, PA: RWS Publications.

Saaty, R., & Saaty, T. (2003). *Decision making in complex environment: The analytic hierarchy process (AHP) for decision making and the analytic network process (ANP) for decision making with dependence and feedback*. Pittsburgh, PA: Creative Decisions Foundation.

Seyed-Hosseini, S. M., Safaei, N., & Asgharpour, M. J. (2006). Reprioritization of failures in a system failure mode and effects analysis by decision making trial and evaluation laboratory technique. *Reliability Engineering & System Safety, 91*, 872–881.

Shang, J. S., Tjader, Y., & Ding, Y. (2004). A Unified framework for multicriteria evaluation of transportation projects. *IEEE Transactions on Engineering Management, 51*, 300–313.

Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S. H., Lund, M. S., Stamatiou, Y. C., & Aagedal, J. O. (2002). *Model-based risk assessment–the CORAS approach*.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. In *National institute of standards and technology*.

Tsai, W.-H., & Chou, W.-C. (2009). Selecting management systems for sustainable development in SMEs: A novel hybrid model based on DEMATEL, ANP, and ZOGP. *Expert Systems with Applications, 36*, 1444–1458.

Tzeng, G. H., Chiang, C. H., & Li, C. W. (2007). Evaluating intertwined effects in e-learning programs: A novel hybrid MCDM model based on factor analysis and DEMATEL. *Expert Systems with Applications, 32*, 1028–1044.

United Kingdom Central Computer and Telecommunications Agency. (2001). CCTA risk analysis and management method, CRAMM user guide.

Wang, P., Chao, K.-M., Lo, C.-C., Huang, C.-L., & Younas, M. (2007). A fuzzy outranking approach in risk analysis of web service security. *Cluster Computing, 10*, 47–55.

Wu, W.-W. (2008). Choosing knowledge management strategies by using a combined ANP and DEMATEL approach. *Expert Systems with Applications, 35*, 828–835.

Yager, R. R. (1988). On ordered weighted averaging aggregation operators in multicriteria decisionmaking. *IEEE Transactions on Systems, Man and Cybernetics, 18*, 183–190.

Yager, R. R. (1993). Families of OWA operators. *Fuzzy Sets and Systems, 59*, 125–148.

Zadeh, L. (1983). A computational approach to fuzzy quantifiers in natural languages. *International series in modern applied mathematics and computer science, 5*, 149–184.