Information Sciences 232 (2013) 482–500

Contents lists available at SciVerse ScienceDirect

Information Sciences

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

A VIKOR technique based on DEMATEL and ANP for information security risk control assessment

Yu-Ping Ou Yang [a,*], How-Ming Shieh [a,b], Gwo-Hshiung Tzeng [c,d]

[a] Department of Business Administration, National Central University, 300 Chung-da Road, Chung-Li City 320, Taiwan
[b] Department of Information Management, National Central University, 300 Chung-da Road, Chung-Li City 320, Taiwan
[c] Department of Information Management, Kainan University, No. 1, Kainan Road, Luchu, Taoyuan 338, Taiwan
[d] Institute of Management of Technology, National Chiao Tung University, 1001 Ta-Hsueh Road, Hsinchu 300, Taiwan

ARTICLE INFO

Article history:
Available online 17 September 2011

Keywords:
VIKOR
Analytic network process (ANP)
DEMATEL
Multiple criteria decision making (MCDM)
Information security
Risk control assessment

ABSTRACT

As companies and organizations have grown to rely on their computer systems and networks, the issue of information security management has become more significant. To maintain their competitiveness, enterprises should safeguard their information and try to eliminate the risk of information being compromised or reduce this risk to an acceptable level. This paper proposes an information security risk-control assessment model that could improve information security for these companies and organizations. We propose an MCDM model combining VIKOR, DEMATEL, and ANP to solve the problem of conflicting criteria that show dependence and feedback. In addition, an empirical application of evaluating the risk controls is used to illustrate the proposed method. The results show that our proposed method can be effective in helping IT managers validate the effectiveness of their risk controls.

1. Introduction

In an era of computers and computer networks, corporations and public organizations have implemented computerization: (i) to reduce labor costs, materials, and financial investment; and (ii) to achieve convenient and effective services. But with the development of computers and computer-networks, the threat of information security incidents that could jeopardize the information held by organizations is becoming increasingly serious; such incidents may even be serious enough to cause the failure of enterprises. To maintain their competitiveness, enterprises should safeguard their information system and try to eliminate the risk of being compromised or to reduce this risk to an acceptable level. There are many studies that deal with methods of information security risk assessment and ways of achieving risk controls. However, few studies calculate the integrated risks or assess the performance of the implemented controls after taking into account the dependence among criteria. Because information-risk factors are usually dependent on each other, it is not advisable to use traditional assessment methods where the assessment factors or criteria are assumed to be independent. Therefore, this study proposes an information security risk-control assessment model (ISRCAM) that combines the *VlseKriterijumska Optimizacija I Kompromisno Resenje technique* (in Serbian, which means Multicriteria Optimization and Compromise Solution), also known as VIKOR, the decision-making trial and evaluation laboratory (DEMATEL), and the analytic network process (ANP) to solve the problem. We hope to use this hybrid MCDM method to accurately model the interdependent risk factors and improve information security. Finally, an empirical example for information security risk control is presented to illustrate our proposed method.

* Corresponding author.
E-mail addresses: ouyang.ping@msa.hinet.net (Y.-P. Ou Yang), ghtzeng@mail.knu.edu.tw, ghtzeng@cc.nctu.edu.tw (G.-H. Tzeng).

0020-0255/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2011.09.012

Multiple criteria decision-making (MCDM) methods are often used to deal with problems in management that are characterized by several non-commensurable and conflicting (competing) criteria, and there may be no solution that satisfies all criteria simultaneously. Risk-related assessment often uses MCDM to deal with problems having multiple and conflicting objectives. Liu et al. [19] stated: "Multicriteria-analysis techniques could help decision-makers evaluate risks and countermeasures (controls) when conflicting criteria must be considered and balanced". Thus, MCDM methods can provide IT (information technology) managers with systematic and repeatable methods for evaluating information-security-risk-related problems. Since understanding the performance gaps of the implemented controls to an assumed ideal performance level is important for assessing the effectiveness of the various risk controls, compromise-programming methods can be used to rank the risk-control areas or objectives. Among the MCDM methods, VIKOR and TOPSIS procedures are based on an aggregating function representing "closeness to the ideal". Furthermore, they use the compromise-programming method to rank and improve alternatives. The TOPSIS method was first developed by Hwang and Yoon [10] based on the concept that the chosen alternative should: (a) have the shortest distance from the ideal solution and (b) be the farthest from the negative-ideal solution, using Euclidean distance [10]. However, Opricovic and Tzeng [28] showed that TOPSIS has several shortcomings in its ranking process. Therefore, their study proposed an alternative VIKOR method to replace TOPSIS [27,28]. This research also uses the VIKOR method to rank the risk-control areas and risk values.

The VIKOR method was developed by Opricovic [26]. Development of the VIKOR method began when Yu [45] proved the L_p-*metric* for a distance function. The VIKOR method introduced the multicriteria ranking index based on a particular measure of "closeness to the ideal/aspired level" and was introduced as an applicable technique within MCDM [26]. This method focuses on the ranking of a set of choices in the presence of conflicting criteria, which helps decision-makers select the "best" compromise choice [27]. The VIKOR method was developed as an MCDM method to solve discrete decision problems with non-commensurable and conflicting criteria [40,41,27–29,31]. However, few papers discuss conflicting (competing) criteria with dependence and feedback using this compromise solution method. Therefore, we developed the VIKOR method based on the ANP and DEMATEL methods to solve the problem of conflicting criteria with dependence and feedback [30]. In addition, using the methods can help us rank the gaps for the risk-control objectives/areas. However, the VIKOR method ranks and selects alternatives based on all the established criteria. Namely, it uses the same criteria to assess each alternative; thus, using traditional VIKOR to rank their orders is unsuitable when each control clause/aspect of information-security risk has its own criteria (different criteria or objectives). Furthermore, because, in practice, each enterprise or government agency has different information-security risk controls, direct comparison is also not possible. Hence, this research adopts an improved VIKOR method, called VIKORRUG—VIKOR for Ranking Unimproved Gap [31]—for ranking the information-security-risk-control objectives and control areas.

ANP was proposed by Saaty as a new MCDM method to overcome the problems of interdependence and feedback among criteria and alternatives in the real world [34]. ANP is an extension of AHP based on the concepts of Markov Chain, and it is a nonlinear dynamic structure [35]. ANP is the general form of AHP [36] and has been used in MCDM to relax the restriction on hierarchical structure. ANP has been applied successfully in many practical decision-making problems [15,17,21,22,39,46]. Furthermore, a hybrid model combining ANP and DEMATEL to solve the dependence and feedback problems has been successfully used in various fields [8,18,42]. When dealing with ANP, we found that using the traditional method of normalizing the unweighted supermatrix is not reasonable. In the traditional method, each criterion in a column is divided by the number of clusters so that each column adds up to unity. Using this normalization method implies that each cluster has the same weight. However, there are different degrees of influence among the clusters of factors/criteria in the real world. Thus, the assumption of equal weights for each cluster to obtain the weighted supermatrix is unrealistic and needs to be improved [32]. Thus, this study uses the results from DEMATEL to improve the normalization process in ANP. Thus DEMATEL [3,4,6,7,44] is used not only to construct the interrelations between factors/criteria in building an NRM (network relations map) but also to improve the normalization process of ANP.

In conclusion, the contribution of this study is to propose an ISRCAM model for criteria with interdependence and feedback to assess the performance of the risk controls of an information system. The results will help IT managers of businesses or government agencies to understand the control areas or control objectives that should be enhanced to conform to the aspired levels or needs. In addition, by using DEMATEL to generate an NRM, the proposed method can help IT managers analyze the reasons behind why some controls having larger gaps and needs to be improved. Furthermore, we use an empirical example of an enterprise information-security controls assessment to show the steps of a novel MCDM that combine VIKOR, DEMATEL, and ANP [30] to solve the problem of conflicting criteria with dependence and feedback. Our results show that this proposed method helps us deal with conflicting problems of criteria with interdependence and feedback and improves the normalization of the supermatrix to reflect reality.

The rest of this paper is organized as follows. In Section 2, the research framework is proposed. In Section 3, the hybrid MCDM model is described. In Section 4, a numerical example with applications is illustrated to show the proposed methods in real case. Discussions and conclusions are presented in Sections 5 and 6, respectively.

2. Research framework

The risk management process model [1] includes four steps: (1) risk assessment; (2) risk remediation; (3) risk monitoring and review; and (4) risk management enhancement. The first step involves identifying and analyzing the vulnerability of

exploitation by a threat. The second step involves using controls to address the risk; this is also called risk treatment. The third step involves monitoring and measuring the risk controls for effectiveness. The fourth step is a continuous improvement process based on observations from each of the previous steps, which serves as feedback for the risk management cycle. The risk management process model is an ongoing process of assessing, addressing, monitoring risks, and subsequent security enhancement. The strategy is the "Plan-Do-Check-Act (PDCA)" cycle, as shown in Fig. 1.

Since the "monitor and review risk" step is also an important process and few articles discuss it for the assessment of the implemented controls in the "Check" step, this research focuses on improving the "monitor and review the risks" step by proposing a risk-control assessment system to improve controls and reduce risk. The purpose of this research is to develop an assessment model for previously implemented controls. The main framework is shown in Fig. 2, and it shows that risk treatments, vulnerabilities, and implemented controls affect the selection of risk controls. The residual risks and the gaps of the implemented controls, which are the distances from the actual performances to the aspired performances on the implemented controls, are obtained by using risk-control assessment. Managers can then decide which controls should be strengthened according to the assessment results. Subsequently, these results are referred to the next step in the process – the risk management enhancement.

Because many studies adopt MCDM methods to assess risk-related problems, MCDM methods are also used to evaluate the performances of the implemented risk controls. However, some articles have proposed risk-control assessment based on the dependence and feedback among criteria during the "Check" phase. Therefore, we propose a suitable ISRCAM—a novel VIKOR method combined with the DEMATEL technique and ANP, to accurately infer the gaps of the implemented controls and control objectives. The following section explains our new methodology in detail.

3. A hybrid MCDM model

A VIKOR technique based on DEMATEL and ANP for evaluating and improving problems is proposed according to the above descriptions. The procedures to this novel hybrid MCDM model, a combination of DEMATEL and ANP with VIKOR, are schematically shown in Fig. 3 and explained in the following subsections.

3.1. DEMATEL

The Battelle Memorial Institute conducted a project concerning the concept of the DEMATEL technique through its Geneva Research Centre [6,7]. The DEMATEL technique constructs the interrelations between factors/criteria to build a *network relations map* (NRM) [8,18,32,42]. The method can be summarized as follows:

Step 1: *Calculate the direct relation average matrix*. Assuming the scales 0, 1, 2, 3 and 4 represent the range from "no influence (0)" to "very high influence (4)", respondents are asked to propose the degree of direct influence each factor/criterion i exerts on each factor/criterion j, which is denoted by d_{ij}, using the assumed scales. A direct relation matrix would be produced by each respondent, and an average matrix $\boldsymbol{D}$ is then derived through the mean of the same factors/criteria in the various direct matrices of the respondents. The average matrix $\boldsymbol{D}$ is shown as follows:

$$\boldsymbol{D} = \begin{bmatrix} d_{11} & \cdots & d_{1j} & \cdots & d_{1n} \\ \vdots & & \vdots & & \vdots \\ d_{i1} & \cdots & d_{ij} & \cdots & d_{in} \\ \vdots & & \vdots & & \vdots \\ d_{n1} & \cdots & d_{nj} & \cdots & d_{nn} \end{bmatrix} \tag{1}$$

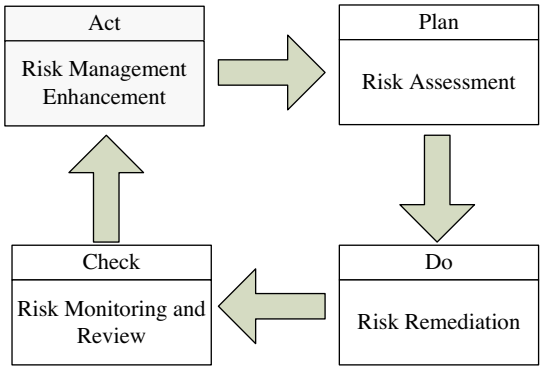

Fig. 1. Risk management process model (Source: [1]).

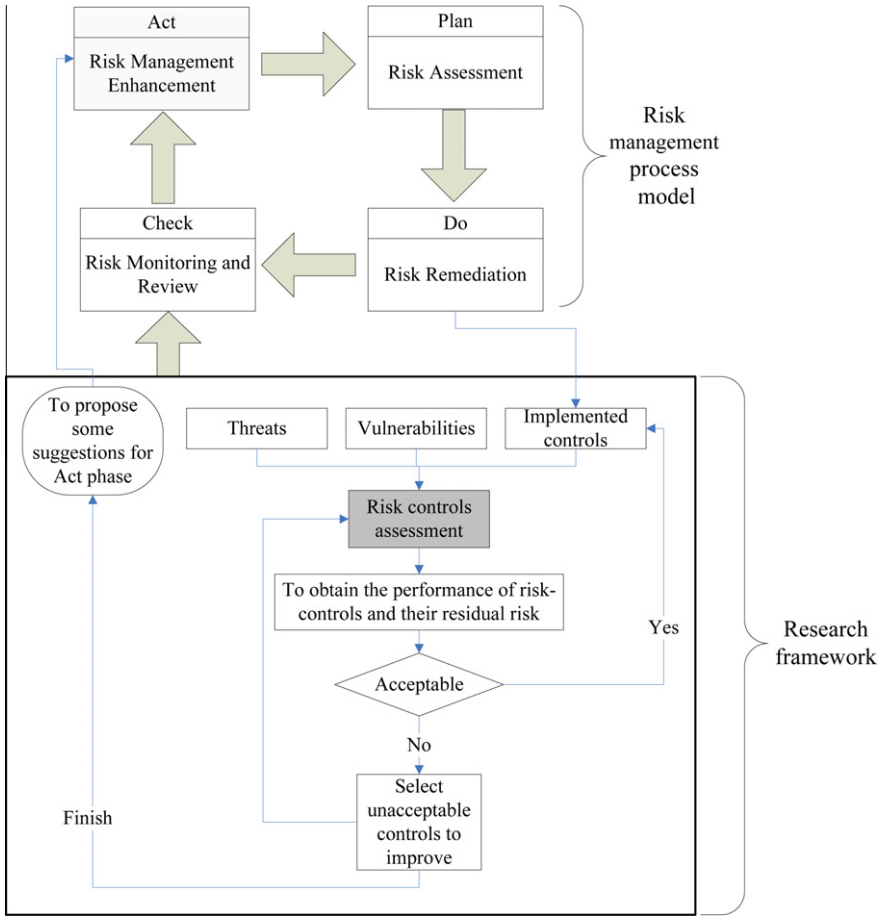

Fig. 2. The relation between the research framework and risk-management process model.

Step 2: *Calculate the initial direct influence matrix.* The initial direct influence matrix $\boldsymbol{X}$ (i.e., $\boldsymbol{X} = [x_{ij}]_{n\times n}$) can be obtained by normalizing the average matrix $\boldsymbol{D}$. In addition, the matrix $\boldsymbol{X}$ can be obtained through Eqs. (2) and (3), in which all principal diagonal criteria are equal to zero.

$$\boldsymbol{X} = s \cdot \boldsymbol{D} \tag{2}$$

$$s = \min\left[1/\max_i \sum_{j=1}^{n} |d_{ij}|, 1/\max_j \sum_{i=1}^{n} |d_{ij}|\right] \tag{3}$$

Step 3: *Derive the total influence matrix.* A continuous decrease of the indirect effects of problems along the powers of $\boldsymbol{X}$, e.g., $\boldsymbol{X}^2, \boldsymbol{X}^3, \ldots, \boldsymbol{X}^h$ and $\lim_{h\to\infty}\boldsymbol{X}^h = [0]_{n\times n}$, where $\boldsymbol{X} = [x_{ij}]_{n\times n}$, $0 \leqslant x_{ij} < 1$, $0 < \sum_i x_{ij} \leqslant 1$ and $0 < \sum_j x_{ij} \leqslant 1$, and at least one column sum $\sum_j x_{ij}$ or one row sum $\sum_i x_{ij}$ equals 1; then we can guarantee $\lim_{h\to\infty}\boldsymbol{X}^h = [0]_{n\times n}$. So the total influence matrix can be calculated as follows.

$$\boldsymbol{T} = \boldsymbol{X} + \boldsymbol{X}^2 + \cdots + \boldsymbol{X}^{\boldsymbol{h}} = \boldsymbol{X}(\boldsymbol{I} + \boldsymbol{X} + \boldsymbol{X}^2 + \cdots + \boldsymbol{X}^{h-1})(\boldsymbol{I} - \boldsymbol{X})(\boldsymbol{I} - \boldsymbol{X})^{-1} = \boldsymbol{X}(\boldsymbol{I} - \boldsymbol{X}^h)(\boldsymbol{I} - \boldsymbol{X})^{-1}, \text{when } \lim_{h\to\infty}\boldsymbol{X}^h = [0]_{n\times n}, \text{ then}$$
$$\boldsymbol{T} = \boldsymbol{X}(\boldsymbol{I} - \boldsymbol{X})^{-1} \tag{4}$$

where $\boldsymbol{T} = [t_{ij}]_{n\times n}$, for $i, j = 1, 2, \ldots, n$ and $(\boldsymbol{I} - \boldsymbol{X})(\boldsymbol{I} - \boldsymbol{X})^{-1} = I$. In addition, the method presents each row sum and column sum of matrix $\boldsymbol{T}$:

$$\boldsymbol{r} = (r_i)_{n\times 1} = \left[\sum_{j=1}^{n} t_{ij}\right]_{n\times 1} \tag{5}$$

$$\boldsymbol{c} = (c_j)_{n\times 1} = (c_j)'_{1\times n} = \left[\sum_{i=1}^{n} t_{ij}\right]'_{1\times n} \tag{6}$$

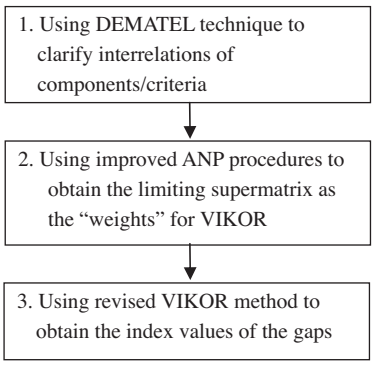

Fig. 3. Hybrid MCDM model procedures.

where r_i denotes the row sum of the ith row of matrix $\boldsymbol{T}$ and shows the sum of total effects (including direct and indirect effects) of factor/element i on the other factors/elements. Similarly, c_j denotes the column sum of the jth column of matrix $\boldsymbol{T}$ and shows the sum of total effects (including direct and indirect effects) that factor/element j has received from the other factors/criteria. Additionally, $(r_i + c_i)$ provides an index of the strength of influences given and received when $i = j$, that is, $(r_i + c_i)$ shows the degree of the central role that factor i plays in the problem. If $(r_i - c_i)$ is positive, then factor i is affecting other factors, and if $(r_i - c_i)$ is negative, then factor i is being influenced by other factors [32,38,42].

Step 4: *Set a threshold value and obtain the NRM*. Based on the matrix $\boldsymbol{T}$, each factor t_{ij} of matrix $\boldsymbol{T}$ provides network information on how factor i affects factor$j$. Setting a threshold value α to filter the minor effects denoted by the factors of matrix $\boldsymbol{T}$ is necessary to isolate the relation structure of the factors. In practice, if all the information from matrix $\boldsymbol{T}$ converts to the NRM, the map would be too complex to show the necessary network information for decision-making. In order to reduce the complexity of the NRM, the decision-maker sets a threshold value α for the influence level to filter out minor effects: only factors whose influence value in matrix $\boldsymbol{T}$ is higher than the threshold value will be chosen and converted into the NRM. The threshold value can be decided by experts. When the threshold value and the relative NRM have been decided, the NRM can be drawn accordingly.

3.2. ANP

ANP is a mathematical theory that can systematically overcome all kinds of dependence [37]. The method can be described in the following steps:

Step 5: *Form an unweighted supermatrix through pairwise comparisons*. The first step of the ANP is to use pair-wise comparisons with the criteria. The relative importance value can be determined assuming a scale of 1 to 9 to represent equal importance to extreme importance [34,36]. The general form of the supermatrix can be described as follows:

$$\boldsymbol{W} = \begin{array}{c} \\ e_{11} \\ e_{12} \\ C_1 \quad \vdots \\ e_{1m_1} \\ \vdots \\ e_{i1} \\ e_{i2} \\ C_i \quad \vdots \\ e_{im_i} \\ \vdots \\ e_{n1} \\ e_{n_2} \\ C_n \quad \vdots \\ e_{nm_n} \end{array} \begin{array}{c} \begin{array}{cccccc} C_1 & \cdots & C_j & \cdots & C_n \end{array} \\ \begin{array}{cccccc} e_{11}\ldots e_{1m_1} & \cdots & e_{j1}\ldots e_{jm_j} & \cdots & e_{n1}\ldots e_{nm_n} \end{array} \\ \begin{bmatrix} \boldsymbol{W}_{11} & \cdots & \boldsymbol{W}_{1j} & \cdots & \boldsymbol{W}_{1n} \\ \vdots & & \vdots & & \vdots \\ \boldsymbol{W}_{i1} & \cdots & \boldsymbol{W}_{ij} & \cdots & \boldsymbol{W}_{in} \\ \vdots & & \vdots & & \vdots \\ \boldsymbol{W}_{n1} & \cdots & \boldsymbol{W}_{nj} & \cdots & \boldsymbol{W}_{nn} \end{bmatrix} \end{array} \tag{7}$$

where C_n denotes the nth cluster, e_{nm} denotes the mth criterion in the nth cluster, and $\boldsymbol{W}_{ij}$ is the principal eigenvector of the influence of the criteria in the jth cluster compared to the ith cluster. In addition, if the jth cluster has no influence on the ith cluster, then $\boldsymbol{W}_{ij} = [0]$.

Step 6: *Obtain the weighted supermatrix by multiplying the normalized matrix, which is derived according to the NRM from DEMATEL.* Normalization is used to derive the weighted supermatrix by transforming each column to sum exactly to unity. The step is similar to the Markov chain concept for ensuring that the sum of the probabilities of all states equals 1 [9]. In traditional ANP, normalization is done by dividing each criterion in a column by the number of clusters so that each column will sum to unity exactly. This implicitly assumes that each cluster is given the same weight. However, we know that the effect that a cluster has on the other clusters may be different in size. Thus, the assumption of equal weight for each cluster in obtaining the weighted supermatrix is not a reasonable one in traditional ANP, and DEMATEL is used to help relax this assumption by influential weights. First, we use the DEMATEL method (Section 3.1) to derive the NRM. Next, this study uses the total influence matrix $\boldsymbol{T}$ and a threshold value α to generate a new matrix (here, we can select to set α or not). Note that α is decided by the decision-makers or experts. If the values in matrix $\boldsymbol{T}$ are less than α, then the values of the clusters in matrix $\boldsymbol{T}$ are reset to zero. Namely, they have a lower influence on other clusters if their values are less than α. The new matrix with $\alpha-$ cut is called the $\alpha-$ cut total influence matrix $\boldsymbol{T}_\alpha$.

$$\boldsymbol{T}_\alpha = \begin{bmatrix} t_{11}^\alpha & \cdots & t_{1j}^\alpha & \cdots & t_{1n}^\alpha \\ \vdots & & \vdots & & \vdots \\ t_{i1}^\alpha & \cdots & t_{ij}^\alpha & \cdots & t_{in}^\alpha \\ \vdots & & \vdots & & \vdots \\ t_{n1}^\alpha & \cdots & t_{nj}^\alpha & \cdots & t_{nn}^\alpha \end{bmatrix} \rightarrow d_i = \sum_{j=1}^{n} t_{ij}^\alpha$$

where if $t_{ij} < \alpha$, then $t_{ij}^\alpha = 0$, else $t_{ij}^\alpha = t_{ij}$, and t_{ij} is in the total influence matrix $\boldsymbol{T}$. The α-cut total influence matrix $\boldsymbol{T}_\alpha$ needs to be normalized by dividing the elements in row i by $d_i = \sum_{j=1}^{n} t_{ij}^\alpha$. Therefore, the normalized α-cut total influence matrix is represented as $\boldsymbol{T}_s$.

$$\mathbf{T}_s = \begin{bmatrix} t_{11}^\alpha/d_1 & \cdots & t_{1j}^\alpha/d_1 & \cdots & t_{1n}^\alpha/d_1 \\ \vdots & & \vdots & & \vdots \\ t_{i1}^\alpha/d_i & \cdots & t_{ij}^\alpha/d_i & \cdots & t_{in}^\alpha/d_i \\ \vdots & & \vdots & & \vdots \\ t_{n1}^\alpha/d_n & \cdots & t_{nj}^\alpha/d_n & \cdots & t_{nn}^\alpha/d_n \end{bmatrix} = \begin{bmatrix} t_{11}^s & \cdots & t_{1j}^s & \cdots & t_{1n}^s \\ \vdots & & \vdots & & \vdots \\ t_{i1}^s & \cdots & t_{ij}^s & \cdots & t_{in}^s \\ \vdots & & \vdots & & \vdots \\ t_{n1}^s & \cdots & t_{nj}^s & \cdots & t_{nn}^s \end{bmatrix} \tag{8}$$

The normalized matrix $\boldsymbol{T}_s$ and the unweighted supermatrix $\boldsymbol{W}$ are used according to Eq. (9) to obtain the weighted supermatrix $\boldsymbol{W}_w$.

$$\boldsymbol{W}_w = \begin{bmatrix} t_{11}^s \times \boldsymbol{W}_{11} & t_{21}^s \times \boldsymbol{W}_{12} & \cdots & \cdots & t_{n1}^s \times \boldsymbol{W}_{1n} \\ t_{12}^s \times \boldsymbol{W}_{21} & t_{22}^s \times \boldsymbol{W}_{22} & \vdots & & \vdots \\ \vdots & \cdots & \cdots & \cdots & t_{ni}^s \times \boldsymbol{W}_{in} \\ \vdots & & \vdots & & \vdots \\ t_{1n}^s \times \boldsymbol{W}_{n1} & t_{2n}^s \boldsymbol{W}_{n2} & \cdots & \cdots & t_{nn}^s \times \boldsymbol{W}_{nn} \end{bmatrix} \tag{9}$$

Step 7: *Calculate the overall priorities with the limiting supermatrix.* The weighted supermatrix $\boldsymbol{W}_w$ is multiplied with itself multiple times to obtain the limiting supermatrix (limiting weighted supermatrix). In other words, the weighted supermatrix is raised to the gth power until the supermatrix has converged and has become a stable supermatrix in order to obtain the global priority-influential vectors, also called the ANP weights.

$$\boldsymbol{W}^* = \lim_{g\to\infty}(\boldsymbol{W}_w)^g \tag{10}$$

The ANP weights for each criterion can be obtained by $\lim_{g\to\infty}(\boldsymbol{W}_w)^g$, where g represents any number of power.

In brief, the overall weights are calculated by using the above steps to derive a stable limiting supermatrix. Therefore, a hybrid model combining DEMATEL and ANP can deal with the problem of interdependence and feedback. The proposed model described above is more suitable for dealing with real-world applications than the traditional method.

3.3. VIKOR method

The compromise ranking method (VIKOR) was proposed by Opricovic as an MCDM method that helps a decision-maker rank a number of choices or alternatives by looking at their performance scores with respect to a set of criteria [26]. Let $k = 1, 2, \ldots, m$ and $A_1, A_2, \ldots, A_k, \ldots, A_m$ denote the m alternatives facing a decision-maker. Let $j = 1, 2, \ldots, n$, with n being the number of criteria. Then the performance score for alternative A_k with respect to the jth criterion is denoted by f_{kj}. Let w_j be the weight on the jth criterion which expresses the relative importance of that criterion (here, weight w_j is derived using DEMATEL and ANP as described earlier). VIKOR uses the following L_p-*metric*:

$$L_k^p = \left\{ \sum_{j=1}^{n} [w_j(|f_j^* - f_{kj}|)/(|f_j^* - f_j^-|)]^p \right\}^{1/p} \tag{11}$$

where $1 \leqslant p \leqslant \infty$; $k = 1, 2, \ldots, m$. In the traditional approach, the positive ideal point with respect to the jth criterion is defined empirically as the highest performance score with respect to the jth criterion among all alternatives or $f_j^* = \max_k f_{kj}$. Likewise, the negative ideal point with respect to the jth criterion is defined empirically as the lowest performance score with respect to the jth criterion among all alternatives or $f_j^- = \min_k f_{kj}$. Of course, instead of empirically searching for the highest and lowest performance scores, we can also set the positive ideal point as the best/aspired level f_j^* in theory and the negative ideal point as the worst value f_j^- in theory. Alternatively, if we flip the range of the scores for f_{kj} so that the aspired level takes a value of 0 and the worst value takes the value of 10, we can define $f_j^* = 0$ and $f_j^- = 10$. This alternative definition would be more appropriate in our empirical analysis of information security risk in real world, with a normalized scale of 0 denoting the best value with no risk gap and a normalized scale of 1 denoting the worst value with the largest risk gap. But in what follows we will revert to the traditional approach in our exposition. The VIKOR method also uses $L_k^{p=1}$ (as S_k) and $L_k^{p=\infty}$ (as Q_k) to formulate the ranking measure [26–29,40,41].

$$S_k = L_k^{p=1} = \sum_{j=1}^{n} [w_j(|f_j^* - f_{kj}|)/(|f_j^* - f_j^-|)] \tag{12}$$

$$Q_k = L_k^{p=\infty} = \max_j \{w_j(|f_j^* - f_{kj}|)/(|f_j^* - f_j^-|) | j = 1, 2, \cdots, n\} \tag{13}$$

$$R_k = v(S_k - S^*)/(S^- - S^*) + (1 - v)(Q_k - Q^*)/(Q^- - Q^*) \tag{14}$$

where $S^* = \min_k S_k$, $S^- = \max_k S_k$, $Q^* = \min_k Q_k$, $Q^- = \max_k Q_k$, and $0 \leqslant v \leqslant 1$, with v as the weight on the strategy of maximum group utility (average gap in scale normalization) and $1 - v$ as the weight on individual regret (maximal gap in special criterion for priority improvement).

VIKOR ranks the alternatives by sorting the values of S_k, Q_k *and* R_k, for $k = 1, 2, \ldots, m$, in decreasing order. Opricovic [26] and Opricovic and Tzeng [27] propose as a compromise the alternative ($A^{(1)}$) which is ranked first by the measure $\min\{R_k | k = 1, 2, \ldots, m\}$ if the following two conditions are satisfied:

- **H1**. *Acceptable advantage*: $R(A^{(2)}) - R(A^{(1)}) \geqslant 1/(m - 1)$, where $A^{(2)}$ is the alternative in the second position of the ranking list by R; m is the number of alternatives.
- **H2**. *Acceptable stability in decision making*: The alternative $A^{(1)}$ must also be the best when ranked by S_k and/or Q_k, $k = 1, 2, \ldots, m$.

A set of compromise solutions is proposed if one of the above conditions is not satisfied. The set of compromise solutions consists of:

(1) Alternatives $A^{(1)}$ and $A^{(2)}$, if **H1** is satisfied and **H2** is not satisfied.
(2) Alternatives $A^{(1)}, A^{(2)}, \ldots, A^{(M)}$, if **H1** is not satisfied. Note that $A^{(M)}$ is determined by the relation $R(A^{(M)}) - R(A^{(1)}) < 1/(m - 1)$ for maximum M (the positions of these alternatives are close).

The compromise solution $\min_k L_k^p$ will be chosen because its value is closest to the ideal/aspired level. In addition, when p is small, group utility is emphasized (such as $p = 1$) and as p increases to $p = \infty$, the individual maximal regrets/gaps receive more importance, as shown by Freimer and Yu [5] and Yu [45]. Therefore, $\min_k S_k$ emphasizes the maximum group utility, whereas $\min_k Q_k$ emphasizes selecting the minimum of the maximum of individual regrets. Based on the above concepts, the compromise ranking algorithm VIKOR is modified by the following steps (for detailed steps see [31] and it is called VIKORRUG (**VIKOR** for **R**anking **U**nimproved **G**ap)).

Step 8: *Normalize the original rating matrix.* In this step, we determine the best f_j^* and the worst f_j^- values of all criterion functions, $j = 1, 2, \ldots, n$. In traditional VIKOR method, we define $f_j^* = \max_k f_{kj}$ and $f_j^- = \min_k f_{kj}$. However, in order to fit an IT managers' needs in the real world, it would be more suitable to define the f_j^* and f_j^- values according to their aspired level and tolerable level (the worst value) for improving the gaps of each criterion in each project. In addition, because each project is ranked according to its own criteria, the ideal point (positive ideal point) function and the non-ideal point (negative ideal point) function are expressed as follows:

$f_{kj}^{*} = aspired\_f_{kj} (\text{or } f_{kj}^{*} = aspired\_level)$

$f_{kj}^{-} = tolerable\_f_{kj}, (\text{or } f_{kj}^{-} = tolerable\_level)$

In general, the benefit or cost must be determined according to the expectation of the decision maker for each criterion in each project, and we call the best f_{kj}^{*} the aspired level and the worst f_{kj}^{-} the tolerable level. Moreover, because each project has its own assessing criteria, the weights w_j^k must be normalized under the same project (where $j = 1, 2, \ldots, n_k$, and n_k is the number of criteria in each project), such that the weights would sum up to unity: $\sum_{j=1}^{n_k} w_j^k = 1$. In addition, for each criterion j of each project k, the best f_{kj}^{*} is the aspired/desired level and the worst f_{kj}^{-} is the tolerable level (for example, f_{11} has an aspired/desired level f_{11}^{*}, f_{12} has an aspired/desired level f_{12}^{*}, etc.). The normalized ratings (i.e., the normalized gaps of the performance scores for each criterion) r_{kj} are denoted by:

$$r_{kj} = (|f_{kj}^{*} - f_{kj}|)/(|f_{kj}^{*} - f_{kj}^{-}|) \tag{15}$$

Step 9: *Compute the values* S_k and Q_k, $k = 1, 2, \ldots, m$, with the following:

$$S_k = \sum_{j=1}^{n} w_j^k r_{kj} \tag{16}$$

$$Q_k = \max_j \{r_{kj} | j = 1, 2, \ldots, n\} \tag{17}$$

where Eq. (16) and (17) show the mean of group utility and maximal regret, respectively. In traditional VIKOR, Q_k is defined as $\max_j \{w_j^k r_{kj} | j = 1, 2, \ldots, n\}$, which implies that group utility is more important than maximal individual regret. Since the individual is part of the group, Q_k is only a part of S_k, and S_k is larger than Q_k. Therefore,S_k is emphasized more than Q_k in traditional VIKOR. However, the maximal individual regret (gap) is also very important in practice and is usually taken into account to reflect its importance. In order to balance S_k and Q_k, Eq. (17) is used to define our Q_k instead of the definition used in traditional VIKOR.

Step 10: *Compute the index values* R_k *by Eq.* (14). Eq. (14) can also be rewritten as $R_k = vS_k + (1 - v)Q_k$ (Here, $S^{*} = Q^{*} = 0$ (the best/aspired level is no risk in our case example), and $S^{-} = Q^{-} = 1$ (the worst value) are set, then $R_k = vS_k + (1 - v)Q_k$).

Step 11: *Rank the alternatives by sorting on the values of* S_k, Q_k *and* R_k, *for* $k = 1, 2, \ldots, m$, *in decreasing order* (refer to the VIKOR method).

The VIKORRUG method determines the compromise solution; the obtained compromise solution is acceptable to the decision-makers because it provides maximum group utility for the majority (represented by min S, Eq. (16)), and a minimum individual maximal regret for the opponent (represented by min Q, Eq. (17)). Our model uses DEMATEL and ANP in Sections 3.1 and 3.2 to obtain the criteria weights with dependence and feedback and uses the VIKORRUG method to obtain the compromise solution.

4. Empirical case: information security risk controls assessment

In this section, we will provide an empirical case to demonstrate the proposed method. In what follows we will discuss the background, the nature of the problem, and the assessment processes respectively.

4.1. Background and problem statements

The Taiwanese government promotes the use of computers and the internet to provide innovative services and improve service efficiency. In January 2001, the government launched the National Information and Communication Security Taskforce [23]. Its primary intention was to set up an integrated information-and-communication-security defense system for the thousands of departments in the government bureaucracy. It has also enforced strict controls on major national infrastructure-information systems that affect national security and social stability. Its preliminary goal has been to achieve the aspired security levels. In 2002, the government expedited an information-security project throughout the government bureaucracy [2]. The project proposed the level of information-security, which was divided into four levels—A, B, C, and D—according to the sizes of the departments, authorized tasks, and the amount of investments. For example, level A represents primary core units; level B represents secondary units; and so on. Different levels within the bureaucracy have different requirements for information-security protection. These government organizations must adjust their information security managements to meet their information security level. They need to check their information security controls regularly to ensure the safety of their information assets. However, since there are a large number of information security controls, the decision-makers usually do not know which control areas and control objectives should be improved. The evaluation and prioritization of these control areas and control objectives constitute an MCDM problem. In fact, MCDM methods can help the IT managers rank the unimproved gaps in these control areas and control objectives. This paper proposes an ISRCAM, which uses a compromise-ranking algorithm—VIKOR for Ranking Unimproved Gap or VIKORRUG, to aggregate the unimproved gaps in terms of the controls for upper-level control objectives and control areas. Moreover, this method considers the dependency among the control areas and control objectives by combining ANP and DEMATEL to obtain the

weights of the control areas for VIKORRUG. Our method can help uncover gaps in the control areas. This will help IT managers diagnose the information security problem by pointing out which control objectives (or control areas) need to be strengthened and improved. Thus, our MCDM method can help IT managers effectively and efficiently manage the information security controls in their respective organizations.

4.2. Generating evaluative criteria and collection of data and weights

To implement a successful ISRCAM, we adopt the audit items from Taiwan's Research Development and Evaluation Commission (RDEC) in designing the information security risk control assessment aspects/objectives/criteria of this study. Since ISO/IEC 17799 (ISO 27002) is widely used to improve security controls and processes [33], we take the audit-items from ISO/IEC 17799 (BS 7799-1) as our list of best practices for control objectives and controls. This list includes the following 11 control areas for information security management: (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 [12,13]. The structure of this research is presented in Fig. A1 (Appendix A). In Fig. A1, the overall risk-control assessment at Level 1 is listed. There are two subgoals in Level 2: organizational/management and operational/technical criteria, which are referred to by René [33] and the NIST [24], and the two subgoals are classified after experienced audits. There are 11 aspects in Level 3: the 11 aspects are taken from Annex A of ISO/IEC 27001 (BS 7799-2). In Level 4, there are 39 main security objectives (categories) in Annex A of ISO/IEC 27001 (BS 7799-2). In Level 5, there are 197 criteria (risk controls), as collected from the RDEC (in Taiwan). The RDEC-proposed audit items are mostly taken from BS 7799. In this case, two unsuitable controls were omitted based on the needs and situations of the organization with reference to information security.

The above subgoals/aspects/objectives/criteria are used to design the three questionnaires. The first phase of our research investigates the interrelations of the aspects (control areas) and subgoals according to the viewpoints of the information-security auditors and the maintenance staff in this case. In the questionnaires, a scale of 0, 1, 2, 3, 4, and 5 represents the range from "no influence" to "very high influence", with respondents proposing the degree of direct influence that each aspect/subgoal exerts on another aspect/subgoal (13 questionnaires were returned with their consensus values less than 5%). The data from the questionnaires are used in DEMATEL. The second phase of our research investigates the grades of importance of the subgoals/aspects/objectives (weights) according to the above-mentioned auditors and maintenance staff (13 questionnaires were returned, their consensuses are less than 5%). Here, a scale of 0, 1, 2, . . ., and 5 represents the range from "absolutely unimportant" to "absolutely important". The corresponding data are used in ANP. The other questionnaire is designed to investigate the performances of the implemented controls by using a scale of 0, 1, 2,. . ., and 10 to represent the range from "the worst" to "the best". In addition, it also investigates the probability of the occurrence of a security breach (P) and the consequence of the occurrence of a security breach (C) under each information-security-risk-control objective after its controls are implemented; and the probability is divided into 7 categories, from "very strongly low" to "very strongly high". This questionnaire was completed by the maintenance staff in this case. The residual risk value of each control objective is obtained using Eq. (A.1) (Appendix B, that is, the range of risk (R) is from 1 to 49). Then, the VIKORRUG method (here, the minimal risk value of 1 is the best f_{kj}^{*} in risk and the maximum risk value of 49 is the worst f_{kj}^{-} in risk) is used to obtain the ranking of the control areas (upper level) from these control objectives (lower level). The steps detailed in Section 3 are used to obtain the risk-control-assessment values (called the gaps of the implemented control areas/objectives) and the residual risk values under each control area and control objective. These steps are described in more detail in the following section.

4.3. Operations and results

The network structure is constructed by using the DEMATEL procedures (in Section 3), that is, from Steps 1 to 3 of DEMATEL to obtain the total influence matrix $\boldsymbol{T}$ for the subgoals, as shown in Table 1. Using Step 4, if a threshold value of 0.1 is chosen, then the resulting NRM is shown in Fig. 4. Similarly, using Steps 1 to 4, the total influence matrix $\boldsymbol{T}$ and the NRM of the aspects (control areas) of the two subgoals are obtained. The components of the total influence matrix $\boldsymbol{T}$ are listed in Tables 2 and 3, and they indicate that all aspects are interdependent. In addition, using Eqs. (5) and (6), the sums of the influence given and received by each dimension can be obtained as shown in Tables 4–6.

Tables 4–6 generate the causal diagram of the total relationship presented in Fig. A2 (Appendix A). In the upper panel of Fig. A2, "C_1 Security policy" is the first in the index of strength of influence given and received, "C_{10} Business continuity management" is next, and "C_2 Organization of information security" is the third in Subgoal G_1 (organizational/management). In

Table 1
The total influence matrix $\boldsymbol{T}$ for the subgoals.

Subgoals	G_1	G_2
G_1	3.52	4.52
G_2	3.52	3.52

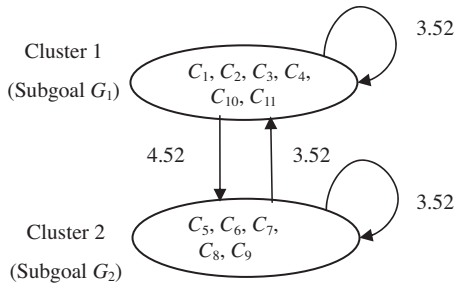

Fig. 4. The structure of subgoals for the empirical case.

Table 2
The total influence matrix ***T*** for the aspects of subgoal G_1.

Aspects	C_1 (e_1)	C_2 (e_2)	C_3 (e_3)	C_4 (e_4)	C_{10} (e_5)	C_{11} (e_6)
C_1 (e_1)	1.31	1.42	1.34	1.41	1.49	1.43
C_2 (e_2)	1.41	1.18	1.26	1.32	1.42	1.34
C_3 (e_3)	1.21	1.15	0.97	1.15	1.22	1.17
C_4 (e_4)	1.21	1.17	1.11	1.02	1.23	1.19
C_{10} (e_5)	1.36	1.29	1.22	1.28	1.20	1.30
C_{11} (e_6)	1.36	1.28	1.20	1.27	1.35	1.14

Table 3
The total influence matrix ***T*** for the aspects of the subgoal G_2.

Aspects	C_5 (e_7)	C_6 (e_8)	C_7 (e_9)	C_8 (e_{10})	C_9 (e_{11})
C_5 (e_7)	1.76	2.15	2.23	2.00	1.96
C_6 (e_8)	2.05	2.09	2.37	2.14	2.10
C_7(e_9)	2.07	2.31	2.16	2.15	2.10
C_8 (e_{10})	1.83	2.06	2.12	1.74	1.87
C_9(e_{11})	1.83	2.06	2.11	1.91	1.71

Table 4
The sum of influences given and received on subgoals.

Subgoals (i)	G_1 Organizational/management	G_2 Operational/technical
$r_i + c_i$	15.09	15.09
$r_i - c_i$	1.00	−1.00

Table 5
The sum of influences given and received on aspects of the subgoal G_1.

Aspects (i)	C_1 (e_1)	C_2 (e_2)	C_3 (e_3)	C_4 (e_4)	C_{10} (e_5)	C_{11} (e_6)
$r_i + c_i$	16.27	15.41	13.96	14.37	15.55	15.18
$r_i - c_i$	0.54	0.44	−0.23	−0.52	−0.25	0.03

Table 6
The sum of influences given and received on aspects of subgoal G_2.

Aspects (i)	C_5 (e_7)	C_6 (e_8)	C_7 (e_9)	C_8 (e_{10})	C_9 (e_{11})
$r_i + c_i$	19.63	21.42	21.79	19.56	19.35
$r_i - c_i$	0.55	0.08	−0.20	−0.31	−0.12

addition, since the values of $r_i - c_i$ for C_1, C_2, and C_{11} aspects are positive, this shows that they affect the other factors more than the other factors affect them in subgoal G_1. Similarly, in the lower panel of Fig. A2, "C_7 access control" is the first in the index of strength of influence given and received, "C_6 communications and operations management" is next, and "C_5 physical and environmental security" is the third in subgoal G_2 (operational/technical). In addition, since the values of $r_i - c_i$ of "C_5

physical and environmental security" and "C_6 communications and operations management" are positive, this shows that they affect the other factors more than the other factors affect them in subgoal G_2. On the other hand, since the values of $r_i - c_i$ of C_7, C_8, and C_9 are negative, this shows that these aspects are influenced by the other factors more than they affect the other factors. Furthermore, the middle panel of Fig. A2 shows that G_1 affects G_2 more than G_2 affects G_1. Subsequently, the total influence matrix $\boldsymbol{T}$ (Table 1) is normalized, as in Table 7.

Using the structure of Fig. 4 and the data computed from the second phase (the grades of importance of the 11 aspects investigated), the unweighted supermatrix can be obtained as follows. Here, e_1, e_2, …, e_{11} represent the control areas in Fig. A1 (Appendix A).

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	
e_1	0.186	0.179	0.157	0.152	0.175	0.187	0.176	0.180	0.174	0.168	0.174	
e_2	0.168	0.198	0.143	0.157	0.164	0.152	0.138	0.152	0.148	0.140	0.162	
e_3	0.155	0.146	0.223	0.146	0.141	0.143	0.188	0.156	0.164	0.162	0.134	
W_{11} e_4	0.155	0.150	0.150	0.220	0.157	0.148	0.148	0.152	0.174	0.178	0.164	W_{13}
e_5	0.166	0.177	0.170	0.159	0.202	0.168	0.184	0.188	0.168	0.184	0.198	
e_6	0.170	0.150	0.157	0.166	0.161	0.202	0.166	0.172	0.172	0.168	0.168	
e_7	0.191	0.191	0.221	0.182	0.182	0.180	0.252	0.170	0.186	0.162	0.168	
e_8	0.202	0.202	0.198	0.193	0.209	0.211	0.196	0.242	0.204	0.194	0.202	
W_{21} e_9	0.214	0.202	0.220	0.234	0.198	0.214	0.212	0.216	0.240	0.208	0.192	W_{23}
e_{10}	0.191	0.184	0.195	0.191	0.193	0.196	0.170	0.186	0.190	0.262	0.176	
e_{11}	0.202	0.221	0.166	0.200	0.218	0.198	0.170	0.186	0.180	0.174	0.262	

Eq. (9) is used to obtain the weighted supermatrix, which is shown as follows:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}
e_1	0.082	0.079	0.069	0.067	0.077	0.082	0.088	0.090	0.087	0.084	0.087
e_2	0.074	0.087	0.063	0.069	0.072	0.067	0.069	0.076	0.074	0.070	0.081
e_3	0.068	0.064	0.098	0.064	0.062	0.063	0.094	0.078	0.082	0.081	0.067
e_4	0.068	0.066	0.066	0.097	0.069	0.065	0.074	0.076	0.087	0.089	0.082
e_5	0.073	0.078	0.075	0.070	0.089	0.074	0.092	0.094	0.084	0.092	0.099
e_6	0.075	0.066	0.069	0.073	0.071	0.089	0.083	0.086	0.086	0.084	0.084
e_7	0.107	0.107	0.124	0.102	0.102	0.101	0.126	0.085	0.093	0.081	0.084
e_8	0.113	0.113	0.111	0.108	0.117	0.118	0.098	0.121	0.102	0.097	0.101
e_9	0.120	0.113	0.123	0.131	0.111	0.120	0.106	0.108	0.120	0.104	0.096
e_{10}	0.107	0.103	0.109	0.107	0.108	0.110	0.085	0.093	0.095	0.131	0.088
e_{11}	0.113	0.124	0.093	0.112	0.122	0.111	0.085	0.093	0.090	0.087	0.131

Next, the limiting supermatrix $\boldsymbol{W}^*$ is obtained by using Eq. (10), which is shown below:

$$\boldsymbol{W}^* = \begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \\ e_9 \\ e_{10} \\ e_{11} \end{array} \begin{array}{c} \begin{array}{ccccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} & e_{11} \end{array} \\ \begin{bmatrix} 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 \\ 0.073 & 0.073 & 0.073 & 0.073 & 0.073 & 0.073 & 0.073 & 0.073 & 0.073 & 0.073 & 0.073 \\ 0.075 & 0.075 & 0.075 & 0.075 & 0.075 & 0.075 & 0.075 & 0.075 & 0.075 & 0.075 & 0.075 \\ 0.077 & 0.077 & 0.077 & 0.077 & 0.077 & 0.077 & 0.077 & 0.077 & 0.077 & 0.077 & 0.077 \\ 0.085 & 0.085 & 0.085 & 0.085 & 0.085 & 0.085 & 0.085 & 0.085 & 0.085 & 0.085 & 0.085 \\ 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 \\ 0.100 & 0.100 & 0.100 & 0.100 & 0.100 & 0.100 & 0.100 & 0.100 & 0.100 & 0.100 & 0.100 \\ 0.108 & 0.108 & 0.108 & 0.108 & 0.108 & 0.108 & 0.108 & 0.108 & 0.108 & 0.108 & 0.108 \\ 0.113 & 0.113 & 0.113 & 0.113 & 0.113 & 0.113 & 0.113 & 0.113 & 0.113 & 0.113 & 0.113 \\ 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 \\ 0.104 & 0.104 & 0.104 & 0.104 & 0.104 & 0.104 & 0.104 & 0.104 & 0.104 & 0.104 & 0.104 \end{bmatrix} \end{array} \tag{18}$$

Table 7
The normalized matrix $\boldsymbol{T}_s$ on $\boldsymbol{T}$.

Subgoals	G_1	G_2
G_1	0.44	0.56
G_2	0.50	0.50

Finally, using the range of ratings for each criterion (control) as 0 (the worst value) to 10 (the best value), the performance ratings of controls (lower level) are integrated by arithmetic average for the upper-level objectives (upper level). Similarly, the ratings of the control objectives (lower level) are integrated for the control areas (upper level). Because the dependence and feedback of aspects (control areas) are involved, the weights of the aspects (from Eq. (18)) are used to calculate the integrated ratings of aspects. The integrated ratings of the objectives and weights are listed in Table 8. Then, the VIKORRUG method (Section 3.3) is used to obtain the ranking index S_k, Q_k, and $\boldsymbol{R}_k$ of the subgoals, as presented in Table 9 (Here, if both maximum group utility and minimum individual regret are considered simultaneously, then $v = 0.5$ is selected).

As shown in Table 8, among the 11 aspects, "C_8 information systems acquisition, development and maintenance" is the farthest from the ideal/aspired level (because its normalized/ local/global ratings are the highest than the others, it shows the unimproved gap is the biggest), whereas "C_1 security policy" is the closest to the ideal/aspired level in both normalized and local ratings (which concerns their corresponding weights). Here, the questionnaire asks respondents to rate the performances of the implemented controls on a scale of 0, 1, 2,. . ., and 10, with the ideal/aspired level being 10. Therefore, "information systems acquisition, development and maintenance" should be improved in this case. Currently, government agencies outsource many of their information systems.

The results in Table 9 show that $S_{G_2} > S_{G_1}$, $Q_{G_2} > Q_{G_1}$, and $R_{G_2} > R_{G_1}$; in addition, the ranks of the subgoals are $G_1 \succ G_2$. Here, these subgoals only satisfy condition **H2**, which represent an acceptable stability. Therefore, the set of compromise solutions is $\{G_1, G_2\}$. Since our research aims to find the worst between the two subgoals, G_2 should be prioritized for improvement when a subgoal is selected. In addition, the overall performance score of the risk controls is 0.329 (The calculation is shown under the notes in Table 9). Simultaneously, this study also uses the revised VIKOR (VIKORRUG) to calculate the residual risk value of each subgoal from their control areas (the minimal risk value of 1 is the best risk f_{kj}^{*}, and the maximum risk value of 49 is the worst risk f_{kj}^{-}). The results are listed in Tables 10 and 11.

Table 11 shows that the risk of operational/technical subgoals is higher than the risk of the subgoal organizational/management. Table 10 shows that, among the 11 aspects, "C_8 information systems acquisition, development and maintenance" is the farthest from the ideal/aspired level (that is, its risk is the highest among the 11 aspects), whereas "C_{11} compliance" is the closest to the ideal/aspired level (that is, its risk is the lowest among others) in both normalized and local ratings (which comprise the ratings with the weights).

In sum, this study finds that the aspect "C_8 information systems acquisition, development and maintenance" has the highest risk and should be improved among the 11 aspects considered in this case. In addition, "operational/technical (G_2)" involves a risk greater than the risk of "organizational/management (G_1)", with the performance of the subgoal "operational/technical" also being lower than the performance of "organizational/management". Therefore, the subgoal "operational/technical" should be improved, and the aspect "C_8 information systems acquisition, development and maintenance" should be given priority for improvement. When most Taiwanese government's information systems are outsourced, it is crucial for information security related requirements to be included in these outsourcing contracts.

5. Discussion

In order to illustrate that the method proposed in this research is better than the traditional methods, we also calculate the limiting supermatrix using the traditional normalization method; the result is as follows.

$$\boldsymbol{W}_{\mathbf{f}} = \begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \\ e_9 \\ e_{10} \\ e_{11} \end{array} \begin{array}{c} \begin{array}{ccccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} & e_{11} \end{array} \\ \begin{bmatrix} 0.087 & 0.087 & 0.087 & 0.087 & 0.087 & 0.087 & 0.087 & 0.087 & 0.087 & 0.087 & 0.087 \\ 0.078 & 0.078 & 0.078 & 0.078 & 0.078 & 0.078 & 0.078 & 0.078 & 0.078 & 0.078 & 0.078 \\ 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 & 0.080 \\ 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 & 0.082 \\ 0.089 & 0.089 & 0.089 & 0.089 & 0.089 & 0.089 & 0.089 & 0.089 & 0.089 & 0.089 & 0.089 \\ 0.084 & 0.084 & 0.084 & 0.084 & 0.084 & 0.084 & 0.084 & 0.084 & 0.084 & 0.084 & 0.084 \\ 0.094 & 0.094 & 0.094 & 0.094 & 0.094 & 0.094 & 0.094 & 0.094 & 0.094 & 0.094 & 0.094 \\ 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 & 0.103 \\ 0.107 & 0.107 & 0.107 & 0.107 & 0.107 & 0.107 & 0.107 & 0.107 & 0.107 & 0.107 & 0.107 \\ 0.097 & 0.097 & 0.097 & 0.097 & 0.097 & 0.097 & 0.097 & 0.097 & 0.097 & 0.097 & 0.097 \\ 0.099 & 0.099 & 0.099 & 0.099 & 0.099 & 0.099 & 0.099 & 0.099 & 0.099 & 0.099 & 0.099 \end{bmatrix} \end{array}$$

Table 8
The weights and the integrated performance ratings for the empirical case.

Subgoals (k)	Using ANP			Using VIKORRUG		
Aspects (j)	Local weights (w_j^k)	Global weights ($^g w_j^k$)	Integrated performance ratings	Normalized ratings (r_{kj})	Local ratings $w_j^k r_{kj}$	Global ratings $^g w_j^s r_{kj}$
Organizational/management	**0.472**		**7.833**	**0.217**	**0.217**	**0.103**
C_1 Security policy (e_1)	0.174	0.082	8.688	0.131[a]	0.023[a]	0.011[a]
C_2 Organization of information security (e_2)	0.155	0.073	7.875	0.213	0.033	0.016
C_3 Asset management (e_3)	0.159	0.075	6.667	0.333	0.053	0.025
C_4 Human resources security (e_4)	0.163	0.077	7.433	0.257	0.042	0.020
C_{10} Business continuity management (e_5)	0.180	0.085	8.000	0.200	0.036	0.017
C_{11} Compliance (e_6)	0.169	0.080	8.217	0.178	0.030	0.014
Operational/technical	**0.528**		**7.639**	**0.236**	**0.235**	**0.125**
C_5 Physical and environmental security (e_7)	0.189	0.100	8.638	0.136	0.026	0.014
C_6 Communications and operations management (e_8)	0.205	0.108	8.239	0.176	0.036	0.019
C_7 Access control (e_9)	0.214	0.113	8.248	0.175	0.037	0.020
C_8 Information systems acquisition, development and maintenance (e_{10})	0.195	0.103	4.806	0.519[b]	0.101[b]	0.053[b]
C_9 Information security incident management (e_{11})	0.197	0.105	8.200	0.180	0.035	0.019

[a] The closest to the ideal/aspired level.
[b] The farthest from the ideal/aspired level.

Table 9
The ranking indexes of performances for the empirical case.

Subgoals (k)	S_k ($v = 1.0$)	Q_k ($v = 0.0$)	R_k ($v = 0.5$)
Organizational/management (G_1)	0.217	0.333	0.275
Operational/technical (G_2)	0.235	0.519	0.377

Note: The overall performance score of the risk controls = $\sum_k w^k R_k = 0.472 \times 0.275 + 0.528 \times 0.377 = 0.329$ (where the R_k of G_1 and G_2 are obtained by using the revised VIKOR and $v = 0.5$,they are 0.275 and 0.377, respectively; 0.472 and 0.528 are the local weight using ANP from Table 8).

Table 10
The weights and the integrated risk ratings for the empirical case.

Subgoals (k)	Using ANP			Using VIKORRUG		
Aspects (j)	Local Weights (w_j^k)	Global weights ($^g w_j^k$)	Integrated risk ratings	Normalized ratings (r_{kj})	Local ratings $w_j^k r_{kj}$	Global ratings $^g w_j^k r_{kj}$
Organizational/management	**0.472**		**7.853**	**0.143**	**0.143**	**0.067**
C_1 Security policy (e_1)	0.174	0.082	7.00	0.125	0.022	0.010[a]
C_2 Organization of information security (e_2)	0.155	0.073	8.75	0.161	0.025	0.012
C_3 Asset management (e_3)	0.159	0.075	8.00	0.146	0.023	0.011[a]
C_4 Human resources security (e_4)	0.163	0.077	8.67	0.160	0.026	0.012
C_{10} Business continuity management (e_5)	0.180	0.085	8.00	0.146	0.026	0.012
C_{11} Compliance (e_6)	0.169	0.080	6.83	0.122[a]	0.021[a]	0.010[a]
Operational/technical	**0.528**		**11.861**	**0.226**	**0.226**	**0.120**
C_5 Physical and environmental security (e_7)	0.189	0.100	13.50	0.260	0.049	0.026
C_6 Communications and operations management (e_8)	0.205	0.108	10.35	0.195	0.040	0.021
C_7 Access control (e_9)	0.214	0.113	9.93	0.186	0.040	0.021
C_8 Information systems acquisition, development and maintenance (e_{10})	0.195	0.103	13.83	0.267[b]	0.052[b]	0.028[b]
C_9 Information security incident management (e_{11})	0.197	0.105	12.00	0.229	0.045	0.024

[a] The closest to the ideal/aspired level.
[b] The farthest from the ideal/aspired level.

This study further analyses the weights obtained using both the proposed model and traditional methods, and the results are shown in Table 12 and Fig. 5, respectively.

Table 11
The ranking indexes of risk for the empirical case.

Subgoals (k)	S_k ($v = 1.0$)	Q_k ($v = 0.0$)	R_k ($v = 0.5$)
Organizational/management (G_1)	0.143	0.161	0.152
Operational/technical (G_2)	0.226	0.267	0.247

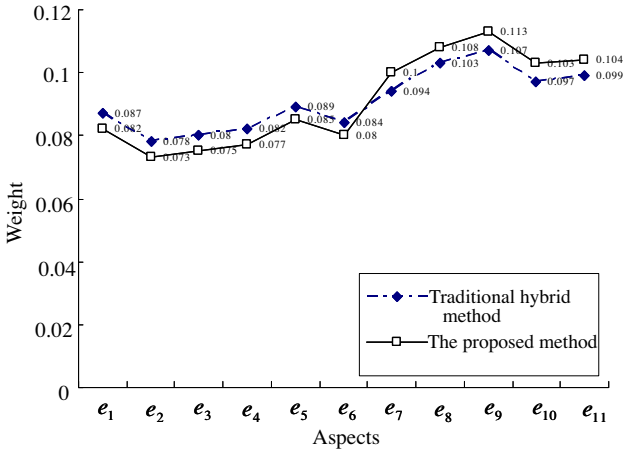

Fig. 5. Comparisons of the weights of each criterion between the traditional hybrid method and herein-proposed method.

Table 12
Comparisons of the weights of each criterion between the traditional hybrid method and the herein-proposed method.

Criteria	Traditional method	The proposed method	Difference
e_1	0.087	0.082	0.005
e_2	0.078	0.073	0.005
e_3	0.080	0.075	0.005
e_4	0.082	0.077	0.005
e_5	0.089	0.085	0.004
e_6	0.084	0.080	0.004
e_7	0.094	0.100	(0.006)[a]
e_8	0.103	0.108	(0.005)[a]
e_9	0.107	0.113	(0.006)[a]
e_{10}	0.097	0.103	(0.006)[a]
e_{11}	0.099	0.104	(0.005)[a]

[a] Parentheses represent negative values.

Several facts are clear from Table 1 and Fig. 4: (a) each cluster has feedback and dependence; (b) the effect of Cluster 1 on Cluster 2 is 4.52, whereas the effect of Cluster 2 on Cluster 1 is 3.52. In other words, the degree to which Cluster 2 is affected is higher (4.52) than that for Cluster 1 (3.52). Therefore, Cluster 2 should be paid more attention than the other clusters in the real world, that is, it should be given additional weight, whereas Cluster 1 should have its weight reduced. Since $e_1, e_2, \ldots, e_6$ belong to Cluster 1 and $e_7, e_8, \ldots, e_{11}$ belong to Cluster 2, these criteria $e_7, e_8, \ldots, e_{11}$ should be paid more attention than $e_1, e_2, \ldots, e_6$. Using the traditional normalization method implies that each cluster has the same weight (each criterion in a column is divided by the number of clusters to normalize the unweighted supermatrix). However, there are different degrees of influence among the clusters of factors/criteria in this empirical case (reference Table 4). Thus, by using DEMATEL to improve the normalization of ANP in the unweighted supermatrix, our study finds these results better suit the real world. In this empirical case, we find that the weights of the criteria $e_1, e_2, \ldots, e_6$ in the traditional method are higher than those in the proposed method, but the weights of the criteria $e_7, e_8, \ldots, e_{11}$ are lower in the traditional method than in the proposed method (Table 12 and Fig. 5). If this research uses the assumption of equal weights for each cluster to normalize the unweighted supermatrix and to obtain the weighted supermatrix, the results of the assessed weights would be higher or lower than the more realistic situation. Fig. 5 shows that the criteria of Cluster 2 ($e_7, e_8, \ldots, e_{11}$) are underestimated, whereas the criteria of Cluster 1 ($e_1, e_2, \ldots, e_6$) are overestimated if this research adopts the traditional method. Therefore, DEMATEL combined with ANP can be used to obtain better and more accurate results in real-world applications.

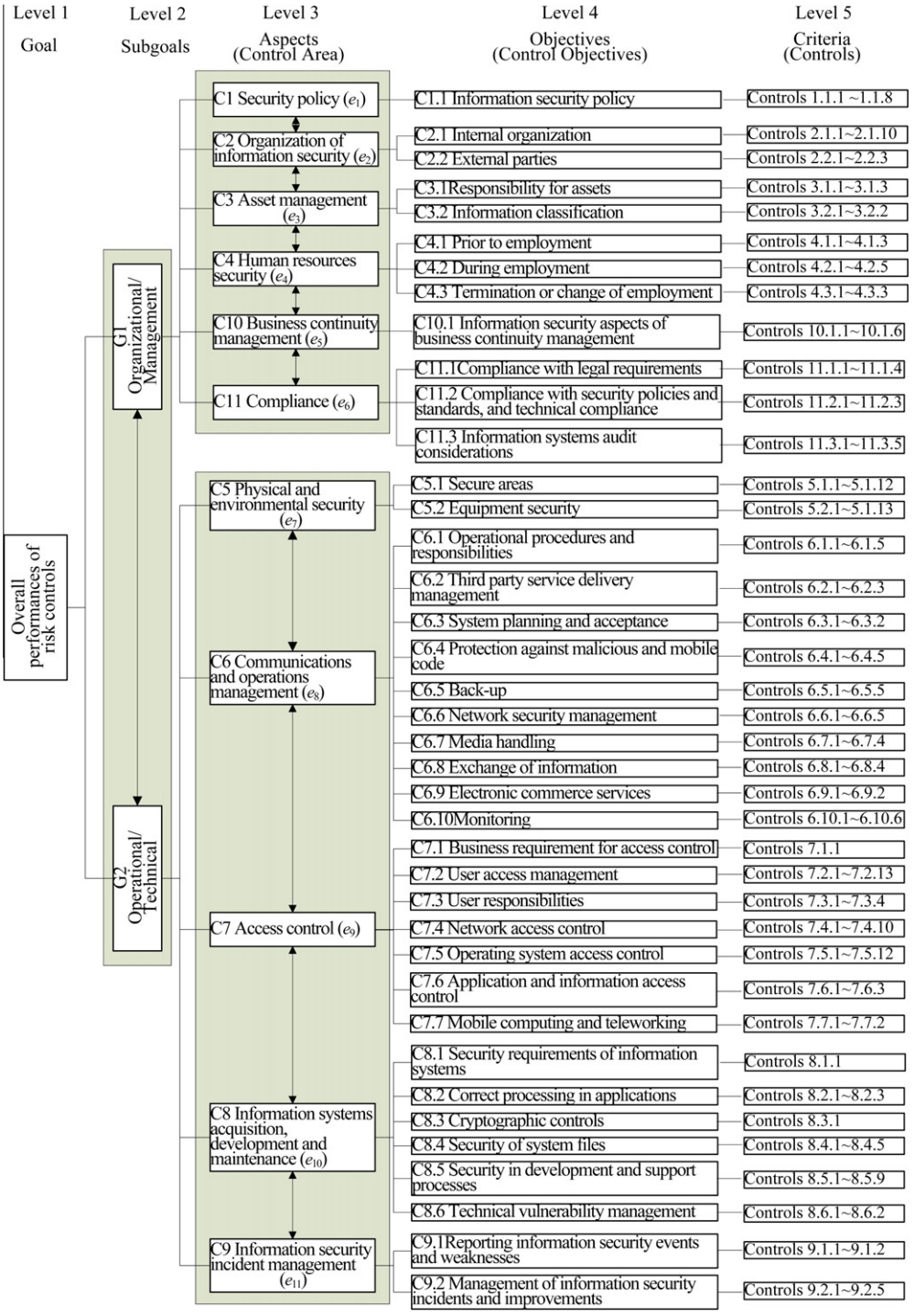

Fig. A1. ISRCS structure for the case governmental agency.

Next, our results show that all aspects (control areas) and subgoals are dependent and relative, according to Tables 1–3. Fig. A2 shows their causal relationship, and it can help managers review the relationships among these control areas. Fig. A2 shows that G_1 affects G_2 more than G_2 affects G_1. G_1 expands its aspects as the upper portion of Fig. A2. For the control areas, the $r_i - c_i$ values for C_1 (security policy), C_2 (organization of information security), and C_{11} (compliance) are positive, which means that they affect other aspects (control areas) more than the other control areas affect them. In other words, when organizations adopt these control areas, "security policy", "organization of information security", and "compliance" will

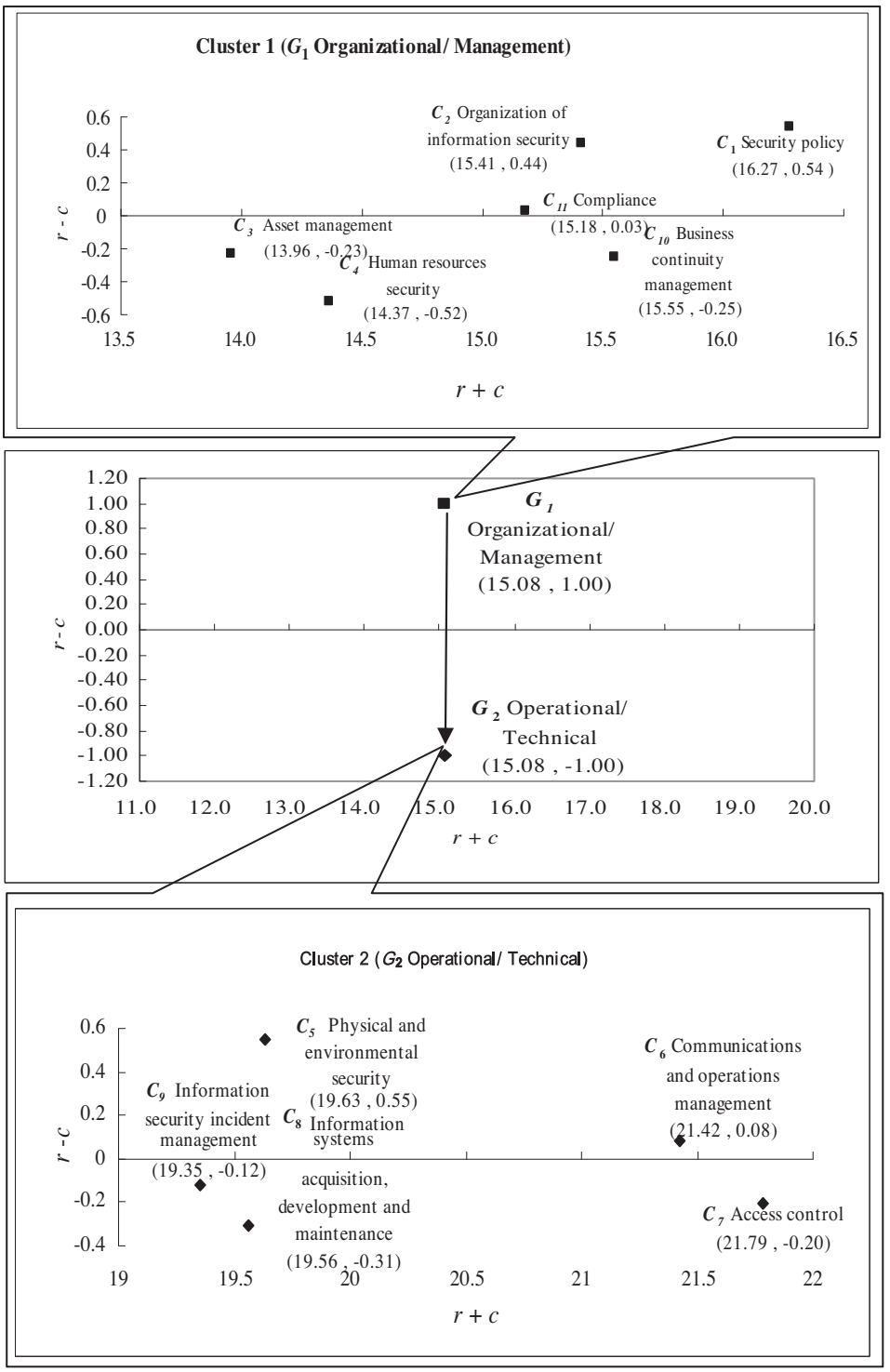

Fig. A2. The causal diagram of total relationship.

affect the success or failure of the other control areas. Similarly, G_2 expands its aspects as the lower portion of Fig. A2. Among the various aspects of G_2, the $r_i - c_i$ values for C_5 (physical and environmental security) and C_6 (communications and operations management) are positive, which means that these two control areas affect the other control areas in the operational/technical subgoal more than the others affect them. Therefore, when organizations adopt these control areas, the areas that can affect others should be adopted first. However, when the organization has adopted controls over a long period,

risk-control assessment should be used to identify the lower performances of controls (control objectives or control areas) that need improvement. Furthermore, when the controls with lower performances are improved, the influencers should also be checked again. For example, "C_8 information systems acquisition, development and maintenance" should be given priority to be improved in this empirical case. However, the influencers C_5 and C_6 within the same cluster and C_1, C_2, and C_{11} in subgoal G_1 (because G_1 affects G_2 more than G_2 affects G_1) should be checked again. Among these, C_5 may need improvement because its risk rating is the second farthest from the ideal/aspired level, as shown in Table 10.

Finally, using the VIKORRUG method aggregates the aspects that have dependence and feedback characteristics to obtain the ranking indexes of performances and risks of the subgoals, as shown in Tables 9 and 11. If we want to maximize group utility and minimize individual regret ($v = 0.5$), the results indicate that $G_1 \succ G_2$. Thus, among the two subgoals, G_1 (organizational/management) is the closest to the ideal/aspired level, whereas G_2(operational/technical) is the farthest from the ideal/aspired level. If managers aim to improve the subgoals according to their performances, then G_2 should be given priority during selection. However, when a manager chooses the subgoal with lower performances for improvement, the influencers among its aspects or subgoals should be considered thoroughly. In Table 4 and Fig. A2, G_1 affects G_2 more than G_2 affects G_1. Therefore, if G_2 is selected for improvement, G_1 should be checked to determine whether it should be improved simultaneously. In general, if G_2 is performing very well, then G_1 will be performing very well too. In this case, if G_2 should be improved, then "C_8 information systems acquisition, development and maintenance" should be improved first, as is clear from Tables 8 and 10. In Table 8, the gaps of the performance rankings are $C_8 > C_3 > C_4 = C_7 > C_9 = C_6 > C_{10} > C_2 > C_5 = C_{11} > C_1$. In Table 10, the gaps of the risk rankings are $C_8 > C_5 > C_9 > C_6 = C_7 > C_2 = C_4 = C_{10} > C_3 > C_1 = C_{11}$. Thus the IT managers should choose the risk controls with lower performances (higher risks) for improvement according to the gaps of performance rankings or risk rankings. In addition, according to the above statements, the influencers C_1, C_2, C_{11}, C_5, and C_6 should be checked (because the $r_i - c_i$ values for C_1, C_2, C_{11}, C_5, and C_6 are positive in Fig. A2, which means that they affect other aspects more than they are being affected). If the IT managers accept the performance and risk of G_1, then the other aspects within the same group—subgoal G_2—such as "C_5 physical and environmental security" and "C_6 communications and operations management" need to be checked. These two aspects should be improved simultaneously because they affect C_8. Especially, "C_5 physical and environmental security" has the second highest risk rating (13.5) in Table 10. In short, these influencers should also be checked again when the controls having lower performance are enhanced. Checking the influencers using the NRM is more comprehensive than the traditional analysis method.

To sum up, the hybrid model that combines DEMATEL with ANP has been widely used in MCDM problems. In this study, the DEMATEL method is used to construct interrelations between criteria/factors, and ANP is used to overcome the problems of dependence and feedback. In addition, this study also shows that using DEMATEL and ANP to normalize the unweighted supermatrix is more reasonable than working by assuming equal weights in each cluster. Furthermore, the weights obtained from the ANP and VIKOR methods are used to derive the ranking index. Our empirical study also shows that this method is more suitable and effective than the traditional ANP method.

6. Conclusions

Because organizations have grown increasingly dependent on their computer-based information systems, information security is becoming very important. Previous researches have proposed information security risk management related issues. PDCA processes are regarded as necessary in information security management. When the "Check Phase" is carried out in an ISMS, ensuring the effectiveness of these implemented controls is important. Therefore, this study proposes an ISRCAM in the Check Phase. Because many studies consider that risk problems are MCDM problems, they adopt the same methods to deal with information-security-risk-related problems.

Among the numerous approaches available for conflict management, MCDM is one of the most prevalent. VIKOR is a method within MCDM; it is based on an aggregating function representing closeness to the ideal, which can be viewed as a derivative of compromise-programming. However, most decision-making methods assume independence between the criteria of a decision and the alternatives of that decision, or simply among either the criteria or the alternatives themselves. However, assuming independence among the criteria/variables is too strict to overcome the problem of dependent criteria in the real world. Therefore, many studies have used ANP to overcome this problem of dependent criteria. In addition, a hybrid model combining ANP and DEMATEL has been widely and successfully used in various fields. The DEMATEL technique is not only used to construct the NRM, but is also used to transform the unweighted supermatrix to a weighted supermatrix. The traditional method overcomes normalization for the weighted supermatrix in the ANP procedure by assuming equal weights for each cluster; however, this ignores the different effects among clusters. Our research uses a new concept to overcome this unreasonable assumption of equal weights. The novel combination model is more suitable than the traditional method to solve problems with different degrees of effects among clusters. This research also uses ANP and VIKOR to obtain the compromise-ranking index. Moreover, an empirical case is used to show the effectiveness and feasibility of our proposed method. In addition, managers should select the unimproved items from the results of the assessment and consider the influencers to improve simultaneously (i.e. those influencers of the aspect that is selected for improvement) through NRM. Our proposed method gives a result that is more comprehensive than the traditional analysis method. Consequently, our proposed method (ISRCAM that is founded on the revised VIKOR based on DEMATEL and ANP) is effective at improving

the compromise-solution method and overcoming the problem of interdependence and feedback among criteria. Furthermore, our proposed method uses NRM, to analyze the results, which is a better way than traditional analysis.

Many uncertain influencers and factors affect risk. Moreover, human beings determine the risk value, risk probability of occurrence of security breach, or the consequence of occurrence of security breach according to their experiences. This implies some subjectivity; accordingly, it would be very appropriate to use the fuzzy concept here. Furthermore, ANP can overcome the problems of interdependence and feedback among criteria. Another method—the fuzzy integral method—can overcome interdependence among criteria. Therefore, when the criteria do not show feedback, the fuzzy integral can also be a very suitable method. Finally, managers should consider the related costs and resources when they implement the controls to reduce risk. How do managers use the lowest cost and the least resources to establish controls to reduce risk to an acceptable level? All these above issues can be investigated in future studies.

Appendix A

Figs. A1, A2

Appendix B

The risk is combination of the probability of an event and its consequence [11,12]. Many studies have introduced the formulas of risk. Several risk formulas are introduced as follows. Firstly, the most popular formula is:

$$R = P \times C \tag{A.1}$$

where R represents "risk", P represents "probability of occurrence of security breach," and C represents "consequence of occurrence of security breach" [14,16,20,25,43].

References

[1] K. Biery, Aligning an information risk management approach to BS 7799-3:2005, SANS Institute InfoSec Reading Room, 2006.
[2] K.J. Farn, S.K. Lin, C.C. Lo, A study on e-Taiwan information system security classification and implementation, Computer Standards & Interfaces 30 (1) (2008) 1–7.
[3] E. Fontela, A. Gabus, DEMATEL, innovative methods, Report no. 2, Structural analysis of the world problematique, Battelle Geneva Research Institute, 1974.
[4] E. Fontela, A. Gabus, The DEMATEL observer, Battelle Institute, Geneva Research Center, 1976.
[5] M. Freimer, P.L. Yu, Some new results on compromise solutions for group decision problems, Management Science 22 (6) (1976) 688–693.
[6] A. Gabus, E. Fontela, World problems an invitation to further thought within the framework of DEMATEL, Battelle Geneva Research Centre, Geneva, Switzerland, 1972.
[7] A. Gabus, E. Fontela, Perceptions of the world problematique: communication procedure, communicating with those bearing collective responsibility (DEMATEL Report No. 1), Battelle Geneva Research Centre, Geneva, Switzerland, 1973.
[8] C.Y. Huang, J.Z. Shyu, G.H. Tzeng, Reconfiguring the innovation policy portfolios for Taiwan's SIP Mall industry, Technovation 27 (12) (2007) 744–765.
[9] J.J. Huang, G.H. Tzeng, C.S. Ong, Multidimensional data in multidimensional scaling using the analytic network process, Pattern Recognition Letters 26 (2005) 755–767.
[10] C.L. Hwang, K. Yoon, Multi-objective Decision Making – Methods and Application – A State-of-the-Art Study, Springer-Verlag, New York, 1981.
[11] ISO/IEC Guide 73, Risk management-vocabulary-guidelines for use in standards, 2002.
[12] ISO/IEC 17799, Information technology-security techniques-code of practice for information security management, 2005.
[13] ISO/IEC 27001, Information technology-security techniques-information security management system-requirements, 2005.
[14] B. Karabacak, I. Sogukpinar, ISRAM: information security risk analysis method, Computers & Security 24 (2) (2005) 147–159.
[15] E.E. Karsak, S. Sozer, S.E. Alptekin, Product planning in quality function deployment using a combined analytic network process and goal programming approach, Computers & Industrial Engineering 44 (1) (2002) 171–190.
[16] A.S. Kirkwood, Why do we worry when scientists say there is no risk? Disaster Prevention and Management 3 (2) (1994) 15–22.
[17] J.W. Lee, S.H. Kim, Using analytic network process and goal programming for interdependent information system project selection, Computers & Operations Research 27 (4) (2000) 367–382.
[18] J.J.H. Liou, G.H. Tzeng, H.C. Chang, Airline safety measurement using a hybrid model, Air Transport Management 13 (4) (2007) 243–249.
[19] F. Liu, K. Dai, Z. Wang, J. Ma, Research on fuzzy group decision making in security risk assessment, Lecture Notes in Computer Science 3421 (2005) 1114–1121.
[20] N. McEvoy, A. Whitcombe, Structured risk analysis, in: InfraSec, LNCS, vol. 2437, 2002, pp. 88–103.
[21] L.M. Meade, A. Presley, R&D project selection using the analytic network process, IEEE Transactions on Engineering Management 49 (1) (2002) 59–66.
[22] J.A. Momoh, J. Zhu, Optimal generation scheduling based on AHP/ANP, IEEE Transactions on Systems, Man and Cybernetics—Part B: Cybernetics 33 (3) (2003) 531–535.
[23] National Information and Communication Security Taskforce (NICST), Background, 2001. <http://www.nicst.nat.gov.tw/content/application/nicst/eng_background/guest-cnt-browse.php?cnt_id=56>.
[24] National Institute of Standards and Technology (NIST), NIST Special Publication 800-53, Information Security, 2005.
[25] National Institute of Standards and Technology (NIST), NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, 2002.
[26] S. Opricovic, Multicriteria optimization of civil engineering systems, Faculty of Civil Engineering, Belgrade, 1998.
[27] S. Opricovic, G.H. Tzeng, Extended VIKOR method in comparison with outranking methods, European Journal of Operational Research 178 (2) (2007) 514–529.
[28] S. Opricovic, G.H. Tzeng, Compromise solution by MCDM methods: a comparative analysis of VIKOR and TOPSIS, European Journal of Operational Research 156 (2) (2004) 445–455.
[29] S. Opricovic, G.H. Tzeng, Multicriteria planning of post-earthquake sustainable reconstruction, Computer-Aided Civil and Infrastructure Engineering 17 (3) (2002) 211–220.
[30] Y.P. Ou Yang, H.M. Shieh, G.H. Tzeng, A VIKOR technique with applications based on DEMATEL and ANP, MCDM 2009, Communications in Computer and Information Science (CCIS), vol. 35, Springer-Verlag, Berlin Heidelberg, 2009, pp.780–799.

[31] Y.P. Ou Yang, H.M. Shieh, J.D. Leu, G.H. Tzeng, A VIKOR-based multiple criteria decision method for improving information security risk, International Journal of Information Technology & Decision Making 8 (2) (2009) 267–287.
[32] Y.P. Ou Yang, H.M. Shieh, J.D. Leu, G.H. Tzeng, A novel hybrid MCDM model combined with DEMATEL and ANP with applications, International Journal of Operations Research 5 (3) (2008) 160–168.
[33] S.G. René, Information security management best practice based on ISO/IEC 17799, Information Management Journal 39 (4) (2005) 60–66.
[34] T.L. Saaty, Decision Making with Dependence and Feedback: Analytic Network Process, RWS Publications, Pittsburgh, 1996.
[35] T.L. Saaty, Fundamentals of the analytic network process, in: International Symposium on the Analytic Hierarchy Process, Kobe, 1999.
[36] T.L. Saaty, The Analytic Hierarchy Process, McGraw-Hill, New York, 1980.
[37] T.L. Saaty, The analytic network process: dependence and feedback in decision making (Part 1): theory and validation examples, SESSION 4B: theory and development of the analytic hierarchy process/analytic network process, in: The 17th International Conference on Multiple Criteria Decision Making, August 6–11, 2004, The Whistler Conference Centre, Whistler, British Columbia, Canada, 2004.
[38] M. Tamura, H. Nagata, K. Akazawa, Extraction and systems analysis of factors that prevent safety and security by structural models, in: 41st SICE Annual Conference, Osaka, Japan, 2002.
[39] U.R. Tuzkaya, S. Önüt, A fuzzy analytic network process based approach to transportation-mode selection between Turkey and Germany: a case study, Information Sciences 178 (15) (2008) 3133–3146.
[40] G.H. Tzeng, M.H. Teng, J.J. Chen, S. Opricovic, Multicriteria selection for a restaurant location in Taipei, International Journal of Hospitality Management 21 (2) (2002) 171–187.
[41] G.H. Tzeng, C.W. Lin, S. Opricovic, Multi-criteria analysis of alternative-fuel buses for public transportation, Energy Policy 33 (1) (2005) 1373–1383.
[42] G.H. Tzeng, C.H. Chiang, C.W. Li, Evaluating intertwined effects in e-learning programs: a novel hybrid MCDM model based on factor analysis and DEMATEL, Expert Systems with Applications 32 (4) (2007) 1028–1044.
[43] United States General Accounting Office (USGAO), Information Security Risk Assessment, 1999. <http://www.gao.gov/special.pubs/ai00033.pdf>.
[44] J.N. Warfield, Societal Systems, Planning, Policy and Complexity, John Wiley & Sons, New York, 1976.
[45] P.L. Yu, A class of solutions for group decision problems, Management Science 19 (8) (1973) 936–946.
[46] I. Yüksel, M. Dağdeviren, Using the analytic network process (ANP) in a SWOT analysis – A case study for a textile firm, Information Sciences 177 (16) (2007) 3364–3382.