The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability

Hui-Lin Hai¹* and Kuei-Min Wang²

Department of Information Management, Shih Chien University, Kaohsiung Campus, Taiwan.

Received 15 April, 2014; Accepted 21 August, 2014

In the era of fast growing information technology, information security management system (ISMS) assessment has become a top priority of considerations in the operational organization because potential crisis increases when ISMS is vulnerable. The impact of ISMS will also bring revolutionary change on the management of business. The example used in study is the computer center at the Shih Chien University in Taiwan that the ISO27001 certification was done by 2011 and 2012. With 54 hours of ISO27001 auditor course training to the task group (TG), we carried out questionnaires and evaluated the weights of critical success factors (CSFs) for ISO27001 certification by the vote-ranking analytic hierarchy process (VAHP) model. The findings show that top-down ranking involves policy and planning, execution and management, checking and correction, management reviews and provides a heuristic two stages and seven-step procedure for introducing the CSFs of ISO27001 certification. There are no significant differences between 2011 and 2012 ranking results.

Key words: Critical success factor (CSF), ISO27001, vote-ranking analytic hierarchy process (VAHP).

INTRODUCTION

When information technology is growing faster than ever before, the information security management system (ISMS) assessment has become a top consideration in the operations of most organizations. The vulnerable ISMS would bring disaster to the enterprise. The impact of ISMS will also bring revolutionary change to the management. The International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) have created a specific system for global standardization. National certification bodies, the members of ISO or IEC, are the technical committees established by a specific organization that they help to deal with technical activities in the specific fields in terms of harmonizing national standards with International Standards. The ISO27001 international standard introduces a system approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving organization’s information security. It adopts the “Plan-Do-Check-Act” (PDCA) process model, which is applied to structure all ISMS processes. There are 11 controls including security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident

*Corresponding author. E-mail: huilin@mail.kh.usc.edu.tw, kmin@mail3.kh.usc.edu.tw.

Authors agree that this article remain permanently open access under the terms of the Creative Commons Attribution License 4.0 International License.
management, business continuity management as well as compliance (ISO/IEC 27001, 2005).

The problem for many organizations is the setup of their information security management system. The solution is to find way to learn and initialize an effective information security management system. In fact, in order to do so, a set of successful management by ISO27001 certification is the right way. The critical success factors (CSFs) in project are the criteria with which the success of the project can be judged and evaluated, and defined distinctly and clearly being an essential issue. Examples for ISMS’s CSFs are to deliver its functionality, fulfill the ISMS requirement of the client, satisfy all stakeholders' needs, and meet the pre-stated objectives. The ISO27001 certificated process is ensured to implement and maintain the appropriate level of information security by the third party certification.

The objective of this study is to complete the third party certification analyses on the implemented ISO27001 in the computer center of Shih Chien University (SCU) in Taiwan. This study has recruited students, who have accepted forty-four hours of ISO27001 auditor course for tackling the questionnaires by test-retest reliability. The test-retest reliability is to measure the reliability by performing the same survey with the same group of people but at different time; then followed by the vote-ranking analytic hierarchy process (VAHP) model for the evaluating the weights of CSFs. The assessment shows the process of validating and accrediting the management information security issues of CSFs for ISO27001 certification.

The rest of this paper is organized as follows: Literature review on CSFs-related issues, then the multiple criteria decision-making methods. Third, the origin and evolution of the methodology of vote-ranking analytic hierarchy process (VAHP), from data envelopment analysis (DEA) is introduced. Fourth, the two stages and seven-step procedures for CSFs of ISO27001 certification project are illustrated and a numerical example is provided with two questionnaires in 2011 and 2012. Discussion and result are the last, where comparison is made in terms of the result of the CSFs of ISO27001 certification.

LITERATURE REVIEW

The awareness of critical issues in ISMS has implications for business, researchers, academic institutions and professional societies. However, what is important in ISMS at any given time is dependent on both the management and technology environment at that time.

Therefore, periodic assessment of the critical issues in IS and MS is necessary. Billions of dollars have been spent in the projects of software security because their success is very important to organizations, system departments, and system managers. Software security is the key factor for deciding the success or failure of a software product in nowadays rapid changing market.

Since software security plays a key role in IS, DeLone and McLean (2003) proposed an IS success model that consists of six interdependent measures of IS success: system quality, information quality, user satisfaction, individual impact and organizational impact. System quality and information quality are two major components of software quality. Hartog and Herbert (1985) employed surveyed MIS managers of Fortune 1000 companies throughout the USA. They ranked 23 issues with top five issues which were: aligning MIS with business goals, data utilization, educating senior personnel, software development, and productivity. The IS chief executives were asked to write down their CSFs. The most cited CSFs were: system development, data processing, human resource development, management control of MIS/DP organization, relationships with the management of parent organizations, and management of change (Martin, 1982).

CSF for non-information issued application

The CSFs provided a simple but theoretically sound multiple-criteria methodology for the evaluation of key performance activities or business alternatives. The strength of CSFs lies in its ability to structure a complex, multi-person, multi-attribute problem hierarchically, and then to separately investigate each level of the hierarchy, combining results as the analysis progressing. This CSFs-evaluated process can then be translated into priority weights or scores for ranking the successful practices or processes. In many situations, this CSFs-evaluated process can be designed for multi-criteria benchmarking and performance management, such as customer relationship management (King, 1988; Alshawi et al., 2011), new product development (Chen and Lee, 2009; Sun and Wing, 2005), enterprise resources planning (Brown and Vessey, 2003; Malhotra and Temponi, 2010; Salmeronand, 2010), knowledge management (Tabrizi et al., 2011), ISO and total quality management (Oakland, 1993; Singels et al., 2001; Poksinska et al., 2003; Sila and Ebrahimpour, 2005; Sambasivan and Fei, 2008; Sammalisto and Brorson, 2008; Ramli et al., 2011), hospital management (Stocka et al., 2007; Blake et al., 2010), IS Integration (Stylianou et al., 1996; Yen et al., 2008).

Belassi and Tukel (1996) suggested a new scheme that classifies the critical factors, and describes the impacts of these factors on project performance. The statistical analyses of the results demonstrated the differences between the critical success factors identifying in a previous study from literature and the factors identifying with the use of their scheme. Many critical factors, such as factors related to project managers’ performance, factors related to team members and environmental factors, become apparent with this study. Hoffmann and Schlosser (2001) used a comprehensive questionnaire which was to interview the random samples of key executive in 164 Austrian small and medium-sized enterprises.
CSF for information issued application

The information system (IS) success model is widely used to evaluate IS implementation. The updated model consists of six constructions, which are net benefits, intention to use system, user satisfaction, and three independent variables including system quality, information quality and service quality. System quality in e-learning studies is defined as help functions and end-user facilitation in the education process. Information quality is defined as end-user performance enhancement resulting from the use of system information. Service quality is defined as providing quality support to facilitate system usage (Guynes and Vanecik, 1996; Soong et al., 2001; DeLone and McLean, 2003; Petter and McLean, 2009).

The perception of critical IS issues depends greatly on environmental characteristics and the backgrounds of the chief executives (Badar, 1992; Fitzgerald, 1993).

Project management and information systems project management usually acquired by organizations as software packages are meant to provide managers with the decision-making support which is needed in planning, organizing, and controlling IS projects. The better information leads to a better insight into what should be delivered by the project. By improving the project planning, budget and design, project risk management is assumed to contribute to the success of the project. In particular, very little has been written on international development project success criteria and critical success factors. Most of the IS projects are too frequently failure to achieve their goals due to a number of problems that could be termed “managerial” and “organizational”: imperfect IS project design, poor definition requirement, delays between project identification and start-up, delays during project implementation, cost overruns, coordination failure, etc. (Chapman and Ward, 1997; Maguire, 2002; Yeo, 2002; Desouza and Evaristo, 2006; Raymond and Bergeron, 2008; Ahsan and Gunawan, 2010; Bakker et al., 2010; Gorla and Lin, 2010; Yang et al., 2012).

While many organizations across all industries have embraced various types of e-business solutions, a considerable number of cases indicate that creating the successful services on the internet or APP-enterprise is a challenging task. Channel conflicts, legacy systems, resistant business partners, confusion on strategy, and corporate cultures prevent existing firms from successfully integrating e-business into business practices. A number of CSFs of e-learning systems studies have been found in both developed and developing countries. Along with the rapid development of e-business, firms around the world currently encounter rigorous business competition. With greater customer demand and newly emerging technologies, firms must implement innovation and reform in response to the significant challenges they face (Dubelaar et al., 2005; Salmeron and Herrero, 2005; Sung, 2006; Cottleer and Bendoly, 2006; Shaha and Siddiquib, 2006; Selim, 2007; Chang et al., 2009; Chang et al., 2011; Bhuasiri et al., 2012).

METHODOLOGY

Data envelopment analysis

Data Envelopment Analysis (DEA) is a set of methods and models based on mathematical programming and used for characterizing the efficiencies and inefficiencies of decision-making units (DMUs) with the same multiple to-be-minimized and to-be-maximized indices. DEA is a relative efficient measurement to calculate weights by comparing the performances. The efficiency index of DEA is the ratio of best-practice performance to actual performance. There are three powerful DEA models include the Additive model (Charnes et al., 1985a), BCC model (Banker et al., 1984), and a classical model known as the CCR model (Charnes et al., 1978). To compare overall supplier performance, they proposed a novel approach which bases on DEA, and provided benchmarks on which the poorly performed suppliers could rely on to improve their service. Their studies employed the questionnaire of supplier’s capability and performance assessment to collect data for those of to-be-minimized and to-be-maximized variables (Seiford, 1996; Ram et al., 2001; Banker et al., 2004).

Given data, we measured the efficiency of each DMU through the optimization process. Let $DMU_o$ be $DMU$ as it was evaluated, where $o$ ranges from 1, 2, ..., $n$, each of which uses an amount $x_{io}$ of input, $i = 1, ..., m$, and produces the output $y_{ro}$, $r = 1, ..., s$. The objective is to find the weight of $v_j$, $j = 1, ..., m$ for inputs, and $u_r$, $r = 1, ..., s$ for outputs. Then to maximize the measurement, it is to divide the outputs by inputs. Charnes et al. (1978) formulated the DEA model as follows:

$$\text{Max } \theta = \frac{\sum_{j=1}^{s} u_r y_{ro}}{\sum_{i=1}^{m} v_i x_{io}}$$

$$\sum_{r=1}^{m} u_r y_{rj} \leq \theta \sum_{i=1}^{m} v_i x_{ij} \leq \frac{1}{\theta} \quad (j = 1, ..., n)$$

$s.f.$ $\sum_{i=1}^{m} v_i x_{ij} \geq \varepsilon, \quad i = 1, ..., m$

$u_r \geq \varepsilon > 0, \quad r = 1, ..., s$
Vote-ranking analytic hierarchy process

DEA is an analytical procedure for measuring the relative efficiency of DMUs that perform the same type of functions and have the identical goals and objectives. The weights used for each DMU are those maximized ratio of the weighted input over the weighted output. A well-known method for ranking candidates in a ranked-voting system is to compare the weighted sum of their votes when the suitable weights are determined. Cook and Kress (1990, 1992) also presented an approach to the problem which is to rank candidates in a preferential voting. They considered an alternative method but it does not specify the sequence of weights by applying DEA.

It is rational to suggest the rule that the weight of higher ranked votes must be no less than the next ranked votes. Let \( n \) be the number of voters which means there are \( R \) candidates vote in \( S \) places, where \( R \) is much larger than \( S \). While considering aggregation of votes where \( x_s \) is the number of the \( s \)-th place votes received by the candidate \( r \), \( r \) ranged from 1 to \( R \), then a discrimination intensity function \( d(s, \varepsilon) \) can be defined, with the model processed (2).

Where, the \( u_r \) is the weight of candidate \( r \) placed on \( s \)-th-place votes; the notation \( Z_r \) is the objective function to evaluate candidate \( r \)'s desirability. The candidate expects for the assigned weight \( u_r \) so as to maximize the sum of weighted votes in terms of candidate. Hence, \( d(t, \varepsilon) \) ensures that first-place votes are not less than second-place votes in theory. It allows the candidate to choose the most favorable weights in terms of one stand under normal DEA condition. With the restriction of additional "assurance region", the weight for a \( s \)-th-place vote should be greater than the \( (s+1) \)-th-place vote.

\[
Z_{rr} = \text{max} \sum_{s=1}^{S} u_{rs} x_{rs} \]

s.t. \[Z_{rq} = \sum_{s=1}^{S} u_{rs} x_{qs} \leq 1, \quad q = 1, 2, \ldots, R; \]
\[u_{rs} \geq d(s, \varepsilon), \quad s = 1, 2, \ldots, S - 1; \]
\[u_{rs} \geq d(s, \varepsilon).\]

Green et al. (1996) further developed this model by setting certain constraints to the weights. They pointed out that the form \( d(s, \varepsilon) \) would affect the ranking result and does not allow DMUs to choose their own weights unreservedly. Therefore, they presented an alternative procedure that involves using each candidate's rating by oneself along with each candidate's rating by all candidates. This procedure is referred to as Green's method and consists of two methods of setting constraints: (1) The difference of weight between \( s \)-th-place and \( (s+1) \)-th-place for any \( s \) is allowed to be zero; and (2) the differences must be greater than zero.

Different vote-ranking methodologies were used in the ranked voting systems such as the DMUs in DEA that have many outputs but with only one input. They proposed a method that determines an entire order of candidates under the condition of decreasing and convex sequence of weights. They incorporated the condition of decreasing and also convex sequence of weights into DEA as the assurance region. They considered that the instability is caused by the above, and inefficient candidates should not be used to discriminate efficient candidates. Efficient candidates would never be changed when discrimination occurs, and under this condition, inefficient candidates are added or removed (Hashimoto and Ishikawa, 1993; Hashimoto, 1997; Obata and Ishii, 2003; Foroughi and Tamiz, 2005).

Noguchi et al. (2002) revised the application of Green's method and showed that the different weights among objects gave rise to different ranking results. In the total ranking method by DEA, if setting particular constraints to a weight, "strong ordering" can be employed, which is characterized by the following constraints: (1') \( u_{rs} > u_{r(s+1)} \geq u_{rS} \geq 0 \). As \( u_{rs} > u_{r(s+1)} \geq u_{rS} \geq 0 \), the inequality (2') is derived from the value of \( \varepsilon \) and inequality (1'). In this multiple criteria case, it is defined as follows:

\[
Z = \sum_{s=1}^{S} u_{rs} x_{rs};
\]

s.t. \[Z_{rq} = \sum_{s=1}^{S} u_{rs} x_{qs} \leq 1, \quad q = 1, 2, \ldots, R; \]
\[u_{rs} \geq d(s, \varepsilon), \quad s = 1, 2, \ldots, S - 1; \]
\[u_{rs} \geq d(s, \varepsilon).\]

To rank alternatives, one of the most popular methods is to compare the weighted sum of votes after the right weights being determined to each alternative. The different weights among objects are made in different ranking results proposing a new method of ordering to solve the decision-making problem in weights ranking (Liu and Hai, 2005, 2006; Hai, 2008; Hai and Tsou, 2009). In the paper, the Noguchi's voting and ranking is used to develop criteria in each level from hierarchy analysis process that this methodology is called Vote-ranking Analytic Hierarchy Process (VAHP).

The critical success factors of ISO27001 certification

For ISO-certification project management, International Standard adopts the ‘Plan-Do-Check-Act’ (PDCA) process model to structure all ISMS processes. PDCA is a robust model for implementing the principles in those guidelines, which govern risk assessment, security design and implementation, security management and reassessment. The PDCA process can be interpreted as follows. (1) Plan (establishing the ISMS): Establish ISMS policy, objectives, processes and procedures that is relevant to managing risk and improving information security and to deliver results in accordance with an organization’s overall policies and objectives. (2) Do (implement and operation of the ISMS): Implement and operate the ISMS policy, controls, processes and procedures. (3) Check (monitoring and reviewing the ISMS): Assess, where is applicable, measure process performance against ISMS policy, objectives and practical experience as well as report the results to management for review. (4) Act (maintaining and improving the ISMS): Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS (ISO/IEC 27001, 2005). In study, we proposed two stages and seven-step procedures for assessing CSFs of ISO27001 certification (Figure 1).

Stage 1: Define ISMS issues and group a task group

Step 1: ISO27001 auditor course training and a successful case study

Initially, 50 junior students from information management department were selected and formed a task group. A particular
ISO27001 auditor course training of up to 54 h was given to this task group (TG) before starting their works such as carrying out questionnaires, evaluating and calculating the weights of critical success factors (CSFs) for ISO27001 certification by using VAHP model. The TG understands the internal auditing procedures for assessing CSFs of ISO27001 certification project, an example of the Shih Chien University, ISO27001 certification.

**Step 2: group a task group to identify a methodology**

In the paper, the Noguchi’s voting and ranking mode (3), originated from DEA method, is used to develop criteria in each level from hierarchy analysis process. This methodology is called VAHP, which has AHP spirits and analytical process, but the weighting method is different.

Comparing the benefits of the VAHP and AHP, the summary is as follows: (1) The VAHP method is easy to understand and used for getting priority or weights. All experts are given the opportunity to examine the priority weights calculating from their initial responses and to assess the reasonableness of the ranking. (2) The construction of the objective hierarchy of criteria, attributes and alternatives facilitates communication of the problem and solution recommendation. (3) It provides “vote ranking” rather than “paired comparison” for quantifying and measuring consistency. (4) The strongest features of the AHP are that they generate numerical priorities from the subjective knowledge expressed by the estimates of paired comparison matrices (Liu and Hai, 2005).

**Stage 1: Define ISMS issues and group a task group**

**Stage 2: Get the CSFs of ISO27001 certification**

The interviewed personnel included ISO27001 leader auditors and the director of information computing center. The first step is to structure the problem into a hierarchy (Figure 2). The goal of top level is to select CSFs of ISO27001 certification. There are four criteria for the second level that support the top goal; they are “Policy and Planning (PP), Execution and Management (EM), Checking and Correction (CC), Management Reviews (MR)”. On the third level, all four criteria on level two are decomposed into twelve sub-criteria. On the bottom level, there are twelve different weights of CSFs evaluated in terms of the sub- criteria of the third level.

The CSFs, in terms of SCU according to ISO27001, were evaluated including S1: Policy and Planning (PP), S2: Execution and Management (EM), S3: Checking and Correction (CC), S4: Management Reviews (MR) (Table 1). The VAHP provided a simple way and with theoretically multiple-criteria methodology, the alternative CSFs was evaluated. It was used to identify sub-criteria, and study each level of the hierarchy independently.

The twelve sub-CSFs are PP-1: Top-manager’s commitment and leadership; PP-2: connect to effective information security policy and objectives; PP-3: Effective process approach; PP-4: Effective information asset risk assessment and improvement, EM-1: Implement and operate the ISMS; EM-2: Establishing roles and responsibilities for ISMS; EM-3: Effective training, awareness and
Table 1. Definitions of the critical successful fraction for ISO27001 certification.

<table>
<thead>
<tr>
<th>CSFs</th>
<th>Sub-CSFs</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1: Policy</td>
<td>PP-1 Top-manager’s commitment and leadership</td>
<td>Developing clear and effective ISMS strategies and supporting activities, etc., selecting and empowering project manager, providing sufficient budgets and motivation through leadership and equipping people to achieve them.</td>
</tr>
<tr>
<td>Planning</td>
<td>PP-2 Connect to effective information security policy and objectives</td>
<td>Clearly defined and properly communicated strategies and objectives, which can be summarized in the form of a mission statement, compatibility with ISMS requirement, from top to bottom, are to work closely as a winning team.</td>
</tr>
<tr>
<td></td>
<td>PP-3 Effective process approach</td>
<td>Using the international standard to promote the adoption of a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s ISMS.</td>
</tr>
<tr>
<td></td>
<td>PP-4 Effective information asset risk assessment and improvement</td>
<td>Identifying the CSFs and critical processes, a term used to represent the most important sub-goal of a business.</td>
</tr>
<tr>
<td></td>
<td>EM-1 Implement and operate the ISMS</td>
<td>Formulating a risk treatment plan that identifies the appropriate management actions, resources, responsibilities and priorities for managing information security risks. They have capability to manage the ISMS activities to meet the organizational objectives or goals.</td>
</tr>
<tr>
<td>S2: Execution</td>
<td>EM-2 Establishing roles and responsibilities for ISMS</td>
<td>Clearly establishing roles and responsibilities for information security. Conforming the information security policy and to meet the information security objectives, communications to the organization are essential responsibilities under the law. It is required for continual improvements. Mangers are responsible for all problem-solving activities.</td>
</tr>
<tr>
<td>Management</td>
<td>EM-3 Effective training, awareness and competence</td>
<td>Manager provides that resources of equipment and for training. Ensuring that all personnel whose responsibilities (assigned) defining in the ISMS are capable to perform the required tasks. Providing the necessary trainings or taking other actions for personnel in order to perform work effectively in ISMS.</td>
</tr>
<tr>
<td></td>
<td>EM-4 Effective information risk management</td>
<td>Defining the independent examination of risk assessment to provide information for overall process of risk analysis and risk evaluation. And effective coordinated activities to direct and control an organization with regard to information security or risk.</td>
</tr>
<tr>
<td>S3: Checking</td>
<td>CC-1 Documentation requirements, control of records and documents</td>
<td>Establishing different level records and documents to meet the documentation requirements specified in ISO 27001. For overall PDCA processes, the operating procedures shall be documented, maintained, and made available to all users. The results of the ISMS shall be clearly documented and records shall be maintained well</td>
</tr>
<tr>
<td>and Correction</td>
<td>CC-2 Emergency events management and controlling</td>
<td>Minimizing the risk of ISMS by avoiding the law suits from a breach of contract, the negligence of consumer protection and the faulty ISMS.</td>
</tr>
<tr>
<td></td>
<td>CC-3 Effective internal and system audit management</td>
<td>Conducting a formal quality and information system audit that is requested by ISO27001 with the Self-audit, second party audit (customer) and third party-audit (ISO27001 assessor). The organization shall conduct internal ISMS audits under the planned intervals to determine the control objectives, controls, processes and procedures of its ISMS.</td>
</tr>
</tbody>
</table>
The PDCA approach must focus on the development of problem-prevention mentality, but it is easy to understand the effort that is required to change attitudes and approaches.

The organization shall continually improve the effectiveness of the ISMS through information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions, as well as management reviews.

The management review system should include the establishment of a process the structure of ISMS improvement team in the organization. It contains the assessing opportunities for the improvements and the necessary changes of ISMS, which includes the information security policy and information security objectives, reviewed inputs and outputs.

Employing manpower effectively, we should develop the culture “person oriented” philosophy that can achieve ISMS by means of participation voluntarily rather than be forced under control. The vision is that each employee is willing to devote their talents in achieving the goal of ISMS.

There are three levels of ISMS knowledge management, at least. First, set up the course to train employees in terms of basic techniques. Second, learn the enterprise system in details, which includes the system’s strengths and vulnerabilities. Third, keep up with the fast-changing world with the potential threats and the way to exploit the talents to cope with it. Professional security consultants or project knowledge management can assist for the initial security strategy setup and a periodic audit. They can provide the continuous learning process and specific system development that can result knowledge creation in the organization.

The test-retest reliability had been applied with same questionnaires carrying out respectively in 2011 and 2012. Fifty effective questionnaires were obtained out of 69 with responsive rate of 72.5%.

The TG selected different orders for the candidates of CSFs or sub-CSFs. TG had votes from 1 to S (S≤R); R is the number of CSFs or sub-CSFs. For this purpose, four CSFs “S-1, S-2, S-3, S-4” and twelve sub-CSFs “PP-1, PP-2, PP-3, PP-4, EM-1, EM-2, EM-3, EM-4, CC-1, CC-2, CC-3, CC-4, MR-1, MR-2, MR-3, MR-4” were obtained. These criteria were regarded as candidates. Four orders were drawn from 1 to 4 and sum up as shown in Tables 2 and 3. Table 2 shows the votes of rank (from 1st to 4th) for CSF “S-1” in 2011 and 2012 (27, 10, 7, 6) and (25, 17, 4, 4), respectively. The managers got the order of criteria without the weight. The weight of each ranking was determined automatically by the total votes of each candidate.

<table>
<thead>
<tr>
<th>S4: Management Reviews</th>
<th>MR-1 Company-wide involving and improvement</th>
<th>MR-2 Effective management review system</th>
<th>MR-3 Effective motivation management</th>
<th>MR-4 Project knowledge management</th>
</tr>
</thead>
</table>

Step 4: prioritize the order of CSFs and sub-CSFs

The TG selected different orders for the candidates of CSFs or sub-CSFs. TG had votes from 1 to S (S≤R); R is the number of CSFs or sub-CSFs. For this purpose, four CSFs “S-1, S-2, S-3, S-4” and twelve sub-CSFs “PP-1, PP-2, PP-3, PP-4, EM-1, EM-2, EM-3, EM-4, CC-1, CC-2, CC-3, CC-4, MR-1, MR-2, MR-3, MR-4” were obtained. These criteria were regarded as candidates. Four orders were drawn from 1 to 4 and sum up as shown in Tables 2 and 3. Table 2 shows the votes of rank (from 1st to 4th) for CSF “S-1” in 2011 and 2012 (27, 10, 7, 6) and (25, 17, 4, 4), respectively. The managers got the order of criteria without the weight. The weight of each ranking was determined automatically by the total votes of each candidate.

Step 5: calculate the weights of CSFs and sub-CSFs

When \( n=69, S=2 \) and \( \varepsilon=0.00145\times(2/(69\times4\times5)) \); in Table 2 and Eqs. (3), the weights of eight criteria can be calculated. Table 2 shows the weight of CSFs “S-1, S-2, S-3, S-4” in 2011 and 2012 (0.993, 1.000, 0.731, 0.584, 0.600) and (0.849, 1.000, 0.737, 0.564). Through normalization process, the results are (0.343, 0.278, 0.242, 0.137) and (0.343, 0.278, 0.242, 0.137).

The weights of Sub-CSF, as shown in Table 3, are also calculated by using the same methodology. The index of S1: “Policy and Planning” indicates the weight for sub-CSFs “PP-1, PP-2, PP-3, PP-4” in 2011 and 2012 (0.993, 1.000, 0.923, 0.788) and (0.849, 1.000, 0.737, 0.564). After normalization, those sub-CSFs value turn out to be (0.268, 0.270, 0.249, 0.213) and (0.270, 0.317, 0.234, 0.179).

Sources: references from (Österlea et al., 2003; Oakland, 1993; Cortada, 1996) and ISO27001:2005.
differences in the ranks (Walpole et al., 1998; Aczel and nonparametric test. The test is carried out by considering the
has been applied in the case of a symmetric continuous distribution
value.

The study of CSFs of ISO27001 certification, the questionnaire and
procedure referring to ISO27001 are discussed and confirmed by
the director of the computer center, leading auditors and TG. All
those contents and contexts should be considered as the "validity"

Table 2. Priority votes and weights for CSFs of ISO27001 certification.

<table>
<thead>
<tr>
<th>CSFs</th>
<th>Votes 1st</th>
<th>Votes 2nd</th>
<th>Votes 3rd</th>
<th>Votes 4th</th>
<th>Weights</th>
<th>Ranks</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1: Policy and Planning</td>
<td>25(27)</td>
<td>17(10)</td>
<td>4(7)</td>
<td>4(6)</td>
<td>1.000[0.343]</td>
<td>1(1)</td>
</tr>
<tr>
<td>S2: Execution and Management</td>
<td>13(8)</td>
<td>22(25)</td>
<td>13(14)</td>
<td>2(3)</td>
<td>0.811[0.278]</td>
<td>2(2)</td>
</tr>
<tr>
<td>S3: Checking and Correction</td>
<td>12(5)</td>
<td>8(13)</td>
<td>21(17)</td>
<td>9(15)</td>
<td>0.705[0.242]</td>
<td>3(4)</td>
</tr>
<tr>
<td>S4: Management Reviews</td>
<td>0(10)</td>
<td>3(2)</td>
<td>12(12)</td>
<td>35(26)</td>
<td>0.398[0.137]</td>
<td>4(3)</td>
</tr>
<tr>
<td>Sum</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>2.914[1.000]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(50)</td>
<td>(50)</td>
<td>(50)</td>
<td>(50)</td>
<td>(2.915[1.000])</td>
<td></td>
</tr>
</tbody>
</table>

WSRT-p value=0.932; Cronbach’s α=0.903. *The number in ( ) belongs to 2011 questionnaire survey data, other than the data in 2012; the number in [ ] represents the normalized data.

Table 3. Priority votes and weights for sub-CSFs of ISO27001 certification.

<table>
<thead>
<tr>
<th>Sub-CSFs</th>
<th>Votes 1st</th>
<th>Votes 2nd</th>
<th>Votes 3rd</th>
<th>Votes 4th</th>
<th>Weights</th>
<th>Ranks</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP-1</td>
<td>16</td>
<td>12</td>
<td>7</td>
<td>15</td>
<td>0.849[0.270]</td>
<td>2</td>
</tr>
<tr>
<td>(15) (13)</td>
<td>(8) (14)</td>
<td>(9.933[0.268])</td>
<td>(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PP-2</td>
<td>21</td>
<td>16</td>
<td>10</td>
<td>3</td>
<td>1.000[0.317]</td>
<td>1</td>
</tr>
<tr>
<td>(16) (11)</td>
<td>(8) (5)</td>
<td>(1.000[0.270])</td>
<td>(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PP-3</td>
<td>7</td>
<td>19</td>
<td>22</td>
<td>2</td>
<td>0.737[0.234]</td>
<td>3</td>
</tr>
<tr>
<td>(9) (22)</td>
<td>(10) (9)</td>
<td>(0.923[0.249])</td>
<td>(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PP-4</td>
<td>6</td>
<td>3</td>
<td>11</td>
<td>30</td>
<td>0.564[0.179]</td>
<td>4</td>
</tr>
<tr>
<td>(10) (5)</td>
<td>(14) (22)</td>
<td>(0.788[0.213])</td>
<td>(4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3: Checking and Correction</td>
<td>15</td>
<td>12</td>
<td>9</td>
<td>14</td>
<td>0.813[0.264]</td>
<td>2</td>
</tr>
<tr>
<td>(12) (11)</td>
<td>(12) (15)</td>
<td>(0.839[0.242])</td>
<td>(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC-2</td>
<td>23</td>
<td>12</td>
<td>13</td>
<td>2</td>
<td>1.000[0.325]</td>
<td>1</td>
</tr>
<tr>
<td>(16) (19)</td>
<td>(10) (5)</td>
<td>(1.000[0.289])</td>
<td>(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC-3</td>
<td>7</td>
<td>13</td>
<td>20</td>
<td>10</td>
<td>0.670[0.218]</td>
<td>3</td>
</tr>
<tr>
<td>(14) (13)</td>
<td>(10) (10)</td>
<td>(0.909[0.262])</td>
<td>(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC-4</td>
<td>5</td>
<td>13</td>
<td>8</td>
<td>24</td>
<td>0.596[0.194]</td>
<td>4</td>
</tr>
<tr>
<td>(8) (7)</td>
<td>(15) (20)</td>
<td>(0.715[0.206])</td>
<td>(4)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

WSRT-p value=0.622; Cronbach’s α=0.815

WSRT-p value=0.924; Cronbach’s α=0.928

Step 6: analyze the validity and reliability of CSFs and sub-CSFs

The study of CSFs of ISO27001 certification, the questionnaire and
procedure referring to ISO27001 are discussed and confirmed by
the director of the computer center, leading auditors and TG. All
those contents and contexts should be considered as the "validity"

Wilcoxon signed rank test (WSRT), proposed by Wilcoxon (1954),
has been applied in the case of a symmetric continuous distribution
and nonparametric test. The test is carried out by considering the
differences in the ranks (Walpole et al., 1998; Aczel and
Sounderpandian, 2002). Table 2 shows these differences of CSFs
"S-1, S-2,S-3,S-4" in 2011 and 2012. It is assumed in the null and
alternative hypotheses that the distributions of the two populations
are identical. The two population distributions are not identical. The
value of the statistic lying inside the non-rejection region (z=-0.085,
p-value=0.932, Cronbach’s α=0.903) is far from the critical point for
any conventional level of significance, if it is to carry out the test at
α=0.05. The CSFs of ISO 27001 certification for "S1: Policy and
Planning (PP), S2: Execution and Management (EM), S3: Checking
and Correction (CC), S4: Management Reviews (MR) between
2011 and 2012 have no significant difference. Other than that, the
WSRT methodology was used to find the tests of sub-CSFs in
Table 4. Priority of the total weights of CSFs and sub-CSFs.

<table>
<thead>
<tr>
<th>CSFs(a)</th>
<th>sub-CSFs(b)</th>
<th>Weights (c=AXB)</th>
<th>CSFs(a)</th>
<th>sub-CSFs(b)</th>
<th>Weights (c=AXB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy and Planning</td>
<td>PP-10.270(0.268)</td>
<td>0.093(0.092)</td>
<td>Execution and Management</td>
<td>EM-10.272(0.297)</td>
<td>↓ 0.076(0.075)</td>
</tr>
<tr>
<td></td>
<td>PP-20.317(0.270)</td>
<td>0.109(0.093)</td>
<td></td>
<td>EM-20.269(0.254)</td>
<td>↑ 0.075(0.064)</td>
</tr>
<tr>
<td>0.343(0.343)</td>
<td>PP-30.234(0.249)</td>
<td>0.080(0.085)</td>
<td></td>
<td>EM-30.281(0.278)</td>
<td>↑ 0.078(0.070)</td>
</tr>
<tr>
<td></td>
<td>PP-40.179(0.213)</td>
<td>0.061(0.073)</td>
<td></td>
<td>EM-40.178(0.172)</td>
<td>↑ 0.049(0.043)</td>
</tr>
<tr>
<td></td>
<td>CC-10.264(0.242)</td>
<td>0.064(0.048)</td>
<td>Management Reviews</td>
<td>MR-10.286(0.315)</td>
<td>0.039(0.065)</td>
</tr>
<tr>
<td></td>
<td>CC-20.325(0.289)</td>
<td>0.079(0.058)</td>
<td></td>
<td>MR-20.252(0.270)</td>
<td>0.035(0.056)</td>
</tr>
<tr>
<td>42(0.200)</td>
<td>CC-30.218(0.262)</td>
<td>0.053(0.052)</td>
<td></td>
<td>MR-30.212(0.178)</td>
<td>0.029(0.037)</td>
</tr>
<tr>
<td>↑</td>
<td>CC-40.194(0.206)</td>
<td>0.047(0.041)</td>
<td></td>
<td>MR-40.249(0.236)</td>
<td>0.034(0.049)</td>
</tr>
</tbody>
</table>

*1. The number in ( ) belongs to 2011 questionnaire survey data, other than the data in 2012; 2. “” symbol indicates the rankings are indifferent. “” symbol means that the comparison between 2011 and 2012 has improved rank. “” symbol means that the comparison between 2011 and 2012 has downgraded rank.

Step 7: prioritize the total weights of CSFs and sub-CSFs

The weights of the second level of CSFs in Table 4 were through the normalization process. The values on the bottom level are the global weight for each of the twelve factors that they can be calculated by the multiplication of the weight of CSFs and sub-CSFs such as the global weight of PP-2 is 0.093.

In Table 4, “” symbol indicates the rankings are indifferent. “” symbol means that the rank between 2011 and 2012 increases. For the global weights of the “S1: Policy and Planning”, the ranks of the CSF and their sub-CSFs stay unchanged. For the total weights, i.e., global weights, of “S3: Checking and Correction” that the rank of the CSF and sub-CSF “CC-1” improves. The changes of the rank of the sub-CSFs are remarkable.

DISCUSSION

The ranking from these two consecutive years reveals there is no significant consistency. The first two CSFs, “Policy and Planning” and “Execution and Management” are consistent in the ranking but the last two CSFs change, where “Checking and Correction” is shifted to the fourth place ranking after “Management Reviews”. The “Policy and Planning” is always on the top level of management hierarchy, the critical factor, and always the initiator of ISO27001. This is because it is the origin of leadership, direction, motivation and support. If it is misplaced, the system will break down. The concern of top manager would be to keep all employees in right track including ISMS. Once there is loose control in management, then there will difficulty in running an ISMS unit or department. The results conform to total quality management (TQM) and Six Sigma that motivate employees to reach ISMS goal, which is actually not an easy task. The leaders need to provide the appropriate working environment for all managers and employees to make it easier to reach the ISMS goals.

The top-down management principle, including the top-manager’s commitment and leadership that improve the effectiveness of organization, is stressed by the results of the implementation and certification of ISO27001. In addition, the internal and external third-party audit activities could also provide assistance to ensure effectiveness. These auditing approaches, which are “Checking and Correction” and “Management Reviews” can certainly enhance the effect of evaluation. The interval observations of the CSFs could illustrate ISO27001 clause by test-retest reliability.

The following is the discussion of the results in Tables 1, 2 and 3.

(1) In the consecutive years of 2011 and 2012, the ratio of unchanged rank for four CSFs and sixteen sub-CSFs of the ISO27001 certification was up to 50 and 75%, which shows no significant difference by statistical test. There is only one place that changed in the ranking indexes of “S3 and S4”, “EM-1 and EM-3”, “CC-1 and CC-3”. For ISO 27001 management, the assessed CSFs are valid and
reliable by test-retest between two years.

(2) In terms of “Policy and Planning” CSF, the two most important indexes are “commitment and leadership” and “connect to effective Information security policy and objectives”. Top-managers should pay more attention to effective policy and planning for establishing and managing the ISMS. Considering the corporate characteristics, organization, location, assets and technology, top manager has the responsibility of clearly defining ISMS policy and identifying risk, such as feasibility assessment, and whether the information security policy can link the business objectives and performance evaluation.

(3) For “Execution and Management” CSF, there is only one place that shifted in the indexes of “EM-1 and EM-3” but shows no significant difference. The two most important indexes for “Implement and operate the ISMS” and “Effective training, awareness and competence” imply that the company should ensure responsibilities are assigned to each personnel, which are defined in the ISMS. They are competent and comprehensive to perform the required tasks. Education should be focused onto a specific team with emphasizing word “comprehensive”, because it needs to work with these ISMS practices cutting across all functions and levels in organization. “4.2.2 Training, awareness and competence” and “4.2.2 Owing to the complexity of interconnections among departments, to implement and operate the ISMS” should start with a chosen department for demonstrations. All personnel should be part of it; a substantive success would not be easy to reach.

(4) For “Checking and Correction” CSF, according to the interval evaluations, there is no significant difference in the ranking of indexes, “CC-1 and CC-3”; it is only one place that changed. Considering the effective guidance documents of internal and external audits, the organization shall conduct the diverse ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of ISMS have been reached. For PDCA process, the operating procedures shall be documented, maintained, and available to all end-users. And then, the records and documents on different level should be established to meet the requirements of the ISO 27001. The documented procedure for emergency events management and risk evaluation of ISMS must be checked by “4.2.3 Monitor and review the ISMS” at each predetermined time.

(5) For “Management Reviews” CSF, there is no significant difference in the interval evaluations in the ranking. The two most important indexes, which are “Company-wide involving and improvement” and “Effective management review system”, imply that each unit of an organization must work closely to achieve perfection. To setup the permanent recognition process team in organizations indicates that all levels and functions with the continuously improvements, monitors, implementations and recognition programs are linked to “8, ISMS improvement”. Management review to check each department for the ISMS’s objectives and effects indicate that the most attacks on or defects of information system are preventable and correctable. In review, it should include the assessed opportunities for the improvement and the need for changes of ISMS, which contain the information security policy and objectives, as well as review inputs and outputs.

There are four major parts have been done in this study. Initially, it focused on functional activities, personnel, assets to ensure the consistency with ISMS policies and objectives, which include a framework for setting the objectives and establishing the sense of directions and principles for actions with regard to information security and organization’s strategic risk management context. In terms of ISMS, with the identifications of the correct methodology for risk assessment, legal and regulatory requirements are carried out. Secondly, it is required to check how the actual ISMS development process functions are measured and managed. On the stage of implementation and operation of the ISMS, the personnel of corporative management and connected departments should have a full understanding of ISMS issues. System management methods must be understood by the employees that would ensure the system’s successful import. Thirdly, it is important to have good communication inside the organization and for all personnel to participate. The process involves identifying and overcoming the barriers on the implementation stage and also to make all personnel passionate to ensure cohesion for achieving objectives. Finally, addressing how to use “never-ending improvement” methodologies is needed.

The result shows the top-down ranking as: “policy and planning, execution and management, checking and correction, management reviews”. We provide a heuristic seven steps to introduce the CSFs of ISO27001 certification: (1) The top management provides an effective “policy and planning” and connect to information security policy and objectives; (2) Formulating a risk treatment plan that identifies the appropriate management actions, resources, responsibilities and priorities for managing information security risks; (3) Selecting a project manager of ISO27001 certification; (4) Obtaining budgets and defining the range of ISO27001 certification; (5) Setting an executive schedule and total companies’ training program; (6) Schedule; (7) Paying attention to emergency events by 80-20 management and controlling; (8) Holding a periodical “Management Reviews meeting” by top management and providing a reasonable amount of resources to corrective actions; (9) Establishing different level records and documents to meet ISO 27001 requirements; (10) Creating a business culture of never-ending improvement system.

Conclusion

This study has completed the CSFs analysis of ISO
27001 certification of the computer center at Shih Chien University in Taiwan, of consecutive two years (2011 and 2012). Based on ISO clauses, the “top-down” ISMS process has been set up with the certification methodology, which included “Policy and Planning, Execution and Management, Management Reviews and Correction” for 4 CSFs and 16 sub-CSFs. The task group was coordinated by the ISO27001 leading auditor and the director of computer center, on which basis the successful discussion, communications and confirmations were made. The analytical process, VAHP approach, is used for decision-makers to generate non-inferior multi-criteria decision-making (MCDM) process, which could analyze the inherent tradeoffs among the relevant CSFs systematically. With the result, it proves that the implementation of ISO 27001 in the computer organization is successful.

With this specific lesson learn, we believe that this methodology is useful for the evaluations of other business organizations with specific CSF. We also expect that this method can be applied effectively on some ISO related topics such as the assessment of ISO 14000, ISO 22000 and OHSAS 18000 to have a reliable and concrete analytical result for decision-makers in their decision processes.

Conflict of Interests

The authors have not declared any conflict of interests.

REFERENCES

Ika LA, DiAllo A, Thullier D (2010). Project management in the