Assessment Mechanism of Internal Control for Information Technology Governance

I-Cheng Chang  
*National Dong Hwa University, icc@mail.ndhu.edu.tw*

She-I Chang  
*National Chung Cheng University, actsic@ccu.edu.tw*

Chuang-Chun Liu  
*National Chiao Tung University, ccliu0406@mis.ccu.edu.tw*

Follow this and additional works at: [http://aisel.aisnet.org/pacis2013](http://aisel.aisnet.org/pacis2013)
ASSESSMENT MECHANISM OF INTERNAL CONTROL FOR INFORMATION TECHNOLOGY GOVERNANCE

I-Cheng Chang, Department of Accounting, National Dong Hwa University, Hualien, Taiwan, R.O.C., icc@mail.ndhu.edu.tw

She-I Chang, Department: Department of Accounting and Information Technology, Chia-Yi, R.O.C., actsic@ccu.edu.tw

Chuang-Chun Liu, Institute of Information Management, National Chiao Tung University, Hsinchu, R.O.C., ccliu0406@mis.ccu.edu.tw

Abstract

More publicly listed firms have emphasized the effectiveness of internal control in an information technology environment. Hence, this study presents a logical assessment mechanism for appraising the internal control of information technology. The strategy is based on Gowin’s Vee structure. On the theory side, this study explores the assessment items of internal controls on information environment by using grounded theory, and then confirms the items via the Delphi methodology. On the empirical side, this assessment model is verified via a multiple-case study to examine its usability in practice. This study expects that management and external IT auditors will apply such a mechanism to enhance the handling of internal control during the IT control evaluation stages.

Keywords: Internal Control, Assessment mechanism, IT governance
1 INTRODUCTION

Information technology (IT) governance is an emerging issue that is widely noticed in the industry. The International Audit and Control Association (ISACA, 2008) conducted an online survey that was distributed to over 3,000 members of the International Credit Insurance and Surety Association (ICISA) from 95 countries. After analyzing the information, IT governance ranked among the top two critical issues.

Effective IT control is an essential process for achieving IT governance. Several studies reported the reliability of financial reporting is a function of the effectiveness of the internal control of a firm (PCAOB, 2004). Effective internal control can help firms to achieve their expected financial goals, to maintain precise records from daily transactions, and to report accurate financial statements (Ernst and Young, 2002). Conversely, Durfee (2005) highlighted the material weakness in the internal control system could result in a drop in stock prices, an increase in share volume, and losses of CFO jobs. To reconstruct investor confidence, the U.S. Congress in 2002 passed the Sarbanes-Oxley Act (SOX). SOX 404 is one of the most critical sections of the Act. SOX 404 and the Public Company Accounting Oversight Board (PCAOB) require company management to report on internal control over financial reporting. Moreover, they require an external auditor to attest to the management reporting and to provide a report on the effectiveness of internal control of the firm (PCAOB, 2007).

Information systems in enterprises need to have several internal controls because of the pervasive implementation of IT and the need to lessen problems. Meanwhile, the complexity of modern systems can overwhelm auditors and management if they do not have sound guidance to follow (Tuttle and Vandervelde, 2007). Therefore, regardless of internal or external controls, auditors and management should increase their understanding of the IT environment and the related IT processes and controls because they perform control assessment procedures (Mock et al., 2009; Norman et al., 2009).

External auditors and management must construct a well-developed assessment or guidance plan that can mitigate their litigation risk for attesting to the effectiveness of internal control in an IT environment. As a result, the Committee of the Sponsoring Organizations of the Treadway Commission (COSO) issued a report entitled “Internal Control-Integrated Framework” (COSO, 1992), which was recommended for use by companies, auditors, regulating agencies, and educational institutions. Internal control, which includes risk assessment and monitoring, is similar to risk management. Hence, to reinforce the COSO (1992) framework, Enterprise Risk Management (ERM), an integrated framework developed in 2004 added event identification and risk response. However, COSO does not provide supplemental criteria that indicate the requirements for IT control objectives and related activities (O’Donnell and Rechtman, 2005). Without sound and comprehensive guidance, sophisticated modern systems will swamp an auditor.

Meanwhile, management and auditors usually use qualitative judgment, such as “High,” “Moderate,” and “Low” rather than quantitative judgment when assessing IT control in practice (Norman et al., 2009). However, precisely measuring the degree of control by using this kind of qualitative evaluation is being challenged (Elliott and Rogers, 1972). Furthermore, several studies indicate that ineffective concern will result from conventional qualitative approaches, such as flow chart, checklists, and test questionnaires (Yu and Neter, 1973). Mock et al. (2009) stated that studies on internal control assessment have been sparse during the past decade. Hence, determining how to improve the precision and effectiveness of IT control assessment in facing a rigorous regulation environment and modern sophisticated information systems is the second research question in this study.

Due to the aforementioned reasons, this study develops an IT control assessment mechanism for internal control in IT governance. IT controls include IT general control (ITGC) and IT application control (ITAC). This assessment mechanism focuses on IT General Control (ITGC), which is important in the context of IT control because it supports application processing. Although ITGC may
not directly influence financial statements, it has an impact on the consistency and effectiveness of the financial application in all systems.

This study has the following objectives:
- To explore the crucial IT control assessment items in the IT environment
- To develop a comprehensive assessment mechanism for management to objectively assess IT control
- To validate the usability of this proposed mechanism in practice

2 LITERATURE REVIEWS

2.1 Information Systems Control and IT Governance

Existing evidence indicates that computer abuse and breaches in the information system security may not necessarily result in serious problems, but may lead to huge losses (Gordon et al., 2005). In general, organizations that lack well-developed information on security may suffer from theft of confidential data, financial fraud, incapacitated Web server, and corrupted operation data (Gordon et al., 2005). Furthermore, the aforementioned attacks may likely influence the accuracy and reliability of financial data derived from the information system (Walters, 2007). Accordingly, understanding related risk management and control is imperative for any organization implementing or adopting an information system.

Meanwhile, given that an increasing number of firms have come to depend on the information system to deal with operational transactions, related information system security must now be emphasized, especially in financial transactions. Walters (2007) indicated that several information system threats, including more severe forms, such as unauthorized access, attacks, and system vulnerabilities, will likely impact on the accuracy and reliability of financial data derived from information systems. Information security acts to protect and control these IT resources, and consequently ensure the accuracy and reliability of the information (Fox and Zonneveld, 2003). Van de Riet et al. (1998) suggested a number of security aspects associated with an ERP system, which includes security policy, user authentication, authorization, time restriction, log and trace, and database security.

IT governance is an emerging issue widely noticed in the industry. The International Audit and Control Association (ISACA, 2008) has conducted an online survey that was distributed to over 3,000 members of the International Credit Insurance and Surety Association (ICISA) from 95 countries. After analyzing the data, the top two critical issues were identified as regulatory compliance and enterprise based IT management/IT governance.

Further, Peterson et al. (2002) proposed three key elements in the field of IT governance, namely, structures, processes, and control frameworks. The structure of IT governance includes three types of mode, which are centralized, decentralized, and federal modes. Accountability within the processes, policies, and procedures is an essential component of the IT governance process (Weill, 2004; Willson and Pollard, 2009). The IT Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (COBIT), and ISO/IEC 20000 are well-known guidelines for IT governance (Cater-Steel and Pollard, 2008).

2.2 Approaches of the Assessment of Internal Control

Over the last three decades, auditors have utilized several techniques in the internal control assessment process, such as internal control questionnaires, flowcharting, checklists, and tests of transactions. These tools assist auditors to collect and to organize raw data for evaluating internal control (Cooley and Hicks, 1983). From the evidence of related studies, these techniques may be viewed as effective tools that can easily deliver relevant task information to junior auditors, and further improve their task
performance (Graham, 1993). Brewster (2008) reported that the flowchart-type technique can facilitate auditors in precisely and comprehensively constructing mental models of complicated systems.

In addition, the internal control matrix becomes a common method to represent internal controls for specified business processes within the SOX audit environment (Gelinas and Dull 2008). This technique contains two elements, namely, internal control objective and activities. Internal control objectives are listed on the top, and followed by internal control activities. Bierstaker et al. (2009) mentioned that internal control matrices could help auditors to evaluate internal control effectively.

However, Cooley and Hicks (1983) indicated that some of the above approaches lack systematic and rigorous procedures to obtain an aggregate evaluation. Yu and Neter (1973) proposed a stochastic model of the internal control system based on the Markov chains. Furthermore, Cushing (1974) also presented a method for evaluating internal control systems in terms of reliability engineering concepts. Although these approaches are based on mathematical procedures, their practical usability is still being argued (Cooley and Hicks, 1983). Cooley and Hicks (1983) suggested that auditors combine internal control questionnaires/flowcharting approach with linguistic measurements as well as mathematical and systematic approaches for deriving internal control evaluation.

According to Elliott and Rogers (1972), auditors have realized the incorrect nature of internal control assessment by using linguistic measurements, such as weak or strong internal controls. According to prior studies, the fuzzy set theory can be regarded as a systematic method for integrating linguistic measurements in the process of internal control assessment, and such an approach has been applied to the rating of computer system security (Clements, 1977; Cooley and Hicks, 1983).

3 RESEARCH METHODOLOGY AND PROCESS

This study utilizes Gowin’s Vee model as a research strategy. Gowin’s Vee (Novak and Gowin, 1989) is a logical application tool that is composed of steps that can be easily followed by users. Gowin’s Vee is a V-shaped structure model originally used for education and research. The model includes the conceptual side (think) and methodological side (do).

This study aims to establish a mechanism for converting the fragmented assessment concept into a final comprehensive assessment concept in accordance with the literature. The grounded theory analysis and Delphi method were used in the theoretical side. The methodological side adopted multiple case studies to verify the proposed mechanism. The following discussion introduces each method and the process of each method. Figure 1 illustrates the research flowchart of this study.
**Figure 1. Research flowchart in this study**
4  IT CONTROL ASSESSMENT MECHANISM PROTOTYPE DEVELOPMENT

Initially, this study obtained IT control assessment items and constructed an assessment item prototype. The main source of the present study is extant literature. Strauss and Corbin (1990) pointed out that a researcher may own a fruitful background of information if she/he were familiar with these publications. Thus, it was necessary to collect and study literature before conducting the grounded theory. Below are the criteria for the chosen studies:

- The title or abstract must contain several keywords such as “internal control,” “general control,” “information technology general control,” “information technology auditing,” “information technology risk assessment,” “information technology control risk,” “information technology control,” and “information technology management.”
- Literature selected for the current study must fall under social science such as business, management, management information systems (MIS), and accounting.
- The publication period of collected literature in this study was limited to the recent years after 2000 (period starting from 2000 to 2010).
- Only full text and academic journal papers that consisted of over five pages were included.

The selected papers must adhere to the above criteria. After filtering out unrelated text and deleting duplicate papers, the study obtained 37 papers that conformed to the in-depth exploration and analysis.

This study first conducted open coding on the content mentioned in the literature that conformed to these conditions. Among the articles, paragraphs related to IT internal control or clearly pointed out the assessment items of IT control were marked and coded. The coding was numbered consecutively from CC0001, in which “C” signified the concept. An example for identifying concepts at the open coding stage follows.

In the article “Navigating the Standards for Information Technology Controls” from O'Donnell and Rechtman (2005), we analyzed the following paragraph:

“General IT controls include the procedures and processes that support the overall processing of business applications of an organization. These controls include areas such as access to programs and data, data center operations, program development, program changes, IT disaster recovery plans, and the proper segregation of duties of information systems department personnel. The general controls are important because they support application processing. Computerized application controls include the controls involving the processing and storing of business transactions. They ensure the completeness, accuracy, authorization, and validity of processed transactions.”

At first, related key terms were marked in this paragraph, such as “access to programs and data,” “data center operations,” “program development,” “program changes,” “IT disaster recovery plans,” and “the proper segregation of duties of information systems department personnel.” Each term was checked, and its meaning was considered. The first term accessed programs and data. To prevent any user with non-authority from accessing data and programs, business entities should set identity management and access control. We labelled this term “Identity Management and Access Control (Coding Number: C0185).”

The second key term was “data center operations.” Data are crucial assets in every entity, and missing data may lead to huge losses. Thus, data backup and restoration are important tasks in the data center. This term was labeled as “Backup and Restoration (Coding Number: C0186).” The third key term was “program changes.” Entities may encounter application software changes or updates, and every change
should be controlled and managed. This term was labeled as “Manage Changes (Coding Number: C0187).”

The fourth term was “IT disaster recovery plans.” Entities must ensure that critical business processes can continue, or be recovered promptly when significant disruption occurs. This concept was labeled “Business Continuity Planning or Disaster Recovery Plan (Coding Number: C0188).” The fifth term was “proper segregation of duties of information systems department personnel.” In an entity, the lack of segregation of duties in information systems department results in weakness such as financial statement manipulation. Appropriate segregation of duties should be established to strengthen internal control. This concept was labeled “Segregation of Duties (Coding Number: C0189).” Through this coding procedure, this study collated 436 conceptualized results from selected publications.

At this stage, this study classified similar concepts into a single sub-category. For example, C0097, C0343, C0388, and C0396 were coded under the concept of “Employee Job Performance Evaluation.” C0082, C0098, C0147, and C0180 were coded “Human Resource Policies and Procedures.” C0100, C0148, C0211, C0292, C0304, C0308, C0348, C0362, C0375, C0386, C0399, and C0425 were coded “IT Personnel Competencies.” All these concepts were associated with IT human resource management. This study, therefore, merged these concepts into a single sub-category and named it, “Manage IT Human Resources.” Following the same rule, this study summarized the 436 concepts into 35 sub-categories.

After processing open coding, this study, in turn, performed axial coding. Axial coding is the process of relating subcategories to a category. The relationships of all categories derived from open coding were reviewed and rechecked. Furthermore, this study aimed to develop an assessment mechanism of internal control for IT governance, hence, 11 elements from the ERM framework and categories from ITGI (2006) were deemed related to the concept of IT governance. These elements are Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Information Communication, Monitoring, Acquire and Implement, Deliver and Support and End-user Computing, and Trading Partner Computing. This study merged the 35 assessment categories that influenced IT general control into these 11 categories in terms of its feature and causality.

The final coding stage of the grounded theory was selective coding. The main purpose of selective coding is to decide core categories from such selected categories. Thus, to accomplish this goal, all the categories obtained from axial coding were considered. The documentation of most organizations of IT controls may include entity- and activity-level controls, which are both regarded as core categories (ITGI, 2006). The 11 categories derived from axial coding were classified into these two main core categories. We constructed the coding process (open coding, axial coding, and selective coding) based on the grounded theory. The obtained IT control assessment prototype included 2 categories, 11 assessment dimensions, and 35 assessment items.

The IT control assessment prototype derived from grounded theory must be validated to confirm its suitability and correct classification. As this procedure should consider group decision making, 25 domain experts were invited to verify all assessment items via expert questionnaire. All of these experts were members of the Computer Audit Association, and had experience in assessing information system control. Thus, they were qualified experts to participate in the Delphi study.

Three rounds of Delphi questionnaires were performed. The main objectives of carrying out three rounds were to “screen the suitability and classification of these assessment items,” “refine modified assessment items,” and “confirm final assessment items.” Developed by Lawshe (1975) for evaluating content validity, content validity ratio (CVR, hereafter) is applied to confirm the assessment items for internal control. The CVR was distributed between 1 and 0.56. Collectively, the CVR of all the items are above the minimum requirement for suitability and classification. However, some panelists provided suggestions for certain items, and this study collated these suggestions by items. Moreover, the modifications and actions undertaken are follows.
The objective of the second round questionnaire was to refine the modified assessment items. Based on the results, the CVR of all items should be further confirmed to have passed the required CVR, with the distribution from 0.61 to 1.00. Overall, the CVR of all items were above the minimum requirement with regard to content precision. Meanwhile, the suitability of the added item (E.2.3. Evaluation of IT Strategy) did not meet the required CVR, and hence, this study deleted this assessment item. Furthermore, the item “E.5.3 Identify Risk Tolerance” that needed to be discussed, still passed (CVR= 0.73). The third round questionnaire aimed to confirm the assessment items refined from the previous two rounds of Delphi questionnaire. Eleven assessment dimensions and 34 assessment items were confirmed within the two main assessment categories. In the final assessment mechanism, three levels of assessment items emerged (Figure 2).
5 USABILITY VALIDATION OF THIS PROPOSED ASSESSMENT MECHANISM BY MULTIPLE CASE STUDY

5.1 Introduction of Case Company and Interviewees

Two publicly listed companies were selected as case companies (hereafter, T Company and Y Company). Both case companies already had internal control guidelines. The chair of the MIS department in each case company was responsible for the control of the information system. Both case companies conducted one or two annual self-assessments of internal control each year. Initially, the internal auditing department delivered checklists of IT control items of the MIS departments. The chief of the MIS department then used the control points to confirm the degree of control of each item. Afterwards, the chief of the internal auditing department double-checked and communicated with the chief of the MIS department for certain control weakness. In addition, with respect to external auditing, the accounting firm regularly assessed the IT control and presented the items for internal control deficiency improvement.

This study invited supervisors of the MIS and auditing departments within each case company as case interviewees. Four interviewees (two from each case company) participated in this case study. In the T Company, the chief of the information officer (hereafter, TMIS) and chief of auditing officer (hereafter, TAU) both have Masters’ degrees, and have more than 10 years of work experience. Similarly, the chief information officer (hereafter, YMIS) and senior auditor (hereafter, YAU) in the Y Company also have rich experience in specific areas. Their work years are 13 and 8, respectively. Taken together, all of the interviewees possessed appropriate professional capability for IT control assessment.

5.2 IT Control Assessment Results of Case Company via the Proposed Mechanism

Based on limited pages, this study only showed the IT control assessment process of TAU. This study drew an example to describe the operational process. Using the results of $W$ and $^\Lambda$, this study calculated the overall IT control fuzzy evaluation set $^F$ of TAU in the case company T.

The overall weight set is $W = \{0.283, 0.044, \ldots, 0.007, 0.001\}$,

$$^\Lambda = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ \ldots & \ldots & \ldots \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

the overall IT control assessment set is

$$^F = W \circ ^\Lambda = \{0.0363075, 0.9649695, 0\},$$

and the overall IT control fuzzy evaluation set is

$$= (0.001, 0.007, \ldots, 0.044, 0.283, 0)$$

Three attributes of “high,” “medium,” and “low” levels were designated to represent the following range of IT control scores: 0–33 points, 33–67 points, and 67–100 points, respectively. The indicator assessment membership in the fuzzy assessment set for IT control was considered as the $Y$-coordinate, while the assessment equal part middle point (e.g., if “high level control” represents 67–100, its middle point is $(100-67)/2=83.5$) was considered as the $X$-axis. This result was used to draw the indicator assessment for membership in the diagram. Each point was connected with straight lines, and expanded externally to the zero point (i.e., 100, 0). Figure 3 illustrates the overall IT control assessment diagram evaluated by TAU.
Subsequently, Figure 3 was divided into four zones (where Zone 1 is a line, Zones 2 and 4 are triangles, and Zone 3 is a trapezoid), and the polygon square measure (or area) formula was applied to obtain a measure of $S_i$ and the individual gravity measure $G_i$, where $i$ is the zone area. For example, the square measure of A2 is $16.16323913 \times \frac{(0.9649695 \times (50-16.5))}{2}$. Meanwhile, the gravity measure of $G_2$ is $38.83 \times \frac{(16.5+50 \times 2)}{3}$. The formula for the whole gravity $X$ is as follows: $X = \frac{\sum G_i \times S_i}{\sum S_i}$. The overall gravity position is the IT control score. Table 1 presents the calculation process of the overall IT control score.

<table>
<thead>
<tr>
<th>Zone</th>
<th>Square measure $S_i$</th>
<th>Gravity $G_i$</th>
<th>$X = 50.7585593$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone 1</td>
<td>0</td>
<td>8.25</td>
<td></td>
</tr>
<tr>
<td>Zone 2</td>
<td>16.16323913</td>
<td>38.83</td>
<td></td>
</tr>
<tr>
<td>Zone 3</td>
<td>16.77138975</td>
<td>61.571583</td>
<td></td>
</tr>
<tr>
<td>Zone 4</td>
<td>0.299536875</td>
<td>89</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Calculation process of the IT control score (TAU)

Thus, the overall IT control score is 50.7585593, which indicated “information technology control is common.” The same operational process was used for other assessment categories and dimensions. The summary of IT control assessment results between these two case companies are shown in Table 2. Taken together, most interviewees except YMIS consider that entity level control category is more important than activity level control category, and “A.1. Internal Environment” is the most important control dimension in the entity level control category.
<table>
<thead>
<tr>
<th>A. Activity-level IT Controls</th>
<th>52.98</th>
<th>52.51</th>
<th>67.48</th>
<th>70.35</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.1. Internal Environment</td>
<td>50.00</td>
<td>50.00</td>
<td>68.81</td>
<td>70.35</td>
</tr>
<tr>
<td>E.2. Objective Setting</td>
<td>50.00</td>
<td>50.00</td>
<td>77.81</td>
<td>70.35</td>
</tr>
<tr>
<td>E.3. Event Identification</td>
<td>50.00</td>
<td>50.00</td>
<td>61.89</td>
<td>70.35</td>
</tr>
<tr>
<td>E.4. Risk Assessment</td>
<td>50.00</td>
<td>50.00</td>
<td>51.65</td>
<td>70.35</td>
</tr>
<tr>
<td>E.5. Risk Response</td>
<td>50.00</td>
<td>50.00</td>
<td>51.46</td>
<td>70.35</td>
</tr>
<tr>
<td>E.6. Information and Comm.</td>
<td>50.00</td>
<td>50.00</td>
<td>54.84</td>
<td>70.35</td>
</tr>
<tr>
<td>E.7. Monitoring</td>
<td>51.56</td>
<td>52.25</td>
<td>51.63</td>
<td>70.35</td>
</tr>
<tr>
<td>A.1. Acquire and Implement</td>
<td>51.89</td>
<td>52.22</td>
<td>64.07</td>
<td>70.35</td>
</tr>
<tr>
<td>A.2. Deliver and Support</td>
<td>50.00</td>
<td>43.27</td>
<td>77.81</td>
<td>70.35</td>
</tr>
<tr>
<td>A.3. End-user Computing</td>
<td>77.83</td>
<td>77.83</td>
<td>62.79</td>
<td>70.35</td>
</tr>
<tr>
<td>A.4. Trading Partner Computing</td>
<td>50.00</td>
<td>50.00</td>
<td>50.00</td>
<td>70.35</td>
</tr>
</tbody>
</table>

Table 2. Summary of IT control assessment results between these two case companies

5.3 Usability of this Proposed Assessment Mechanism

The main objective of the case study is to understand the usability of the IT control assessment mechanism developed by this study. Usability was identified as a set of attributes that bear on the effort needed for use and on the individual assessment of such use by a stated or implied set of users (ISO, 2001). Bevan (1999) indicated that the concept of usability was similar with the “Quality in use” of the ISO 9126 framework. Quality in use measures the result of using software via the perspective of the user. Table 3 summarizes the points of usability provided by the two case companies.

6 CONCLUSION

The main purpose of this study is to establish an IT control assessment mechanism. First, the assessment categories/dimension/items of internal controls within this mechanism were derived from the grounded theory. This study adopted the Delphi method to confirm all assessment categories/dimension/items, which resulted in 2 main assessment categories, 11 assessment dimensions, and 34 assessment items. Finally, this study utilized the case study approach to validate the usability of the proposed assessment mechanism.

From a practical standpoint, the outcome of this study suggests that IT control assessment is important and potentially useful for the auditing profession. Using this proposed IT control assessment mechanism, which is considered to have comprehensive assessment categories/dimensions/items, internal auditors and chiefs of MIS departments can verify the effectiveness of internal control with a complete mechanism to comply with government regulations for IT governance. This study, owing to time limitation, selected 37 pieces of relevant literature to construct the IT control assessment categories/dimensions/items for review and coding. As a result, this study did not prove that the coding process reached saturation; other evaluation items might have been missed.
<table>
<thead>
<tr>
<th>Features</th>
<th>Features explanation</th>
<th>Case company</th>
<th>Y Company</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Suitability</strong></td>
<td>The functionality of this assessment mechanism fits the needs of a user to fulfill a certain task</td>
<td>T Company</td>
<td>Y Company</td>
</tr>
<tr>
<td><strong>Accuracy</strong></td>
<td>The results of assessment mechanism is correct</td>
<td>The outcome of this assessment mechanism can correctly find out the weak IT control in the T Company.</td>
<td>The mechanism can calculate the objective assessment results, which are close to the perception of the assessors. The outcome of this assessment mechanism can correctly find out the weak IT controls in the T Company such as E.7 monitor dimension, A.4 trading partner information system, E.4.2. Appraise Risk, E.5.2. Identify Risk Tolerance, and E.6.2. Communicate Entity External Information.</td>
</tr>
<tr>
<td><strong>Time efficiency</strong></td>
<td>The capability of the assessment mechanism to improve decision making time of the assessor</td>
<td>When more than one control needs should be improved, the sequence can be quickly worked out according to these weights, and the decision-making time can be considerably saved.</td>
<td>The control weight set can quickly allow other occupational agents to know the critical control points when implementing IT control assessment.</td>
</tr>
<tr>
<td><strong>Understandability</strong></td>
<td>The effort of the user for recognizing the logical concept of an assessment mechanism</td>
<td>Some assessment items are not available in the company at the time of the study, and this structure can be used to adjust the present version of the company. The assessment mechanism has more diversified items based on the COSO framework.</td>
<td>The weight concept of each assessment category/dimension/item could be understandable.</td>
</tr>
<tr>
<td><strong>Operability</strong></td>
<td>The effort of the user for operation and operation control</td>
<td>The assessment process of this assessment mechanism is not difficult to operate.</td>
<td>The weight determination is subject to pairwise comparison, which increases difficulties in answering. Since pairwise comparison of various category/perspective/item should be conducted before determining the weights of the information system control category/perspective/item, the problem of judgment consistency should be noted.</td>
</tr>
</tbody>
</table>

*Table 3. Summary of the usability validation of this assessment mechanism between the two case companies*
References


