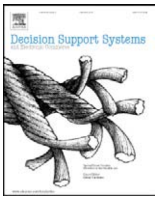
Decision Support Systems 50 (2011) 692–701

Contents lists available at ScienceDirect

Decision Support Systems

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



Building the evaluation model of the IT general control for CPAs under enterprise risk management

Shi-Ming Huang [a,1], Wei-Hsi Hung [b,2], David C. Yen [c,*], I-Cheng Chang [a,3], Dino Jiang [a,3]

[a] *Department of Accounting and Information Technology, National Chung Cheng University, Chia-Yi 62102, Taiwan, ROC*
[b] *Department of Information Management, National Chung Cheng University, Chia-Yi 62102, Taiwan, ROC*
[c] *Department of DSC & MIS, Miami University, Oxford, OH 45056, USA*

ARTICLE INFO

Available online 19 August 2010

Keywords:
Enterprise Risk Management (ERM)
Information Technology General Control (ITGC)
Control Objectives for Information and Related Technology (COBIT)

ABSTRACT

The purpose of this study is to build the evaluation model of the Information Technology General Control (ITGC) for the certified public accountants (CPAs) under an Enterprise Risk Management (ERM) — Integrated Framework. First, this study investigates and sorts out the control objectives of ITGC over financial reporting under ERM. The control objectives were prioritized by Analytic Hierarchy Process (AHP) and then, the ITGC evaluation model was constructed accordingly. Finally, the study utilizes the case study approach to verify the CPAs' acceptance for the evaluation model of ITGC. According to case study and post hoc confirmations conducted with two experts, the evaluation model can be accepted by CPAs and employed to enhance the efficiency of ITGC assessment for CPAs to meet the challenges in a dynamic information technology environment.

1. Introduction

Recently, the essential tasks in the financial reporting processes are mainly performed and supported by utilizing information technology (IT). In order to ensure a reliable financial reporting, more and more companies emphasize the use and development of effective IT control in this dynamic environment. If the firm employs a weak internal control, managers can easily override the imposed controls to manipulate or bias accrual estimate to take advantage of the stakeholders [5]. This situation has created a unique challenge for auditors. Sarbanes–Oxley Act Section 404 (SOX 404 hereafter) requires independent auditors to attest if appropriate and effective IT control over financial reporting is in place in the company. Consequently, some foreign private issuers who want to be listed in the US are required to establish corresponding accounting policy and control procedures to comply with SOX 404 [44]. In addition, after SOX emerged, some other countries such as Australia, Germany and Japan have also developed their own regulations for corporate reporting and other related disclosure laws [8,12,39]. The Statement on Auditing Standards (SAS) No. 94 [6] declared that auditors must take into account the importance of IT processes and relevant controls to prepare the financial statements. In summary, auditors have responsibility to provide the assertion to the effectiveness of IT control established by the company.

In general, the risk of audit can be composed of three parts and they are inherent risk, control risk and detection risk. If the auditor has some evidences to demonstrate that the effectiveness of internal control is well designed and operated in its entity, the risk of material misstatement might be mitigated. To reduce the audit risk in the IT environment, the auditor should have a clear and thorough understanding for IT control. Since IT General Control (ITGC) supports application processing, it is important that ITGC works well in the context of IT control. Even if ITGC may not directly influence a financial statement, it has created an impact on/to the consistency and effectiveness of financial application in all systems. Auditing Standard No. 2 of Public Company Accounting Oversight Board (PCAOB) [41] noted that the adoption of IT automated application may help increase audit efficiency when ITGC is effective.

To fulfill SOX 404 compliance, it is important for auditors to select and implement a suitable internal control framework to assess IT control. Committee of the Sponsoring Organizations of the Treadway Commission (COSO) issued a report entitled "Internal Control — Integrated Framework" [10] which had been highly recommended for companies, auditors, regulating agencies and educational institutions. After extending and refining the original concept of risk analysis, COSO released "Enterprise Risk Management (ERM) — Integrated Framework" in 2004. ERM, which is a comprehensive and systematic framework for internal control, can help firms/organizations evaluate and respond to the risks that may influence their strategies and targets [11]. However, COSO does not provide the supplemental criteria to define the needed requirements

[*] Corresponding author. Tel.: +1 513 529 4827; fax: +1 513 529 9689.
E-mail addresses: smhuang@mis.ccu.edu.tw (S.-M. Huang), fhung@mis.ccu.edu.tw (W.-H. Hung), yendc@muohio.edu (D.C. Yen), Changbenson@yahoo.com.tw (I.-C. Chang), zayin@jiang.tw (D. Jiang).
[1] Tel.: +886 5 2720411#16810; fax: +886 5 2723943.
[2] Tel.: +886 5 2720411#24620; fax: +886 5 2721501.
[3] Tel.: +886 5 2720411#34513; fax: +886 5 2721197.

0167-9236/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2010.08.015

for such IT control objectives and related activities [36]. On the other hand, when auditors perform the assessment of ITGC, they usually use the qualitative level such as “High”, “Moderate”, and “Low” to assess IT control risks based on their professional judgment and experience. However, inexperienced auditors may fail to measure the degree of risk precisely [23]. Hence, how to build up a quantitative evaluation model to aid auditors in assessing ITGC objectively is critical, and it is the main research question of this study.

There are three research objectives in this study. Firstly, this study wants to sort out the objectives of ITGC based on an ERM framework. Secondly, this study employs the Analytic Hierarchy Process (AHP) technique to analyze/rank the priority of control objectives and to construct a quantitative ITGC evaluation model. Finally, based on available data, the acceptance of the evaluation model for CPAs will be verified by conducting a case study and post hoc confirmation.

The rest of this article is divided into four sections. Section 2 describes the background of IT security, IT control, COSO-ERM, and auditors' responsibility in the internal control. In Section 3, the AHP methodology is discussed and then, development and verification of the evaluation model is covered after the introduction of research procedures by both quantitative and qualitative analyses of AHP and case study support are provided in Section 4. Finally, this paper concludes with the last section.

2. Literature review

2.1. Previous literature of IT controls

The utilization of IT in an organization can be a double-sided sword. It can help organization establish and maintain new governance processes [18,21]. Yet, IT may also increase the organizational risk, if entities do not implement key process linkages and integrated controls [55]. Previous studies indicated that traditional controls may not detect the risks arising from customization, process reengineering, bolt-on software, and incompatibilities during ERP implement process [7,56]. To be more specific, the issue of IS security has been an extremely important topic in recent years. IS security concept, in general, means that organization can employ certain measures to protect and control IS resource in order to mitigate risks and the influence of system threats to an acceptable level [54]. Dhillon [15] indicates that IS security in organizations can be of different aspects such as formal (security governance), technical (technological safeguards and controls), and informal (education and ethics). If the entities lack proper information security, they cannot guarantee the accuracy and reliability of financial data confidently [40]. For example, weak IS security can result in an unauthorized user accessing of the system, and thus, increase the risk of data being modified. Since IS security can protect/control information technology resources and enhance the accuracy and reliability of financial reporting, it has a close relationship with internal control [54].

In the meantime, to avoid the reduction of the accuracy and reliability of financial data derived from IS threats, organizations extensively use IT to support internal control over financial reporting. IT controls would exist in the entire system of internal controls, and it ensures the accuracy, integrity, and availability of transaction data in the financial statements [16,20]. IT controls can be also classified as general and application controls. General controls include security management, software acquisition, development and maintenance that can support reliable application controls and ensure the continued operation of information system [18]. Conversely, if the relevant ITGC fails, it would create a pervasively impact on all systems in its entity [25].

There are only a few studies to discuss the control test strategies for auditors [2]. Waller [53] found that the majority of auditors' risk assessments on control risks were assessed at the high score. Therefore, auditors often use substantive test when they believe it is more efficient than testing internal control [34,37]. However, SAS No. 55 [3] requires auditors to understand the internal control. Elder and Allen [17] indicated that it is more cost effective and reliable by utilizing rotational test of control. In addition, being different from Waller's [53] study, they also found that the later practices frequently show lower control risk assessment and high reliance of internal controls. Allen et al. [2] also expect auditors to extend more effective internal controls after SOX 404 being released.

SOX 404 and Auditing Standard No. 2 [41] require management level and auditors to report on internal controls over financial reporting. In the past, management level focused on control-based activities in their organizations. It is not until now the increasingly complex nature of business risks urges companies to develop proper guidance for managing their risks properly. However, no enterprise risk management framework is found for companies to follow [28]. To solve this potential problem, COSO released an Enterprise Risk Management (ERM) — Integrated Framework [11] by expanding its 1992 Internal Control-Integrated Framework in 2004. In summary, The COSO defined ERM as follows:

> “Enterprise Risk Management is a process, effected by an entity's board of directors, management, and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”.

Recently, more and more companies rely on IT heavily to ensure the reliable and trustable operation. In order to attest to and report on management assessment of the entities' internal control structure and procedures, it is truly important for auditors to follow such a framework to assess the effectiveness of their IT controls. Since ERM by nature, is a conceptual framework, it does not provide a detailed criterion about IT control objectives and related activities. However, it is found to be useful and feasible for auditors to have a guideline for IT control such as “The Control Objectives for Information and Related Technology” (COBIT) to follow. Now in its fourth edition, COBIT is widely accepted as a reliable and comprehensive framework to manage risks and IT control, and explains how IT processes deliver the information that a business needs to achieve its objectives. The COBIT, which is accepted by most entities in the world, in fact provides critical information of IT governance and control framework for management and reliable assurance of the IT control [9,43].

Furthermore, COBIT is an in-depth IT control reference for auditors to determine what to notice [18,36,38,50]. Tuttle and Vandervelde [51] examined the conceptual model of COBIT framework and found that the model can be useful for auditors while they assess IT control. Rozek [45] posited that the maturity model such as COBIT can assist auditors assess overall attitudes about IT control, and it provides a standard way to record the state of internal control. In an IT environment, the COBIT is a broadly recognized control framework, and regarded as the appropriate framework to complement the COSO evaluation framework [24,42]. Lainhart [31] mentioned that COBIT can help firms reduce IT risks. From the practical perspective, auditors agree on the function of the COBIT and its role in IT auditing [30]. However, Tuttle and Vandervelde [51] indicated that the COBIT framework could not consider some critical variables for assessing risks on IT processes, and hence, suggested that COBIT could be expanded to contain other variables such as the environment outside the organization. In spite of COBIT's involving various aspects of control items, its framework may possibly miss a few variables that can affect the audit risk. The main objective of this study is to develop an ITGC evaluation model. ERM can strength the COBIT framework, since it consists of certain components such as event identification which identifies any inside or outside vulnerability in the entity.

Table 1 lists all prior studies and/or literature which provide the different interpretations of IT controls and their key findings.

2.2. The objectives of ITGC under ERM

This study aims at determining the objectives defined for affecting financial statement of ITGC under ERM. First, ITGC starts with including all objectives at the entity level (for the overall organization) and activity level (for a specific process or business unit). The entity level control aims at a full understanding of the operation style and culture in the organization. On the other hand, the activity level control focuses on IT controls of financial reporting. The most relevant internal controls for financial statement assertions are considered to include activities that prevent, detect, and correct a significant misstatement in the financial reporting or other required disclosures (e.g., recording amounts in the general ledger, and recording journal entries).

In the entity level control, control elements under ERM consist of seven related components and they are internal environment, objective setting, event identification, risk assessment, risk response, information/communication, and monitoring. The internal environment is a foundation for all other components of ERM, and management establishes risk culture and risk taking in the entire entity. The objective setting can be employed to link vision with strategic objectives at the entity level. The event identification setting enables management to consider both external and internal factors that affect what/which event to happen. The risk assessment makes entities to consider how latent events might affect the accomplishment of objectives. The risk response setting includes risk avoidance, reduction, sharing, and acceptance. The information/communication setting can provide feedbacks and also connection and communication between the board and the management. The monitoring is a process to check the performance of entity.

In the contrast, the activity level control component under ERM is concerned with the control activity. This study follows the structure of IT Control Objectives for Sarbanes–Oxley [24] to include three kinds of control activities and they are, “Acquire and Implement”, “Deliver and Support”, and “End-User Computing”.

Secondly, even if the ERM provides a framework for ITGC, it does not provide the detailed control objectives for auditors to design and assess ITGC. The detailed objectives of ITGC are based on the IT Control Objectives for Sarbanes–Oxley [25] which is a reference to combine COSO-ERM and COBIT. In comparison, COSO-ERM is the high-level and integrated internal control framework whereas COBIT provides detailed guidance for information technology. The IT Control Objectives for Sarbanes–Oxley [25] is the combination framework that aligns COSO components with control objectives of COBIT. Furthermore, compared to other frameworks such as information security management of ISO 17799 and Information Technology Infrastructure Library (ITIL) for service management, both of them are focused on operational and financial objectives rather than the controls of financial reporting selected by ITGI [24]. The brief description of each control objective of the framework [25] is illustrated in Appendix A.

3. Research methodology

3.1. Analyze the priority of ITGC objectives

This study employed the AHP method to construct the quantitative ITGC evaluation model for IT auditors. The AHP is a multi-criteria decision making method introduced by Saaty [46], and can be applied to many areas such as accounting and social sciences [4,47]. Vargas' study [52] also pointed out that the AHP can be applied in both private and public organizations. The study of Forman and Gass [19] suggested eight applications of the AHP: (1) choice; (2) prioritization/evaluation; (3) resource allocation; (4) benchmarking; (5) quality management; (6) public policy; (7) health care; and (8) strategic planning. This study employs AHP to construct the ITGC evaluation model for the following reasons. Firstly, the AHP can be used to evaluate multiple objectives decision-making problems under uncertainty [4], and many objectives need to be assessed for the ITGC evaluation model in this research. Secondly, the AHP can help analyze

Table 1
Previous literature about IT controls and their key findings.

Author	Key findings	Implications
Edelstein [16]	IT controls would ensure the accuracy, integrity, and availability of transaction data in the financial statements.	Interpretations of IT controls from different perspectives
Flowerday and Solms [18]	IT controls can be classified as general and application controls. General controls include security management, software acquisition, development and maintenance that can support reliable application controls and ensure the continued operation of information system.	
Walters [54]	IS security can protect and control information technology resources and the accuracy and reliability of financial reporting, it has closed relationship with internal control.	
ITGI [25]	If the relevant ITGC fails, it would have pervasive impact on all systems in the entity.	If lack of proper IT control, entity may encounter potential risk.
Proctor and Vignaly [40]	If the entities lack of proper information security, they cannot guarantee the accuracy and reliability of financial data confidently. For example, weak IS security can result in unauthorized user accessing the system, and increase the risk of data being modified.	
COSO [10]	COSO issued a report entitled Internal Control-Integrated Framework which had been recommended for companies, auditors, regulating agencies and educational institutions.	Some frameworks can assist auditor to perform IT control evaluation. However, there may exist some specific natures and defeat or impede effective control evaluation.
COSO [11]	COSO released an Enterprise Risk Management (ERM) — Integrated Framework, which is a high-level and integrated internal control framework.	
ITGI [25]	Other IT control frameworks such as ISO 17799 for information security management and Information Technology Infrastructure Library (ITIL) for service management, both of them are focused on operational and financial objectives rather than controls of financial reporting.	
KPMG [30]	From a practical perspective, some auditors also agree on the function of the COBIT and its role in IT auditing.	
Lainhart [31]	COBIT can help firms reduce IT risks.	
Reghavan [43]	COBIT accepted by entities in the world provides critical information of IT governance and control framework for management and reliable assurance of the IT control.	
Tuttle and Vandervelde [51]	COBIT framework still could not consider some critical variables for assessing risks on IT processes, and suggested that COBIT could be expanded to contain variables such as the environment outside the organization.	

priorities based on a decision maker's judgment in a hierarchical structure [48,49]. This research has a necessity to identify the relative importance of objectives to help auditors assess the ITGC. The AHP in fact, helps to accomplish this aforementioned purpose. Thirdly, compared with other methods such as Analytical Network Process (ANP) and Fuzzy Integral, the AHP is relatively easy to utilize and can be utilized with a broad domain of applications. Finally, it has the capability to check the consistency with the opinion which subjects make. Further, even Delphi method can be used for making a group decision, it has some drawbacks such as much time spent on more-rounds survey, more costly, and easily distorted expert opinion [22].

Designing the hierarchy and evaluating the hierarchy are two necessary phases to perform the AHP analysis [52]. The ITGC hierarchy developed for this study is involved four levels. Level 1 of the hierarchy is the overall objective of the ITGC and Level 2 refers to two major kinds of controls from IT Control Objectives for Sarbanes–Oxley [25], namely Entity-level IT Control and Activity-level IT Control. Level 3 has 10 ERM components. “Acquire and Implement”, “Deliver and Support”, and “End-User Computing” are classified into Activity-level IT Control and the rest components are classified into the Entity-level IT Control. Finally, Level 4 consists of 26 control objectives, which come from COBIT.

To evaluate the priority of each control objective, the AHP model asks subjects to make all pair-wise comparisons of the ITGC objectives at each level of the hierarchy. The measurement scale shows the degree of importance of the objectives related to each other [47]. The scale is built with a range from one (similarly important) to five (extremely important) to contrast different degrees of importance among these objectives. Once four levels of pair-wise comparisons are completed, these aforementioned data can be used to calculate local priority of each control element (the relative importance of each ITGC objective at each level) and global priority of each control element (the relative importance of each ITGC objective at the overall level). Since all ITGC objectives are adopted from ERM and COBIT which is well known and widely accepted models, the construct validity of questionnaire is acceptable. Besides, the content of questionnaire was pre-tested and modified by two CPAs for semantic and syntactic checking purposes. We adopted consistency ratio (C.R.) ≦0.1 as an acceptable standard to verify the reliability of the AHP questionnaire [46]. In terms of the reliability of AHP questionnaire, smaller C.R. value typifies a higher degree of accuracy from decision makers' consistent assessment.

3.2. Case study for ITGC evaluation model

This study selected one of Big 4 CPA firms in Taiwan as a case sample to verify whether or not CPAs accept the ITGC evaluation model under ERM. The CPA firm is an international CPA firm and it has a large number of branches worldwide. The CPA firm helps its clients to handle with tax, consulting, and related accounting issues, and it also possesses the required professional skills for computer auditing. In practice, after IT auditors assessed the ITGC of an entity, CPAs would define auditing strategies and procedures for auditing risks.

Two-step surveys were performed for this case study. In the first step, this study invited several senior IT auditors from the CPA firm and a selected auditing company from manufacturing industry in Taiwan for assessing its ITGC. This aforementioned company was established in 1971 and publicly listed in 1988. In addition, it is one of the world's leading computer manufacturers of switching power supplies, DC brushless fans, and a major source for power management solutions, components, visual displays, industrial automation, networking products as well as renewable energy solutions. Furthermore, this company has its sales offices worldwide and manufacturing plants located at Taiwan, China, Thailand, Mexico, India and Europe. At the end of 2005, its gross profit was NT$7.3 billion and the number of employee was around 4760. In terms of corporate structure, there are eight directors and one independent director in the board.

Before assessing the ITGC, this study provided the subjects some related information such as an introduction of this task, and an introduction of this company which encompasses organizational chart; information of board of director, Chief Executive Officer, and Chief Information Officer; financial statement, demographic data of MIS department, responsibilities and accountability of MIS department, hardware devices of the company, software framework, ITGC relevant documents, and description of current ITGC.

After understanding the ITGC of the entity, participants performed the evaluation for each objective of ITGC (shown in Appendix B) on a four-level scale (i.e. All/Most Operation, Moderate Operation, Low Operation, and No Operation). According to the survey, we can get the total score and define the degree of reliability of the overall ITGC for the case (a total score of 0–33 implies low reliability; 34–66 indicates moderate reliability; and 67–100 represents high reliability).

In the second step, based on the quantitative result of case evaluation, respondents filled in the questionnaire based on the 5-point Likert Scale for three dimensions (i.e., perceived usefulness, perceived ease of use, and intention to use) of Technology Acceptance Model (TAM). This questionnaire had been pre-tested by 2 CPAs first to ensure its validity. TAM has been a powerful and solid framework for explaining users' adoption of IT [13,14]. Based on TAM, usage of an information system is determined by users' beliefs. TAM includes two kinds of important beliefs — perceived usefulness and perceived ease of use of the system. Perceived usefulness is defined as users' belief that using the system will enhance their job performance. Perceived ease of use is defined as the users believe that using the system will be free of effort. Furthermore, the model is widely applied and tested empirically to deal with a number of issues in the area of end-user technologies [33].

3.3. Research procedure/process

This study involves two stages of survey that were performed in late 2006 to early 2007. In the first stage, in order to analyze the priority of evaluated objectives of ITGC evaluation model, data were collected by an e-mail survey. In practice, the auditing plan and control risk assessment are carried out by senior auditors. Since only Big 4 accounting firms own the department of computer auditing in Taiwan, the major study subjects are the IT auditors of Big 4 accounting firms in Taiwan. This stage of survey originally yielded 32 responses from 83 questionnaires mailed. In order to ensure a representative sample, we deleted three subjects whose work experiences were below two years. After that exclusion, we deleted 10 subjects to satisfy consistency ratio criteria (C.R.≦0.1) [46]. At the end, 19 surveys are usable for calculating the priority of objectives of ITGC. All of respondents are senior auditors who have worked in the Big four CPA firms (Deloitte, KPMG, Price Waterhouse Coopers, and ERNST & YOUNG) for more than two years.

In the second stage of survey, we employed the case study method to investigate the acceptance degree of CPAs for the proposed ITGC evaluation model. From the prior literatures, usability evaluation is one of the ways to provide a convincing evidence of utility [32]. Moreover, the study of usability approach is suggested to include an ideal group of 10–20 evaluators, and some studies had applied it successfully to examine the subjective perception [1,29,57]. This process had two steps. Firstly, selected from the IT auditors in Big 4 accounting firms, 15 subjects had joined the previous stage of survey. They were introduced with the chosen ITGC case first, and then completed the ITGC evaluation model (shown in Appendix B). For the second step, six CPAs who belong to the same CPA firm and are in charge of auditing the case based on the results of auditor's evaluation for ITGC on the case. Most importantly, these six CPAs who are new to the evaluation model performed the questionnaire for acceptance. This evaluation model was disclosed to two domain experts who are in charge of ITGC project, and subsequent interviews were conducted with them to elicit more feedbacks such as what benefits could be derived using this evaluation model.

4. Results and discussion

4.1. The priority of ITGC objectives

As shown in Table 2, the "Activity-level IT Control" category was judged as more important in the ITGC. Its local priority is 0.58 which is higher than the local priority of "Entity-level IT Control" (local priority = 0.42). The study of Klamm and Watson [27] collected the data about the firms that are involved with material weakness, and found out that control activities contained much more types of material weakness than any other COSO components. Furthermore, ITGI [26] indicates that some firms' documentation just focus only on the control activities component. On the other hand, in terms of the sub-components of entity-level and activity-level controls, the result shows that the Internal Environment (global priority = 0.117) is rated less than Monitoring (0.131), Deliver and Support (0.218), Acquire and Implement (0.190), and End-User Computing (0.173) by the survey subjects in spite of the fact that the Internal Environment was being served as the foundation for all other components of ERM. One possible reason may be is that the controls of this component are more related to IT infrastructure, and hence, they may not been viewed as the major component leading to risk in the financial reporting.

Table 2
AHP judgment model — summary of results.

Information Technology General Control	Local priority	Global priority	Rank
Activity-level IT Control	0.580	0.580	1
Entity-level IT Control	0.420	0.420	2
Entity-level IT Control			
Monitoring	0.311	0.131	1
Internal Environment	0.278	0.117	2
Information/Communication	0.124	0.052	3
Objective Setting	0.114	0.048	4
Event Identification	0.074	0.031	5
Risk Assessment	0.057	0.024	6
Risk Response	0.042	0.018	7
Activity-level IT Control			
Deliver and Support	0.375	0.218	1
Acquire and Implement	0.327	0.190	2
End-User Computing	0.298	0.173	3
Entity-level (Internal Environment)			
Define IT processes, organization and relationships	0.541	0.063	1
Manage IT human resources	0.328	0.038	2
Educate and train users	0.131	0.015	3
Entity-level (Objective Setting)			
Define IT strategic planning	0.615	0.029	1
Align risk appetite	0.385	0.018	2
Entity-level (Information/Communication)			
Acquire information	0.635	0.033	1
Communicate management aims and directions	0.365	0.019	2
Entity-level (Monitoring)			
Manage quality	0.466	0.061	1
Monitor and evaluate IT performance	0.298	0.039	2
Monitor and evaluate internal control	0.236	0.031	3
Activity-level (Acquire and Implement)			
Enable operations and use	0.343	0.065	1
Manage changes	0.266	0.050	2
Install and accredit solutions and changes	0.174	0.033	3
Acquire and maintain application software	0.114	0.022	4
Acquire and maintain technology infrastructure	0.103	0.020	5
Activity-level (Deliver and Support)			
Manage data	0.324	0.071	1
Ensure systems security	0.263	0.057	2
Manage the configuration	0.125	0.027	3
Manage problems and incidents	0.092	0.020	4
Manage operations	0.076	0.017	5
Define and manage service levels	0.069	0.015	6
Manage third-party services	0.051	0.011	7

Within the Activity-level IT Control category, "Deliver and Support" (local priority = 0.375) was considered as the most important IT control objective and "Acquire and Implement" (local priority = 0.327). Because the control items of "Deliver and Support" are related to system management, those items may have direct impact on the final outcome of financial reporting. ITGI [25] also indicates that the deficiency in this part could negatively impact the company's financial reporting and disclosure activities. "Manage Data" (local priority = 0.324) and "Enable Operations and Use" (local priority = 0.343) were assessed to be the most important controls within "Deliver and Support" and "Acquire and Implement" categories respectively. In terms of "Manage Data", the financial information derived may not be reliable if without appropriate authorization controls in overall process of transactions, A variety of controls are set up to support the recording of financial information, and those controls should be paid more attention when evaluating this area. On the other hand, auditors should review service level agreements and operational practices to make sure that relevant system programs have been developed and maintained for achieving the control of "Enable Operations and Use".

Furthermore, Table 2 shows that "Monitoring" (local priority = 0.311) was determined as the most important one within the "Entity-level IT Control", and "Internal Environment" (local priority = 0.278) took the second place. This result is similar with the findings of Klamm and Watson's [27] work. They found that Monitoring and Internal Environment are ranked as top two IT-related material weaknesses among the COSO components (except for control activity). "Manage Quality" (local priority = 0.466) and "Define IT Process, Organization and Relationships" (local priority = 0.541) were found to be the most important control within "Monitoring" and "Internal Environment" categories respectively. Table 2 also shows the global priority of all objectives of ITGC.

4.2. The result of case study for ITGC Evaluation model

The result of case study for ITGC evaluation model is shown in Table 3. "Define IT Process, Organization and Relationships" (average score is 2.60), "Acquire and Maintain Application Software" (average score is 2.60), "Manage IT Human Resources" (average score is 2.53) and "Acquire and Maintain Technology Infrastructure" (average score is 2.53) were the items with a higher score of ITGC in the case study. The total score of case company is 65.06, and it was evaluated as a moderate reliable ITGC in the study.

This study demonstrates the acceptance of ITGC evaluation model for the case company by using descriptive analysis for illustration purpose. In terms of perceived usefulness, 71% of the CPAs agree that the ITGC evaluation model can help them make an effective decision; 57% of the CPAs believe that it can improve the reliability of their decision; 43% of the CPAs think that it is useful tool for decision-making. In terms of perceived ease of use, 87% of the CPAs agree that it is easy for them to use for evaluating IT auditing and related risks, and 71% of the CPAs agree that it is easy for them to understand. In terms of intention to use, 57% of the CPAs expect to choose it to evaluate IT auditing risks, and 57% of the CPAs have strong intention to use it.

For ensuring the reliability of questionnaire responses, this study uses Cronbach's α to test the consistency. All dimensions (perceived usefulness is 0.7473, perceived ease of use is 0.8247, intention to use is

Table 3
ITGC evaluation model (case).

The objectives of ITGC evaluation model			Full score[a]	Average score[b]	Score[c]
Entity-level IT Control	Internal Environment	Define IT processes, organization and relationships	6.30	2.60	5.46
		Manage IT human resources	3.80	2.53	3.20
		Educate and train users	1.50	1.87	0.94
	Objective Setting	Define IT strategic planning	2.90	2.27	2.19
		Align risk appetite	1.80	1.47	0.88
	Event Identification	Event identification	3.10	1.40	1.45
	Risk Assessment	Risk assessment	2.40	1.53	1.22
	Risk Response	Risk response	1.80	1.93	1.16
	Information/Communication	Acquire information	3.30	1.93	2.12
		Communicate management aims and directions	1.90	2.47	1.56
	Monitoring	Manage quality	6.10	1.93	3.92
		Monitor and evaluate IT performance	3.90	2.27	2.95
		Monitor and evaluate internal control	3.10	2.13	2.20
Activity-level IT Control	Acquire and Implement	Acquire and maintain application software	2.20	2.60	1.91
		Acquire and maintain technology infrastructure	2.00	2.53	1.69
		Enable operations and use	6.50	1.93	4.18
		Install and accredit solutions and changes	3.30	2.27	2.50
		Manage changes	5.00	1.93	3.22
	Deliver and Support	Define and manage service levels	1.50	1.27	0.64
		Manage third-party services	1.10	1.87	0.69
		Ensure systems security	5.70	2.33	4.43
		Manage problems and incidents	2.00	1.67	1.11
		Manage the configuration	2.70	1.60	1.44
		manage data	7.10	1.93	4.57
		Manage operations	1.70	2.40	1.36
	End-User Computing	End-user computing	17.30	1.40	8.07
Total score			100.00		65.06

[a] The full score means the weight (by 100) in this evaluation model, calculated by AHP in Section 3.1.
[b] The average score of objectives is the mean from the first step survey in Section 3.2. Range of score is from 0 to 3.
[c] Final score of this control objective = $a*(b/3)$.

0.7837, overall questionnaire is 0.7762) are above the suggested value of 0.7 [35]. This aforementioned fact proves that the questionnaire data is reliable. As for enhancing the content validity, the questionnaire has been pre-tested by two CPAs as discussed earlier.

In order to explore whether or not the evaluation model is helpful and useful to CPA firms, this study followed the process utilized by the study done by Xiang et al. [57], and reviewed it with two domain experts (the senior auditors who were in charge of ITGC project). To summarize, they were pleased with the system and believed that this evaluation model could be useful for ITGC assessment in practice in the following aspects:

- to assist CPA in planning ITGC evaluation by referencing rigorous framework and control items. Furthermore, this tool helps auditor to focus on crucial items and hence, mitigate the auditing risk.
- to easily communicate with clients through the use of a logical model based on ERM and COBIT.
- to identify which items are of higher priority for each specific client in terms of its unique industry characteristics or the distinct nature of their information systems. Moreover, the priority of each control item serves as a guideline for developing necessary evaluation items to compensate the high amount of fees paid by the client.
- to considerably reduce the time when auditors plan ITGC evaluation for their first client. Moreover, this merit also can reduce the auditors' work load and decrease the turnover rate of a CPA firm. From the long term perspective, it can be used to effectively reduce the re-training cost for CPA firms.
- to help CPA firms in predefining relevant document for assessing each control item in the training stage. Moreover, it will also improve the auditing efficiency in the evaluation stage.

5. Conclusion

Nowadays, IT control assessment is increasingly emphasized by CPAs since more and more companies use IT to generate financial reports. The ITGC is relatively important because it supports application processing, and it may even influence financial statements and/or specific accounts. However, SOX 404 does not require any specific framework when auditors assess and report the effectiveness of internal control over financial reports annually. This study developed four levels of hierarchies of ITGC objectives under ERM for independent auditors to report on the effectiveness of internal control over financial reports and constructed the quantitative ITGC evaluation model by employing AHP.

After analyzing the priority of ITGC objectives, this study finds out that the item “Activity-level IT Control” is more important than the item “Entity-level IT Control” in the ITGC. This result means that the auditors would pay more attention to the activity-level control. In the Activity-level IT Control, “Deliver and Support” is the most important objective, and this typifies that auditors would put more emphasis on the area whether entity is able to use the information systems effectively and safely. In the entity-level control, “Monitoring” is the most important objective, and this shows that the internal control through continuous and point-in-time assessment processes made by management is becoming increasingly important to implement IT governance. By ranking the overall objectives of ITGC, the top five important objectives for auditors to evaluate ITGC are “End-User Computing”, “Manage Data”, “Enable Operations and Use”, “Define IT Process, Organization and Relationships”, and “Manage Quality” respectively.

By far, End-User Computing is served as the most crucial objective. Since users are not easy to control, or they can more easily move outside the boundary of managerial influence. Hence, users may pose the greatest risk in these circumstances. This item contains two aspects for checking (spreadsheets and other user-developed programs) which are documented and regularly reviewed for reporting the result precisely. Moreover, user-developed systems and data are regularly backed up and stored in the secure manner. User-developed systems need to be protected from unauthorized access. Hence, while auditors evaluate a firm's end user computing, they need to perform some evaluation activities, such as obtaining the End-User Computing policies and procedures; confirming that they perform security and processing integrity controls; selecting users and inquiring whether they understand this policy and comply with it; reviewing user-developed systems; testing their ability to sort, summarize and report appropriately; inquiring how end-user systems are backed up and where they are stored; selecting a sample of user-developed systems; and determining whether or not unauthorized users can access.

Apart from prioritizing, the model has several applications. The first is that the ITGC evaluation model provides objectives under ERM and incorporates the concept of risk management. Thus, the auditors can follow this framework to mitigate audit risk when they assess ITGC and plan level of substantive tests (including the nature, timing, extent, and staffing of tests) as required in performing the audit tasks. The framework, on the other hand, can also help management verify their effectiveness of complying SOX 404 and other government/state related regulations for IT governance. The other application comes from the fact that it is a quantitative ITGC evaluation model. Thus, the model helps auditors assess IT control risk more precisely than traditional qualitative assessment. Furthermore, the result of top five weighted ITGC objectives would provide junior or inexperienced auditors an important and useful reference to perform their jobs.

5.1. Managerial implications

After SOX 404 was enacted, the responsibility of CPAs in attesting the effectiveness of internal control for their clients is clearly regulated. Within the changing information technology environment, auditor must have a good understanding of internal control and information security. If the auditor does not have a clear understanding, the auditing work may be full of uncertainty and risks. This study constructs an assessment model based on ERM and COBIT, and it can help auditor evaluate the effectiveness of ITGC. Moreover, the result provide a substantial help for auditors to decide its auditing strategy and auditing program in order to detect the weaknesses of internal control. Overall, the assessment model can enhance the efficiency of evaluating ITGC and mitigate the audit risk for auditors.

In practice, auditors often use qualitative levels in a traditional way to assess IT control risk based on their professional judgment and experience when performing the assessment of ITGC. When junior or inexperienced auditors have insufficient experience to perform such work, they may fail to measure the risk of ITGC precisely. Through the use of the model provided by this study, senior auditors are able to quantitatively assess an organization, and leave the results as a reference for junior auditors to assess the ITGC more efficiently.

5.2. Limitations and future research

This study can have two limitations. First, these ITGC objectives under ERM framework may not be suitable for some industries and certain types of information systems utilization, so auditors may amend or delete some control objectives to fit some specific circumstances. ITGI [25] also indicates that each organization must carefully take into account the adequate IT control objectives as necessary according to its own specific circumstances. There may be a case that one organization may decide not to include all the control objectives mentioned in the COBIT. Meanwhile, they may consider others which are not discussed in the COBIT. Similarly, the description of control objectives, illustrative controls, and illustrative tests of controls listed in the COBIT may need to be modified for reflecting the specific characteristics of certain industry or entity. In the proposed framework of this study, for instance, service industry and virtual team project based companies may emphasize the control objective of “manage project” which is not included in this evaluation model. Due to more regulations given by the government, financial sector needs to add more control items into the framework. Furthermore, for Internet based companies, such as Google, “manage performance and capacity” may be considered as a crucial control item.

Secondly, although this study used a representative case to construct an innovative and effective ITGC evaluation model, our detailed assessment results should be cited carefully for the purpose of comparison. Thirdly, this evaluation model can be used to judge the degree of ITGC as high, moderate, or low based on the total score calculated. Despite that the total scores of might be closely located in the level boundary, auditors can professionally utilize the result produced from our model to judge client's ITGC. For instance, two companies assessed the score of 35 and 65 are identified as the moderate reliability via this evaluation model. However, auditors can differentiate the ITGC degree of these two companies by their professional judgment. In addition, despite the eyes being caught by high total score of the ITGC result, the auditor must also pay attention to check whether those control items with extreme low or zero scores will generate serious risk to the company.

There are some directions for future research. First, since the ITGC evaluation model is based on the higher level of risk evaluation under ERM, future research can verify current detailed objectives or even add more specific detailed objectives to tailor the assessment of different industries and information systems (e.g. SAP, Oracle, and JDE). Secondly, future research can develop more interactive and more user friendly application programs for ITGC evaluation model. Finally, it may be possible for CPAs to conduct more case studies in other industries, and then use the results to construct the related norm database of evaluation model for the establishment of the industrial best practice examples.

Acknowledgements

The work presented in this paper has been supported by The National Science Council, Taiwan, R.O.C., under Grant No. NSC97-2410-H-194-074-MY3. The authors of this research appreciate deeply their financial support and encouragement.

Appendix A. Description of ITGC objectives

The objectives of ITGC evaluation model		Description
Internal Environment	Define IT processes, organization and relationships	An IT organization must be defined considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organization is to be embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management.
	Manage IT human resources	Acquire, maintain and motivate a competent workforce for creation and delivery of IT services to the business. This is achieved by following defined and agreed practices supporting recruiting, training, evaluating performance, promoting and terminating.
	Educate and train users	Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group.
Objective Setting	Define IT strategic planning	IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realized from project and service portfolios.

Appendix A (*continued*)

The objectives of ITGC evaluation model		Description
	Align risk appetite	Integrate the IT governance, risk management and control framework with the organization's (enterprise's) risk management framework. This includes alignment with the organization's risk appetite and risk tolerance level.
Event Identification	Event identification	Identify any event (threat and vulnerability) with a potential impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects.
Risk Assessment	Risk assessment	Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods.
Risk Response	Risk response	Identify a risk owner and affected process owners, and develop and maintain a risk response to ensure that cost-effective controls and security measures mitigate exposure to risks on a continuing basis.
Information/ Communication	Acquire information	Management should ensure the original data and information is reliable and provides it to make decision effectively. This information is consisted of historical and concurrent data that is uniform format, and utilized by authorized users.
	Communicate management aims and directions	Management should develop an enterprise IT control framework and define and communicate policies. An ongoing communication program should be implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management.
Monitoring	Manage quality	A quality management system should be developed and maintained, which includes proven development and acquisition processes and standards.
	Monitor and evaluate IT performance	Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, a systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.
	Monitor and evaluate internal control	Establishing an effective internal control program for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews.
Acquire and Implement	Acquire and maintain application software	Applications have to be made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the actual development and configuration according to standards.
	Acquire and maintain technology infrastructure	Organizations should have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed technology strategies and the provision of development and test environments.

Appendix A (*continued*)

The objectives of ITGC evaluation model		Description
	Enable operations and use	This process requires the production of documentation and manuals for users and IT, and provides training to ensure proper use and operations of applications and infrastructure.
	Install and accredit solutions and changes	New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review.
	Manage changes	All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner.
Deliver and Support	Define and manage service levels	Effective communication between IT management and business customers regarding services required is enabled by a documented definition and agreement of IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels.
	Manage third-party services	The need to assure that services provided by third parties meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance.
	Ensure systems security	The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents.
	Manage problems and incidents	Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes identification of recommendations for improvement, maintenance of problem records and review of the status of corrective actions.
	Manage the configuration	Ensuring the integrity of hardware and software configurations requires establishment and maintenance of an accurate and complete configuration repository.
	Manage data	Effective data management requires identifying data requirements. The data management process also includes establishing effective procedures to manage the media library, backup and recovery of data, and proper disposal of media.
	Manage operations	Complete and accurate processing of data requires effective management of data processing and maintenance of hardware.

(*continued on next page*)

Appendix A (*continued*)

The objectives of ITGC evaluation model		Description
End-User Computing	End-user computing	Effective End-user computing requires policies and procedures concerning security and processing integrity exist and are followed. Next, End-user computing, including spreadsheets and other user-developed programs, are documented and regularly reviewed for processing integrity, including their ability to sort, summarize and report accurately. Further, user-developed systems and data are regularly backed up and stored in a secure area. User-developed systems, such as spreadsheets and other end-user programs, are secured from unauthorized use.

Appendix B. ITGC evaluation model

There are 4 levels to our general IT control measurement scale: 0. No operation (no items achieve control objectives); 1. Low operation (few items achieve control objectives); 2. Moderate operation (a few items don't achieve control objectives or have material deficiency); 3. All/most operation (most items achieve control objectives and no material deficiency). According to general IT control of the case, please given suitable scale for each item.

		Assessment items	Scale
Entity-level IT Control	Internal Environment	Define IT processes, organization and relationships	
		Manage IT human resources	
		Educate and train users	
	Objective Setting	Define IT strategic planning	
		Align risk appetite	
	Event Identification		
	Risk Assessment		
	Risk Response		
	Information/Communication	Acquire information	
		Communicate management aims and directions	
	Monitoring	Manage quality	
		Monitor and evaluate IT performance	
		Monitor and evaluate internal control	
Activity-level IT Control	Acquire and Implement	Acquire and maintain application software	
		Acquire and maintain technology infrastructure	
		Enable operations and use	
		Install and accredit solutions and changes	
		Manage changes	
	Deliver and Support	Define and manage service levels	
		Manage third-party services	
		Ensure systems security	
		Manage problems and incidents	
		Manage the configuration	
		Manage data	
		Manage operations	
	End-User Computing		
Total			

References

[1] J. Allan, A. Leuski, R. Swan, D. Byrd, Evaluating combinations of ranked lists and visualizations of inter-document similarity, Information Processing and Management 37 (3) (2001) 435–458.

[2] R.D. Allen, D.R. Hermanson, T.M. Kozloski, R.J. Ramsay, Auditor risk assessment: insights from the academic literature, Accounting Horizons 20 (2) (2006) 157–177.

[3] American Institute of Certified Public Accountants (AICPA), Consideration of Internal Control in a Financial Statement Audit, Statement on Auditing Standards No. 55, AICPA, New York, 1988.

[4] B. Apostolou, J.M. Hassell, An overview of the analytic hierarchy process and its use in accounting research, Journal of Accounting Literature 12 (1993) 1–28.

[5] H. Ashbaugh-Skaife, D.W. Collins, W.R. Kinney, R. LaFond, The effect of SOX internal control deficiencies and their remediation on accrual quality, The Accounting Review 83 (1) (2008) 217–250.

[6] Auditing Standards Board (ASB), The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit, Statement on Auditing Standards No.94, Auditing Standards Board, Washington, D. C., 2001.

[7] B. Bae, P. Ashcroft, Implementation of ERP systems: accounting and auditing implications, Information Systems Control Journal 5 (4) (2004) 43–48.

[8] U. Breandle, J. Noll, A fig leaf for the naked corporation, Journal of Management and Governance 9 (1) (2005) 79–99.

[9] M.J. Coe, Trust services: a better way to evaluate I.T. controls, Journal of Accountancy 199 (3) (2005) 69–75.

[10] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control-Integrated Framework, COSO, New York, 1992.

[11] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management — Integrated Framework, COSO, New York, 2004.

[12] Commonwealth of Australia, Corporate Disclosure: Strengthening the Financial Reporting Framework, 2002 Retrieved from http://www.treasury.gov.au/contentitem.asp?NavId=&ContentID=403.

[13] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly 13 (3) (1989) 319–340.

[14] F.D. Davis, R.P. Bagozzi, P.R. Warshaw, User acceptance of computer technology: a comparison of two theoretical models, Management Science 35 (8) (1989) 982–1003.

[15] G. Dhillon, Principles of Information System Security: Text and Cases, John Wiley & Sons, New Jersey, 2007.

[16] S.M. Edelstein, Sarbanes–Oxley compliance for nonaccelerated filers, CPA Journal 74 (12) (2004) 52–59.

[17] R.J. Elder, R.D. Allen, A longitudinal field investigation of audit risk assessments and sample size decisions, The Accounting Review 78 (4) (2003) 983–1002.

[18] S. Flowerday, R.V. Solms, Real time information integrity = system integrity + data integrity + continuous assurances, Computers & Security 24 (8) (2005) 604–613.

[19] E.H. Forman, S.I. Gass, The analytic hierarchy process — an exposition, Operations Research 49 (4) (2001) 469–486.

[20] Global Technology Audit Guide (GTAG), Information Technology Controls, Global Technology Audit Guide, Illinois, 2005.

[21] S. Hamaker, Principles of IT governance, Information Systems Control Journal 2 (2004) 47–50.

[22] T.H. Hsu, T.H. Yang, Application of fuzzy analytic hierarchy process in the selection of advertising media, Journal of Management & Systems 7 (1) (2000) 19–39.

[23] S.S. Hwang, T. Shin, I. Han, CRAS-CBR: internal control risk assessment system using case-based reasoning, Expert Systems 21 (1) (2004) 22–33.

[24] IT Governance Institute (ITGI), Control Objectives for Information and related Technology (COBIT) Version 4.0, ITGI, Illinois, 2005.

[25] IT Governance Institute (ITGI), IT Control Objectives for Sarbanes–Oxley, 2nd Edition, ITGI, Illinois, 2006.

[26] IT Governance Institute (ITGI), COBIT 4.1: Framework Control Objectives Management Guidelines Maturity Models. Rolling Meadows, ITGI, Illinois, 2007.

[27] B.K. Klamm, M.W. Watson, SOX 404 reported internal control weakness: a test of COSO framework components and information technology, Journal of Information Systems 23 (2) (2009) 1–23.

[28] A.E. Kleffner, The effect of corporate governance on the use of enterprise risk management: evidence from Canada, Risk Management & Insurance Review 6 (1) (2003) 53–74.

[29] S. Koshman, Visualization-based information retrieval on the web, Library & Information Science Research 28 (2) (2006) 192–207.

[30] KPMG, Frontiers in Finance for Decision Makers in Financial Services, KPMG LLP, Chicago, 2003.

[31] J.V. Lainhart, An IT assurance framework for the future, Ohio CPA Journal 60 (1) (2001) 19–23.

[32] S.T. Li, W.C. Chang, Design and evaluation of a layered thematic knowledge map system, Journal of Computer Information Systems 49 (2) (2009) 92–103.

[33] Q. Ma, L. Liu, The technology acceptance model: a meta-analysis of empirical findings, Journal of Organizational and End User Computing 16 (1) (2004) 59–72.

[34] T.J. Mock, A. Wright, An exploratory study of auditors' evidential planning judgments, Auditing: A Journal of Practice & Theory 12 (2) (1993) 39–61.

[35] J.C. Nunnally, I.H. Bernstein, Psychometric Theory, McGraw, New York, 1994.

[36] J.B. O'Donnell, Y. Rechtman, Navigating the standards for information technology controls, The CPA Journal 75 (7) (2005) 64–69.

[37] T. O'Keefe, D. Simunic, M. Stein, The production of audit services: evidence from a major public accounting firm, Journal of Accounting Research 32 (2) (1994) 241–261.

[38] M. Petterson, The keys of effective IT auditing, Journal of Corporate Accounting & Finance 16 (5) (2005) 41–46.

[39] PricewaterhouseCoopers, Sarbanes–Oxley — Internal Control Solutions Framework, 2003 Retrieved from http://www.pwc.com.

[40] P. Proctor, J. Vignaly, The Security Implications of Sarbanes–Oxley. Symantec Enterprise Solutions Webcast, 2004 Retrieved from http://www.symantec.com/press/2004/n040218c.html.

[41] Public Company Accounting Oversight Board (PCAOB), Auditing Standard No.2: An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, PCAOB, Washington, D. C., 2004.

[42] M. Ramos, Evaluate the control environment, Journal of Accountancy 197 (5) (2004) 75–78.

[43] K.R. Reghavan, Internal control and operational risk: FDICIA, Sarbanes–Oxley and Basel II, Bank Accounting and Finance 19 (3) (2006) 3–9.

[44] P. Rikhardsson, P. Best, C. Juhl-Christensen, Sarbanes–Oxley compliance, internal control, and ERP systems: the case of mySAP ERP, in: C. Ferran, R. Salim (Eds.), Enterprise Resource Planning for Global Economies: Managerial Issues and Challenges, Ch. 12, Hershey, New York, 2008.

[45] P. Rozek, Putting IT governance into action, Internal Auditor 65 (3) (2008) 29–31.

[46] T.L. Saaty, The Analytic Hierarchy Process, McGraw-Hill, New York, 1980.

[47] T.L. Saaty, Absolute and relative measurement with the AHP: the most livable cities in the United States, Socio-Economic Planning Science 20 (6) (1986) 327–331.

[48] T.L. Saaty, Rank generation, preservation and reversal in the analytic hierarchy decision process, Decision Sciences 18 (2) (1987) 157–177.

[49] T.L. Saaty, How to make a decision: the analytic hierarchy process, European Journal of Operational Research 48 (1) (1990) 9–26.

[50] B.V. Solms, Information security governance: COBIT or ISO17799 or both? Computers and Security 24 (2) (2005) 99–104.

[51] B. Tuttle, S.D. Vandervelde, An empirical examination of CobiT as an internal control framework for information technology, International Journal of Accounting Information Systems 8 (4) (2007) 240–263.

[52] L.G. Vargas, An overview of the analytic hierarchy process and it applications, European Journal of Operational Research 48 (1) (1990) 2–8.

[53] W.S. Waller, Auditors' assessments of inherent and control risk in field settings, The Accounting Review 68 (4) (1993) 783–803.

[54] L.M. Walters, A draft of an information systems security and control course, Journal of Information Systems 21 (1) (2007) 123–148.

[55] M.L. Weidenmier, S. Ramamoorti, Research opportunities in information technology and internal auditing, Journal of Information Systems 20 (1) (2006) 205–219.

[56] S. Wright, A.M. Wright, Information system assurance for enterprise resource planning systems: unique risk considerations, Journal of Information Systems 16 (1) (2002) 99–114.

[57] Y. Xiang, M. Chau, H. Atabakhsh, H. Chen, Visualizing criminal relationships: comparison of a hyperbolic tree and a hierarchical list, Decision Support Systems 41 (1) (2005) 69–83.

Shi-Ming Huang received his PhD degree at the School of Computing and Information Systems, University of Sunderland, U.K. He is currently a Dean for College of Management and a Director for the Research Center of e-Manufacturing and e-Commerce at National Chung Cheng University, Taiwan. He has published five books, three business software and over 60 articles in refereed information system journals, such as Information and Management, Decision Support Systems, Journal of Computer Information Systems, European Journal of Operational Research, Journal of Database Management, ACM SIGMOD, etc. He has received over 10 achievement awards in information system area. He has served as an editorial board member in several international journals and has acted as a consultant for a variety of Taiwan government departments, software companies and commercial companies.

Wei-Hsi Hung is an Assistant Professor of Information Management at National Chung Cheng University, Taiwan. He received his Ph.D. and Master's degree (with 1st Class Hons) from the Department of Management Systems at the University of Waikato, New Zealand. Prior to his postgraduate studies, his major was industrial engineering. His research interests are in the areas of B2B e-commerce, IS alignment, knowledge management, and supply chain management. His research papers appeared in journals such as Decision Support Systems, Journal of Information Management, and Pacific Asian Journal of Association for Information Systems.

David C. Yen is currently a Raymond E. Glos Professor in Business and a Professor of MIS of the Department of Decision Sciences and Management Information Systems at Miami University. Professor Yen is active in research and has published books and articles which have appeared in *Communications of the ACM*, *Decision Support Systems*, *Information & Management*, *Information Sciences*, *Computer Standards and Interfaces*, *Government Information Quarterly*, *Information Society*, *Omega*, *International Journal of Organizational Computing and Electronic Commerce*, and *Communications of AIS* among others. Professor Yen's research interests include data communications, electronic/mobile commerce, database, and systems analysis and design.

I-Cheng Chang is currently a PhD student at the Department of Accounting and Information Technology, National Chung Cheng University (Taiwan). His direction is focusing on information technology governance and computer auditing. He has published research papers in journal such as Information Systems Management and Information Systems Frontier.

Dino Jiang is a Senior Audit Controller at Charoen Pokphand Group in China. He received his Master's degree from the Department of Accounting and Information Technology at the University of Chung Cheng, Taiwan. He has 12 years of experience in various fields as a financial assurance, IT audit, performance audit and ERP improvement. He also holds the CISA, CIA, MCDBA, MCSA and MCSE certifications.