



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.

© 2010 Elsevier B.V. All rights reserved.

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), yencd@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.

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.

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات