



Internal control framework for a compliant ERP system



She-I Chang^a, David C. Yen^{b,*}, I-Cheng Chang^c, Derek Jan^d

^a Department of Accounting and Information Technology, National Chung Cheng University, Taiwan, ROC

^b School of Economics and Business, SUNY College at Oneonta, USA

^c Department of Accounting, National Dong Hwa University, ROC

^d KPMG, Taiwan, ROC

ARTICLE INFO

Article history:

Received 1 February 2012

Received in revised form 17 October 2013

Accepted 4 November 2013

Available online 20 November 2013

Keywords:

Internal control framework
Enterprise resource planning
IT control

ABSTRACT

After the occurrence of numerous worldwide financial scandals, the importance of related issues such as internal control and information security has greatly increased. This study develops an internal control framework that can be applied within an enterprise resource planning (ERP) system. A literature review is first conducted to examine the necessary forms of internal control in information technology (IT) systems. The control criteria for the establishment of the internal control framework are then constructed. A case study is conducted to verify the feasibility of the established framework. This study proposes a 12-dimensional framework with 37 control items aimed at helping auditors perform effective audits by inspecting essential internal control points in ERP systems. The proposed framework allows companies to enhance IT audit efficiency and mitigates control risk. Moreover, companies that refer to this framework and consider the limitations of their own IT management can establish a more robust IT management mechanism.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

The popularity of information technology (IT) applications has increased reliance on computers for processing business transactions. Companies adopt IT systems to improve their operations. Surveys on the collaborative operations of IT systems conducted by the Market Intelligence and Consulting Institute [42] indicate that the enterprise resource planning (ERP) system is the most widely adopted IT system among large companies.

Given that ERP is a popular and all-encompassing information system utilized by many organizations and because of the increased consideration of the risks associated with IT, information system security and internal control related to information systems have greatly increased [17,45,63,75]. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as “a process, effected by an entity’s board, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives such as effectiveness and efficiency of operation, reliability of financial reporting, and compliance with regulation” [15]. The internal control related to information systems is commonly referred to as IT control and is composed of controls (i.e., policies and procedures) over the

organizational IT infrastructure and systems [47,63]. IT control consists of general and application controls. General controls refer to the relevant controls designed to ensure that an entity’s control environment is well managed and applied to all sizes of systems ranging from large mainframe systems to client/server systems and to desktop and/or laptop computer systems. Application controls include input, processing, and output control based on the flow of data processing. In other words, application controls focus on the accuracy, completeness, validity, and authorization of the data captured, entered in the system, processed, stored, transmitted to other systems, and reported [54]. Further, general controls can be used to support the application controls and, hence, allow the smooth operation of the information system [22]. Given that financial reporting in many entities is based on information systems such as ERP systems, IT controls help entities achieve the objective of internal control. Similar to information security, IT controls can also manage and protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [68].

An attack on information generally leads to the theft of confidential data, financial fraud, incapacitated web servers, and corrupted operational data [27], which all influence the accuracy and reliability of the financial data derived from the information system [75]. If entities fail to establish proper information security, they cannot guarantee the accuracy and reliability of their financial data [51]. ERP built-in control features may positively impact the effectiveness of internal controls over financial reporting. However, ERP does not necessarily safeguard against some deliberate

* Corresponding author at: School of Economics and Business, SUNY College at Oneonta, USA. Tel.: +1 607 436 3458; fax: +1 607 436 2543.

E-mail addresses: actsic@ccu.edu.tw (S.-I. Chang), David.Yen@oneonta.edu (D.C. Yen), icc@mail.ndhu.edu.tw (I.-C. Chang), Derek.Jan@seed.net.tw (D. Jan).

system manipulations, for example, a few control features might not be activated in a timely manner in the implementation stage [45]. Further, to manipulate the date to perform earnings management, top managers may attempt to override some control features [6]. Following a number of reported business scandals, investors are beginning to question the accuracy of financial reports, including those generated by major companies around the world. In fact, investor confidence in the accuracy of financial reports and the shared holding positions of large companies has collapsed over recent years [56]. Durfee [18] emphasizes that an announcement of material weakness in the internal control system may result in a drop in stock prices, an increase in share volume, and the loss of chief financial positions. Goel and Shawky [26] also indicate that announcements of security breaches would decrease the market share of firms. Conversely, effective internal control can help firms to achieve their expected financial goals, maintain precise records of daily transactions, and produce accurate financial statements [20]. The accuracy and reliability of data within the ERP system are critical to ensure the transparency of the company's situation at all times, to help rebuild investor confidence, and to ensure low cost of capital [3].

Software vendors establish “built-in” control within ERP systems [45]. Companies also have an internal control framework in their ERP systems. Management is required to establish the framework, especially when a company is publicly listed. Companies constantly audit the effectiveness of their ERP system's internal control. Thus, an increasing number of companies have started to focus on the implementation of effective controls in their ERP systems while simultaneously providing management and external auditors a suitable framework within which to assess the ERP system's internal control. COSO released a report entitled “Internal Control-Integrated Framework” [15] in 1992 in an attempt to illustrate a systematic framework for internal control. However, the report failed to list supplemental criteria in the implementation and assessment of IT controls [49]. Referring to specific control items would allow management and auditors to execute IT control procedures [29]. However, IT control procedures not only consider the environment within the entity but also control as it relates to the external environment [66]. In addition, given the minimal compliance guidance in the use of IT established by the government, the interpretation of the scope and nature of the IT environment is inconsistent [8]. These limitations increase the difficulty of compliance. Despite the importance of deploying proper internal control frameworks to fully develop the effectiveness of the ERP system, only a few academic studies have assessed this issue. Accordingly, this study derives its primary research question: what are the types of internal control that must be considered when auditing an ERP system? The primary objective of this study is to develop a preliminary internal control framework for application in an ERP system.

2. Research background

The growing awareness of IT's role in managing knowledge derived from information systems has caused the production of accurate and relevant information to become the focus of studies on information systems such as accounting information systems (AIS) and management information systems (MIS) [76]. IT governance has been recently discussed and has gained attention; IT governance is “used to describe how those persons entrusted with governance of an entity will consider IT in this supervision, monitoring, control, and direction of the entity” [32]. Well-defined controls are considered to be an imperative and necessary part of IT governance. This study attempts to establish good internal control standards for ERP systems by proposing an internal control framework for such systems. Three subtopics are discussed in this

section. The first subsection describes system security and internal controls in the ERP system. The second subsection introduces the audit and inspection challenges associated with the ERP system. The third subsection presents and discusses the internal control framework.

2.1. System security and internal controls in the ERP system

An increasing number of firms depend on ERP to address operational transactions. Therefore, information system security must be emphasized, especially in financial transactions [70,73]. Walters [75] states that many information system threats, such as unauthorized access and system vulnerability attacks, influence the accuracy and reliability of the financial data derived from information systems. Information security protects and controls IT resources and ensures the accuracy and reliability of information [1]. Van de Riet et al. [69] note a number of security aspects associated with an ERP system; these aspects include security policy, user authentication, authorization, time restrictions, log and trace, and database security.

Information security control maintains the reliability of the information system resource and the availability and integrity of financial data. Thus, information security control is closely linked with information security and internal controls. After the occurrence of numerous worldwide financial scandals, company management teams and auditors are now required to take responsibility for their respective financial reports. The effectiveness of internal control has been emphasized during this decade [52]. If firms lack the proper level and types of information security, they cannot ensure the effectiveness of their internal controls and the integrity of their financial data [51]. Thus, identifying the necessary control-related considerations in an ERP system is an important initial task for management and auditors.

2.2. Audit and inspection challenges in the ERP system

The introduction of a new information system in a company may generate a new risk that is different from the risks initially associated with the legacy framework: the risks that accompany new framework operations may not be similar to those of the original system [50]. Reengineering business processes and the organizational changes brought about by the introduction of a new system may also lead to changes in the control requirements of a company in terms of ERP [11]. Problems frequently associated with ERP systems are generally contained. Such issues include business interruption, process interdependency, network security, database security, application security, and overall internal controls [31]. Therefore, many key aspects of the risk control environment must be considered [56]. Glover et al. [25] suggest that internal auditors consider the relevant risks and controls required for system planning based on their knowledge of risk management and of the internal risks present in the company during the introduction of the ERP system. Auditors and inspectors should first understand the basic architecture of the ERP system to effectively exert internal control over it [2,9]. In the comprehensive application of the IT environment, “owning” the control framework can help auditors to evaluate the effectiveness of IT control and decide on an auditing strategy and program. The control framework can also enhance the efficiency of IT control evaluation and mitigate the audit risk for auditors [29].

2.3. Internal control framework

Management and the auditors must follow a suitable and holistic internal control framework to ensure the effectiveness of internal control in a firm. COSO released a report entitled “Internal

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