Are Financial Auditors Overconfident in Their Ability to Assess Risks Associated with Enterprise Resource Planning Systems?

James E. Hunton  
_Bentley College and University of Maastricht_  
Arnold M. Wright  
_Boston College_  
Sally Wright  
_University of Massachusetts Boston_

**ABSTRACT:** The first objective of the current study is to examine the extent to which financial auditors recognize heightened risks associated with an enterprise resource planning (ERP) system, as compared to a non-ERP (legacy) system, in the presence of a control weakness over access privileges. The second objective is to assess the propensity of financial auditors to consult with information technology (IT) audit specialists within their firm when assessing ERP and non-ERP system risks during the planning stage of an audit. One hundred sixty-five auditors participated in an experiment in which we manipulated system type (ERP versus non-ERP) and measured auditor type (IT audit specialists versus financial auditors). Both auditor types indicate significantly higher business interruption, process interdependency, and overall control risks with the ERP, as compared to the non-ERP, system. Additionally, while IT audit specialists assess significantly higher network, database, and application security risks with the ERP system, financial audits do not recognize higher security risks in these areas. Perceived risk differentials from the non-ERP to the ERP system across all risk categories are significantly greater for IT audit specialists than financial auditors. Finally, financial auditors do not indicate a greater need to consult with IT audit specialists when auditing an ERP versus a non-ERP system and they are equally highly confident in the ability of financial audit teams to assess risks in both computing environments. Overall, evidence from this study suggests that financial auditors may be overconfident in their ability to assess ERP system risks.

**Keywords:** enterprise resource planning; ERP; audit risks; business risks; audit specialists.

**Data Availability:** Data are available from the authors; however, requests for data should specify the intended use.

We thank those who attended the 2002 American Accounting Association Auditing Midyear Meeting, the Eighth AIS Research Symposium, and the 2001 European Conference on Accounting Information Systems (ECAIS) for their valuable input. We also thank those who participated in workshops at the University of Connecticut, University of Georgia, University of Washington, and University of Wisconsin for their helpful advice. Finally, we specifically thank Michael Bamber, Stan Biggs, Pat Dorr, Kathy Hurt, Karla Johnstone, Kathryn Kadous, Jane Kennedy, Bill Messier, Jay Rich, Andy Rosman, Dan Stone, Scott Vandervelde, and two anonymous _JIS_ reviewers for their insightful comments.
I. INTRODUCTION

Enterprise resource planning (ERP) systems facilitate horizontal and vertical integration of business processes across an organization via a synchronized suite of software applications. Although very costly to implement, many companies have adopted ERP systems due to potential efficiency improvements (e.g., employee productivity and inventory savings) and effectiveness gains (e.g., product quality and customer satisfaction) (e.g., Brown 1997; Hayes et al. 2001; Poston and Grabski 2001; Scheer and Habermann 2000; Soh et al. 2000). Despite their acclaimed advantages, ERP systems pose potentially heightened business, security, and audit risks primarily due to automated interdependencies among business processes and integrated relational databases (Girard and Farmer 1999).

Statement on Auditing Standards (SAS) No. 94 (AICPA 2001) calls for auditors to understand the computerized procedures used to prepare an entity’s financial statements and related disclosures. More specifically, SAS No. 94 requires auditors to consider how the client’s information technology (IT) infrastructure affects the audit strategy, to design audit tests to determine the extent to which computerized internal controls are operating effectively, and to possess requisite skills to evaluate and test IT systems or obtain help from specialists who have such skills.

A recent statement by the Panel on Audit Effectiveness (POE) highlights its concerns regarding the ability of auditors to properly assess risks associated with advanced business information systems, such as ERP systems (POE 2000). Specifically, the POE (2000, 171) states:

Increasingly, auditors will find it necessary to understand fully the risks associated with new and advanced business information systems, and the controls that are needed to respond to those risks. Auditors also will find that they must expand their technological knowledge and skills, devise more effective audit approaches by taking advantage of technology, and design different types of audit tests to respond to new business processes. Highly skilled technology specialists will become even more essential members of audit engagement teams.

In light of the mandates of SAS No. 94 and concerns raised by the POE, one purpose of the current study is to examine the extent to which financial auditors and IT audit specialists recognize potentially heightened risks associated with ERP, as compared to non-ERP (legacy), systems during the planning phase of an audit engagement. A second purpose is to investigate the propensity of financial auditors to consult with IT audit specialists when evaluating ERP system risks. To our knowledge, researchers have not investigated these issues in prior accounting studies.

We examine the risk assessments of 82 IT audit specialists and 83 financial auditors with regard to an experimental case where a client operates either an ERP or a non-ERP computer system. Both the ERP and non-ERP case scenarios contain the same seeded control weakness that results in significantly greater security risks in the ERP setting. After reading the case, participants assess the following risk categories: business interruption, process interdependency, network security, database security, application security, and overall internal control. IT audit specialists assess significantly higher risks across all categories in the ERP, as compared to the non-ERP, system condition. Financial auditors assess greater business interruption, process interdependency, and overall internal control risks for the ERP system; however, despite the presence of the seeded control weakness, they indicate similar risks in both computing environments for network security, database security, and application security. Risk assessment differences between the two system types are significantly greater for IT audit specialists than for financial auditors in all risk categories. Further, financial auditors do not indicate a greater need to consult with IT specialists in the ERP, as compared to the non-ERP system environment, and, they are equally highly confident in the ability of financial audit teams to assess risks in both computing environments. The study findings suggest that financial auditors are overconfident in their ability to assess IT-related risks in an ERP computing environment.
The next section provides a review of relevant literature and identifies research hypotheses. The subsequent two sections describe the research method and present the study findings. The final section discusses the results, identifies future research ideas, and suggests implications for IT and financial audit practices.

II. BACKGROUND AND HYPOTHESES

Kumar and Hillegersberg (2000, 23) define ERP systems as “information systems packages that integrate information and information-based processes within and across functional areas in an organization.” ERP and non-ERP computing environments differ in many ways. Most notably, ERP systems link related business processes to one another through workflow automation and relational databases, which can facilitate real-time capturing and processing of economic events. As a result, ERP systems offer a number of potential operational and control advantages over traditional non-ERP systems. For instance, once the ERP system captures a sale, workflow automation can automatically track manufacturing, order filling, shipping, billing, and collecting processes, thus increasing the likelihood of fulfilling and completing the order in an accurate and timely manner. Despite the potential advantages of ERP systems, the interdependent nature of system applications and the reliance on relational databases expose a company to significantly different business interruption, process interdependency, and system security risks than traditional non-ERP systems (O’Leary 2000).

Business interruption risk refers to the likelihood that endogenous or exogenous factors, such as computer hardware or software failures, labor strikes, or natural disasters will disrupt a company’s ability to accurately process and record economic transactions in a timely manner. Process interdependency risk represents the likelihood that disturbances in automated or manual workflow procedures will fail to transmit information from upstream processes (e.g., sales orders) to related downstream processes (e.g., procurement, production, shipping, and billing). System security risk reflects the likelihood that a variety of possible undesirable actions committed by mischievous employees, dishonest employees, or outside hackers will compromise the integrity of a company’s information system.

An audit perspective classifies business interruption as an inherent or client business risk and the other two categories as control risks. Regarding the latter two categories, if management does not incorporate proper control procedures into the computing environment, then unintentional or intentional errors can occur, which can lead to significant financial losses and material financial statement errors. For instance, a major error introduced during the sales ordering process (e.g., quantity ordered on a specialty product is erroneously doubled) might propagate downstream to the production function (process interdependency risk), thereby resulting in a material loss, or unauthorized system access (system security risk) may lead to fraudulent behavior (e.g., unauthorized purchases) with material consequences.

A recent interview study by Wright and Wright (2002) illustrates the concerns of IT audit specialists regarding heightened internal control risks in ERP settings. Thirty participants identify examples of internal control risks arising from a host of issues, such as inadequate user training, poor user involvement, incomplete process reengineering, incompatible “bolt-on” applications (i.e., applications from other vendors to supplement the ERP system), reduced data integrity during conversions, and increased error and fraud potential. Notably, about 40 percent of the participants indicate that ERP systems often lack adequate internal controls, primarily because clients and consultants unduly focus on “going live” by a particular date, thereby bypassing critical business process reengineering activities. Additionally, a substantial body of practitioner literature suggests that ERP system implementations can increase overall control risk (Gibbs and Keating 1995; Helms 1999; Lilly 1997; Manello and Rocholl 1997; Niccolai and LaMonica 1999; Pfenning 1999; Turner 1999; Wah 2000).
We recognize that in some settings, ERP systems can lead to an overall decrease in inherent and control risks when compared to a non-ERP system. From a technical perspective, most ERP vendors design adequate controls into their integrated application suites. Such control mechanisms are only effective, though, if they are properly established from the beginning and subsequently maintained. Under certain conditions, the technical potential of ERP systems to reduce inherent and control risks can be compromised, especially if key process linkages are loosely coupled or broken and integrated internal controls are partially adopted or bypassed (O’Leary 2000). Importantly, during ERP system implementation and subsequent operation, managers sometimes compromise or overlook security controls surrounding ERP system access rights, especially if they place undue focus on bringing the system online quickly and cheaply. This can be especially problematic from a security risk perspective due to the vulnerability of integrated relational databases to mischief or malfeasance by unauthorized users (O’Leary 2000).

Guidance on Assessing Computer System Risks

The Committee of Sponsoring Organizations (COSO 1992) report provides a framework for the consideration of control risks, which expands the focus of the traditional view of controls at the detailed account and assertion level to include a global business perspective. Auditing standard setters have integrated the COSO framework into SAS No. 55 (AICPA 1988), SAS No. 78 (AICPA 1995), and SAS No. 94 (AICPA 2001). These standards direct the auditor to consider broad inherent and control risks that can have a direct impact on potential financial statement errors and omissions. SAS No. 94 instructs auditors to understand the clients’ automated and manual procedures used to prepare financial statements and related disclosures, and to consider how errors and irregularities could occur in the clients’ computing environment. Further, SAS No. 94 identifies factors to consider in determining whether the financial auditor should request the assistance of IT specialists to accurately assess business and control risks, and to design a proper audit strategy. Three of the factors specified in SAS No. 94 are particularly salient to an ERP setting: the complexity of the entity’s systems and controls, the extent to which the multiple systems share data, and the entity’s use of emerging technologies.

The Panel on Audit Effectiveness (POE 2000) discussed the issue of unique risks and controls posed by increasingly sophisticated information processing systems. The POE encourages auditors to expand their knowledge of new business-oriented information systems to facilitate the development of more effective audit approaches. The POE also recognizes the need to attract and retain qualified technology specialists for audit support. The POE (2000, 171) states, “Auditors cannot cede addressing all technology matters to technology specialists,” thereby suggesting that financial auditors must be aware of the unique risks posed by new technology, such as ERP systems.

To date, no empirical research compares ERP versus non-ERP system environments with regard to the incidence and nature of errors or irregularities. However, in a study of detected errors, Bell et al. (1998) report significant variations in the frequency and causes of errors for a traditional computerized accounting system versus a manual system. They emphasize the need to “adequately consider the nature and reliability of such systems in the planning stages of an engagement” (Bell et al. 1998, 13). The authors highlight the importance of understanding the IT infrastructure on which the company relies to produce financial statements, and stress the need to recognize the unique risks and controls associated with emergent computerized systems.

ERP versus Non-ERP System Risks

Based on the literature review and three pilot-test focus group meetings with IT audit specialists, we posit that business interruption and process interdependency risks are greater in an ERP environment. The purpose of these sessions was to validate prior research findings regarding the three risk categories (business interruption, process interdependency and system security) that are potentially more vulnerable in an ERP environment, as compared to a non-ERP computing environment.
ERP setting, as compared to a non-ERP setting, due primarily to automated workflow and relational database features of the ERP system. We further suggest that system security risk is potentially higher in an ERP environment, as compared to a non-ERP environment, if system access controls are relatively weak. That is, in the presence of strong controls over issuing and monitoring user passwords and authorizations, there would be no reason to expect that system security risk would be greater in an ERP environment. However, a weakness in such controls takes on greater significance in an ERP setting, as a compromise of security can provide the opportunity for unauthorized access to the enterprise-wide database. As a result, anyone who bypasses system security controls could, for instance, inadvertently create a recording error or modify an audit trail to cover a defalcation.

At the heart of this security problem lies a key concern with ERP systems; that is, engineered business processes often times alter and weaken the segregation of incompatible functions (O’Leary 2000). Accordingly, compensating controls must be implemented via user passwords and authorizations over three key security aspects of the ERP environment—network, database, and application (Jones and Hunton 2000; O’Leary 2000). Recognition of the potential risks associated with security weaknesses in these areas would demonstrate a knowledge differential between specialists and nonspecialists (Libby 1995; Frederick and Libby 1986). As will be described in the next section, the experimental case contains a seeded weakness of this nature. In a similar manner, seeded errors and weaknesses have been utilized in prior studies to evaluate judgment performance (e.g., Bedard and Biggs 1991; Wright and Wright 1997).

Finally, we examine the extent to which overall internal control risk assessments differ between ERP and non-ERP environments. We recognize that control risk assessments encapsulate many factors. With respect to the experimental case, process interdependency and security risks (exacerbated by the seeded weakness) can heighten control risk concerns. The compound effect of these risks suggests that overall control risk is higher in the ERP environment, as compared to the non-ERP computing environment.

While we expect that IT audit specialists will assess higher risk levels with the ERP system, as compared to the non-ERP system, due to their intricate knowledge of both computing environments, we are unsure whether financial auditors possess sufficient in-depth knowledge of both system environments to draw such distinctions. The literature on knowledge differences between specialists and nonspecialists offers further guidance in this regard.

### The Knowledge Differential of Specialists

While differences in declarative knowledge (e.g., memory stores of facts and events) and procedural knowledge (various schemata for processing information) of specialists and nonspecialists are difficult to observe directly, such knowledge differential can be inferred by comparing their judgments (e.g., risk assessments) (Frederick and Libby 1986; Libby 1995; Libby and Luft 1993; Solomon et al. 1999). For instance, Solomon et al. (1999) suggest that auditors who are industry specialists possess a knowledge differential over nonspecialists due to the specialists’ more focused indirect experience (e.g., education and training) and direct experience (e.g., audits and consultations with clients in specific industries). Solomon et al. (1999) also indicate that the specialists’ knowledge differential typically yields judgments that are more accurate. Other accounting researchers, e.g., Libby (1985), Kaplan and Reckers (1989), and Kaplan et al. (1992), indicate similar judgment accuracy differences.

Additionally, Bedard and Biggs (1991) suggest that auditors with more task-specific experience are better at identifying a seeded error than are less experienced auditors. Johnson et al. (1991) report a positive relationship between industry experience and fraud detection. Wright and Wright (1997) indicate that industry experience leads to greater accuracy in risk assessments and error identification.
The current study tests the knowledge differential between IT audit specialists and financial auditors by seeding a security weakness into the case materials. Accordingly, we offer the following multi-part hypothesis:

**H1:** Holding all non-system business interruption and process interdependency risk factors constant, IT audit specialists will assess significantly greater risk differentials between the non-ERP and ERP system than financial auditors in the following areas:

- **H1a:** business interruption risk;
- **H1b:** process interdependency risk;
- **H1c:** network security risk;
- **H1d:** database security risk;
- **H1e:** application security risk;
- **H1f:** overall internal control risk.

**Perceived Need for Consultation**

Auditors cannot possess high levels of knowledge in all areas, which is why specialists are often consulted when needed (Gibbons and Emby 1984). With regard to how IT affects the independent audit, SAS No. 94 (AICPA 2001) requires financial auditors to seek the advice of IT audit specialists if the financial auditors do not possess the requisite skills to properly evaluate and test automated internal controls. Given the complexities of an ERP system and limited experience of financial auditors in assessing risks and controls in this computing environment, one would expect that financial auditors would seek consultation of IT audit specialists in an ERP setting. However, if financial auditors are equally highly confident in their ability to assess ERP and non-ERP system risks, then they will likely not seek consultation from IT audit specialists when auditing in an ERP environment.

Research findings in psychology indicate that less experienced individuals in a given domain often exhibit as much confidence as more experienced individuals, even though the former realize that their performance is inferior to the latter (e.g., Klayman et al. 1999; Mahajan 1992; Arkes et al. 1987; Christensen-Szalanski and Bushyhead 1981; Koriat et al. 1980; Einhorn and Hogarth 1978). Such findings suggest that financial auditors’ confidence level with regard to assessing ERP system risks is likely to be relatively high. Although research evidence on this issue in auditing is somewhat mixed, the predominant results support a general tendency for auditors to be overconfident, even when they are outside their range of expertise (e.g., Ahlawat 1999; Moeckel 1990; Moeckel and Plumlee 1989).

These research findings lead us to predict that financial auditors are no more likely to seek consultation with IT audit specialists in an ERP system environment, as compared to a non-ERP system environment. Hence, we expect that there will be no difference between ERP and non-ERP settings with respect to financial auditors assessments of the need to consult with IT audit specialists. Accordingly, we offer the second hypothesis:

**H2:** There will be no significant difference in financial auditors perceived need to consult with IT audit specialists between the ERP and non-ERP settings.

### III. RESEARCH METHOD

**Design**

In this study, we manipulate the variable of interest (system type: ERP system and non-ERP system) and indirectly measure a knowledge differential (auditor type: IT audit specialist and financial auditor). Libby (1995) and Frederick and Libby (1986) suggest the use of this experimental method...
as a way to examine the expertise paradigm. Hence, the current experiment involves a 2 × 2 (system type × auditor type) between-participants design, where system type is randomized across participants. Appendix A presents the system type manipulation. Importantly, we portray the business processes surrounding the ERP system as tightly integrated throughout the company, while the non-ERP system consists of independent business processes with manual controls.

We embed a security weakness into the case. In a similar manner, prior studies have utilized seeded weaknesses to evaluate judgment performance (e.g., Bedard and Biggs 1991; Wright and Wright 1997). The objective is to identify a weakness that would potentially result in significantly greater security risks in the ERP environment, as compared to a non-ERP setting. This research design allows us to test for a knowledge differential between IT audit specialists and financial auditors. We developed and seeded the following control and security weakness in the case:

Medical Solutions has a client-server computer network, with access to the Internet. A network manager handles computer security throughout the company. The network manager started out with the company 15 years ago. Over the years, he built an outstanding reputation throughout the company as a computer hardware specialist. He was promoted to network manager three years ago. His technical knowledge of Medical Solutions computer hardware and communication systems is excellent. While most of his day is consumed with handling technical network issues, the network manager is also responsible for the issuance of passwords throughout the entire company. The passwords given to each employee provide access to the company’s client-server network and the Internet, as well as to authorized software applications (such as order entry, accounts receivable, accounts payable, etc.). When new employees are hired, the network manager initially establishes their network and application password privileges, and then he shows them how to create their own unique passwords. Employees are allowed to change their passwords (but not their privileges) any time they desire while employed at Medical Solutions, Inc. Only the network manager can make changes to user privileges, and he only makes such changes when authorized by the user’s departmental supervisor.

Given the interdependent, linked business processes in the ERP setting, coupled with the loss of traditional segregation of duties, unauthorized access to the network, database, and software applications indicate significant risk exposure with respect to invalid transactions or undetected errors. The embedded system security weakness arises for three reasons. First, the network manager is technically knowledgeable, but not particularly competent in the area of system security. He has complete control over the passwords for the network, database, and applications. Proper controls would call for a database administrator or security manager who is also involved in this process. Second, there is no apparent mechanism for mandating password changes. Good controls should require periodic password changes. Last, departmental supervisors set user privileges—a policy that could lead to inadvertent or intentional violations of segregation of incompatible functions. Appropriate controls would entail overseeing and monitoring user privileges at the enterprise level. These security weaknesses are especially of concern in an ERP environment, where a relational database consolidates enterprise-wide information, an integrated suite of applications tightly couples business processes, and improper access security begets significant risks and exposures.

Task
The participating auditors read a realistic case (Medical Solutions, Inc.) regarding a pharmaceutical manufacturer and assess various risks for the clients computerized system. The case begins with background information about the client, including its size, customers, competitive environment, control environment (described as good), and the auditing firm’s past experiences with the company (portrayed as positive). The case includes a comprehensive business process map, which is adapted from an industry solutions map developed by SAP®, a major ERP vendor. We used the process map as a basis to develop the computer system manipulations (non-ERP or ERP) presented in Appendix
A. After presenting the background information, we describe the computing environment as either a non-ERP or an ERP system. The intent is to provide an overall similar level of inherent risk (e.g., industry setting and financial condition) and fraud risk for the two versions of the case. We successfully achieve our intention, as the participants’ inherent risk perceptions are similar across the experimental conditions.2

Measures

Based on a review of relevant literature (e.g., Girard and Farmer 1999; O’Leary 2000; Wright and Wright 2002) we identified a priori the following potential heightened risk categories in the experimental ERP case setting: business interruption, process interdependency, network security, database security, application security, and overall control risk. To validate the list, we conducted three focus group meetings with IT specialists from three of the (then) Big 5 CPA firms.3

After reading the case materials, we asked the experimental participants to assess a series of system-related risks using seven-point Likert-type scales with semantic midpoints and anchors (see Appendices B and C).4 To preclude an order effect, we randomized the order of the questions and distributed two versions of the case materials within each treatment condition.

IV. RESULTS

Participants

We administered the experiment at four continuing professional education (CPE) sessions involving a broad spectrum of auditors with varied financial and IT auditing backgrounds. One of the authors conducted the CPE sessions, lasting three hours each. The instructor held morning and afternoon sessions over a contiguous two-day period, resulting in four experimental sessions. The resulting sample is comprised of participants from four of the (then) Big 5 CPA firms. The managing partners of the participating firms determined that SysTrustSM should be the topic of the CPE sessions, as they felt that this subject matter would help them to recruit successfully an equal number of financial and IT audit specialists—a desirable criterion that the authors made clear a priori.

2 We performed the following analyses to assess the similarity of inherent risk perceptions among the system and auditor types. The overall mean assessment of inherent risk was relatively high (mean = 6.63 [standard deviation = 1.03], where 1 = low risk; 7 = high risk), most likely due to the pharmaceutical industry setting of the client in the case. ANOVA testing yielded no significant difference for system type (F = 0.05, p = .83), and marginally significant differences for auditor type (F = 2.83, p = .09) and the interaction term (F = 3.35, p = .07). Scheffe’s and Tukey’s multiple pairwise testing (p = .10) indicated no significant differences among treatment means for inherent risk assessments. The overall mean assessment of fraudulent financial reporting risk was near the mid-point of the same seven-point scale (mean = 3.78 [standard deviation = 1.88]). ANOVA testing yielded no significant differences for system type (F = 0.01, p = .95), auditor type (F = 0.01, p = .92), or the interaction term (F = 0.35, p = .55).

3 The first group included two seniors, four managers, and one partner; the second group included three seniors, three managers, and one partner; and the third group included two seniors, four managers, and two partners. We asked the specialists to identify and explain specific risks that are potentially heightened in an ERP environment, as compared to a non-ERP system environment. After discussing the risks, they read the seeded weakness and discussed any further impact on their previously identified risks, and identified new risks. We then requested the specialists to place their identified risks into discrete categories. Afterward, we revealed our risk categories and asked which of their categories were and were not essentially the same as ours. In all three groups, the vast majority of identified risks and categories were similar to our risk constructs. Within each group, a few additional risk categories arose, but there was no consistency across the groups in this regard, and all participants assessed that the other categories were relatively minor in comparison to those identified by our risk constructs.

4 We also conducted a pilot test to ensure that the case information was complete and understandable, the manipulation of system type was successful, and the dependent variables (risk factors) and response scales were clear. Eight financial auditors and seven IT audit specialists from three of the (then) Big 5 CPA firms participated in the pilot. All participants were CPAs. Responses to the risk assessment and the manipulation check items strongly supported the success of the ERP versus non-ERP manipulation. We made minor changes to the background information and some of the response items based on pilot test input.
During the CPE sessions, neither the instructor nor the participants discussed ERP systems.

One hundred sixty-five auditors, all CPAs from two large cities in the southeastern portion of the United States, participated in the study. Table 1 presents the sample demographics. Statistical testing indicates no significant differences across experimental conditions (system type or auditor type) on any of the demographic variables, except Computer Information Systems Auditor (CISA) certification, and percent experience assessing computer systems and controls. Thirty-eight percent of the IT audit specialists hold the CISA certification, while none of the financial auditors do. Further, the IT audit specialists report that the vast majority of their overall auditing experience (92.68 percent) directly relates to assessing computer system controls, as compared to a significantly (p < .01) smaller percentage (18.67 percent) for the financial auditors. This difference suggests a deeper level of direct experience for IT audit specialists.

When asked what percentage of their overall client base uses ERP systems, the mean percentage is equivalent (p = .77) for financial auditors (37.35 percent) and IT audit specialists (36.22 percent), which presumably represents the base rate of companies adopting such systems. Since the nature of IT audit work focuses on evaluating IT-related risks and controls, IT audit specialists have opportunities to gain narrow, deep experience in assessing the risks and controls surrounding such systems, thereby increasing their direct experiential knowledge of the unique risks posed by ERP systems.5

Additionally, IT audit specialists have opportunities to acquire requisite indirect experience through education and training. During oral debriefings, the experimenter asked how many participants had taken one or more college courses in IT auditing. All 82 IT audit specialists responded in the affirmative, whereas only six of the 83 financial auditors had taken a course of this nature. Additionally, we asked participants if they had completed one or more IT audit-related professional training courses (firm-sponsored or otherwise). Once again, all IT audit specialists indicated that they had taken at least one professional training course in IT auditing, while none of the financial auditors had participated in such training.

In comparing the risk assessments of IT audit specialists and financial auditors, we recognize the importance of considering potential variations in perspectives. For instance, an IT auditor may have a different risk focus (e.g., system effectiveness, efficiency, and privacy risks, in addition to financial statement and fraud risk) than a financial auditor, who is most concerned with material financial statement errors and fraud. It is important to note that the participating IT audit specialists are all CPAs and work with financial auditors on a routine basis; thus, one would expect that they understand the objectives of assessing risks in planning an audit engagement. However, given that the mean years of experience for the IT audit specialists (5.46) and financial auditors (5.51) are equivalent (p = .94), one can reasonably assume that the former group likely has less direct and perhaps indirect experience assessing overall control risk for audit clients.

Manipulation Check

The following manipulation check question was included in the study materials as a way to assess the participants’ basic understanding of the differences in process and information integration between non-ERP and ERP computer systems:

How would you characterize the extent to which enterprise-wide information is integrated throughout the entire organization at Medical Solutions, Inc.? 
(1 = Not at all Integrated, 4 = Somewhat Integrated, 7 = Totally Integrated).

5 Only six of 82 IT audit specialists (7.3 percent) indicated that zero percent of their client base uses ERP systems. The analyses were also performed excluding these six participants and the findings were qualitatively equivalent.
We use an ANOVA model with independent variables of system type (ERP versus non-ERP) and auditor type (financial versus IT) to test the manipulation check responses. The (mean) [standard deviation] response for the ERP condition (6.35) [1.01] is significantly greater (F = 188.16, p < .01) than the non-ERP condition (3.56) [1.55].6 Neither the main effect for auditor type (F = 0.01, p = .97)

6 Within each system type condition (ERP and non-ERP), we conducted outlier tests to determine whether any observations fell outside of three standard deviations from the mean. We noted no outliers in either condition.
nor the interaction term ($F = 1.58, p = .21$) is significant. Thus, we deem the manipulation of system type to be successful.

**Response Measures**

For analysis purposes, all response item scales are oriented as follows: $1 =$ very low risk-concern and $7 =$ very high risk-concern. Appendix B presents the item wordings and Table 2 offers descriptive statistics related to the dependent variable metrics. Since reliability estimates (Pearson correlation for two items and Cronbach’s alpha for three items) are relatively high, we average multiple items used to measure the risk categories into single risk indices.

**Preliminary Testing**

We conduct MANCOVA testing on all dependent measures, where the independent variables are system type (non-ERP versus ERP), auditor type (financial auditor versus IT audit specialists), CPA firm (four of the Big 5), and version number (two versions of the case with response measures in different random orders). The covariate represents participant’s client base percentage with ERP systems (0 to 100). MANCOVA results indicate statistical significance for system type ($F = 119.69, p < .01$), auditor type ($F = 249.31, p < .01$), and the interaction of system and auditor types ($F = 52.32, p < .01$).\(^7\) CPA firm is nonsignificant ($F = 0.33, p = .85$), as is version number ($F = 1.70, p = .13$). The covariate is also nonsignificant ($F = 0.91, p = .32$). Additionally, all interaction terms including version, CPA firm, or both are nonsignificant ($p > .10$). Accordingly, we use ANOVA analyses to test H1 and H2.

### TABLE 2

**Descriptive Statistics for Response Items**

<table>
<thead>
<tr>
<th>Number of Items</th>
<th>Reliability Estimate(^a)</th>
<th>Mean(^b)</th>
<th>Standard Deviation</th>
<th>Low (c)</th>
<th>High (c)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Interruption Risk(^d)</td>
<td>2</td>
<td>.70</td>
<td>3.22</td>
<td>1.89</td>
<td>1</td>
</tr>
<tr>
<td>Process Interdependency Risk(^d)</td>
<td>2</td>
<td>.63</td>
<td>3.54</td>
<td>1.98</td>
<td>1</td>
</tr>
<tr>
<td>Network Security Risk(^d)</td>
<td>3</td>
<td>.75</td>
<td>3.94</td>
<td>1.85</td>
<td>1</td>
</tr>
<tr>
<td>Database Security Risk(^d)</td>
<td>3</td>
<td>.82</td>
<td>3.51</td>
<td>2.00</td>
<td>1</td>
</tr>
<tr>
<td>Application Security Risk(^d)</td>
<td>2</td>
<td>.64</td>
<td>3.39</td>
<td>2.12</td>
<td>1</td>
</tr>
<tr>
<td>Internal Control Risk(^d)</td>
<td>1</td>
<td>NA</td>
<td>3.93</td>
<td>2.03</td>
<td>1</td>
</tr>
<tr>
<td>Need for Consultation(^e)</td>
<td>1</td>
<td>NA</td>
<td>2.18</td>
<td>1.59</td>
<td>1</td>
</tr>
</tbody>
</table>

\(^a\) For two item indices, reliability estimates are assessed via Pearson Correlation (r). For three or more item indices, reliability estimates are indicated by standardized Cronbach $\alpha$, adjusted for number of items in the index. All reliability estimates are significant ($p < .01$).

\(^b\) Multiple items were averaged to form variable indices that range from 1 to 7.

\(^c\) The range reflects low and high recorded responses as well as the maximum theoretical range of the dependent variables.

\(^d\) Sample size equals 165.

\(^e\) Only financial auditors responded to this item, hence, the sample size is 83.

\(^7\) Box’s M test for homoscedasticity was nonsignificant ($p = .37$), suggesting that the assumption of equal variance was not violated.
Risk Recognition (H1)

The first hypothesis stipulates that differential risk assessments from the non-ERP to the ERP systems will be significantly higher for IT audit specialists than financial auditors across all risk categories (H1a through H1f). This proposition suggests an interaction between auditor and system types. Since the omnibus MANCOVA model is significant, we use six ANOVA models to test H1—one model for each dependent variable.8 The independent variables in the ANOVA models are auditor type, system type, and the interaction term.

Table 3, Panel A presents mean responses by auditor and system types. As indicated by Table 3, Panel B, all main effects and interactions are significant (p < .01).9 The planned contrast results shown on Table 3, Panel C indicate that differential risk assessments of IT audit specialists, as compared to financial auditors, are significantly higher in all risk categories. Accordingly, the evidence supports H1.10

We anticipated that the seeded weakness would lead to higher security risks in the ERP environment, as described earlier. The pairwise comparisons shown in Table 3 reveal no significant differences in financial auditors risk assessments between the ERP system and the non-ERP system across all three security risk factors (network, database, and application security). This finding is in direct contrast to the IT audit specialists’ significantly higher security risk assessments. These results provide further support for H1, suggesting that financial auditors’ risk assessments are not sensitive to the security risk exposures introduced by the seeded control weakness.

Consultation (H2)

The second hypothesis (H2) examines the extent to which financial auditors seek the services of IT audit specialists. To test this assertion, we compare the financial auditors perceived need for consultation in both the ERP and non-ERP settings. The mean (standard deviation) responses are 2.36 (1.64) and 1.97 (1.51) for the ERP and non-ERP settings, respectively. A t-test reveals no significant difference between the two means (t = 1.12, p = .265). As posited by H2, financial auditors do not indicate a significant difference in their perceived need to consult with IT specialists between ERP and non-ERP settings.11

Confidence

We also examine confidence levels regarding the capability of financial audit teams to assess risks in ERP and non-ERP settings. Specifically, the participating auditors record their confidence in the capability of financial audit teams to assess the internal controls over network security, database security, and application security. The scales are oriented such that 1 = low confidence and 7 = high confidence. The three confidence items are averaged to form a single confidence index (overall mean = 4.92, standard deviation = 2.18, range 1–7, Cronbach α = .88).

The ANOVA model yields significant effects for system type (F = 208.29, p < .01), auditor type (F = 1,202.33, p < .01), and the interaction term (F = 212.06, p < .01). Treatment means (standard deviations) are as follows: 1.32 (0.60) [IT auditor by ERP system], 5.55 (0.58) [IT auditor by

---

8 For each of the six ANOVA models, Levine’s test of homogeneity of variance was nonsignificant (all p-values exceeded .10), indicating that the assumption of equal variance was not violated in any model. Additionally, within each treatment condition, we conducted tests to determine whether any observations fell more than three standard deviations from the mean. We noted no outliers with regard to any of the six dependent variables.
9 The power of each ANOVA model was as follows: .94 (business interruption risk), .97 (process interdependency risk), .92 (network security risk), .95 (database security risk), .96 (application security risk), and .91 (internal control risk).
10 Obtained results were not substantially different when we subdivided the IT audit specialists into those (1) with and without CISA certification, (2) above and below the mean percentage of clients with ERP systems and (3) in the upper and lower quartiles based on the percentage of clients with ERP systems.
11 The power of the test was .95. We also conducted an ANCOVA to assess this variable, using “mean years’ experience” as the covariate, which was not significant (p = .72), and the results were substantially the same.
TABLE 3
Hypothesis 1 (H1)

Panel A: Variable Index Means\(^a,b\)

<table>
<thead>
<tr>
<th>Dependent Variable</th>
<th>Non-ERP System IS Auditors</th>
<th>Financial Auditors</th>
<th>ERP System IS Auditors</th>
<th>Financial Auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
<td>S.D.</td>
<td>Mean</td>
<td>S.D.</td>
</tr>
<tr>
<td>Business Interruption Risk</td>
<td>1.76* (0.88)</td>
<td>1.92* (0.92)</td>
<td>5.75** (1.03)</td>
<td>3.48*** (1.23)</td>
</tr>
<tr>
<td>Process Interdependency Risk</td>
<td>3.24* (1.07)</td>
<td>1.72** (0.78)</td>
<td>6.43*** (1.01)</td>
<td>2.82* (1.00)</td>
</tr>
<tr>
<td>Network Security Risk</td>
<td>4.40* (0.71)</td>
<td>2.42** (1.01)</td>
<td>6.54*** (0.59)</td>
<td>2.50** (0.83)</td>
</tr>
<tr>
<td>Database Security Risk</td>
<td>3.64* (0.89)</td>
<td>2.02** (1.03)</td>
<td>6.42*** (0.64)</td>
<td>2.05** (1.04)</td>
</tr>
<tr>
<td>Application Security Risk</td>
<td>3.31* (1.09)</td>
<td>2.06** (1.22)</td>
<td>6.54*** (0.63)</td>
<td>1.80** (0.92)</td>
</tr>
<tr>
<td>Internal Control Risk</td>
<td>3.48* (1.64)</td>
<td>1.97** (1.01)</td>
<td>6.43*** (0.55)</td>
<td>3.84** (1.56)</td>
</tr>
</tbody>
</table>

Panel B: Results of ANOVA Testing

<table>
<thead>
<tr>
<th>System Type</th>
<th>Auditor Type</th>
<th>Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F</td>
<td>p</td>
</tr>
<tr>
<td>Business Interruption Risk</td>
<td>297.84</td>
<td>.01</td>
</tr>
<tr>
<td>Process Interdependency Risk</td>
<td>199.23</td>
<td>.01</td>
</tr>
<tr>
<td>Network Security Risk</td>
<td>80.29</td>
<td>.01</td>
</tr>
<tr>
<td>Database Security Risk</td>
<td>96.71</td>
<td>.01</td>
</tr>
<tr>
<td>Application Security Risk</td>
<td>91.88</td>
<td>.01</td>
</tr>
<tr>
<td>Internal Control Risk</td>
<td>143.82</td>
<td>.01</td>
</tr>
</tbody>
</table>

Panel C: Results of Planned Comparisons

<table>
<thead>
<tr>
<th>ERP minus Non-ERP System Index Means</th>
<th>IT Auditors</th>
<th>Financial Auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Interruption Risk (H1a)</td>
<td>3.99 &gt; 1.56</td>
<td>7.58 .01</td>
</tr>
<tr>
<td>Process Interdependency Risk (H1e)</td>
<td>3.19 &gt; 1.10</td>
<td>6.87 .01</td>
</tr>
<tr>
<td>Network Security Risk (H1b)(^c)</td>
<td>2.14 &gt; 0.08</td>
<td>8.31 .01</td>
</tr>
<tr>
<td>Database Security Risk (H1c)(^c)</td>
<td>2.78 &gt; 0.03</td>
<td>9.64 .01</td>
</tr>
<tr>
<td>Application Security Risk (H1d)(^c)</td>
<td>3.23 &gt; –0.27</td>
<td>11.33 .01</td>
</tr>
<tr>
<td>Internal Control Risk (H1f)</td>
<td>2.95 &gt; 1.87</td>
<td>2.70 .01</td>
</tr>
</tbody>
</table>

\(^a\) Higher means indicate greater perceived risk.
\(^b\) *, **, and *** indicate the results of Scheffe’s and Tukey’s multiple pairwise comparison tests (both yielding consistent results) for each dependent variable. Specifically, reading across the rows, means with different superscripts indicate significant differences (p = .05).
\(^c\) Risks related to the seeded control weakness.

Overall, financial auditors are equally highly confident in the capability of financial audit teams to assess computer system risks in both system environments. IT audit specialists record a relatively high level of confidence in the capability of financial audit teams to assess risks in a non-ERP environment, but a relatively low level of confidence in an ERP environment.
Supplemental Survey

Financial auditors might base their high level of confidence and low perceived need for consultation in an ERP setting on an assumed routine presence of IT audit specialists in assessing controls for such clients as a standard firm practice. To evaluate this possibility, we sent a post-experiment supplemental survey to four of the (then) Big 5 firms and an international consulting firm. The resulting sample of 106 respondents (71 percent response rate) is comprised of 58 financial auditors, 22 IT auditors, and 26 consultants (with direct experience working with ERP systems). Respondents include 11 partners, 32 managers, 36 seniors, and 27 staff. Appendix D presents the supplemental survey questions and Table 4 displays the statistical findings.

The results indicate a relatively low base rate where IT auditors are consulted, ranging from a high of 20.43 percent of audit engagements to a low of 4.04 percent. Importantly, for recurring engagements (the setting of the experimental case), financial auditors indicate that they believe IT auditors will be consulted in an ERP environment in about 12.72 percent of audits. Based on this supplemental analysis, the findings regarding consultation and confidence for the experimental case are not likely wholly attributable to a presumption by participants that consultation had already or would likely take place.

V. DISCUSSION

One purpose of this study is to examine the extent to which financial auditors recognize potential differences in business, security, and audit risks between non-ERP (legacy) and ERP computing systems in light of relatively weak security controls. A second objective is to determine the propensity of financial auditors to seek consultation of IT audit specialists in both computing environments when assessing IT risks in planning an engagement. Our review of the literature and discussion with three focus groups of IT audit specialists reveals that ERP systems can pose at least the following potential elevated risks under certain conditions: business interruption, process interdependency, network security, database security, application security, and overall internal control.

The research findings indicate that financial auditors may not be fully aware of the greater risk exposure associated with an ERP system, as compared to a non-ERP system environment when security controls are relatively weak. The IT audit specialists and financial auditors who participated in the current study assessed higher levels of business interruption and process interdependency risks

<table>
<thead>
<tr>
<th>Survey Question</th>
<th>Financial (n = 58)</th>
<th>IT Specialist (n = 22)</th>
<th>Consultant (n = 26)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Pre-Implementation Consultation</td>
<td>20.43* (7.33)</td>
<td>15.45** (5.99)</td>
<td>11.35** (5.51)</td>
</tr>
<tr>
<td>2. Post-Implementation Consultation</td>
<td>12.72* (5.30)</td>
<td>6.78** (4.83)</td>
<td>4.04** (2.99)</td>
</tr>
<tr>
<td>3. Integral Part of the Audit Team</td>
<td>11.24* (6.50)</td>
<td>9.91* (5.64)</td>
<td>7.58** (4.09)</td>
</tr>
</tbody>
</table>

* and ** indicate the results of Scheffe’s and Tukey’s multiple pairwise comparison tests (both yielding consistent results) for each dependent variable. Specifically, reading across the rows, means with different superscripts indicate significant differences (p = .05).

12 Consultants’ responses are included, since they reflect individuals who have extensive experience working with financial auditors as part of ERP implementations and post-reviews. In such engagements, the development of appropriate controls is often an issue.
for the ERP system, as compared to the non-ERP system. Although the risk differentials in these two areas are significantly greater for IT audit specialists, as predicted by the first hypothesis (H1), the findings nevertheless suggest that financial auditors do recognize the impact of automated workflow procedures and integrated relational databases on business interruption and process interdependency risks.

IT audit specialists assess significantly higher levels of network, database, and application security risks with the ERP system, as compared to the non-ERP system, while the financial auditors record similar security risk assessments in both environments. Given the nature of the seeded weakness in the experimental case, these findings suggest that the participating financial auditors are unaware of the pervasive nature of security risks in an integrated database environment.

Assessments of overall internal control risk are higher in the ERP system, as compared to the non-ERP system environment for IT audit specialists and financial auditors; however, the specialists risk differential is significantly greater. There can be multiple explanations for this discrepancy. For instance, the seeded weakness in the case involves a situation where a technically oriented network manager controls all passwords. While this circumstance reflects an IT-related control environment weakness, as apparently recognized by the IT audit specialists, the financial auditors might have considered this issue in the broader context of the company’s overall control environment. For instance, a strong code of ethics, sanctions for unethical behavior, and compensating controls might mitigate the possibility of password misuse by employees. While we did not mention such mitigating factors in the case materials, the participating financial auditors could have presumed that such offsetting controls were likely present in the client’s environment.

The results further reveal an equally high level of confidence by financial auditors in the capability of financial audit teams to assess risks in both the non-ERP and ERP settings, which may help to explain their reluctance to consult with IT audit specialists. Interestingly, despite a potential self-serving bias of IT audit specialists (i.e., their livelihood is partially dependent on consultation engagements with financial auditors), the specialists nonetheless assess the capability of financial audit teams in a non-ERP environment as quite high. If the self-serving bias is overwhelmingly strong and pervasive, then one might expect the IT audit specialists to express relatively low confidence levels across both computer environments.

Economic pressures on audit fees could also contribute to the financial auditors’ seeming reluctance to consult with IT audit specialists. That is, by including IT audit specialists, financial audit teams can incur increased overall audit costs, since specialists’ billing rates can be higher than rank-equivalent nonspecialists’ rates. Moreover, if the financial auditors believe that they are capable of assessing ERP system risks, holding billing rates constant, then they can minimize audit costs if they perform the risk assessment themselves rather than absorbing the added costs of specialists. A non-economic reason that financial auditors might be hesitant to consult with IT audit specialists is that they might not perceive a link between ERP system risks and the likelihood of material financial misstatements or fraud.

One should consider some inherent limitations in this study when interpreting the results. First, there are no normative benchmarks available to determine the level of risks for the ERP and non-ERP settings examined. Thus, consistent with prior research (e.g., Bedard and Biggs 1991; Solomon et al. 1999; Wright 1988), we use surrogate benchmarks, i.e., the judgments of specialists and the seeding of a control weakness designed to demonstrate the knowledge differential held by financial auditors and IT audit specialists. Second, we recognize that, given the mean years’ experience of the financial auditors in our sample (5.51), these participants might not be responsible for ultimately deciding whether to consult with an IT audit specialist. Third, while we identify selected risk dimensions from extant literature and focus group discussions with IT audit specialists, we do not suggest that these dimensions reflect a comprehensive identification of the risks posed by ERP
Finally, our experiment involves an incomplete design, as we did not evaluate financial auditor and IT specialist responses without the seeded weakness. Due to sample size restrictions, we do not include a third condition (without seeded weakness) and we believe that a within-participants manipulation of this nature would induce considerable demand effects. Given the early state of the research in this area, we believe our experimental approach is an appropriate way to establish a first approximation of the issues; however, future empirical research needs to more fully identify and assess the nature of risks associated with ERP systems.

Future research could also more fully investigate factors that may lead to potential overconfidence by financial auditors in assessing risks in an ERP and other complex IT environments, as well as their apparent reluctance to seek expert consultation. Preliminary discussions with eight financial auditors from three of the (then) Big 5 firms who participated in the focus groups suggest that economic self-interests may lead to a predisposition to avoid consultation, because financial auditors would have to hire the services of IT audit specialists, thereby increasing the cost of the audit. Further, IT audit specialists appear to be somewhat resentful of financial auditors, as the auditors do not seem to recognize and respect the specialists knowledge and skill level. Both IT audit specialists and financial auditors in this study express a great deal of intra-firm tension on this issue.

However, the underlying dynamics of the relationships among firm managers, financial auditors, and IT audit specialists may have changed recently, given the enactment of the Sarbanes-Oxley Act (SOX) (2002). SOX places more responsibility on audit committees and makes them independent of management, thus, economic pressure to hold down audit fees appears to be less of an issue than it has been in the past. Also, given the rigorous internal control reporting requirements of the SOX, company managers and financial auditors now have more incentives to include IT audit specialists on audit teams. Hence, a fruitful avenue for future research is to examine more fully the nature and extent of potential organizational conflict in this regard and discover ways to mitigate further such conflict.

Clients will inevitably adopt increasingly complex computer systems that present the possibilities of efficiency and effectiveness gains, but such systems might also unintentionally introduce potential client business, control, and inherent risks that auditors need to consider when planning an audit engagement. Auditing firms face the challenge of how to obtain the requisite knowledge to properly evaluate such risks in an effective yet efficient manner. Will financial auditors need enhanced training in the area of IT-related risks; will IT audit specialists become a permanent integral part of the audit team; or, will enhanced auditor training and full-time integration of IT audit specialists become the norm? The findings of the current study suggest that these are significant unresolved issues facing the profession.
APPENDIX A
MANIPULATIONS FOR NATURE OF THE COMPUTER SYSTEM

Non-ERP System

The computerized accounting system used by Medical Solutions, Inc. includes general ledger, accounts receivable, accounts payable, joint venture accounting, cash management, payroll, fixed assets, and various cost/managerial accounting applications. The accounting system applications at Medical Solutions are integrated with each other, as are the computerized applications within each business process category. However, company information is not integrated across the company’s business processes, as databases for each process are maintained separately. Thus, workflow procedures across business processes are, for the most part, performed manually. For example, when a customer places an order (face-to-face with a salesperson, over the telephone, or via the Internet) with Medical Solutions, the following events take place:

1) a sales person enters the customer order in the sales order system (SOS);
2) the salesperson notifies customer relationship management (CRM) of the order;
3) a CRM employee records the order in the CRM system;
4) the sales person notifies accounting of the order;
5) an accounting employee records the sale in the accounting system;
6) the sales person notifies the warehouse of the order;
7) a warehouse employee records the order in the warehouse management system (WMS);
8) the warehouse employee notifies packing and shipping of the order;
9) a shipping employee records the order in the packing and shipping system (PSS);
10) the shipping employee notifies procurement of the order;
11) a procurement employee records an order for replacement raw materials in the procurement management system (PMS);
12) the procurement employee notifies production of the need to replenish the sold goods; and
13) a production employee records a manufacturing order in the production planning system.

ERP System

The computerized accounting system used by Medical Solutions, Inc. includes general ledger, accounts receivable, accounts payable, joint venture accounting, cash management, payroll, fixed assets, and various cost/managerial accounting applications. The accounting system applications at Medical Solutions are integrated with each other, as are the computerized applications within each business process category. Also, company information is integrated throughout the company’s business processes via an enterprise resource planning (ERP) system that is built on a relational database. Thus, workflow procedures across business processes are, for the most part, performed automatically. For example, when a customer places an order (face-to-face with a salesperson, over the telephone, or via the Internet) with Medical Solutions, the ERP automatically executes the following events:

1) a sales person enters the customer order in the sales order system (SOS);
2) the SOS notifies customer relationship management (CRM) of the order;
3) the SOS records the order in the CRM system;
4) the SOS notifies accounting of the order;
5) the SOS records the sale in the accounting system;
6) the SOS notifies the warehouse of the order;
7) the SOS records the order in the warehouse management system (WMS);
8) the WMS notifies packing and shipping of the order;
9) the WMS records the order in the packing and shipping system (PSS);
10) the PSS notifies procurement of the order;
11) the PSS records an order for replacement raw materials in the procurement management system (PMS);

12) the PMS notifies production of the need to replenish the sold goods; and

13) the PMS enters a manufacturing order in the production planning system (PSS).

APPENDIX B
WORDING OF DEPENDENT VARIABLE ITEMS

Business Interruption Risk
How concerned are you about material, negative financial consequences of business interruptions that could occur at Medical Solutions due to computer systems problems?
(1 = Very Unconcerned, 7 = Very Concerned)

How concerned are you that Medical Solutions could experience a major business interruption due to computer systems problems?
(1 = Very Unconcerned, 7 = Very Concerned)

Process Interdependency Risk
How concerned are you that a problem in one business process (e.g., an improperly input customer sales order) will lead to problems in other processes?
(1 = Very Unconcerned, 7 = Very Concerned)

I believe there are sufficient controls to prevent a problem in one business process from affecting other processes?
(1 = Totally Disagree, 7 = Totally Agree)

Network Security Risk
How concerned are you that outside intruders (hackers) can get into Medical Solutions computer network and perform illegal activities, such as stealing company information or planting computer viruses?
(1 = Very Unconcerned, 7 = Very Concerned)

How concerned are you that Medical Solutions employees can get into the computer network and perform illegal activities, such as stealing company information or planting computer viruses?
(1 = Very Unconcerned, 7 = Very Concerned)

I believe that the current situation of having a network security manager provides a secure firm-wide network environment.
(1 = Totally Disagree, 7 = Totally Agree)

Database Security Risk
How concerned are you that outside intruders can gain unauthorized access to highly proprietary computerized information at Medical Solutions, Inc.?
(1 = Very Unconcerned, 7 = Very Concerned)

How concerned are you that employees can gain unauthorized access to highly proprietary computerized information at Medical Solutions, Inc.?
(1 = Very Unconcerned, 7 = Very Concerned)

I believe that the current situation of having a network security manager provides a secure firm-wide information environment.
(1 = Totally Disagree, 7 = Totally Agree)
Application Security Risk

How concerned are you that employees can legitimately gain entry into software applications and then be able to view unauthorized information at Medical Solutions?
(1 = Very Unconcerned, 7 = Very Concerned)

I am satisfied with the way in which application passwords are issued and controlled at Medical Solutions.
(1 = Totally Disagree, 7 = Totally Agree).

Control Risk

CONTROL RISK is defined as the risk that the client’s controls will fail to prevent or detect material misstatements (SAS Nos. 55 and 78). Provide an assessment of the CONTROL RISK associated with the accounting system applications of Medical Solutions by circling the appropriate number on the scale below.
(1 = Low Risk, 7 = High Risk)

APPENDIX C

WORDING OF CONSULTATION AND CONFIDENCE ITEMS

Perceived Need for Consultation

The engagement partner also wants your opinion with respect to the necessity of conferring with the practice within your CPA firm that specializes in security and control risks associated with computerized systems. Given the need for efficient audits, such specialists are not consulted on every engagement, but rather when the engagement team believes the audit program may not reduce audit risk to a tolerable level. Please provide your assessment of the necessity to consult with your CPA firm’s computer specialists before finalizing the audit plan for Medical Solutions by circling the appropriate number below.
(1 = Absolutely Unnecessary, 7 = Absolutely Necessary)

Confidence in Financial Auditors Risk Assessment Ability

I believe that members of the financial audit team are qualified to assess the internal controls over Medical Solutions computer network security.
(1 = Totally Disagree, 7 = Totally Agree)

I believe that members of the financial audit team are qualified to assess the internal controls over Medical Solutions data files.
(1 = Totally Disagree, 7 = Totally Agree)

I believe that members of the financial audit team are qualified to assess the internal controls over Medical Solutions computerized application security.
(1 = Totally Disagree, 7 = Totally Agree)

Assume that the engagement partner wants your opinion concerning the ability of the financial audit team to properly consider the firm’s exposure in addressing the risks that may be present with the computerized applications at Medical Solutions. On the scale below, please circle your level of confidence that the financial audit team is capable of assessing the audit risks associated with the computer systems used at Medical Solutions.
(1 = Very Low Confidence, 7 = Very High Confidence)
APPENDIX D
WORDING OF THE SUPPLEMENTAL SURVEY ITEMS

Pre-Implementation Consultation

When one of your audit clients implements an ERP system, how often do you (or someone else on the audit engagement) bring in IT audit specialists within your firm to consult with in order to assess control risks?

(Percentage of time)

Post-Implementation Consultation (recurring engagements)

For audit engagements after an ERP system is implemented, how often do you (or someone else on the audit engagement) bring in IT audit specialists within your firm to consult with in order to assess control risks?

(Percentage of time)

Integral Part of the Audit Team

How frequently do you believe an IT audit specialist is an integral part of the financial audit team for an ERP client setting?

(Percentage of time)

REFERENCES


