The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0268-6902.htm

Information technology and its implications for internal auditing

An empirical study of Saudi organizations

Ahmad A. Abu-Musa
Department of Accounting and MIS, College of Industrial Management, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

Abstract

Purpose – The purpose of this paper is to investigate empirically the impact of emerging information technology (IT) on internal auditors' (IA) activities, and to examine whether the IT evaluations performed in Saudi organizations vary, based on evaluation objectives and organizational characteristics.

Design/methodology/approach – A survey, using a self-administered questionnaire, is used to achieve these objectives. About 700 questionnaires were randomly distributed to a sample of Saudi organizations located in five main Saudi cities. In total, 218 valid and usable questionnaires – representing a 30.7 percent response rate – were collected and analyzed using Statistical Package for Social Sciences – SPSS version 15.

Findings – The results of the study reveal that IA need to enhance their knowledge and skills of computerized information systems (CIS) for the purpose of planning, directing, supervising and reviewing the work performed. The results of the study are consistent with Hermanson *et al.* that IA focus primarily on traditional IT risks and controls, such as IT data integrity, privacy and security, asset safeguarding and application processing. Less attention has been directed to system development and acquisition activities. The IA's performance of IT evaluations is associated with several factors including: the audit objectives, industry type, the number of IT audit specialists on the internal audit staff, and the existence of new CIS.

Practical implications – From a practical standpoint, managers, IA, IT auditors, and practitioners alike stand to gain from the findings of this study.

Originality/value – The findings of this study have important implications for managers and IA, enabling them to better understand and evaluate their computerized accounting systems.

Keywords Communication technologies, Internal auditing, Risk assessment, Saudi Arabia

Paper type Research paper

Introduction

The information technology (IT) function is responsible for designing, implementing and maintaining many of controls over an organization's business processes. IT has a critical role in collecting, processing and storing data that is summarized and reported in financial statements (Cannon and Crowe, 2004, p. 31). Many organizations are

The current research has been completed under the research fund No. JF050017, sponsored by King Fahd University of Petroleum and Minerals, Saudi Arabia. The researcher acknowledges the comments received from Professor Mohammed Youssef, KFUPM, Saudi Arabia, Professor Dana Hermanson from Kennesaw State University, and Professor Dan Ivancevich, University of North Carolina, USA. The author would like to thank the reviewers of the *Managerial Auditing Journal* (*MAJ*) for their constructive suggestions, and the Editors of *MAJ* for their superb, thorough editorial support and guidance.

Managerial Auditing Journal
Vol. 23 No. 5, 2008
pp. 438-466
© Emerald Group Publishing Limited
0268-6902
DOI 10.1108/02686900810875280

www.mana

becoming increasingly dependent on IT with such elements as fully integrated information systems (IS) and electronic document management becoming more prevalent. IT increases the accuracy and speed of transaction processing, and can lead to competitive advantages for many organizations in terms of operational efficiency, cost savings and reduction of human errors. On the other hand, there are many types of risk associated with IT, this includes loss of computer assets, erroneous record keeping, increased risk of fraud, competitive disadvantages if the wrong IT is selected, loss or theft of data, privacy violations and business disruption (Warren *et al.*, 1998; Gelinas *et al.*, 1999; Hermanson *et al.*, 2000b; Hadden *et al.*, 2003; Abu-Musa, 2006b).

Cannon and Crowe (2004) state that many internal controls over financial data are incorporated in computer programs, processes and procedures that are written, implemented and maintained by the IT function. Accordingly, an organization's assets can be transferred and liabilities incurred through transactions by computerized processes without human action. Securities transactions, purchases of materials and wire transfers are routinely initiated and consummated within computer processes residing within external entities. The degree of automation can be such that human activity is limited to promulgating policies and rules and reviewing results (p. 32).

It is also argued that internal auditors (IA) are struggling to maintain their identity and purpose as the organizations they audit undergo radical changes. Total quality management, business process reengineering, globalization and self-directed teams are dismantling hierarchical command and control structures. Advances in IT continuously render control procedures obsolete, and the "value" of traditional internal audit has become seriously questioned (Tongren, 1997). As IT changes occur more quickly, auditors must keep pace with emerging technological changes and their impact on their organization's data processing system, as well as their own audit procedures (Rezaee and Reinstein, 1998, p. 465).

The objectives of this study are to investigate empirically the impact of emerging technology (IT) on IA' activities and to examine whether the IT evaluations performed by Saudi organizations vary based on evaluation (audit) objectives or organizational characteristics. This study is organized in eight sections as follows: the second section highlights the statement of the research problem, while the third section highlights the research objectives. Section four addresses the research questions and section five introduces and analyzes the literature review related to the IT evaluation and its related activities. Section six introduces the research methodology of the current study. In section seven, the main results of the empirical survey are analyzed and discussed and finally, the last section is the conclusion of the study and recommendations for further research.

Statement of the research problem

In designing audit procedures, the auditor should consider the significance of the risk, the materiality of any misstatement, the characteristics of the class of transactions, account balance or disclosure involved, the nature of the specific controls used by the organization including the organization's use of IT, and whether the auditor expects to obtain audit evidence to determine if the organization's controls are effective in preventing, or detecting and correcting, material misstatements.

The International Standard on Auditing 401 – Auditing in a Computer Information Systems Environment – states that auditing processes for both IA and external

المنارة للاستشارات

www.mana

auditors have been rapidly changing. Factors prompting these changes include: the globalization of business, advances in technology, demands for value-added audits, the organizational structure of the client's computerized information systems (CIS) activities, the extent of concentration or distribution of computer processing throughout the organization, particularly as they may affect segregation of duties, and the availability of data source documents. Some computer files and other evidential matter that may be required by the auditor may exist for only a short period or only in machine-readable form. Accordingly, the auditor should have sufficient knowledge of the CIS to plan, direct, supervise and review the work performed. The auditor should also consider whether specialized CIS skills are needed in an audit.

Rishel and Ivancevich (2003) state that IA serve a key role in addressing controls, risks and other important factors throughout the IT implementation process. However, in an effort to reduce the number of IT failures, IA should also provide value-added services in areas that are often overlooked. An auditor's involvement in evaluating and improving the quality of the processes used to validate and document systems and train personnel could contribute to achieving a successful IT implementation. During the validation and testing phase of implementation, IA could also provide valuable input about configuring the systems in a way that incorporates appropriate controls in their organizations.

Meredith and Akers (2003) also highlighted the evolutionary development of the management's expectations of the internal audit function related to IT development in the last 30 years. The scope of internal audit has expanded from measuring and evaluating the effectiveness of internal controls to providing consulting services related to IT and systems developments. However, one potential problem with IA acting as consultants for systems-related projects is that their independence might be impaired.

Again, The International Standard on Auditing 401 (2002) confirms that although the overall objective and scope of an audit does not change in a CIS environment, the use of a computer changes the processing, storage and communication of financial information and may affect the accounting and internal control systems employed by organizations. Accordingly, a CIS environment may affect:

- The procedures followed by the auditor in obtaining a sufficient understanding of the accounting and internal control systems.
- The consideration of inherent risk and control risk through which the auditor arrives at the risk assessment.
- The auditor's design and performance of tests of control and substantive procedures appropriate to meet the audit objectives.

As new CIS technologies emerge, they are frequently employed by organizations to build increasingly complex computer systems that may include micro-to-mainframe links, distributed databases, end-user processing and business management systems that feed information directly into the accounting systems. Such systems increase the overall sophistication of CIS and the complexity of the specific applications that they may affect. As a result, CIS may increase risk and require further consideration. The auditor should obtain an understanding of the significance and complexity of the CIS activities and the availability of data for use in the audit. According to the International

المنارة للاستشارات
www.mana

Standard on Auditing – 401, an application may be considered complex when, for example:

- the volume of transactions is such that users would find it difficult to identify and correct errors in processing;
- the computer automatically generates material transactions or entries directly to another application;
- the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently; or
- transactions are exchanged electronically with other organizations (as in electronic data interchange systems) without manual review for propriety or reasonableness.

Pathak (2003) argued that the overall quality of various internal controls facilitates, to a great extent, the internal auditing of business systems applications in general. An IT audit can be performed for small-sized systems by auditing the end products, assuming that the internal controls are well placed. However, in large and complex systems, auditors may need to collect further evidence of the quality of the internal control systems (both operational and application) in order to vouch for the data integrity, system efficiency and effectiveness, and asset safeguarding objectives of IT audit. If the internal control system is intact, the IA can have more confidence in the quality of the application systems being evaluated.

According to Silltow (2003), the IA receive considerably more exposure to IT systems nowadays than in the past. IT plays a fundamental role in the way modern organizations function, and it has become integrated to the degree that virtually every type of audit requires at least some consideration of IT issues. Whereas technology was once considered the domain of specialized IT auditors, it is now the concern of all auditors, including audit generalists. Pathak (2003) also suggested that:

> [. . .] the integration of applications and enterprise-wide IS will be a key trend for the future and will surely have a great impact on the entire set of knowledge, skills, methods, algorithms, and strategies of IA. Accordingly, the audit practitioners and educators need to expand their skill sets and knowledge bases to cope not only with current changes but also with future challenges.

The rapid changes in IT and managerial practices force many organizations to move away from rigid, documented control to situations where responsibility for control is being pushed down the organization hierarchy and where oversight by management could not be achieved through traditional, compliance-based internal audit (Spira and Page, 2003). Fadzil *et al.* (2005) also confirmed that internal auditing has undergone dramatic changes that have expanded its scope in a way that allows it to make greater contributions to the organization it serves. Internal auditing is also performed in diverse legal and cultural environments, within organizations that vary in purpose, size, and structure, and also by persons within or outside the organization. The internal auditing profession also walks a tightrope between serving as a management consultant and an independent professional (p. 844).

The purpose of the current study is to examine the impact of emerging IT on IA's activities and to examine the IT evaluations performed by IA in Saudi organizations.

المنارة للاستشارات

www.mana

The current study attempts to address what Saudi organizations are doing and to examine whether the IT evaluations performed by them vary based on audit objectives or organizational characteristics, such as industry, number of computer auditors (CA), or age of computer systems. From a practical standpoint, managers and practitioners alike stand to gain from the findings of this study. The results will enable managers and practitioners to better understand the internal controls of their CIS and to champion IT development for the success of their businesses.

The objectives of the research

The Kingdom of Saudi Arabia has been selected to conduct the current empirical survey. Saudi Arabia is an oil-based economy having the largest reserves of petroleum in the world (26 percent of the proved reserves), ranks as the largest exporter of petroleum, and plays a leading role in OPEC. The kingdom of Saudi Arabia, the largest country in the Middle East, has launched a wave of economic reforms aimed among others, at diversifying its oil-based economy and is on the threshold of joining the WTO, which is an evidence of its efforts to succeed in the developing global integration of the world's leading economies. IT has become a necessity rather than a luxury for many Saudi organizations. Such organizations need IT more than ever before to improve their performance, to satisfy their customers' needs and to reduce operating costs without compromising service quality. Saudi Arabia has also a dynamic interaction between the traditional culture and modern economic and business realities, which make Saudi Arabia a unique cultural environment in which to implement the current study (Curtiss, 1995; Yavas, 1997; Yavas and Yasin, 1999; Jasimuddin, 2001; Sohail and Al-Abdali, 2005; Abu-Musa, 2006a).

The main objective of this exploratory study is therefore to investigate the IT evaluations and other IT-related activities performed by Saudi organizations. The study also examines whether the IT evaluations vary across Saudi organizations based on evaluation (audit) objectives or organizational characteristics, such as industry type, IA's experience, number of CA, or age of computer systems. Enhancing the awareness of IT evaluations and its related activities in the Saudi business environment is a general objective for the current research.

The research questions

The current study explores and investigates the following research questions:

RQ1. What are IA currently doing with respect to evaluating the IT risks in Saudi organizations?

RQ2. Do IT evaluations performed by IA vary across Saudi organizations based on audit objectives or organizational characteristics?

RQ3. Are there any significant differences regarding the IT evaluation activities performed in Saudi organizations?

Literature review

A review of the literature reveals a paucity of empirical studies related to investigating the impact of emerging IT on internal auditing and evaluating IT-related activities performed by IA in developing countries. Abdul-Gader (1990) stated that most of the

المنارة للاستشارات

www.mana

previous studies focusing on computing practices in developing countries, including Saudi Arabia, are mainly descriptive, and much work needed is to promote adoption of computer systems on a wider scale. The current study responses to Abdul-Gader's call by carrying out further empirical research in Saudi Arabia.

The Committee of Sponsoring Organizations – COSO (1992) introduced a framework for the consideration of control risks, which expanded the focus of the traditional view of controls at the detailed account and assertion level to include a global business perspective. The Information Systems Audit and Control Foundation (1998) issued the "Control Objectives for Information and Related Technology" (COBIT) framework. COBIT follows a business orientation that begins with business objectives, which drives IS strategy (e.g. planning and organization of IT) and the subsequent evaluation of risks and controls over information and data processing. According to Chan (2004), some auditors have found that the IT Governance Institute's COBIT aligns well with their Sarbanes-Oxley Act (SOA) compliance efforts. The institute's IT Control Objectives for Sarbanes-Oxley further clarifies COBIT's relevance to SOA projects and reveals a high concentration of IT processes around COSO's "control activities" and "information and communication" components.

Rezaee and Reinstein (1998) studied the impact of emerging IT on auditing functions. The study discussed the main issues of SAS No. 80, which offers auditors guidance to accumulate sufficient evidence to audit CIS of their clients. Rezaee and Reinstein (1998) argued that IT has made inputting information for transactions and events more simple – and evaluating the related controls and results more critical. Accordingly, accumulating sufficient evidence needed to construct an informed decision means understanding where to look for that evidence, what control procedures to consider, and how to evaluate such procedures.

Saudi culture is a unique culture, shaped by the influences of religion, tradition, tribal structure and distinct values and behaviors. In their study, Yavas and Yasin (1999) explored the influences of the unique culture of Saudi Arabia on the IT resources of Saudi business organizations. They studied the impact of cultural forces on the organizational role and application of information and computer skills in the Saudi environment. The study provided some pointers for action to facilitate the diffusion of computers in Saudi organizations.

The statement issued by the Public Oversight Board – POB (2000) highlighted its concerns regarding the ability of auditors to properly assess risks arising from rapidly evolving information processing systems. POB encouraged auditors to expand their knowledge of new business-oriented IS; as such knowledge would facilitate the development of more effective audit approaches. The POB also recognized the need to attract and retain qualified IT specialists for audit support. POB also confirmed that increasingly, auditors will find it necessary to understand fully the risks associated with new and advanced business IS, and the controls that are needed to respond to those risks.

Hermanson *et al.* (2000a) conducted an exploratory study to examine the IT-related activities of IA in US organizations. Information gathered from over 100 internal audit directors indicated that IA focus primarily on traditional IT risks and controls, such as IT asset safeguarding, application processing, data integrity, privacy and security. However, other areas such as risks related to systems development and acquisition received little attention from IA. The results also revealed that several factors have

المنارة للاستشارات

www.mana

been associated with IA' performance of IT evaluations, including the nature of the audit objective, the prevalence of computer audit specialists on the internal audit staff and the existence of new CIS. The current study is carried out in response to the call of Hermanson *et al.* (2000a) to investigate the role of other groups beyond IA that might be potentially involved in IT risk assessment and management, particularly for areas receiving little attention from IA, and to examine the efforts of other groups in addressing such risks.

Rishel and Ivancevich (2003) discussed some important responsibilities for IA in the IT implementation process. They argued that IA' responsibilities traditionally have been centered on risk management issues and control testing, particularly in the pre-implementation and monitoring phases of IT projects, rather than playing an integral role in enhancing the viability of IT implementations. The study suggested that IA can and should provide input with regard to system configuration in order to ensure that the proper integral controls are in place. IA should also communicate with the IT team to ensure that new systems and modifications to existing systems are adequately documented. As proper documentation can be so vital to internal audit in its evaluation of controls and risks, IA should mandate that CIS changes be tracked by documentation.

The debate about whether consulting impacts the independence of the internal audit function has been documented in the auditing literature. Meredith and Akers (2003) surveyed 241 chief executive officers (CEOs) to investigate their opinions on internal audit's involvement in systems development, including whether IA' independence is compromised by such involvement and whether auditors should act as consultants for systems development projects. The results of the study revealed that CEOs are more concerned with the internal audit function remaining independent than with auditors acting as consultants to an organization. The respondents were essentially indifferent regarding internal audit's involvement in the planning and design phases and did not support internal audit involvement in the development, implementation, and maintenance phases. The results of the comparison of the perceptions between CEOs and chief audit executives (CAEs) show that there are significant differences between the groups regarding their expectations. CEOs placed more importance on independence while CAEs emphasized the need for IA acting as consultants.

Hadden *et al.* (2003) examined the perceived IT qualifications and IT activities of audit committees, IA and external auditors regarding IT risk management. The results of the study revealed that some organizations were able to achieve more effective IT oversight by tapping into the resources of the audit committee and external auditors to a greater extent. The audit committee members indicated that their IT oversight role should be greater than what it presently is. The results suggested that although audit committees appear to provide limited oversight of IT-related risks, they generally believe that their committees should take a more active role in overseeing this area. The results also revealed no significant differences in internal audit's perceived IT qualifications or activities between the in-house versus outsourced groups. The results suggested that the IA' commitment to IT oversight was rated "above moderate"; while the external auditors' involvement in IT oversight was rated moderate, significantly lower than the IA' mean rating.

Chan (2004) studied the IT dimension of SOA in order to determine the manner and extent to which IT systems play into meeting the act's requirements. Chan (2004)

المنارة للاستشارات

www.mana

mentioned that the connection between IT and SOA could be found in several recent documents, including an auditing standard proposed in October 2003 by the Public Company Accounting Oversight Board (Release No. 2003-017). The document stated that "the nature and characteristics of a company's use of IT in its IS affect the company's internal control over financial reporting." The Information Systems Audit and Control Association's IT Governance Institute has also addressed this issue in its recent discussion document, IT Control Objectives for SOA, and in a written response to the PCAOB's proposal in November 2003. Chan argued that still, relatively little formal attention has been devoted to the IT aspect of the SOA.

Cannon and Crowe (2004) discussed the importance of IT to the internal control environment and described many aspects of IT professional culture that might affect IT's perception of its role with respect of financial controls and compliance with SOA. The paper highlighted the importance of the IT function to the control environment and the success of any SOA initiative. Cannon and Crowe (2004) argued that the IT area does not necessarily view effectiveness of financial controls as their own responsibility. However, SOA imposed new responsibilities on organizations, some of which should necessarily be delegated by the IT function. Accordingly, the IT function and IA need to understand and accept these responsibilities. The study suggested that only few individuals in the IT area have a background in internal controls or business processes.

Al-Twaijry *et al.* (2004) examined the relationship between internal and external audit in Saudi organizations using a questionnaire survey. The results of the study revealed that external auditors expressed much concern about the independence, scope of work and small size of many internal audit departments in Saudi organizations. IA considered co-operation between internal and external audits to be limited, although external auditors were more positive regarding the same issue. The findings also revealed that the extent of reliance by the external auditors on the work of the IA varied with the quality of the internal audit department. External auditors believe that the internal audit function in many Saudi organizations lacked professionalism and independence from management, which adversely affected their work and the potential for reliance on it. They recommended devoting more resources to establish independent and competent internal audit departments in order to enhance the reliability of internal audit in Saudi organizations. The current study empirically investigates the main activities carried out by IA in Saudi organizations, and whether they are involved in designing and evaluating their CIS internal controls.

Goodwin (2004) surveyed a sample of chief IA to explore the similarities and differences of internal auditing between the public and the private sectors in Australia and New Zealand. The results of the study suggested that there were differences in status between internal auditing in the two sectors. However, public sector internal audit functions have a higher status than their private sector counterparts, where more than a third of chief IA report to the chief financial officer. The results revealed no significant differences between internal audit activities and interactions with external audit in the two sectors. However, the time spent on different internal audit activities is quite similar in both sectors. Interactions with the external auditor also do not differ significantly between the two sectors.

Hunton *et al.* (2004) conducted an experimental study to understand, assess and examine the extent to which financial auditors and IS audit specialists recognize

المنارة للاستشارات

www.mana

differences in the nature and unique business and audit risks associated with ERP systems, as compared with traditional computerized (non-ERP) systems. The results suggested that financial auditors are significantly less concerned about ERP risks compared with IS audit specialists. Moreover, IS audit specialists are less confident in financial auditors' abilities to recognize the unique risks posed by ERP systems, which could have harmful effects on audit quality.

Fadzil *et al.* (2005) conducted a survey on the listed companies in the Bursa Malaysia in 2001 to investigate whether the internal audit department of the listed companies complied with the Standards for the Professional Practice of Internal Auditors – SPPIA (2000), and, whether compliance to the SPPIA would affect the quality of the internal control system of the company. The results of the study revealed that management of the internal audit department, professional proficiency, objectivity, and review significantly influenced the monitoring and risk assessment aspect of the internal control system. The performance of audit work and audit reporting significantly influence the control activities aspect of the internal control system.

Abu-Musa (2006a) investigated the perceived threats of computerized accounting information systems (CAIS) in Saudi organizations. The results of the study revealed that almost half of the responding Saudi organizations suffered financial losses due to internal and external CAIS security breaches. The results also revealed that accidental and intentional entry of bad data, accidental destruction of data by employees, employees' sharing of passwords, introduction of computer viruses to CAIS, suppression and destruction of output, unauthorized document visibility, and directing prints and distributed information to people who were not entitled to receive are the most significant perceived security threats to CAIS in Saudi organizations. The study introduced some suggestions and recommendations to strengthen the IT security controls and to enhance the awareness of CAIS security issues in Saudi organizations in order to manage the IT risks and to achieve a better protection to their CAIS and IT internal controls.

In another recent study, Abu-Musa (2006b) empirically examined the existence and adequacy of CAIS security controls to prevent, detect and correct security breaches in Saudi organizations. The results of the study highlighted a number of inadequately implemented CAIS security controls, and introduced some suggestions and recommendations to strengthen the weak points and to close the loopholes in the CAIS security controls in Saudi organizations.

Goodwin-Stewart and Kent (2006) investigated the voluntary use of internal audit by Australian publicly listed companies to identify the main factors leading listed companies to have an internal audit function. The results of the study showed that a large proportion of Australian listed companies do not use internal audit and many of those organizations that do, have only one or two internal audit staff. The results also revealed an association between the use of internal audit and a commitment to strong risk management. A strong association between internal audit and the size of the organization has been found, suggesting that smaller organizations do not regard internal audit as cost effective. The results also revealed a significant relationship between internal audit and the complexity of the organization's business structures. However, the study found only weak support for an association between the use of internal audit and strong corporate governance.

المنارة للاستشارات

www.mana

Arena *et al.* (2006) carried out a multiple case study to describe and compare the main characteristics of internal audit departments in six Italian companies and investigate the influence of enacted regulations on their development. The results of the study revealed a wide range of the diversity in internal audit department characteristics, confirming the relevance of institutional pressures, and also providing evidence of the influence of additional elements in their development. The study demonstrated that there was a significant influence of regulations on the development of internal audit, and this influence was stronger with regulation imposed sanctions.

Bierstaker *et al.* (2006) surveyed 86 accountants, IA and certified fraud examiners to examine the extent to which they use fraud prevention and detection methods, and their perceptions of the effectiveness of these methods. The results indicated that firewalls, virus and password protection, and internal control review and improvement are quite commonly used to combat fraud. However, continuous auditing, discovery sampling, data mining, forensic accountants, and digital analysis software are less often used, despite receiving high ratings of effectiveness due to lack of resources and their reluctance to invest in fraud prevention and detection control systems.

Sarens and de Beelde (2006) interviewed CAEs in ten different large manufacturing and service companies located in Belgium and Belgian subsidiaries of US companies. The results of the study suggested that in the Belgian cases, IA' focus on severe shortcomings in the risk management system creates opportunities to demonstrate their value. IA are playing a pioneering role in the creation of a higher level of risk and control awareness and a more formalized risk management system. However, in the US cases, IA' objective evaluations and opinions are a valuable input for the new internal control review and disclosure requirements mentioned in the SOA. The study introduced some recommendations for improving internal control system as an integral valuable part of the assurance role.

It is observed there is a lack of efficient and effective professional standards in Saudi Arabia in the area of IT and internal auditing compared with other countries. In the USA, for example, the AICPA (1974, 1984, 1988, 1995, 2001) issued many standards related to IT and its affect on the auditor's consideration and evaluation of internal controls (SAS No. 3, SAS No. 48, SAS No. 94). Furthermore, ISACA (1997a, b, c, d, e, f, g, h) issued eight standards for IS auditing which guides their members in evaluating IT internal controls and auditing CIS. However, a review of the professional standards issued by the Saudi Organization for Certified Public Accountants (SOCPA) revealed the existence of only one exposure draft issued in July 2004 in that area. The exposure draft was entitled "Internal Audit and Behavioral Conduct Rules" and required IA to be aware of IT internal controls and its related risks. However, the exposure draft did not introduce any suggestion for evaluating such internal controls and IT risks. SOCPA (2000) also issued its Auditing Standard No. 8 entitled "Auditing standards for companies using computers." The standard is mainly directed to external auditors who auditing the financial statements of listed companies rather than IA. Accordingly, Saudi Arabia seems to be so far behind the developed countries in this regard.

It is observed that many of the previous studies have been implemented in developed countries but few have investigated the role of IA in designing and evaluating internal controls in developing countries. It is believed that conducting this research in one of the developing countries, namely Saudi Arabia, can thus yield fruitful results. From a practical standpoint, managers and IA alike stand to gain from the findings of this study.

المنارة للاستشارات

www.mana

The results should enable managers and IA to better understand and evaluate the implemented internal controls and other IT activities carried out by internal audit departments, and to champion IT development for the success of their businesses.

The research methodology

In this study, a survey, using a self-administered questionnaire (see Appendix), was conducted to explore and evaluate the effect of IT and its related activities on IA in Saudi organizations. The study used the questionnaire developed by Hermanson *et al.* (2000a). It was revised to take into consideration the comments and suggestions raised by Burton (2000) and Jackson (2000). Hermanson *et al.* (2000a) developed the original questionnaire based on the elements of IT as grouped by IFAC in the statement IT in the Accounting Curriculum (IFAC, 1995, 2002).

The questionnaire contains four main parts. In the first part, the respondents were asked to answer four questions related to the objectives of their audit evaluations of CIS using an interval scale rated from 1 – rarely done to 5 – always done for each objective. The second part of the questionnaire requested the respondents to provide information on the 36 specific tests outlined by IFAC (classified under eight main groups) using a five interval scale rated from 1 – rarely done to 5 – always done for each individual test. The third part of the questionnaire collected primary information related to the usage of computer assisted audit techniques by the IA in the Saudi organizations. Finally, the last part of the questionnaire contains questions addressing the main organizations' characteristics and respondents' profile. The questionnaire was pre-tested, again on a selected number of academic staff and accounting practitioners, and was piloted on a selected sample of Saudi organizations. Comments and suggestions were considered in developing and revising the final copy of the questionnaire used in this survey (see Appendix).

The respondents were asked to respond to the questionnaire based on their internal audit department's "typical" audit approach or "typical" portfolio of audit activities (see Appendix). The respondents were given strict guarantees of anonymity regarding the collected data, and were assured that it would be used only for academic research purposes.

About 700 copies of the questionnaires were randomly distributed to different organizations (manufacturing companies, merchandising companies, banks, services companies, oil and gas companies, governmental units and others) in five main cities (Al-Khoubar, Dammam, Dhahran, Jeddah and Riyadh) in Saudi Arabia. After excluding incomplete and invalid questionnaires, the research ended with 218 valid and usable questionnaires – representing a 30.7 percent response rate.

A reliability test was carried out on the collected data using the Cronbach α model, to explore the internal consistency of the questionnaire, based on the average inter-item correlation. The result of the reliability test shows that the questionnaire design is highly reliable, and the collected data are highly reliable and consistent ($\alpha = 0.8421$). The student test (t-test) was also carried out to investigate if there were any significant differences between early responses (150 questionnaires) and late responses (68 questionnaires). The results of the student test revealed no significant differences between early and late responses (at significance level $p = 0.05$), providing evidence of a representative and unbiased research sample.

The collected data show that 58 of the respondents were services organizations and 50 were manufacturing companies, representing 26.6 and 22.9 percent of the total responses, respectively (Table I). While 34 respondents were merchandising companies

المنارة للاستشارات
www.mana

The research sample according to business type			The research sample according to respondent type		
Type of business	Frequency	Percent	Job title	Frequency	Percent
Manufacturing	50	22.9	Executive manager	33	15.1
Merchandising	34	15.6	Internal auditor	83	38.1
Banking	25	11.5	Staff accountant	30	13.8
Services	58	26.6	Cost accountant	7	3.2
Oil and gas	20	9.2	IT specialist	22	10.1
Government	15	6.9	Controller	10	4.6
Other	16	7.3	EDP auditor	4	1.8
			Other	29	13.3
Total	218	100.0	Total	218	100.0

Table I.
The research sample

(15.6 percent) and 25 of the respondents – representing 11.5 percent of the total responses – were banks, 20 respondents (9.2 percent) belonged to oil and gas industry and 15 respondents (6.9 percent) were from the governmental sector. Finally, 16 respondents (7.3 percent of the total) belonged to other organizations, such as hotels, car rental organizations, décor and carpentry firms, publishing and printing organizations, accounting and auditing firms, construction companies and design organizations.

Table I also shows that the vast majority of respondents (83 respondents representing 38.1 percent of the total response) were IA. About 33 respondents (15.1 percent) were executive managers, 30 respondents (13.8 percent) were staff accountants, seven respondents were cost accountants, and ten respondents (4.6 percent) were controllers. While, 22 respondents (10.1 percent) were IT specialists and four respondents were EDP auditors.

The collected data were processed using the SPSS version 15. Descriptive statistics of the collected data were analyzed for the purpose of understanding the main characteristics of the research variables and to answer the *RQ1* of what IA are currently doing with respect to evaluating the IT risks in Saudi organizations. The *RQ2* related to the relationship between IT evaluation categories ($EVAL_{ij}$) carried out by IA (dependent variable), and the IT evaluation objectives and organizational characteristics (independent variables) was examined using the following ordinal least squares (OLS) regression model:

$$EVAL_i = \beta_0 + \sum_{j=1}^{9} \beta_j X_j + \varepsilon \quad (1)$$

$EVAL_i$ = IT evaluation No. i; $i = 1, 2, \ldots, 8$ (index of dependent variables); $j = 1, 2, \ldots, 9$ (index of independent variables); β_0, constant (y intercept); β_J, regression confession, ϵ, regression error, $EVAL_1$, system development and acquisition; $EVAL_2$, system implementation; $EVAL_3$, system maintenance and program changes; $EVAL_4$, IT asset safeguarding; $EVAL_5$, data integrity, privacy, and security; $EVAL_6$, continuity of processing/data recovery plan; $EVAL_7$, operating system/network; $EVAL_8$, application processing; X_1, evaluation of efficiency, effectiveness, economy of IT use; X_2, evaluation of compliance with policies, statutes, and regulations; X_3, evaluation of internal control in computer-based systems; X_4, completeness of computerized accounting records; X_5, type of industry (merchandising, manufacturing,

المنارة للاستشارات

www.mana

services . . . , etc.); X_6, number of IA; X_7, percentage of CA on the internal audit staff (No. of CA/No. of IA); X_8: organization's CIS (central = 1 if centralized, and 0 otherwise); and X_9, percentage of new computer systems in the organization.

The model was run using the collected data. The dependent variable, EVAL*i*, is measured as the average of the ratings for the individual tests suggested for use by the IFAC within that evaluation category. For example, $EVAL_1$ is computed as the average score of: evaluation of acquisition/development standards and methods, tests of compliance of development methods with standards, evaluation of acquisition and development controls, and evaluation of system development technology (see Appendix).

The independent variables of the IT evaluation objectives (from X_1 to X_4) are measured using a five-point Likert scale where 1 – rarely and 5 – always done. The rest of independent variables which measure organizational characteristics, were measured as explained in the methodology section. Eight regression runs were done, one for each dependent variable. Then, an average score for the eight evaluation models was computed and labeled "COMP-EVAL." In the overall evaluation model, the dependent variable "COMP-EVAL" was regressed on the nine independent variables, using the OLS regression equation (1).

The results and discussion

The descriptive statistics address the *RQ1* regarding the frequency of performing the various IT evaluations by IA in Saudi organizations. The descriptive information on IT evaluation objectives and organizational characteristics highlights the independent variables used in the proposed regression model to address the *RQ2*.

Evaluation objectives and organizational characteristics

The statistical results in Table II show that evaluating internal control is the most common objective when evaluating CIS (OBJ_3, 3.89). This is followed by evaluation of compliance with policies, statutes, and regulations (OBJ_2, 3.87), and then evaluation of fairness of financial representations and computer records (OBJ_4, 3.52). Relatively little attention is devoted to evaluating the efficiency/effectiveness/economy of IT use (OBJ_1, 3.39). However, this task may be performed more commonly at a higher level rather than internal audit since it involves evaluation of the use of the organization's capital resources.

The result of the Kruskal-Wallis test reveals no significant differences among the Saudi organizations regarding the evaluation objectives expected for the evaluation of compliance with policies and regulations (OBJ_2) at significance level $p = 0.05$. It is also

Evaluations objectives	Mean	SD	K-W industry	K-W job
X_3: evaluation of internal control in computer-based systems (OBJ_3)	3.8853	1.14024	0.090	0.000
X_2: evaluation of compliance with policies, statutes, and regulations (OBJ_2)	3.8716	1.17266	0.033	0.001
X_4: evaluation of fairness of financial statement representations and the accuracy and completeness of computerized accounting records (OBJ_4)	3.5229	1.47543	0.436	0.029
X_1: evaluation of efficiency/effectiveness/economy of IT use (OBJ_1)	3.3899	1.24408	0.167	0.000

Table II.
Evaluations objectives

المنارة للاستشارات
www.mana

observed that the banking sector and financial service organizations showed more concern regarding the compliance with policies and regulations compared with other organizations. On the other hand, the statistical results of the Kruskal-Wallis test show significant differences in the opinions of different respondent groups regarding the same issue (at significance level $p = 0.05$). The results suggested that IT specialists, IA and executive managers devoted relatively more intentions and high concern to IT evaluation objectives compared with the others (Table II).

The statistics also reveal that one-half of the responding organizations are privately held, while 35.3 percent are publicly held and approximately 15 percent are joint venture organizations. It is also observed that more than three quarters of the responding organizations have centralized data processing systems (Table III). Approximately, 42 of the respondents have a typical style to perform audit primarily with the computer using audit software, while 35 percent of the respondents audit by computer, and 23 percent of the respondents are practice audit around the computer (Table III).

The results also revealed that slightly more than half of the respondents confirmed that the evaluation of their CIS was typically performed by computer audit specialists and approximately 37 percent indicated that they were carried out by their IA (Table III). The results of Kruskal-Wallis show significant differences among different Saudi organizations regarding the above issues. Moreover, significant differences had been found in the opinions of the respondent groups regarding the same investigated issues (at significance level $p = 0.05$).

The responding organizations have an average of 2.2 IA and median of 2, indicating very few particularly large internal audit departments in the sample (Table IV). On average, the responding organizations have only one computer audit specialist

		Frequency	Percent	K-W industry	K-W job
Company's data processing	Centralized	166	76.1	0.013	0.006
	Decentralized	52	23.9		
Organization's typical style to audit primarily	Around the computer	50	22.9	0.001	0.001
	Through the computer	77	35.3		
	With the computer	91	41.7		
Evaluations of computerized systems typically performed	Only by computer audit specialists	123	56.4	0.006	0.002
	By all of your IA	80	36.7		
	By others	15	6.9		
Company ownership	Publicly-held	77	35.3	0.000	0.008
	Privately-held	109	50.0		
	Joint venture	32	14.7		

Table III. Company's ownership, data processing and auditing style

	Number of IA	Number of computer audit specialists	Percentage of new computer systems	Percentage of outdated computer systems
Mean	2.2431	1.3486	71.2431	23.7844
Median	2.0000	1.0000	75.0000	15.0000
SD	1.46560	0.61286	21.84214	23.88653

Table IV. Organizational characteristics

المنارة للاستشارات

www.mana

in place. The results also revealed that about three-quarters of the respondents have had new CIS installed within the last three years and approximately 24 percent reported that they have outdated CIS in place (Table IV).

Types of IT evaluation

The 36 evaluation tests introduced by the IFAC (1995) statement had been grouped under eight main categories. However, due to the large number of tests, the mean and standard deviation of the specific tests within each evaluation category has been presented in Table V. Because of using the means of the tests within each evaluation category, the results pertaining to the evaluations must be interpreted considering the number of tests within each category, since just one infrequently used test could alter the relative ranking of that category (Hermanson *et al.*, 2000a).

The mean ratings within each evaluation category are illustrated in Table V. Based on these mean ratings (and tests of differences in means), it is observed that the IA in Saudi organizations place more attention and considerations on data integrity, privacy and security ($EVAL_5$), IT asset safeguarding ($EVAL_4$), and application processing ($EVAL_8$). The results are consistent with the results of Hermanson *et al.* (2000a) that IA devoted more attention to traditional IT risks and controls.

The results also revealed that moderate attention has been devoted to operating systems and network processing activities ($EVAL_7$), continuity of processing and disaster-recovery planning ($EVAL_6$) and system maintenance and program changes ($EVAL_3$). It is also observed that IA in Saudi organizations devoted the least attention to system implementation ($EVAL_2$) and systems development and acquisition ($EVAL_1$). According to Hermanson *et al.* (2000a), $EVAL_1$ may be less frequently employed because IA are often not involved with systems being developed, perhaps due to the reluctance of managers to assign a scarce resource (an IA) to a long-term system development effort. It is possible that CIS development and acquisition is addressed more extensively by in-house IT experts or outside consultants.

According to the results of the Kruskal-Wallis tests (Table V), it seems that there are significant differences among Saudi organizations regarding the evaluation of IT except for evaluating IT systems development and acquisition, systems maintenance and program changes, and evaluating the operating systems and network processing

Types of IT evaluations	Mean	SD	No. of tests	K-W industry	K-W job
$EVAL_5$: data integrity, privacy, and security	3.7523	0.93534	6	0.000	0.000
$EVAL_4$: IT asset safeguarding	3.6147	1.29450	1	0.000	0.000
$EVAL_8$: application processing	3.4954	0.99508	4	0.003	0.000
$EVAL_7$: operating system/network processing activities	3.4279	1.00000	7	0.629	0.045
$EVAL_6$: continuity of processing/disaster recovery planning	3.3735	0.96568	7	0.002	0.000
$EVAL_3$: system maintenance and program changes	3.2993	1.11836	4	0.256	0.000
$EVAL_2$: system implementation	3.2294	1.08869	3	0.017	0.005
$EVAL_1$: system development and acquisition	3.0264	1.06182	4	0.072	0.000

Table V.
Types of IT evaluations

المنارة للاستشارات

www.mana

activities at significance level $p = 0.05$. It is also observed that banks, service organizations and manufacturing companies showed a high rating for such activities compared with the others. Again, the Kruskal-Wallis test statistics (Table V) show significant differences in the opinions of different respondent groups regarding the IT evaluation activities in their organizations at $p = 0.05$. The results also suggest that IA, IT specialists and EDP auditors show more concern for IT evaluation activities compared with the other respondent groups. The details results of specific tests within each evaluation category are illustrated in Table VI.

Regression results

OLS regression models are used to address the *RQ2* related to investigating the relationship between IT evaluation aspects (dependent variable) and the IT evaluation objectives and organizational characteristics (independent variables). The following regression equation is used:

$$\begin{aligned} \text{EVAL} = {} & \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 \\ & + \beta_7 X_7 + \beta_8 X_8 + \beta_9 X_9 + \varepsilon \end{aligned} \tag{2}$$

The results of the eight models (one for each EVAL) provide insight into the factors associated with differential performance of IT evaluations across Saudi organizations. The statistical results revealed that across the eight individual OLS regression models, the adjusted R^2 has varied from 18 to 40 percent, and all eight models are significant at $p = 0.05$. The results suggest that the regression models appear to have substantial explanatory power and provide evidence that the evaluations of IT activities performed by IA are related to the audit objectives and organizational characteristics in Saudi organizations. The results of OLS regression models are illustrated in Table VII.

$EVAL_1$ (system development and acquisition)

The results of the study reveal that several factors are associated with differential emphasis with system development and acquisition of CIS ($EVAL_1$). $EVAL_1$ positively and significantly correlated with the objective of evaluating the efficiency, effectiveness, and economy of IT use (OBJ_1), and the evaluation of compliance with policies, statutes, and regulations (OBJ_2) at significance level $p = 0.05$ (Table VII).

Regarding the organizational characteristics, the statistics show a negative association between the IA' involvement in CIS development and acquisition process ($EVAL_1$) and the number of IA and the percentage of CA (No. of CA/No. of IA) in Saudi organizations at significance level $p = 0.05$. The results are surprising and in conflict with the results of Hermanson *et al.* (2000a) which suggested that IA are more involved in evaluating system development when they are part of larger internal audit departments, and when there are more CA. It is also claimed that this may be due to the greater resources and technical expertise likely to be in place in larger organizations' internal audit departments. In addition, the larger the department, the more able they are to "spare" internal audit resources for a long-term development project (p. 47).

The potential reasons for the above result could be the lack of resources, lack of technical sophistication of internal audit management, or lack of technical strength of individual IA. The lack of qualified internal audit staff and the small size of many internal audit departments have led to the reliance of outsourcing of such services through external professional experts. They also observed that most of the responding organizations used off-the-shelf rather than customized and in-house

المنارة للاستشارات

www.mana

Types of evaluations	Mean	Median	K-W industry χ^2	K-W industry P	K-W job χ^2	K-W job P
1. System development and acquisition						
a. Evaluation of acquisition/development standards and methods	3.0183	3	16.602	0.011	30.694	0.000
b. Tests of compliance of development methods with standards	3.1330	3	13.998	0.030	22.165	0.002
c. Evaluation of acquisition/development controls	3.0826	3	5.402	0.493	19.924	0.006
d. Evaluation of system development technology (e.g. CASE)	2.8716	3	16.289	0.012	21.720	0.003
2. System implementation						
a. Acceptance testing methodologies	3.2752	4	9.534	0.146	19.024	0.008
b. System conversion methodologies	3.1560	3	4.137	0.658	13.442	0.062
c. Evaluation of post-implementation review practices	3.2569	3	15.207	0.019	11.090	0.135
3. System maintenance and program changes						
a. Evaluation of system maintenance and program change standards	3.0229	3	5.635	0.465	13.414	0.063
b. Tests of system maintenance and program change controls	3.4358	4	8.447	0.207	25.001	0.001
c. Tests of production library security and controls	3.3486	4	7.257	0.298	21.412	0.003
d. Evaluation of system maintenance and program change controls	3.3899	4	12.956	0.044	25.964	0.001
4. IT asset safeguarding – evaluation of facilities management and IT asset safeguarding	3.6055	4	24.478	0.000	27.462	0.000
5. Data integrity, privacy, and security						
a. Understanding of data protection legislation, if applicable	3.6009	4	23.591	0.001	16.699	0.019
b. Consideration of personnel issues and confidentiality	3.7018	4	22.075	0.001	42.402	0.000
c. Evaluation of security standards and procedures	3.9128	4	36.660	0.000	25.332	0.001
d. Evaluation of security technologies, physical and logical access controls	3.8670	4	25.264	0.000	9.561	0.215
e. Tests of compliance with security standards and policies and effectiveness of controls	3.6651	4	11.718	0.069	20.123	0.005
f. Tests of effectiveness of controls	3.7661	4	16.194	0.013	18.449	0.010
6. Continuity of processing/disaster recovery planning						
a. Evaluation of threat and risk management methods	3.3257	3	18.628	0.005	20.571	0.004
b. Evaluation of software and data backup techniques	3.7202	4	46.520	0.000	33.433	0.000
c. Evaluation of alternate processing facility arrangements	3.2615	3	21.623	0.001	26.848	0.000
d. Evaluation of disaster recovery procedural plan, testing, and documentation	3.5229	4	8.657	0.194	43.924	0.000
e. Evaluation of integration of IS plans with user department plans	3.0596	3	11.170	0.083	15.404	0.031
f. Tests of compliance of recovery procedures with standards	3.3761	4	18.429	0.005	16.274	0.023
g. Tests of effectiveness of recovery procedures with standards	3.3486	3	6.305	0.390	13.756	0.056
7. Operating system/network processing activities						

(*continued*)

Table VI.
Specific tests within each evaluation category (scale range from 1 – rarely done to 5 – always done)

المنارة للاستشارات

www.mana

Types of evaluations	Mean	Median	K-W industry χ^2	K-W industry P	K-W job χ^2	K-W job P
a. Evaluation of operational activities	3.6514	4	9.544	0.145	14.381	0.045
b. Evaluation of performance monitoring methods	3.5917	4	13.905	0.031	3.871	0.794
c. Evaluation of controls over productivity and service quality	3.3761	4	12.564	0.051	3.882	0.793
d. Evaluation of technologies used to automate IS operations	3.0275	3	13.023	0.043	22.769	0.002
e. Tests of compliance with operational policies	3.4495	4	3.060	0.801	23.519	0.001
f. Tests of effectiveness of general controls	3.5046	4	0.801	0.462	25.635	0.001
g. Tests of performance achievements	3.3945	4	11.366	0.078	16.336	0.022
8. Application processing						
a. Identification of transaction flows	3.5459	4	22.598	0.001	28.732	0.000
b. Evaluation of strengths and weaknesses of the application	3.4679	4	22.355	0.001	28.914	0.000
c. Tests of controls within the application	3.4954	4	15.458	0.017	34.124	0.000
d. Integration of evaluation of application controls and general control	3.4725	4	8.737	0.189	13.974	0.052

Table VI.

www.mana

Dependent variables	Adj. R^2	Model *P*-value	Constant	Independent variables *P*-values sign of coefficient or significant variables *X1* IT use	*X2* Compliance	*X3* Internal controls	*X4* Financial statements	*X5* Industry	*X6* No. of IAs	*X7* No. of CAs/No. of IAs	*X8* Central	*X9* Percentage of new
$EVAL_1$ (system development and acquisition)	0.326	0.000	2.271 (0.000)	0.467 (0.000)	0.184 (0.007)	0.014 (0.854)	−0.046 (0.459)	−0.089 (0.143)	−0.207 (0.015)	−0.329 (0.000)	0.039 (0.486)	−0.027 (0.650)
$EVAL_2$ (system implementation)	0.210	0.000	2.070 (0.000)	0.411 (0.000)	0.073 (0.319)	−0.116 (0.150)	−0.084 (0.216)	−0.149 (0.024)	0.015 (0.873)	−0.170 (0.056)	0.126 (0.040)	0.154 (0.018)
$EVAL_3$ (system maintenance and program changes)	0.199	0.000	1.626 (0.0050)	0.251 (0.001)	0.127 (0.085)	−0.063 (0.438)	0.241 (0.000)	−0.045 (0.501)	0.049 (0.596)	−0.154 (0.083)	0.071 (0.248)	0.042 (0.521)
$EVAL_4$ (IT asset safeguarding)	0.198	0.000	1.905 (0.005)	0.093 (0.219)	0.076 (0.298)	−0.021 (0.799)	0.081 (0.235)	−0.315 (0.000)	0.187 (0.043)	0.044 (0.623)	0.178 (0.004)	0.098 (0.134)
$EVAL_5$ (data integrity, privacy, and security)	0.404	0.000	1.012 (0.016)	0.306 (0.000)	0.357 (0.000)	−0.042 (0.549)	0.147 (0.013)	−0.122 (0.033)	0.140 (0.078)	0.078 (0.311)	0.057 (0.289)	0.115 (0.043)
$EVAL_6$ (continuity of processing/DRP)	0.178	0.000	1.613 (0.002)	0.272 (0.000)	0.111 (0.135)	0.120 (0.145)	−0.022 (0.754)	−0.050 (0.458)	−0.101 (0.279)	−0.105 (0.244)	0.102 (0.105)	0.157 (0.019)
$EVAL_7$ (operating system/network processing)	0.229	0.000	1.483 (0.004)	0.281 (0.000)	0.263 (0.000)	−0.197 (0.014)	0.172 (0.010)	−0.005 (0.933)	0.056 (0.537)	−0.142 (0.104)	0.107 (0.078)	0.145 (0.024)
$EVAL_8$ (application processing)	0.197	0.000	1.331 (0.010)	0.254 (0.001)	0.254 (0.001)	−0.094 (0.249)	0.065 (0.341)	0.127 (0.056)	0.298 (0.001)	0.104 (0.245)	−0.089 (0.150)	0.059 (0.366)
COMP-EVAL (overall evaluation model)	0.319	0.000	1.664 (0.000)	0.370 (0.000)	0.225 (0.001)	−0.065 (0.389)	0.090 (0.153)	−0.115 (0.060)	0.073 (0.389)	−0.110 (0.182)	0.101 (0.078)	0.118 (0.051)

Table VII.
Regression results: evaluation models

www.mana

developed software. The managers of those organizations might also be reluctant to involve the IA in such activities because they are busy with daily routine work activities or are utilizing them in other value added activities. It could also be argued that IA in Saudi organizations were reluctant to be involved in the development and acquisition process of CIS to maintain high levels of independency.

$EVAL_2$ (system implementation)
$EVAL_2$ relates to the testing and conversion aspects of CIS implementation. The results revealed a positive significant association between CIS implementation and the evaluation of efficiency, effectiveness and economy of IT use (OBJ_1) at significance level $p = 0.05$ (Table VII). It is also observed that there is a positive relation between the implementation of CIS and the percentage of the new CIS acquired in the last three years (X_9) and the type of data processing (X_8). On the other hand, the results reveal a negative association between the implementation of CIS and the industry type at a significance level $p = 0.05$.

$EVAL_3$ (system maintenance and program changes)
$EVAL_3$ relates to testing the CIS maintenance and program changes in Saudi organizations. The statistics provide evidence of the positive relation between $EVAL_3$ and the evaluation of efficiency, effectiveness and economy of IT use (OBJ_1), and the accuracy of accounting records and fairness of financial statements (OBJ_4) in Saudi organizations at significance level $p = 0.05$ (Table VII). With respect to the organizational characteristics, it is observed that more emphasis is placed on system maintenance and program changes in certain industries and when more CA are in place. The results are consistent with Hermanson *et al.* (2000a) that the industry result reflects greater work done in this area by auditors in banks and the financial services industry. This may be due to the intense reliance on CIS in the banks and financial services industry and the high cost of CIS or program problems.

$EVAL_4$ (IT asset safeguarding)
Although asset safeguarding is the most important physical access security internal control, the statistical result does not show any significant association of that variable with any of the four evaluation audit objectives. However, the result reveals a significant association between IT asset safeguarding ($EVAL_4$) and CIS type (X_8), the more decentralized the organization's IT assets, the more internal audit effort is directed at IT asset safeguarding. This result supports the contention that it is more difficult to control and secure distributed assets (Warren *et al.*, 1998). $EVAL_4$ is also significantly associated with industry type (X_5). The results provide strong evidence that auditors in banks and financial services place greater emphasis on this area compared with other industries ($p = 0.05$). The statistical results show a significant positive association between $EVAL_4$ and the number of IA (X_6) at $p = 0.05$. The larger the internal audit department the more likely the organization will be able to devote more resource and time for asset safeguarding in the long term in Saudi organizations.

$EVAL_5$ (data integrity, privacy, and security)
The regression model for $EVAL_5$ has the most explanatory power ($R^2 = 40$ percent). $EVAL_5$ considers restricting access to computer systems, password control, and effectiveness of security controls. The results revealed that IA pay a great deal of attention

المنارة للاستشارات

www.mana

on data integrity, privacy, and security in evaluating the efficiency, effectiveness, and economy of IT use (OBJ_1) at $p = 0.05$. There is strong evidence that IA direct more attention to restrict access to computer systems, password control, and effectiveness of security controls to achieve compliance with policies, regulation (OBJ_2) and data protection, and to produce highly reliable and accurate accounting records and financial statements (OBJ_4) at $p = 0.05$. Again, it seems that banks and financial service organizations have more emphasize on data integrity, privacy and security at significance level $p = 0.033$. Furthermore, new CIS are associated with greater testing of data integrity, possibly due to initial testing of new systems to ensure proper data protection ($p = 0.043$).

$EVAL_6$ (continuity of processing/DRP)

Many organizations simply cannot conduct business if their IS are not functioning; therefore, a data recovery plan (DRP) is a significant part of the internal control environment (Ivancevich *et al.*, 1998). The results show that evaluating continuity of processing and DRP ($EVAL_6$) has the weakest model ($R^2 = 18$ percent). $EVAL_6$ is found significantly and positively associated with the evaluation of the efficiency, effectiveness and economy of IT use (OBJ_1) at $p = 0.05$. $EVAL_6$ is also significantly associated with acquiring and implementing new CIS (X_9) in Saudi organizations at $p = 0.019$. The results are consistent with Hermanson *et al.* (2000a) suggesting that the implementation of new systems raises awareness of DRP issues or simply creates an opportunity to begin addressing DRP issues. In addition, this result may be due to consultants or vendors cross-selling new systems and disaster-recovery programs.

$EVAL_7$ (operating system/network)

$EVAL_7$ relates to the evaluation of operating systems and network processing aspects of CIS in Saudi organizations. The statistical results provide strong evidence that $EVAL_7$ is significantly and positively related to three of the audit objectives: evaluation of the efficiency, effectiveness, and economy of IT use (OBJ_1), evaluation of compliance with policies, rules and regulations (OBJ_2), and evaluation of completeness of CIS records and fairness of financial statements (OBJ_4) at $p = 0.05$. $EVAL_7$ is negatively associated with the evaluation of internal controls (OBJ_3) at a significant level $p = 0.01$. With respect to organizational characteristics, the results provide evidence that greater testing of operating systems and networks is associated with acquiring and implementing new systems (X_9) in Saudi organizations.

$EVAL_8$ (application processing)

Finally, the statistical results reveal that $EVAL_8$ has a positive and significant association with evaluation of the efficiency, effectiveness and economy of IT use (OBJ_1) and evaluation of compliance with policies, rules and regulations (OBJ_2). However, $EVAL_8$ is found to be positively and significantly associated with the number of IA $p = 0.05$.

COMP-EVAL (overall evaluation model)

The results suggest that the overall evaluation regression models appear to have substantial explanatory power (adj. $R^2 = 32$). The statistical results provide strong evidence that the overall evaluation model (COMP-EVAL) is significantly and positively related to three of the audit objectives: evaluation of the efficiency, effectiveness, and economy of IT use (OBJ_1) $p = 0.05$. In contrast, the results reveal a negative significant

المنارة للاستشارات

www.mana

association between COMP-EVAL and the evaluation of compliance with policies, rules and regulations (OBJ_2) at significance level $p = 0.05$. With respect to the organizational characteristics, the results reveal that the overall evaluation model is significantly associated with acquiring and implementing new CIS (X_9) in Saudi organizations at $p = 0.05$. The results provide evidence the overall IT evaluation model is positively associated with industry type (X_5), where banks and financial services place greater emphasis on the evaluation activities comparing with other industries. Al-Twaijry *et al.* (2004) believe that internal audit function is not independent, and most of the IA are more involved in the ordinary and routine daily non-audit work. IA may not be given the full access, or management does not support and listen to their recommendations. They claimed that the lack of qualified internal audit staff and the small size of many internal audit departments are likely to restrict the range and scope of duties and activities carried out by the internal audit departments in Saudi organizations.

Conclusion

The current exploratory research represents a first step in addressing the main IT-related activities performed by IA for the assessment and management of IT-related risks in Saudi organizations. The study provides evidence of the relation between IA' IT evaluations with audit objectives and organizational characteristics in the Saudi environment. IA appear to focus primarily on non-traditional application controls and system security. The most frequently performed evaluations are $EVAL_5$ (data integrity, privacy, and security), $EVAL_4$ (IT asset safeguarding – evaluation of facilities management and IT asset safeguarding), $EVAL_8$ (application processing), and $EVAL_7$ (operating system/network processing). The least performed evaluations are $EVAL_1$ (system development and acquisition), $EVAL_2$ (system implementation) and $EVAL_3$ (system maintenance and program changes).

Several interesting patterns emerge from the eight regression models. First, OBJ_1 (evaluation of the efficiency, effectiveness, and economy of IT use) appears to have the greatest association with the areas of testing identified by IFAC. Auditors with an internal control objective are more likely to perform testing in six of the eight evaluation categories. Second, both OBJ_2 (evaluation of compliance with policies, rules and regulations) and OBJ_4 (evaluation of completeness of CIS records and fairness of financial statements) are found positively and significantly associated with two non-traditional application controls and system security namely $EVAL_5$ (data integrity, privacy, and security) and $EVAL_7$ (operating system/network processing).

Third, the existence of new systems may play a role in auditors' testing strategies. There is strong evidence in five of the eight categories that testing is more extensive when new computerized systems are involved. Fourth, there is limited evidence of inter-industry differences in testing. Despite the broad range of industries represented, industry appeared to influence testing in only three of the eight categories. In those cases, banks and financial services organizations show relatively more attention to the evaluation activities compared with the others. Finally, it seems that the size of the internal audit departments, the number of computer audit specialists and the type of data processing do not significantly affecting performing the evaluation process. The factors only appear to significantly affect two of the eight evaluation categories.

It is recommended to carry out further studies in developing countries and in the Middle East to further investigate why IA seem to be performing so little work related to

المنارة للاستشارات

www.mana

IT asset safeguarding ($EVAL_7$), CIS implementation ($EVAL_2$), application processing ($EVAL_8$), and continuity of processing and DRPs ($EVAL_5$). The results of the study reveal that IA can play an integral role in enhancing the viability and usefulness of IT implementations in Saudi organizations. However, IA need to enhance their knowledge and skills of CIS to plan, direct, supervise and review the work performed. From a practical standpoint, managers and practitioners alike stand to gain from the findings of this study. The results should enable them to better understand and evaluate CIS and to champion IT development for businesses success in Saudi environment.

References

Abdul-Gader, A. (1990), "End-user computing success factors: further evidence from a developing nation", *Information Resources Management Journal*, Vol. 3 No. 1, pp. 2-13.

Abu-Musa, A.A. (2006a), "Evaluating the security controls of CAIS in Saudi organizations: the case of Saudi Arabia", *The International Journal of Digital Accounting Research*, Vol. 6 No. 11, pp. 25-64.

Abu-Musa, A.A. (2006b), "Exploring perceived threats of CAIS in developing countries: the case of Saudi Arabia", *Managerial Auditing Journal*, Vol. 21 No. 4, pp. 387-407.

AICPA (1974), *Statement on Auditing Standards No. 3: The Effects of EDP on the Auditor's Study and Evaluation of Internal Control*, AICPA, New York, NY.

AICPA (1984), *Statement on Auditing Standards No. 48: The Effects of Computer Processing on the Examination of Financial Statements*, AICPA, New York, NY.

AICPA (1988), *SAS 55: Consideration of Internal Control in a Financial Statement Audit*, AICPA, New York, NY.

AICPA (1995), *SAS 78: Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement of Auditing Standards No. 55*, AICPA, New York, NY.

AICPA (2001), *Statement on Auditing Standards No. 94: The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*, AICPA, New York, NY.

Al-Twaijry, A., Brierley, J.A. and Gwilliam, D.R. (2004), "An examination of the relationship between internal and external audit in the Saudi Arabian corporate sector", *Managerial Auditing Journal*, Vol. 19 No. 7, pp. 929-44.

Arena, M., Arnaboldi, M. and Azzone, G. (2006), "Internal audit in Italian organizations: a multiple case study", *Managerial Auditing Journal*, Vol. 21 No. 3, pp. 275-92.

Bierstaker, J.L., Brody, R.G. and Pacini, C. (2006), "Accountants' perceptions regarding fraud detection and prevention methods", *Managerial Auditing Journal*, Vol. 21 No. 5, pp. 520-35.

Burton, R.N. (2000), "Discussion of information technology-related activities of internal auditors", *Journal of Information Systems*, Vol. 14 No. 1, pp. 57-60, Supplement.

Cannon, D.M. and Crowe, G.A. (2004), "SOA compliance: will IT sabotage your efforts?", *The Journal of Corporate Accounting and Finance*, Vol. 15 No. 5, pp. 31-7.

Chan, C. (2004), "Sarbanes-Oxley: the IT dimension", *The Internal Auditor*, Vol. 61 No. 1, pp. 31-3.

COSO (1992), *Internal Control: Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission, New York, NY.

Curtiss, R.H. (1995), "Four years after massive war expenses Saudi Arabia get its second wind", The Washington Report on Middle East Affairs, September, pp. 48-52.

Fadzil, F.H., Haron, H. and Jantan, M. (2005), "Internal auditing practices and internal control system", *Managerial Auditing Journal*, Vol. 20 No. 8, pp. 844-66.

المنارة للاستشارات

www.mana

Gelinas, U., Sutton, S. and Oran, A. (1999), *Accounting Information Systems*, South-Western College Publishing, Cincinnati, OH.

Goodwin, J. (2004), "A comparison of internal audit in the private and public sectors", *Managerial Auditing Journal*, Vol. 19 No. 5, pp. 640-50.

Goodwin-Stewart, J. and Kent, P. (2006), "The use of internal audit by Australian companies", *Managerial Auditing Journal*, Vol. 21 No. 1, pp. 81-101.

Hadden, L.B., DeZoort, F.T. and Hermanson, D.R. (2003), "IT risk oversight: the roles of audit committees, internal auditors, and external auditors", *Internal Auditing*, Vol. 18 No. 6, pp. 28-31.

Hermanson, D.R., Hill, M.C. and Ivancevich, D.M. (2000a), "Information technology-related activities of internal auditors", *Journal of Information Systems*, Vol. 14 No. 1, Supplement, pp. 39-53.

Hermanson, D.R., Hill, M.C. and Ivancevich, D.M. (2000b), "Reply to discussion of information technology-related activities of internal auditors", *Journal of Information Systems*, Vol. 14 No. 1, pp. 39-53, Supplement.

Hunton, J., Wright, A. and Wright, S. (2004), "Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?", *Journal of Accounting Information Systems*, Vol. 18 No. 2, pp. 7-28.

IFAC (1995), *Information Technology in the Accounting Curriculum, Education Guideline No. 11*, International Federation of Accountants, New York, NY.

IFAC (2002), *Audit Risk Proposed International Standards on Auditing and Proposed Amendment to ISA 200, "Objective and Principles Governing an Audit of Financial Statements"*, International Federation of Accountants, New York, NY, International Auditing and Assurance Standards Board, Exposure Draft, October.

Information Systems Audit and Control Foundation (1998), *Control Objectives for Information and Related Technology (COBIT)*, ISACF, Rolling Meadows, IL.

International Standard on Auditing 401 (2002), *Auditing in Computer Information Systems Environment*.

ISACA (1997a), *Standards for Information Systems Auditing 010: Audit Charter*, ISACA, Rolling Meadows, IL.

ISACA (1997b), *Standards for Information Systems Auditing 020: Independence*, ISACA, Rolling Meadows, IL.

ISACA (1997c), *Standards for Information Systems Auditing 030: Professional Ethics and Standards*, ISACA, Rolling Meadows, IL.

ISACA (1997d), *Standards for Information Systems Auditing 040: Competence*, ISACA, Rolling Meadows, IL.

ISACA (1997e), *Standards for Information Systems Auditing 050: Planning*, ISACA, Rolling Meadows, IL.

ISACA (1997f), *Standards for Information Systems Auditing 060: Performance of Audit Work*, ISACA, Rolling Meadows, IL.

ISACA (1997g), *Standards for Information Systems Auditing 070: Reporting*, ISACA, Rolling Meadows, IL.

ISACA (1997h), *Standards for Information Systems Auditing 080: Follow-up Activities*, ISACA, Rolling Meadows, IL.

Ivancevich, D.M., Hermanson, D.R. and Smith, L.M. (1998), "The association of perceived disaster recovery plan strength with organizational characteristics", *Journal of Information Systems*, Spring, pp. 31-40.

المنارة للاستشارات

www.mana

Jackson, C. (2000), "Discussion of information technology-related activities of internal auditors", *Journal of Information Systems*, Vol. 14 No. 1, pp. 55-6, Supplement.

Jasimuddin, S. (2001), "Analyzing the competitive advantages of Saudi Arabia with Porter's model", *Journal of Business & Industrial Marketing*, Vol. 16 No. 1, pp. 59-68.

Meredith, M. and Akers, M.D. (2003), "Internal audit's role in systems development: the CEO's perspective", *Internal Auditing*, Vol. 18 No. 1, pp. 35-9.

Pathak, J. (2003), "IT auditing and electronic funds transfers", *Internal Auditing*, Vol. 18 No. 5, p. 28.

POB (2000), *The Panel on Audit Effectiveness: Report and Recommendations*, Public Oversight Board, New York, NY, available at: www.pobauditpanel.org

Rezaee, Z. and Reinstein, A. (1998), "The impact of emerging information technology on auditing", *Managerial Auditing Journal*, Vol. 13 No. 8, pp. 465-71.

Rishel, T.D. and Ivancevich, S.H. (2003), "Additional opportunities for internal auditors in IT implementations", *Internal Auditing*, Vol. 18 No. 2, pp. 35-9.

Sarens, G. and de Beelde, I. (2006), "Internal auditors' perception about their role in risk management: a comparison between US and Belgian companies", *Managerial Auditing Journal*, Vol. 21 No. 1, pp. 63-80.

Silltow, J. (2003), "Shedding light on information technology risks", *The Internal Auditor*, Vol. 60 No. 6, p. 32.

Sohail, M. and Al-Abdali, O. (2005), "The usage of third party logistics in Saudi Arabia current position and future prospects", *International Journal of Physical Distribution & Logistics Management*, Vol. 35 No. 9, pp. 637-53.

Spira, L.F. and Page, M. (2003), "Risk management: the reinvention of internal control and the changing role of internal audit", *Accounting, Auditing & Accountability Journal*, Vol. 16 No. 4, pp. 640-61.

SPPIA (2000), *The Standards for the Professional Practice of Internal Auditing*, The Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.

Tongren, J.D. (1997), "Coactive audit: the enhancement audit model", *Managerial Finance*, Vol. 23 No. 12, pp. 44-51.

Warren, J., Edelson, L., Parker, X. and Thrun, R. (1998), *Handbook of IT Auditing*, Warren, Gorham & Lamont, New York, NY.

Yavas, U. (1997), "Management know-how transfer to Saudi Arabia: a survey of Saudi managers", *Industrial Management & Data Systems*, Vol. 97 No. 7, pp. 280-6.

Yavas, U. and Yasin, M. (1999), "Organizational significance and application of computer skills: a culturally-based empirical examination", *Cross cultural Management – An International Journal*, Vol. 6 No. 4, pp. 11-21.

(For Appendix see following page)

المنارة للاستشارات

www.mana

Appendix

بسم الله الرحمن الرحيم

Ministry of Higher Education
King Fahd University of Petroleum & Minerals
COLLEGE OF INDUSTRIAL MANAGEMENT
DEPARTMENT OF
ACCOUNTING & MANAGEMENT INFORMATION SYSTEMS

وزارة التعليم العالي
جامعة الملك فهد للبترول و المعادن
كلية الإدارة الصناعية
قسم المحاسبة ونظم المعلومات الإدارية

Dear Sir

I am examining the usage and evaluation of IT by IA in Saudi organizations. The study is designed:

- to provide internal audit directors with an overview of other companies' approaches to auditing CIS; and
- to provide accounting educators with greater insight into the IT dimension of internal auditing practice so that we can better prepare future graduates for professional success.

The impetus for this research is the release of the International Federation of Accountants' Education Guideline No. 11, "Information Technology in the Accounting Curriculum." The Guideline summarizes the IT competencies required of practicing accountants and auditors. Our study will examine the tie between the competencies listed in the guideline (the system evaluator role) and current internal audit practice. In other words, "How are the competencies in the Guideline reflected in internal audits today in Saudi Arabia?"

Please take a few (approximately 15) minutes to complete the enclosed questionnaire. You have our personal and professional assurance that all responses will remain anonymous. No results will be attributed to any particular organization.

I would very much appreciate your assistance with this research. Your response is very important to the study, and I thank you in advance for your participation.

Sincerely,

Dr Ahmad Abu-Musa.

Please respond to the questions below by circling the appropriate number on the scale. **Please answer all questions based on your internal audit department's "typical" audit approach or "typical" portfolio of audit activities. If a question is not applicable to your organization, please leave the response blank.** You have my personal and professional assurance that all responses will remain anonymous. No results will be attributed to any particular organization.

Part A – Evaluation Objectives

As your internal audit department evaluates computerized information systems, what are the primary (most common) objectives of your evaluation? Please rate the four possible objectives below.

Evaluation Objectives	Rarely Done (1)	Occasionally Done (2)	Frequently Done (3)	Often Done (4)	Always Done (5)
1. Evaluation of efficiency / effectiveness / economy of IT use					
2. Evaluation of compliance with policies, statutes, and regulations					
3. Evaluation of internal control in computer-based systems					
4. Evaluation of fairness of financial statement representations and the accuracy and completeness of computerized accounting records					

المنارة للاستشارات

www.mana

Part B -- Types of Evaluations

Evaluations of computerized information systems (CIS) can involve a number of specific tests. Please rate the frequency of your department's performance of the following specific evaluations and tests.

Types of Evaluations	Rarely Done (1)	Occasionally Done (2)	Frequently Done (3)	Often Done (4)	Always Done (5)
1. System development and acquisition					
a. Evaluation of acquisition / development standards and methods					
b. Tests of compliance of development methods with standards					
c. Evaluation of acquisition / development controls					
d. Evaluation of system development technology (e.g., CASE)					
2. System implementation					
a. Acceptance testing methodologies					
b. System conversion methodologies					
c. Evaluation of post-implementation review practices					
3. System maintenance and program changes					
a. Evaluation of system maintenance and program change standards					
b. Tests of system maintenance and program change controls					
c. Tests of production library security and controls					
d. Evaluation of system maintenance and program change controls					
4. IT asset safeguarding – evaluation of facilities management and IT asset safeguarding					
5. Data integrity, privacy, and security					
a. Understanding of data protection legislation, if applicable					
b. Consideration of personnel issues and confidentiality					
c. Evaluation of security standards and procedures					
d. Evaluation of security technologies, physical and logical access controls					
e. Tests of compliance with security standards and policies and effectiveness of controls					
f. Tests of effectiveness of controls					
6. Continuity of processing / disaster recovery planning					
a. Evaluation of threat and risk management methods					
b. Evaluation of software and data backup techniques					
c. Evaluation of alternate processing facility arrangements					
d. Evaluation of disaster recovery procedural plan, testing, and documentation					
e. Evaluation of integration of IS plans with user department plans					
f. Tests of compliance of recovery procedures with standards					
g. Tests of effectiveness of recovery procedures with standards					
7. Operating system / network processing activities					
a. Evaluation of operational activities					
b. Evaluation of performance monitoring methods					
c. Evaluation of controls over productivity and service quality					
d. Evaluation of technologies used to automate IS operations					
e. Tests of compliance with operational policies					
f. Tests of effectiveness of general controls					
g. Tests of performance achievements					
8. Application processing					
a. Identification of transaction flows					
b. Evaluation of strengths and weaknesses of the application					
c. Tests of controls within the application					
d. Integration of evaluation of application controls and general controls					

المنارة للاستشارات

www.mana

Part C – Usage of Computer Assisted Audit Techniques

Please rate the extent to which your internal audit department uses the following techniques.

Usage of Computer Assisted Audit Techniques	Rarely Done (1)	Occasionally Done (2)	Frequently Done (3)	Often Done (4)	Always Done (5)
1. System analysis and documentation (e.g., flowcharting packages, review of program logic)					
2. System / program testing (e.g., test data, integrated test facility, parallel simulation)					
3. Data integrity testing (e.g., generalized audit software, utilities)					
4. Problem-solving aids (e.g., spreadsheet, database, on-line databases)					
5. Administrative aids (e.g., word processing, audit program generators, work paper generators)					

Part D – Company Information and Other Questions

1. Are evaluations of computerized information systems **typically** performed (check one):
   a. only by computer audit specialists? _____
   b. by all of your internal auditors? _____
   c. other (explain below). _____

2. Is your organization's **typical** style to audit primarily (check one):
   a. around the computer? _____
   b. through the computer? _____
   c. with the computer? _____

3. Company demographics:
   a. Revenues in most recent year SR_____
   b. Number of internal auditors _____
   c. Number of computer audit specialists _____
   d. Industry (check one):
      Manufacturing _____
      Service _____
      Retail / Wholesale _____
      Banks _____
      Regulated _____
      Other _____ _____
   e. Is company (check one):
      Publicly-held? _____
      Privately-held? _____
      Joint Venture? _____

4. Computer system information
   a. Is company's data processing generally (check one):
      Centralized? _____
      Decentralized? _____
   b. Approximately what percentage of the company's computer systems is new within the last 3 years? _____
   c. Approximately what percentage of the company's computer systems is, in your opinion, outdated? _____

5. What is your job title? _____

المنارة للاستشارات

www.mana

THANK YOU VERY MUCH FOR PARTICIPATING IN THIS STUDY.

Please return the questionnaire in the business reply envelope to:

Dr. Ahmad A. Abu-Musa
Department of Accounting and MIS
College of Industrial Management
King Fahd University of Petroleum and Minerals
P O Box 1755, Dhahran, 31261, Saudi Arabia
Phone: 00966-3-860-1420
Fax: 00966-3-860-3489
mailto:abumusa@kfupm.edu.sa

IF YOU WOULD LIKE TO RECEIVE A COPY OF THE RESULTS, PLEASE ENCLOSE A BUSINESS CARD.

Corresponding author
Ahmad A. Abu-Musa can be contacted at: abumusa@kfupm.edu.sa

To purchase reprints of this article please e-mail: **reprints@emeraldinsight.com**
Or visit our web site for further details: **www.emeraldinsight.com/reprints**

المنارة للاستشارات

www.mana

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

www.manaraa.com