African Journal of Business Management Vol. 5(9), pp. 3523-3539, 4 May, 2011
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM10.1047
ISSN 1993-8233 ©2011 Academic Journals

Full Length Research Paper

The impact of information technology on internal auditing

M. Krishna Moorthy[1]*, A. Seetharaman[2] Zulkifflee Mohamed[3], Meyyappan Gopalan[4] and Lee Har San[5]

[1]Faculty of Business and Finance, Universiti Tunku Abdul Rahman, Perak Campus, 31900, Kampar, Perak D.R., Malaysia.
[2]S. P. Jain Center of Management, Singapore.
[3]Faculty of Business Administration, Universiti Tun Abdul Razak, PINTAR Campus, 16-1,Jalan SS6/12, 47301 Petaling Jaya, Selangor Darul Ehsan, Malaysia.
[4]Faculty of Management, Multimedia University, Cyberjaya, Malaysia.
[5]School of Accounting and Finance, Legenda Education Group, Negeri Sembilan, Malaysia.

Accepted 21 January, 2011

This paper evaluates the role of information technology and how it affects internal audit process in the organization. The study also stresses on the global trend of adopting IT system (software/ hardware) in producing a more controlled environment in delivering the auditing process. It also constitutes on how IT affects internal control (control environment, risk assessment, control activities, information and communication and monitoring) and provides guidelines and best practices in evaluating techniques available to effectively perform auditing tasks internally. It also addresses how technology, Information system (IS) and electronic data processing (EDP) have changed the way organizations conduct its business, promoting operational efficiency and aid decision-making. It also spotlights many aspects of IT risks and controls and highlights whether the right people are overseeing IT risks to the degree they should. It demonstrates the impact of technology convergence on the internal control mechanism of an enterprise. It emphasizes that the auditor also has a responsibility to assure that the governance level of management (the audit committee and board of directors) understand risks accepted by management and the liabilities potentially transferred to board members.

Key words: Internal audit, audit tools, IT audit, continuous auditing.

INTRODUCTION

Internal audits are designed to evaluate the effectiveness of an operation's internal controls by first gathering information about how a unit operates, identifying points at which errors or inefficiencies are possible, and identifying system controls designed to prevent or detect such occurrences. Then, they test the application and performance of those controls to assess how well they work. Managers ought to routinely evaluate controls in their department's operations by following the same process.

Computers and networks provide most of the information needed for auditing. In order to be effective, auditors must use the computer as an auditing tool, audit automated systems and data, understand the business purposes for the systems, and understand the environment in which the systems operate. The other important uses for computers and networks by auditors are in audit administration. By seeking new uses for computers and communications, auditors improve their ability to review systems and information and manage their activities more effectively. Automated tools allow auditors to increase individual productivity and that of the audit function.

By recognizing the importance of emerging environment and requirement to perform audit task effectively, auditors must recognize the key reasons to use audit tools and software, which will be further explored, in later section. The key reasons include:

(i) On a personal level, learn a new skill.
(ii) Improve company decision-making using improved data.

*Corresponding author. E-mail: krishnam@utar.edu.my.

(iii) Increase the efficiency of an audit.
(iv) Reduce routine tasks to provide more time for creative and business analysis.
(v) Provide improved transparency governance of the organization.
(vi) Identify quantitative root causes for issues.
(vii) Reduce fraud and abuse.
(viii) Identify savings in supplier, customer, human resource, computer, and enterprise management.

This paper provides a brief analysis of the main areas where software tools are used in auditing, technology impacts on the auditing profession, audit impacts on emerging business and technology issues, and an example list of information technology products frequently used by auditors.

Research problem

From the literature reviews, it appears that the several issues on IT and internal audit have to be addressed and need to be answered. In essence, the research problems are summarized as follows:

1. No specific guidelines are available to ensure information technology impact can be softened through audit best practices.
2. Absence of accounting standards to educate relevant auditors in performing audit task and mitigate organizational risk.
3. The role of internal auditor has not been specified thoroughly, and correctly to ensure necessary capability and competencies being addressed and help auditor to perform auditing task effectively.
4. To study on global trend of adopting IT system (software/ hardware) in implementation of continuous controlled environment (continuous auditing).

Objectives of the research

The objectives of the research are:

1. To identify reasons for lack of guidelines available to best practices.
2. To address and suggest accounting standards to educate and help relevant auditors in performing audit task and mitigate organizational risk.
3. To suggest a detailed role of internal auditor and required skills and competencies in IT related audit.
4. To address and detailed out IT system (software/ hardware) for continuous auditing.

Scope of study

The application of information technology and its impact to internal audit profession is somehow beyond an organizational control. Mismanagement and untested presumption on this impact can be very much precious to the organization and may lead to conflict in achieving effective internal control mechanism. Proper handling of resources, maintaining records, effective communication through adopting technology offered by information technology is critical to ensure completeness of audit process and benefited auditors. This paper focuses on above critical basis and limiting the research scope within functional audit task within an organization - mainly about the tools and techniques used by auditors in audit management and administration.

SURVEY OF LITERATURE

For a better understanding and revisit previous studies on the information technology application to internal audit, literature review is outline as a basis for defining research problem and objective of this paper. The survey of literature covers the vigorous implication of technology advancement towards internal audit profession and audit management. The survey has been divided into a categories such as changing role of auditors, continuous auditing, oversight IT risks and technology implication.

Changing role of auditors

David Yang and Liming Guan (2004) discussed on the evolution of auditing in the rapid escalation of technology, which openly contribute to information technology (IT) auditing and internal control standards and guidelines. Technology, information system (IS) and electronic data processing (EDP) have changed the way organizations conduct its business, promoting operational efficiency and aid decision-making. In this essence, and in the case of United States (US) as being explored by the authors, various authoritative bodies, such as the American Institute of Certified Public Accountants (AICPA) and the Information Systems Audit and Control Association (ISACA), have issued standards to facilitate and provide sufficient guidance to auditors. According to AICPA's SAS No. 3, the objectives of accounting control are the same in both a manual system and an IT system. However, procedures used by an auditor may be affected. SAS No. 48, "the effects of computer processing on the examination of financial statements," explained and recommended auditors to evaluate the methods of computer data processing and other significant factors such as *"p*lanning and supervision, study and evaluation of internal control, evidential matter, analytical review procedures, and qualifications of the audit team*"*. It also highlighted the distinguishing characteristics of IT systems that should be considered by the auditor when conducting the evaluation process. Under SAS No. 94*,* the AICPA specify factors auditors need to consider in

financial statement auditing process and its implication to audits of all size of businesses. The authors has also reviewed and discussed the five most significant aspects of No. 94, and this supported by Tucker (2001). In addition, SAS No. 94 recognized the types of systems, controls and evidence auditors encountered. The author has touched briefly on the Statement Of Information System Auditing (SISA), which defined mandatory requirements for IS auditing and reporting. This is reviewed through SISA 010 to SISA 080. The authors have provided thorough explanation on auditing standard and guideline available in US, and suggest on how this standards and guidelines can assist auditors fundamentally in IT auditing. However, the authors have not specified type of IT auditing application and how it directly affects auditing profession. The authors also failed to prove significance impact of technology to the auditor's roles and responsibility.

Iqbal Khadaroo (2005) has explored on the widespread of corporate reporting on the Internet and its implication to auditing profession. The phenomenal growth of Internet ultimately contributes to electronic, web-based Internet reporting information. The author first had revised several literature and accounting standards to understand the nature of best practice and code of conduct for web-based business reporting. The author later had examined Internet reporting practices in Malaysia and set the limit of the study to 100's Kuala Lumpur Stock Exchange Composite Indexed (KLSE CI) companies in Malaysia for year 2003 and 2004. The author found out that there was a significant increase of companies using the internet to supply information to the public. The core activities of disclosing information are mainly on general web page attributes (line of product, business function and product promotional activities), Investor relations, and financial information; including audit reports. The author has suggested that although usage of Internet can benefits the company, reliability and verification of information disclosed has to be guarded. Based on his survey, a large number of the KSLE listed companies (14%) are hyper-linking audited financial statements to unaudited information. This may contributed to a potential manipulation by the company and influence users in accessing valid and reliable information. The accounting profession has to play an important role in improving the quality of information provided and assuring users about their reliability. The author suggested that specific audit procedures to be taken, for instance as recommended by auditing guidance issued in Australia and New Zealand (AASB, 2002; PPB, 2003). The author also suggested several security measures, for example the hosting of audited information on an auditor's web site, may provide auditors with better control, reducing audit risks and further improve the credibility and reliability of information to users. Nevertheless, the author has only discussed and analyzed implication of auditing profession on the surface level and did not conclude the real effect of internet's corporate reporting to auditors.

Jenny Goodwin (2004) has compared features of the internal audit function between organizations in the private and public sector. Several aspects has been carefully examined in which include organizational status, using internal audit as a "tour of duty" function, outsourcing of audit function, risk management, and interactions with external auditors. The study is based on a survey done in Australia and New Zealand organizations. Survey was done to indicate the length of time spent by respondents in internal audit process and it has appeared that internal audit has a higher status in the public sector rather than in private sector entities. On outsourcing, survey indicated that both sectors engaged in some outsourcing of internal audit activities particularly in information technology and system. The percentage outsourced is quite similar between these two sectors. Author has also discussed on the major activities affiliated with internal audit, specified as financial audit and internal controls, risk management operations and systems audits. The author has explored internal audit interaction with external auditors from the perspective of the chief internal auditor and results indicated there are no significant differences between public and private sector responses. Further, in both sectors, external auditors have a high level of access to internal audit reports. This may reflect the greater level of competition in the private sector audit market compared to public sector. In conclusion, the author suggested that there are differences in status between internal audit functions in the two sectors but that internal audit activities and interactions with external auditors are similar. The author only discussed on the comparison of internal auditing activities and features on structural basis without further elaborate on the functionality of internal audit process in the organization.

Jayalakshmy et al. (2005) has highlighted the pressures auditors would face in the era of globalisation and challenges in order to maintain trust and integrity. The authors have reviewed a wide range of articles and journals published and covered areas of audit fraud, true and fair view interpretation, auditor independence and role of internal auditors. This is analysed by many authors such as Hillison et al. (1999), where the authors have discussed the role and responsibility of internal auditors in the detection and prevention of fraud. In addition, Roufaiel and Dorweiler (1994) expressed that computer fraud is easy to commit but difficult to prevent and therefore, the auditors should define their responsibility for computer fraud. The authors have defined the lack of independence, integrity and credibility of the auditing profession on the role and responsibility to detect and prevent audit fraud. They also discussed on the accounting uncertainty and changes in standards over time have affected auditors in forming a true and fair view (TFV) opinion. The concept of "true and fair view" (TFV)

(TFV) is well known to accountants as well as auditors. It has been the fundamental basis of audited accounts for many years. The recent audit failure cases have revealed the issue on the concept of TFV and whether this concept certify by auditors or not, needs an overhaul to strengthen the audit process. This should be supported by taking account the judgments from stakeholders of the company and the auditors. The authors have provided acceptable awareness to the auditors, corporations and general public on the necessity to revamp the existing auditing practices. This can help the auditors not only to be professionals, but also to be seen as professionals. It is noted that internal auditors, rather than external auditors, will be more helpful in detecting and reporting fraud, since internal auditors work with the management. This automatically brings into consideration that the internal auditors should possess the same level of independence, integrity and professionalism as the external auditors. The authors have suggested that apart from defining the role of the auditors, it is also necessary to consider whether an overhaul in the concept of TFV will help the auditors in performing their duties sincerely. Unfortunately, the authors have not thoroughly provides field and statistical data on study, and the argument is purely based on secondary data. The authors have also not defined each role and responsibility taken by the auditors to detect and prevent audit fraud. No analysis was done on the possibility of actual application.

Russel Jackson (2004) explored the auditors approaches in utilising the audit tools, softwares and how technology evalution affecting their practises. The author has illustrated the Internal Auditor's 10th annual software survey in discussing the issues interconnected with audit software in United States. The author observed that the limitation of implementing audit software particularly concerned with cost implication, failure of software to meet audit departments needs, and resistance in training to auditors. The author has cited the key note presented by several experts in the audit-related software who had various experience in implementing and maintaining the software inside the organization. Richard Lanza (2004), as one of them, an audit manager, and founder of AuditSoftware.net has shared his extensive experience in the fields by suggesting several method in ensuring the successful implementation of audit software in the organization. Richard Lanza noted that, although audit programs in general are simple to open, they can be complex to run. This can be achiever through interactive training, and continuously monitor the learning process. Lanza (2004) has noted that the business sponsor (management) might reluctant to accommodate and approved the training since they perceived the training-time might led to un-productivity. The author also disclosed much information on the type of software adopted in the organization, its popularity, reliability and overall satisfaction. Many audit related software enable an organization to subsribe to and implement them in the organization. However, several issue on reliability and consistency arised when those software are not meeting auditors expectation. The author also discussed on the availibility of open-source software available in the web format. Using open-source software has distinct operational advantages. Auditors with very specific software needs may have to look beyond the built-in capabilities of available products and consider crafting their own audit tools. The author also observed customazation in developing fraud-auditing techniques. The article does not provide any detailed analysis on impact of technology advancement and availability of complex audit software could promote to efficient and effective audit performance.

Romas Staciokas and Rolandas Rupsys (2005) has aimed to understand internal audit functions, explore implication of information technology (IT) and analyze advantages of internal audit in the organizational governance. The author has explored the origin and acceptable definition of internal audit by reviewing literature, comparative analyses, and review latest research. The definition of Internal audit has continually changed and revised decade by decade, and still we are still facing certain issues understanding of internal audit function and it position within the organization. At present, the function of internal audit includes not only of internal control effectiveness, fraud investigations or assistance to external auditors, but also identification of organizational risks, consultations to the senior management with regard to risk management, process improvement or global operations. It is vital for all members of organization (management, accountants, audit committee, etc.) to have same and adequate understanding of what internal audit is all about. According to author and supported by Ruud and Bodenmann (2001), it is important to understand needs and expectations of internal and external decision makers towards internal audit function. The author has also explained that there is some independency problem faced by internal audit being as an integral part of organization. In exploring the implication of IT, the author has defined the significant benefits of IT in auditing process. Auditors aided by IT based application; Computer Assisted Audit Tools (CAATs) increased effectiveness of internal audit in the organization. On the other hand, IT development for example, automation and computerization had increased risk of discontinuing organizations activity, data loss, network breakdown and influence business monitoring and control process. The author has reemphasized the aim of internal audit function is to monitor, evaluate and improve risk management, controls, and governance process. Unfortunately, the author has not provided enough analysis on how different corporate governance's approaches can influence internal audit process in the organization.

Harrison and Datta (2007) compared the user perceptions of feature level usages and application level usages and found that users perceive a software

application as a sum of features.

According to Kim et al., (2009), Technology features have a large impact on technology acceptance in the internal audit profession as influencing system usage, perceived usefulness, and perceived ease of use. System usage, perceived usefulness, and perceived ease of use are high in basic features and low in advanced features. Technology features will have a large influence on technology acceptance in other professions.

Continuous auditing

Zabihollah Rezaee et al. (2001) have discussed on the technological advances in which will change the audit process in near future. The focus of the study is on continuous auditing (CA) and its implications to independent auditors; analyzing internal control in the ever-changing IT world; and examine key auditing aspects. The audit process has evolved from the traditional manual audit of an accounting system to the methods of auditing with and through computers. The paperless, electronically, on-line, and real-time application had contributed to continuous auditing methodologies. The authors have explored several auditing application, in which would allow real-time preparation, publication, examination, and extraction of financial information. Real-time accounting (RTA) systems, financial information and audit evidence are available in electronic form and create a new procedure in conducting financial audit. Technological advancements have also increased the importance of internal controls. This has been supported by the Committee of Sponsoring Organizations (COSO) report where indicated that components of the internal control structure are control environment, risk assessment, information and communication, control activities, and monitoring. If adequate control procedures exist in the organization, then the auditor should perform tests of controls to determine the effectiveness of internal control structure, policies and procedures. The authors have also suggested that Independent Auditors to anticipate thoroughly in scrutinize electronic evidences and evaluate its implication to the organization. This can be monitored through a substantive test, which designed to test for conformity of accounting procedures in validating financial statements. The major benefit of utilizing CA can reduce time and costs auditors traditionally spent on manual examination of transactions and account balances. It may also enable auditors to focus more on understanding a client's business and industry, and its internal control structure. The authors had profoundly explored and defined Continuous Auditing, highlight its importance, discussed conceptual framework, and examined significant audit issues of performing CA. However, the authors have not provided sufficient suggestion on how auditors should react in adapting continuous auditing process and technology advancement as a whole.

DeWayne Searcy and Jon Woodroof (2003) have assessed the continuous auditing advantages over traditional auditing, and also present significant hurdles in its implementation. According to the CICA/AICPA research report, CA is “a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors’ reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter.” A CA relies heavily on information technology. A CA leverages technology and opens database architecture to enable auditors to monitor a company’s systems over the Internet using sensors and digital agents.

The entire audit routines described above is done electronically and automatically, in real time basis. The author has defined the only constraints of CA are the performance limitations of the client’s system and the update frequency of the client’s records. The author also suggested the more frequent audit to ensure the integrity of the data. Implementing CAs can facilitate the elimination of audit wastes possible in the current audit area. In general, there are several types of wastes that can occur which are over-auditing, waiting for the data to complete the audit task, a significant delay between the reporting period and the issuance of the audit report to investors and creditors, inefficiencies in the audit process itself and audit errors and mistakes. Furthermore, by leveraging technology, a CA allows firms to produce audited financial statements immediately as demanded by interested parties. CAs will require initial increases in investments for technology and different skill sets for auditors. CAs also, in the long run allows the firms to redeploy their audit staff and resources to other services, while maintaining high levels of reliability and quality. The author stressed that CPA firms must be ready for the time when more companies realize the financial incentives for moving to the CA. The author has clearly discussed on the challenges to implementing CA but do not provide critical suggestion on what is immediate action to be taken by an organization to ensure reliability and quality of audit work is maintained by adopting CA.

Junaid Shaikh (2004) discussed on the impact of e-commerce to the auditing process and methodologies. The author aimed to explore the application of technologies, in which may assist auditors in improving the quality of their auditing process and how to use computer-assisted auditing techniques (CAATs) more effectively with the emerging information technologies. The author has disclosed a concept of electronic auditing (EA) where some of the audit tasks conducted electronically over the internet with the support of information technologies. The author has identified three emerging information technologies to constitute a software framework to facilitate EA. These technologies include object-oriented distributed middleware, internet security technologies, and intelligent agents. The author has also proposed a new CAAT called GASI based on the EA framework. GASI

inherits most of the existing GAS features and is able to achieve the same objectives as other concurrent CAATs. Moreover, GASI can be designed and deployed independently from the auditee's EDP systems. The author has demonstrated on how a CPA may conveniently audit the loan account of a bank with EA framework. The author also implicated that this system emulates EDP applications in the banking industry and is based on the CORBA architecture industrial standard. However, the EA has some limitations. This approach depends on distributed middleware standard that is CORBA, DCOM, or Java RMI, to enable the interconnections of the auditor's GASI, auditee's EDP systems, and the internet. All of these middleware technologies are in their infantry stage and this implies that they are evolving standards.

The author has successfully defines the implication and suggested practical approach in enabling auditors to improve audit tasks within the emerging information technolo-gies available. However, the author has not provide example of how auditors need to design specialized audit software for each auditee's electronic data processing (EDP) system if the EDP system uses proprietary file formats or different operating systems.

Yining Chen (2004) has explored the strategic systems approach in performing continuous auditing. With rapid emergence of information technology (IT) and the demand for timelier assurance of financial information, auditors required to invent new approaches to continuously monitor, gather, and analyze audit evidence. Historically, continuous auditing meant using programs or software to detect auditor-specified exceptions from transactions that are processed either in a real-time or a near real-time environment. The recent development of extensible business reporting language (XBRL) will also enhance the availability, exchangeability, and relevance of financial statements. With all this progress, information is made available to decision-makers on a real-time and electronic financial reporting basis. Continuous auditing depends on a continuous flow of transaction data and analysis. Continuous auditing using a strategic-systems approach will allow the auditor to continuously monitor and analyze the transactions processed in a real-time accounting system. The strategic-systems approach can also provide a greater ability to detect material misstatements in financial auditing. Auditors need to work through the seven components of the strategic-systems Knowledge Acquisition Framework, including: considering the company's strategic advantages; determine and analyzing risks; understanding key processes and competencies required to realize strategic goals and objectives; measuring and benchmarking process performance; preparing the entity-level business model to serve as a strategic-systems lens; using the model to create expectations about key assertions in the financial statements; and comparing reported financial results to expectations, using professional judgment. The strategic-systems approach offers a framework and guidance for internal auditors to develop and implement continuous auditing, despite the fact that it was originally proposed for external auditors performing financial audits. In fact, internal auditors may find advantages over external auditors in adopting the strategic-systems approach in continuous auditing. The author has clearly defined the framework on how strategic system approach can separates the traditional continuous auditing with recent IT development. However, the author has not defined the skill required by auditors in performing this theoretical approach of continuous auditing process.

Oversight IT risks

Linda Hadden et al. (2003) had explored the role of the audit committee and internal auditors in the IT area and have called for greater audit committee and internal audit involvement in IT risk oversight. The authors have suggested that an organization may be able to achieve more effective IT oversight by tapping into the resources of the audit committee and external auditors to a greater extent. In this essence, audit committee members should take a more active role in overseeing this area. Many companies rely heavily on information technology (IT) and constitute increases in organizational risk. In addressing these risks, three key questions must be answered:

1. Who is qualified to address IT risks?
2. Who is trying to address IT risks?
3. Does there appear to be a good match in terms of who is most qualified to oversee IT risks and who is actually overseeing such risks?

The first question is important because many aspects of IT risks and controls are technical in nature. In many organizations, it is unclear who has the technical expertise to address IT risks. The second question is relevant because a number of governance participants, beyond management, could be involved in IT risk oversight, including the audit committee, internal auditors, and external auditors. Coordinating efforts across these groups is an important part of effective and efficient control of IT risks. Finally, the third question is important because it addresses whether the right people are overseeing IT risks to the degree they should. During the survey, the audit committee members were asked to and the authors have derived several justification and summary on which, audit committee members are perceived to have moderate IT qualifications, while internal and external auditors are perceived to have "above moderate" qualifications. The audit committee members also rated the activity level or commitment of the audit committee, internal auditors, and external auditors with respect to IT risk oversight. In this age of reliance on IT and multiple participants in governance, internal auditors are urged to assist management and the audit committee in assessing

the organization's IT skill set, promote greater IT risk involvement on the part of the audit committee and external auditors, assist management and the audit committee in identifying gaps or overlaps in IT risk coverage and encourage the organization to explore enterprise risk management (ERM) techniques to address IT and other risks at an enterprise level. The authors through this study and survey results suggested all corporate governance players; management, audit committee, internal auditors, and external auditors to increase their IT-related efforts in minimizing the chances of an IT-related control failure.

John Siltow (2003) has explored the interconnection of internal audit practice and exposure to IT risks in general way and almost every path of the auditors in performing their job. Due to fast magnitude of IT ever-changing environment, the author has suggested the internal auditors to ensure organization to form a scenario planning in verifying the integrity of data and its sources. Auditors also need to be aware of the risks associated with these areas to help their organizations review vital systems and ensure the enterprise runs smoothly. Outside threat such as intruders, or hackers, may also target companies for illicit gain or other malicious purposes. Recent security surveys have shown that a large number of information security breaches originate from inside the organization. Employees can inadvertently harm the organization's systems by deleting important files, opening e-mail attachments that contain viruses, or attempting to fix malfunctioning devices without adequate knowledge or training. To help mitigate the risk of both deliberate and unintentional damage, organizations need to establish effective access-control measures. The author has also suggested internal auditors to pay more attention towards authorization processes. In this essence, access control represents as the "front door" to the organization. On network security risks, auditor needs to consider exploitation of social engineering, where penetration into the organization's system can be done without any technical know-how. This threat can be mitigated through training and educating employees. Apart from internal and external threat, the auditor has also need to deal with hardware and software risks, as well as threats stemming from the employees who use these assets. Discovery of illegal software can lead to reputation harm, and unnecessary damages to the organization. In this essence, the author suggested an effective software management helps optimize the organization's IT systems and reduce the total cost of ownership. Addressing potential technology risks can be extremely difficult, as the process requires organizations to predict problems within a complex, ever-changing environment. However, sufficient internal audit awareness can help deter attackers, ensure decisions are made based on accurate and timely information, and keep overall IT risks to a minimum. The author has only briefly explained the impact of IT risk to auditor without accessing in depth on how IT risk can affect the audit scope of work.

Technology implication

Jagdish Pathak (2005) has demonstrates the impact of technology convergence on the internal control mechanism of an enterprise. It is important for an auditor to be aware of the security hazards faced by financial or the entire organizational information system. The author specified the modern auditor as a complex, trained and eclectically educated person since most of the professsional audit organizations expect auditors to possess skills not only in the conventional aspects of financial systems but also in the eclectic sphere of knowledge related to the information technology and management, security and forensics, sociology, and professional judgment. International information technology (IT) security standards are identified and used to select the best technical solution for an organization's risk and security problems. Despite the technological benefits brought to security, the technology also directly impacting risk management functions throughout the organization. At this point of the convergence trend, technology can bring new capabilities and vulnerabilities to physical security and risk management. A number of factors are causing a paradigm shift in risk and security philosophy. This shift is being driven by the "convergence" of IT security methods with those of the more traditional physical security methods. The impact is being felt throughout the community, but is perhaps currently most evident at the risk management or governance level. To understand the impact technology has on risk, it is important to understand the dynamics involved when technology is added into the physical security paradigm. The author offered brief description on the difference between static and dynamic security systems and take into consideration the inherent weaknesses in security system. The author also suggested the risk management components of physical security and technology to be treated as financial assets, and auditors to perform due diligence in locating the vulnerabilities of new technological components before they are fully implemented. The author has only provided a conceptual analysis of the current state of affairs and there are no specific findings presented and lack of data analysis to support the relationship of risk management, internal control and organizational vulnerabilities.

Charles Le Grand (2001) has discussed on the basis of information technology usage in audit management in an organization. Audit management is charged with providing an effective audit force, directing audit resources for maximum benefit to the organization, and complying with laws, regulations, and policies regarding auditing. The definition of internal auditing, as approved by The IIA in June 1999, indicates “Internal auditing is an independent, objective assurance and consulting activity designed to

add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." The authors has described the tools used by auditors and classified it accordingly. On risk analysis and risk management, the auditor must assess risk and risk management and find ways to communicate with management to assure consistent views on risk. The auditor also has a responsibility to assure that the governance level of management (the audit committee and board of directors) understands risks accepted by management and the liabilities potentially transferred to board members. The author has stressed the auditor to establish the priorities in performing audit tasks monitor the changing environment and examine the organizational and operational controls surrounding information privacy. This would provide assurance that the organization not only have appropriate privacy policies, but remain in compliance with them. The author also defined the control self assessment (CSA) as a popular methodology for identifying and evaluating internal controls. CSA allows business owners and operators to focus on risk exposures and the means to mitigate, or better manage, those risks. The author also suggested auditors to make use their websites to provide a continuously available executive information system. Auditors may use the Internet to send secure communications over an unsecured medium. Internet use also changes rapidly and experience in this area will provide knowledge and skills that are valuable in audits and audit planning. The author has provide a better understanding on how IT application used in the audit management process but, somehow has not producing any empirical suggestion to help an auditors to accomplish the audit objectives, by improving the effectiveness of risk management, control, and governance processes.

Deloitte and Touche (1996) discussed the current impact of information technology on Internal Audit department. The survey on "Internal Auditing Self-Assessment Tool" helps the author to determine the proficiency of internal auditing process, which level of technology used in organizations and the impact of technology to the organization. Survey shows that information systems have become tools to assist auditors in their day-to-day activities and most organizations perceived themselves as equally exposed to any technology and their obligation to audit proficiently.

Coinciding with this trend, information systems are increasingly able to support remote workers and facilities. Network technology, groupware, and on-line services such as the Internet had shrink distances. However, survey showed that the heaviest use of technology is focused on workflow-related tools such as computer networks, e-mail, electronic working papers, and presentation graphics. By comparison, newer technologies that directly support the auditing process, such as file interrogation, automated risk analysis, decision support, and neural networks are not as heavily used. It is also noted that technologies had put information systems to a new and different use: communication, rather than computation. On the other hand, rapid development of information technologies causes continued worry about new auditing risks. The major concern to internal auditors is the methodologies available to tackle modern information systems and technologies. The author also discussed on the differentiating factor for leaders in defining what technologies are used and how extensively they should involve. Auditing leaders also rely significantly on formal training rather than on-the-job training. Author revealed and identified level of information technologies used and examined variances of implementation of different sizes and types of organizations. The concerns of auditing professional had about their profession and methodology are also explored where respondents are dissatisfied with their ability to audit new technology. The author had proposed how best to leverage technology in auditing practice and achieved auditing efficiencies through the new means of technology. The author did not explored and elaborated more on the aspect of competencies and methodology acquired to leverage and absorbed the challenges faced by the auditors.

David Coderee (1993) has explained how computer assisted audit tools and techniques (CAATT) based programs can automate certain audit function in the organization. Firstly, the author has presented numerous benefits of CAATT for audit planning and reporting. It can be used to increase audit coverage, improve the integration of audit skills, strengthen independence of auditing from information system functions, and foster greater credibility and increase cost-effectiveness through the development of reusable computerized techniques. The author demonstrates and suggests how automated tools and techniques have improved the value, efficiency, and effectiveness of audit. Example of several aspects was included in supporting author's argument. This has been defined in "internal control over hazardous material" where the ultimate audit's objective was to review controls over the procurement, distribution, storage, and disposal of hazardous materials. With the help of CAATT-based application, the auditors were able to identify the high-risk, high-materiality sites and generated transaction lists for the on-site manual review. This is resulting in minimization of risks associated with hazardous material and benefited the internal control process. From another perspective, the author has given an example of workforce reduction program where CAATT used to review the efficiency and effectiveness of this program. With programs such as workforce reduction system, personnel information system, and payroll system, the audit was successfully provides senior management with an assessment of the effectiveness of the program. The author also observed on how auditor examined the

controls over the closure process of a production plant. In this scenario, the audit team helps the organization to determine whether equipment and inventory items were sold at an appropriate price, and properly safeguarded to prevent theft or loss. The CAATT developed for this closure were successfully used and reduced timing of the planning phase generally by more than 50%. The article has profoundly demonstrate the benefits and effectiveness of CAATT in automating audit functions in the organization and allowed improvement of efficiency and effectiveness of auditing process be established. However, the author has not provided any research survey and reports to support and justify his statements. The analysis of how CAATT automating of audit function is merely based on survey and suggestion of unverifiable sources.

James et al. (2001) have explored the current impact of technology on the audit process, and discussed the future implications of technological trends to the audit profession. The author briefly provides information on current usage of technology by audit firms. In future years, paperless audits will become common where audit clients tend to shift towards paperless systems, and will be depending on audit software for enhancing related auditing procedures. Technologies such as electronic data interchange (EDI), image processing, and electronic file transfer (EFT) will make traditional audit trails disappear. The authors have taken an interview approach to analyse and investigate which audit technologies being used and any future planning within the organization. Observations on how technology has impacted audit planning, testing, and documentation are discussed. The author noted that as clients become more technically sophisticated, auditing processes from beginning to end becomes a requirement. The new-age process audit should address and guide client's business process and capable in measure performances. Many firms have adopted a risk-based audit approach to evaluate on how external and internal risks affect the audit process. For example, risk control workbench (PricewaterhouseCoopers LLP) used to advise clients on which internal control process needs to be improved to address certain risks. On audit testing in control environment, auditors must obtain an in-depth understanding of such systems to be able to audit through the client's enterprise system. In this new audit environment, software packages (for example, ACL and IDEA) are capable to improve audit efficiency by performing a variety of audit tasks that previously were completed manually. It would also be used for fraud detection. The author has noted that continuous monitoring will become increasingly important in the future as audit paper trails slowly disappeared. In lieu with the globalization, remote access software and client/server technology are essential to keep pace with businesses in the information age. The author has concluded that technology will continue to have a dramatic impact on virtually every phase of the audit process. Unfortunately, the authors have not implied which level of technology adopted ultimately can revamp and incriminate the current auditing procedures and profession.

Financial reporting

Zezhong Xiao et al. (1997) had explored the relationship between Information Technology and Corporate Financial reporting. The authors had put an effort to investigate of whether contingent factors can explain the degree and pattern of IT impact on CFR. The authors had described the contingency perspective, the hypotheses formulated on the basis of this perspective and the results of the tests of those hypotheses. It segmented the sample into sub-samples according to the specified contingent factors and examined the contingent relationships in sub-samples. The authors suggested that the effect of IT use in accounting is not confined to accountants and individual organizations, but it requires monitoring and control at the communal level. In the discussion to prevent further increase in the information asymmetry between managers and external users, the authors suggested the financial reporting regulators to encourage companies to make greater use of IT to improve external reporting. The authors noted on the effect of IT on the information asymmetry, and its implications to managers in which led to moral hazard and adverse selection. It would be interesting to investigate further how the enlarged information asymmetry has been exploited, and whether it is more likely for companies to experience moral hazard and adverse selection problems. While support for an agency theory perspective was identified in relation to the level of gearing, it was not consistent across all levels of gearing, suggesting that other unidentified factors were affecting the relationship. Overall, the findings show that the impact of IT on CFR is not unconditional and that the contingency perspective is a useful framework for investigating this impact. However, further contingent factors need to be explored by the authors before conclude any statement on correlation and relationships between IT and corporate financial reporting. The authors also failed to bring IT-related issues into perspective and possibly suggest raising awareness of opportunities and threats especially in term of corporate financial reporting (CFR).

Roger Debreceny et al. (2005) has reviewed audit software used in facilitating auditing process in financial services sectors, in particular, the extent and nature of use of computer assisted audit tools (CAATs) by local and international commercial banks in Singapore. Interviews were conducted with internal auditors and found out that CAATs are frequently being used in special investigation audits. One of the most widely deployed CAATs is GAS. Examples of GAS include the audit command language (ACL), interactive data extraction

and analysis (IDEA) and Panaudit Plus. These softwares assist auditor for data investigation. The auditor must understand the application of technology in order to identify the risk factors, which have a direct impact on audit procedures. Auditors have to focus their attention on the computerized internal control systems and test these systems for accuracy and completeness (Coderre, 1996, 1998). GAS in this assertion can aid in performing substantive tests in banks to obtain audit evidence. GAS is also used to help detect material misstatements in the financial statements. Given the wide range of risks faced by banks and their highly computerized state coupled with the functionality that GAS provides, it can be expected that bank auditors will use GAS. There is little evidence on the usage of GAS in substantive testing in audits of banks. The study found that external auditors from the major professional accounting firms make no use of GAS, either in the conduct of the information systems component of the external audit or in the testing of financial statement assertions. One finding on why GAS is not usually used by bank internal auditors is that they perceive GAS as interrogation tools to perform fraud investigations rather than as general audit tools. From these findings, it can be concluded that bank auditors do use GAS, but only to a limited extent. The authors have also contributed to better understanding and provide guidance on the role that CAATs play in the audit process of financial institutions. Unfortunately, the guidelines and suggestion provided is limited and the authors had generalized the CAAT's impact to financial institutions as a whole.

Joseph Brazel (2005) is trying to develop, assess, and provide uses for a measure of perceived enterprise resource planning (ERP) systems expertise for financial statement auditors. ERP systems are the dominant system used by the public company clients of audit firms. In such settings, the theory of planned behavior suggests that auditor perceptions of their own ERP systems expertise should influence their perceived behavioral control and, in turn, explain auditor behavior. The author has reviewed this theory and suggested that auditors who have higher levels of ERP systems expertise should perceive they have more behavioral control in ERP settings. Recent accounting research has shown that, in ERP system settings, auditors are not apt to recognize heightened inherent and control risks; and auditors with higher perceived ERP systems expertise are better able to use IT audit specialists and plan the scope of substantive procedures to mitigate ERP system related risks. Possible future uses of the measure include examining its effects on the performance of ERP system related audit tasks and customizing the measure to determine the systems expertise levels of other types of auditors. There are several limitations to this study and the measure it has developed. First, the measure captures auditors' perceptions or self-assessments of ERP systems expertise, not their actual experience, training, etc. Second, the theory of planned behavior (Ajzen, 1991) indicates that intentions can combine with perceived behavioral control to affect behavior. The construct of auditor intent with respect to ERP systems was excluded from this study in an attempt to achieve a parsimonious measure. Given that auditors are part of a profession and thus abide by a code of conduct, intentions toward auditing may be a perception that lacks the variation present in perceived behavioral control, which is affected by personal training/experience. Notwithstanding, future research could evaluate whether the measure can be improved (that is better explain about auditor behavior) by adding questions to capture the construct of intent. Third, more research is needed to evaluate the predictive and concurrent validity (that is criterion validity) of the measure and its stability over time. Fourth, the measure relates to a specific form of system: ERP systems. While this form of system may be the dominant type encountered by auditors of public companies (Cerullo and Cerullo, 2000), there are variety of systems in use and this measure may not properly measure auditor perceptions of expertise with respect to other IT. Lastly, the audit expertise literature has clearly shown that experience and training combine to create expertise in auditors. Still, other dimensions of ERP sys-tems expertise not included in the measure (for example ERP implementation knowledge) may be relevant to determining perceived auditor ERP systems expertise. The author suggested auditors on how self-perception with a tool to examine how auditor self-perceptions of ERP systems expertise can affect auditor behavior and the quality of contemporary audit services. The author has not explained further on ERP system type and its usage in the organization in estimating how ERP would impact Auditors.

METHODOLOGY

The topic gave a preliminary understanding to further understandding the role, impact and IT risk toward auditors. The information and data of the research project were gathered from various sources of secondary data. Sources of secondary data include journal articles published in magazines and downloaded from the Internet Websites including Emerald and EBSCO Host Research Databases. The Internet search engine like Google, Lycos and Yahoo also offered excellent search for locating on-line articles. Other references were also made on the research topic from various chapters of relevant accounting and textbooks. The research framework is developed as shown in Figure 1.

RESULTS AND DISCUSSION

Use of information technology in audit management

Audit management is charged with providing an effective audit force, directing audit resources for maximum benefit to the organization, and complying with laws, regulations, and policies regarding auditing. This involves reviewing processes, activities, and information that represent the

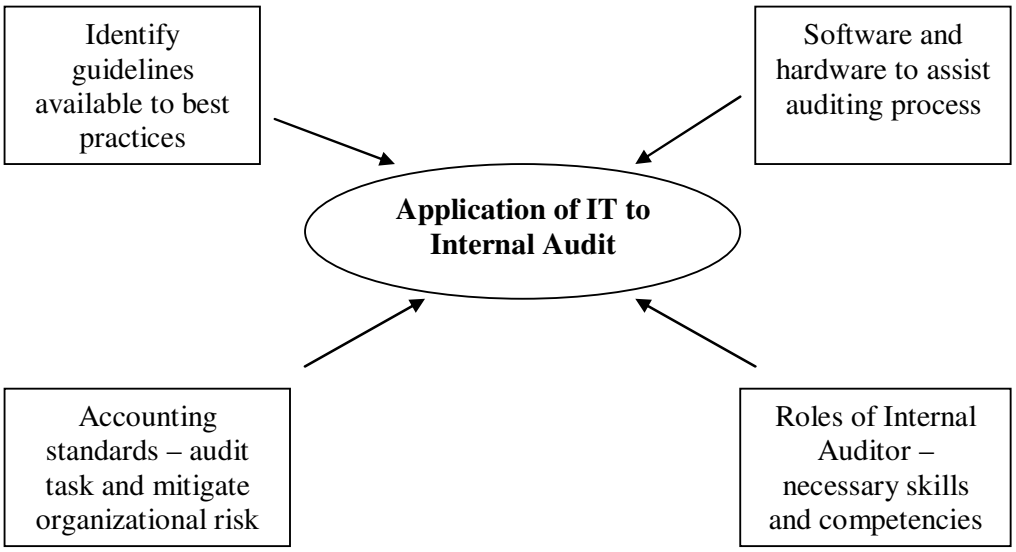

Figure 1. Research framework.

greatest risks, planning and managing individual audit engagements, maintaining records of prior and current audits, directing and scheduling personnel, and communicating effectively with audit clients, senior management, and the board of directors. Audit management includes a lot more that just using the right tools, but this paper is mainly about the tools and techniques.

Understanding risk analysis and risk management

The scope and direction for auditing objectives should be determined by assessing those areas representing greatest risks to the organization. There are many approaches to risk analysis and management. Ideally risk analysis will be performed as a risk management process within the organization – with or without direct involvement from internal auditing. If risk management is not a formal management process, then the auditor must assess risks and risk management and find ways to communicate with management to assure consistent views on risks.

Risk assessment is an iterative process and the results of risk assessments should be maintained in a manner to facilitate reference and updating by auditors during subsequent audit projects. The definition of internal auditing, approved June 1999, indicates an active role for internal auditors in risk management for their organizations: Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Sometimes auditors may focus on business controls and bypass the fact that controls exist for the purpose of managing risks. Auditors, also, may pursue risk reduction rather than perceiving the greater scope and importance of risk management.

Managers outside of auditing typically do not think of management responsibilities in terms of controls. They think of the processes and activities they manage, and how they manage risks. So an important communication tool for auditors is a clear and understood identification and assessment of risks. Managers understand risks and can probably describe the most significant risks they manage. An auditor can supplement the manager's list of risks by asking questions about the types of things auditors know can typically go wrong. It is generally more effective to proceed from a discussion of threats and risks to an assessment of controls than to start by talking about controls.

The list of risks provided by management and supplemented by the auditor is the first element of the auditor's risk analysis. The next steps involve assessing the probabilities of exposures resulting from risks and the potential costs. For this, an auditor can use tools as simple as spreadsheets or databases, or can opt for more complex systems possibly tied into an integrated audit management system. Whatever the approach and tools used, the auditor's risk assessment should be shared with management, and a general consensus should be sought to assure effective communication of objectives, priority, and scope of the audits.

The auditor also has a responsibility to assure that the governance level of management (the audit committee and board of directors) understand risks accepted by management and the liabilities potentially transferred to board members. If governance and executive management do not have a clear understanding of risk management within the organization three results are likely:

1) Risk decisions will be made at levels of the organization that are too low to adequately understand and assume responsibility for the potential consequences for risks accepted.
2) Risk decisions will not be adequately communicated to governance and executive management and they will be unaware of some risks accepted on behalf of the organization and individuals.
3) Inadequate resources may be provided for risk management in critical areas (for example, information security) because senior management is not aware of the potential consequences.

Understanding and monitoring the changing environment

The audit universe can also be subject to change – sometimes significant change. For example, five years ago Internet electronic commerce was a small item on the audit universe inventory – if it was listed at all. Today it is a major item on most audit inventories but is still not listed on some. Issues related to information security, privacy, and secure electronic commerce, especially over the unsecured medium of the Internet, are items of major importance to many organizations. In many cases internal auditors will soon be required to demonstrate expertise in subjects they cannot currently explain.

Understanding internal control evaluation

Control self assessment (CSA) is a popular methodology for identifying and evaluating internal controls. CSA allows business owners and operators to focus on risk exposures and the means to mitigate, or better manage, those risks. Often an internal auditor will become familiar with CSA and may act as a facilitator for group discussions to identify and assess internal controls, address their strengths and weaknesses, and discuss opportunities for improvements. Popular technology for CSA involves hardware and software with interactive devices for group communications in face-to-face meetings. A facilitator poses questions or statements to participants, with a set of response choices – typically projected on a large screen. The software produces a graph of the results of keypad responses, and projects it for the group to see. Some systems provide for unstructured text responses. Responses are typically anonymous to encourage frankness and openness. Immediate feedback is a key feature of CSA systems.

Understanding audit planning and scheduling

Audit planning is both strategic and tactical. The inventory of the audit universe, priority for audits, and availability of audit resources provide input to the strategic audit schedule. Tactical planning is performed for each audit project.

Strategic audit planning

Strategic scheduling factors are both logical and logistical. For example, known problems with systems development methods, system and program change control, or access controls should be addressed before auditors consider getting involved in individual systems development projects or application system reviews. Weak-nesses in key control areas such as access management and change control can also impact the reliability of any information used by auditors and may impact the scope and time required to assess and test controls.

In conducting audits of systems, information, or business processes in areas where auditors know or suspect key control weaknesses, the audit approach may be improved by initially targeting information for retrieval and analysis that will provide evidence of the consequences of control weaknesses. This approach can generate evidence of the consequences of weak controls and may be a more effective use of the auditor's time than conducting extensive analyses of the systems and control environments to identify and assess controls.

Tactical audit planning

Software tools can assist in assessing available auditor skills and assigning the appropriate people to audit project teams. Audit scheduling software should support assignment of auditors with critical skills as needed within an audit project, and allow such auditors to proceed to other projects once their tasks are completed, even if the audit is not finished. Such software should also assess the impacts of schedule and priority changes, compensate for special assignments, and extend the impacts of schedule overruns to other projects remaining in the schedule.

Changing role of auditors: The use of computer assisted audit tools and techniques (CAATTs)

As audit tools are growing more powerful and sophisticated, they are also becoming easier to learn and use. But they also must fit into a complex and ever changing environment. Features of audit software can easily conflict with features of other software on the computer or network, and must be carefully managed. As tools become more powerful, auditors may use features or services provided in the software that command large amounts of system resources (memory, processing cycles, communication bandwidth, and storage) and

compete with other users of those resources. For example, an auditor may request access to a file with a program that will examine each record in the file and may lock other users out until the process is complete. The processing could also require large amounts of network storage space at a time when it is in short supply and could cause a server to "crash." It is important to schedule such processing at times when other system users will not be delayed or prevented from performing their work. Alternatively, many audit organizations perform their audit analyses using files copied or archived from the live production files.

CAATTs may also be large, powerful, or specialized enough to require a dedicated server for audit purposes. A server may be needed to support the audit Web site, or just to assure the independence and security required by audit functions. And, as evidenced by the list of software tools attached to this document, there are more tools available than the amount of time an auditor may have to learn to use those tools. So the need for software specialists to support internal auditing is increasing even as the software is getting easier to use.

Understanding continuous internal control monitoring

Continuous monitoring in systems and networks will be a byproduct of the increasing demand for immediate and continuous access to reliable information by management, owners, investors, and regulators of organizations of all types and sizes. The pervasive availability of electronic communications drives the demand for reliable information and related assurance services.

Integrated accounting systems are rapidly becoming commonplace, and will soon be the established basis for the expectation of timeliness in availability of financial information. Immediate financial reporting and availability of information for comparison and analysis are becoming byproducts of integrated applications across all areas of businesses and industries – combining operational and financial information in integrated databases and management reporting. The emergence of standards such as Extensible Markup Language (XML) and the related Extensible Business Reporting Language (XBRL) will also help to accelerate the pace of increasing expectations for the availability of information and the related assurance of its integrity.

As previously indicated, advancements in information monitoring and analysis are being accelerated both by increasing demands for timely and accurate information, and by advances in technology that contribute to the intelligence, capabilities, and timeliness of monitoring and analysis systems. Continuous monitoring systems are not new, but they also cannot be considered widespread at this time. But the advances in systems and the increasing expectations of information availability will ensure that continuous monitoring and auditing systems will be the rule rather than the exception in the near future.

Understanding electronic audit reporting

Some audit tools today provide automatic linking between work performed, information gathered, auditor assessments, and information used in or supporting audit reports. Intelligent work papers may note answers in Internal Control Questionnaires (ICQ) that indicate actual or potential weaknesses and automatically prepare a section in the audit report to document the weakness and/or resolution of the problem.

Audit reporting too, can automatically provide information about sections of audits performed by individual auditors as they are completed so the audit supervisor will know the ongoing status of audit projects. Such reporting will also allow the supervisor to concentrate on audit processes that indicate problems and/or provide additional resources in areas falling behind schedule.

The audit report can easily contain links to work paper documents, worksheets, graphs or other information that will be automatically updated as data changes. Report files can be shared by audit team members and management by implementing simple controls over access such as read-only access to those not authorized to change the files. Audit reports can be distributed in electronic format via email, file transfer, or audit web site. In such cases auditors must assure appropriate security, confidentiality and access controls for such reports. Encryption technology is rapidly developing and will become the standard mechanism for electronic message integrity, sender and receiver authentication, and access control.

Virtual office and its implication to audit profession

A search on the World Wide Web identifies hundreds of companies promoting virtual office equipment, software, and services, but little on the subject of security, controls and auditing. A search through the literature and reference works familiar to IT security, control and auditing professionals provides plenty of information about controlling the familiar components used to facilitate the virtual office, but little in terms of the combination of risk factors inherent in virtual office environments.

The professionals responsible for implementing IT security and controls must constantly adapt their standards, practices and techniques to meet the demands of not only virtual offices, but the myriad other applications that can be accommodated and enhanced with today's burgeoning technologies. Since many new IT environments, including virtual office, are implemented primarily by people who are not IT security, control or audit specialists, the study can expect a number of installations to create environments with unacceptable levels of risks. This will create opportunities for the malefactors to exploit

security and control weaknesses which the study can hope will be sufficiently publicized to allow others to learn from their mistakes.

The IIA research foundation's systems auditability and control (SAC) reports identify business and technology risks in greater detail and relate them to associated controls and auditing. The structure of SAC modules is based on specific areas and applications of technology. In order to locate descriptions of virtual office risks, controls and auditing check the modules covering the related technologies. ISACA's control objectives for information and related technology (COBIT) identify risk assessment as an IT management process subject to auditing. COBIT also provides a checklist format for control objectives and audit guidelines under the categories of planning and organization, acquisition and implementation, delivery and support, and monitoring. Descriptions of the related technologies and risk elements are not included.

Some postulate that IT security, controls, and auditing consistently lag behind technology innovation and implementation. But as long as the studies have had computers, there have been those who predicted doom and spectacular losses from uncontrolled application of technology. Indeed there have been some spectacular losses, frauds and thefts. But overall the security, control and auditing communities have adapted well to new technologies using effective combinations of old and new security, control and auditing techniques. Auditing professionals routinely adopt and adapt the tools needed to assess the extent of risks in any environment, select the controls and data to be tested, conduct tests, evaluate the results, and provide meaningful recommendations to management at all levels in dealing with such issues as virtual offices.

The virtual office/workplace presents a new level of risk and exposure for corporations. This emerging concept will have significant impacts on the internal auditing profession. Virtual office increases the complexity in the tasks of assessing internal controls and security requiring new auditing procedures, tools and skills.

Traditional internal audits tend to rely extensively on face-to-face interviews and reviewing various data and reports. However, in a virtual office the employees or contract workers supporting a function or project may be located in numerous locations around the world. Some data and reports too may exist only in distributed or virtual office locations. Auditing the virtual office or the related processes and projects will be a function of both how well auditability is planned and provided in the new environments and how effectively the auditor can apply "virtual audit" techniques. In traditional office environments most information used to support various business functions and decisions is processed and stored at a central location or at specific offices. In the virtual environment critical and confidential information is processed and stored on many platforms: Central host computers distributed mini computers, local area network servers, desktop personal computers, notebook computers, and hand held computers.

Virtual office audits include general reviews of the overall security and control environment, information manage-ment, individual application and support systems, and business processes. Whatever the scope or approach of individual virtual office audits, the auditors will have to be knowledgeable of the business, technical, and human risk factors involved. And they will have to know where to look for specific guidance on assessing risks, understanding relevant control objectives, identifying and testing the controls in place, evaluating test results, and making appropriate recommendations. Sources for the knowledge and guidance needed in virtual office audits include:

1. Current business and technical publications.
2. Reference materials and guides such as those published by professional associations.
3. Vendors' system and auditing technical guides.
4. Professional and technical standards.
5. Numerous Internet resources.

Oversight IT risk: Risks associated with software tools and techniques

Software ease of use may also result in the implementtation of features that unintentionally weaken information security provisions. While software vendors may not be particularly open about their potential weaknesses, a growing body of web sites document software weakness and available corrections. This provides both positive and negative opportunities.

As weaknesses in software are discovered and documented, the vendors of those software products develop corrections, or “patches” that may be applied until the weakness is corrected in the next formal “release” version of the software. However, many organizations do not apply such patches, for a variety of reasons. Hackers know software frequently goes unmatched, so they search for particular versions of software with known weaknesses. They may then launch an attack against that system using software developed to exploit known weakness. Such software, called a “script,” may require little or no knowledge to use. The successful attack using a script may give the attacker unlimited, or “root” access to the target system. Normally root privileges are reserved for system administrators and are closely monitored. Once an attacker has root access they have virtually unlimited access to the system, and may also obtain access privileges to other systems with an established trust relationship.

Another element contributing to risk in information systems and networks is the configuration of systems as they are provided by vendors. Frequently systems are

initially installed with the security and control features turned off. System and network engineers and administrators must select the appropriate mix of control features they need and turn them on when the system is installed. Sometimes security and control features will conflict with features of other system components or may add considerable overhead to system processing, such as through the use of system logging. When security components conflict with operations, the typical response is to turn those components off. Unless the organization provides strong security policy administration and/or auditing, management may be unaware security features are not being used. Therefore, frequent assessment and monitoring are important elements of information security management.

Auditor's task: Electronic commerce and internet security

Electronic commerce via the Internet has increased at an explosive pace in recent years. Most organizations have implemented business to business (B2B) and business to consumer (B2C) ecommerce systems using Internet tools. Competition and opportunity are driving forces for this growth. But rapid growth in an area of new technological developments sets a stage for introduction of new problems and escalation of the significance of some older problems.

The Internet facilitates communications via email. Today, email is the standard for the rate of progress and responsiveness for virtually every organization. Similarly, browsers and Web sites set the standard for providing information about an organization and its products and services. And in many cases the Web site is the vehicle for delivery of information, products, and services. To be useful, information must be available, but this availability puts it at risk. Connectivity makes information available when and where it is needed and is the nature of doing business today. Because organizations are linked through the Internet and other public networks to suppliers, customers, and business partners, they are also connected to virtually everyone else in the world. Connectivity exposes information to risks outside the organization's control. In the modern world, everything that business or government does with their information technology becomes part of the global information infrastructure. Organizations must build infrastructure to a very high standard. Attaching weak components to the infrastructure puts your organization as well as your neighbors at risk. Responsible citizens will contribute only sound components to that cooperative infrastructure. Therein lays the essence of the auditor's involvement in providing assurance of the security of information and systems operating in connection with the Internet.

Ecommerce tools for auditors are just beginning to emerge. Mostly auditors are using the same tools as systems administrators, information security professionals, and even hackers. An organization concerned about their security may employ auditors or others to assess system security using "tiger team" tactics – authorized attempts to break into their systems. In many, if not most, cases such attacks are successful and provide management with information about various ways outsiders can break into systems or insiders can exploit system security weaknesses. Non-invasive tools are also used to probe networks for security flaws that might be exploited. New tools are also being introduced that will evaluate the configuration of security features in key network components such as the operating system, firewalls, intrusion detection systems, virus protection systems, and more.

Ecommerce tools also include encryption, Public Key Infrastructures (PKI) and the Related Certification Authorities (CA) that facilitate the distribution and validation of encryption keys and related services. A key feature of being able to conduct business over the Internet while being assured of a valid agreement and protecting privacy is obtaining the services of third-party trusted agents. Assessment of PKI, CA, and third-party trust features built into systems, networks, and business operations is beyond the capabilities of most auditors today. Notable exceptions – auditors who must be fully capable of addressing ecommerce systems, security, controls, and assurance auditing – include those auditors working with organizations who are the leaders in implementing Internet ecommerce systems. Such organizations include major banks and related financial institutions, credit card providers and processing entities, large manufacturing organizations engaged in B2B and/or B2C commerce, leading technology providers, and similarly advanced organizations.

But, as previously noted, advancements in ecommerce are occurring at an accelerating pace. E-business is becoming synonymous with business. The automated tools and techniques being developed and deployed by the leaders today will become standard assurance and auditing techniques used by auditors at all levels in the near future. A factor contributing to the increased capability of auditors in ecommerce will be the demands by boards of directors, insurers, and regulatory bodies for improved assurance of effective and continuous information security.

Best practices

Information technology (IT) is pushing each phase of business, increasing efficiency and productivity, allowing instantaneous communications, processing transactions in real-time, and facilitating global relationships with customers and vendors.

Best practices in conducting internal audits stem from a diverse, experienced, and skilled audit staff who possess

the professional training. Leading companies capitalize on the professionalism of IA staff by assigning management trainees a rotation in the department to offer first hand insight into company operations and develop skills in recognizing and mitigating risk. Additionally, smart companies provide their audit functions with the resources and authority to effectively fulfill the department's mandate, which is defined in the audit charter created by the board, audit committee, and senior management. In this instance, the best practices for internal audit are to collaborate with the information technology department to mitigate information systems risk proactively.

LIMITATIONS

The shortcoming of this study is that it adopts a conventional approach, as opposed to more proactive research methods and in-depth study to suggest any practical implication to auditors at large. While it is important to note there is no generic model for technology tools applicable to all organizations, it is also important to recognize the increasing dependence on technology to accomplish and/or support virtually all-auditing activities. The study stress that this shortcoming is common in the benchmarking literature, and one important research question is how to incorporated risk of emerging technology in shaping business controls, and audit approaches and techniques.

Conclusions

This paper barely scratches the surface of information related to auditor uses of technology. It is important to note there is no generic model for technology tools applicable to all organizations. It is also important to recognize the increasing dependence on technology to accomplish and/or support virtually all-auditing activities. Technology topics make up an ever-increasing percentage of the auditor's professional knowledge and skills set. While technology background is important in understanding new developments and directions, it is of little use without continuous acquisition of new knowledge.

Effective use of audit technology tools is critical to the success of audit activity, but is only one step toward understanding the changes technology is bringing about in business and the auditing profession. Emerging technologies will continuously change the shape of and approach to business controls, and audit approaches and techniques must change accordingly.

Another important role for auditors, and the auditing profession, is to encourage and support the efforts of providers of systems and new technologies to enhance the built-in monitoring and assurance features of systems without considering them as processing overhead or as elements that contribute to decreased performance. An important role for auditors is to not only understand and change with the technologies, but to also explain the effects of such changes to others. And finally, it is also important to remember the importance of interpersonal contact in auditing as keyboards and email will never replace the need for interpersonal skills.

REFERENCES

ACL Service Ltd URL: http://www.acl.com/solutions/audit.aspx

Brazel JF (2005). A measure of perceived auditor ERP systems expertise: Development, assessment, and uses. URL: http://www.emeraldinsight.com/Insight/Articles/0113409604.html

Chen Y (2004). Continuous Auditing Using A Strategic System Approach. URL: http://www.emeraldinsight.com/Insight/Articles/055501101.html

Coderee DG (1993). Automating the audit function
URL: http://www.findarticles.com/p/articles/aut0_audit

Deloitte, Touche (1996). The Current Impact of Information Technology on InternalAuditing Departments. URL: http://www.theiia.org/ecm/tech.cfm?doc_id=859

Debreceny R, Lee SL, Neo W, Toh JS (2005) Employing generalized audit software in the financial services sector. URL: http://www.emeraldinsight.com/Insight/Articles/0210909604.html

Goodwin J (2004). A comparison of internal audit in the private and public sectors. URL: http://www.emeraldinsight.com/Insight/Articles/0251314604.html

Grand CL (2001). Use of Information Technology in Audit Management. URL:http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=345

Hadden LB, DeZoort FT, Hermanson DR (2003). IT Risk Oversight: The Roles of Audit Committees, Internal Auditors, and External Auditors. URL: http://www.findarticles.com/p/articles/we_m11/is_4_59/ai_d02a7860

Harrison MJ, Datta P (2007). An empirical assessment of user perceptions of feature versus application level usage. Commun Assoc Inf Syst. 20: 300-321

Jackson RA (2004). Get the most out of audit tools URL: www.findarticles.com/p/articles/mi_m4153/is_4_61/ai_n6169113

James L. Bierstaker JL, Burnaby P, Thibodeau J (2001). The impact of information technology on the audit process: an assessment of the state of the art and implications for the future URL: http://www.emeraldinsight.com/Insight/Articles/0382201206.html

Jayalakshmy R, Seetharaman A, Khong TW (2005). The changing role of the auditors. URL: http://www.emeraldinsight.com/Insight/Articles/057785604.html

Khadaroo I (2005). Corporate reporting on the Internet: some implications for the auditing profession. URL: http://www.emeraldinsight.com/Insight/Articles/0665856604.html

Kim HJ, Mannino M, Nieschwietz RJ (2009). Information technology acceptance in the internal audit profession: Impact of technology features and complexity. Int. J. Accounting Inf. Syst. 10(4): 214-228

Lanza RB (2004). Can Excel Double as Audit Software. URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5483

Pathak J (2005). Risk manage, internal controls and organizational vulnerabilities. URL: http://www.emeraldinsight.com/Insight/Articles/0213406604.html

Searcy DL, Woodroof JB (2003). Continuous Auditing: Leveraging Technology. URL: http://www.emeraldinsight.com/Insight/Articles/0619806601.html

Shaikh JM (2004) E-commerce impact: emerging technology – electronic auditing URL: http://www.emeraldinsight.com/Insight/Articles/0415560199.html

Siltow J (2003). Shedding Light on Information Technology Risks. URL: http://www.theiia.org/iia/index.cfm?doc_id=4517

Staciokas R, Rupsys R (2005) Internal Audit and its Role in Organizational Government. URL: http://www.ktu.lt/en/science/journals/econo/infaut038.html

The Need for Continuous Controls Monitoring. URL: http://www.metagroup.com/webhost/ONLINE/739743/d2951.htm

Tucker GH (2001) IT and the Audit. URL:

http://www.aicpa.org/pubs/jofa/sept2001/tucker.htm
Virtual Office Risk Manage. Security, Control, and Auditing. URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=644
Xiao Z, Sangster A, Dodgson JH (1997). The relationship between information technology and corporate financial reporting. URL: http://www.emeraldinsight.com/Insight/Articles/0510200604.html
Yang, David C, Guan, Liming (2004). The evolution of IT auditing and internal control standards in finan. statement audits: The case of the United States. URL: http://emeraldsight.com/0268-6902.htm
Zabihollah Rezaee Z, Elam R, Sharbatoghlie A (2001). Continuous auditing: the audit of the future. URL: http://lysander.emeraldinsight.com/vl=5729087/cl=81/nw=1/rpsv/~1155/v16n3/s6/p150