

## **Audit Risk, Complex technology, & Auditing Processes**

Dr. Jagdish Pathak  
Assistant Professor of Accounting Systems & IT Auditing  
Accounting & Auditing Area  
Suite # 411  
Odette School of Business  
University of Windsor  
401 Sunset Avenue  
Windsor N9B 3P4 ON  
Canada  
E-Mail: [jagdish@uwindsor.ca](mailto:jagdish@uwindsor.ca)  
Web: <http://www.uwindsor.ca/business>  
Phone: (519)253-300 ext 3131  
FAX: (519)973-7073

Mary R. Lind  
Professor of Information Systems  
School of Business & Economics  
North Carolina A&T State University  
Merrick Hall  
Greensboro, NC 27411  
E-mail: [lindm@ncat.edu](mailto:lindm@ncat.edu)  
Web: <http://www.ncat.edu/~lindm>  
Phone: (336)334-7189 ext 4033  
Fax: (336)-334-7093

## **The Objectives**

While growing organizations often embrace risk, these risks should not be taken blindly. These entities should have a clear understanding of the potential consequences of increased risk and how to insure positive outcomes. As firms are increasingly experiencing "virtualization" in their relationships with suppliers, partners and consumers, there is an increasing need for trust and assurance in these relationships. There is greater pressure on independent auditors to attest to this trust and assurance. Ronen & Cherny (2002) indicated that independent auditors are expected to be trust providers to the level of being 'insurers'. Auditors have talked of 'reasonable assurance' and 'true and fair presentation' but now their stakeholders expect these auditors to be insurers of their investment! While bizarre, this is a reality for auditors (Barrier, 2002). In this outsourced scenario, the American Institute of Certified Public Accountants (AICPA) promulgated a new statement of auditing standards (SAS) No. 94, replacing the SAS-55; however, it keeps the definition of 'internal controls' unchanged. The purpose of this paper is to discuss the new SAS 94 audit standards for organizations making extensive use of IT. The paper is divided into two major parts: (1) an examination of complex information technologies in terms of audit risk, and (3) the effect of SAS-94 on the audit processes.

Auditors should consider focusing on the e-commerce strategies for their clients, the e-commerce risk that must be managed to achieve these strategies, and the ensuing audit risks from this e-commerce (Morgan & Stocken, 1998). Since auditors will have to make more serious attempts to do a formal analysis of an organization's e-commerce strategy with SAS-94, the auditor needs to understand the IT-based/dependent internal controls.

To work with the IT specialists, auditors need reasonable IT capabilities for conducting their detailed audit. This IT understanding becomes more crucial as auditors are faced with accounting transactions entirely in electronic form without supporting paper documentation. Technologies such as electronic data interchange, image processing and electronic funds transfers (Deshmukh & Romine, 2002) use little, if any, paper. Auditors performing attest services for such clients will need to be both financially and technically competent regarding IT. They will also need to revise their traditional (annual) audit approach by focusing on an organization's e-commerce strategy (Good & Schultz, 2002) and the associated e-commerce risks that may occur.

### **Complex Information Technologies and Audit Risks**

The identification of risks associated with e-commerce (Koldzinski, 2002) becomes increasingly important given the difficulty of estimating future benefits. While e-commerce financial statement risks are similar to those traditionally considered, these risks may be exacerbated by the e-commerce environment. As an alternative to a company managed Internet connection, a firm's transactions may take place electronically through an intermediary service provider or a virtual private network (Yusuf et al, 2002). The external auditor may feel it necessary to obtain policies and procedures manuals and transaction log files from the network service provider to better understand the manipulation and to track the flow of material (financial) statement assertions.

Dynamic audit trails (Helms, 2002) generated in real time have become a major concern of auditors. For an auditor to offer an opinion on the material correctness of a corporation's financial statements, the auditor must rely heavily on the company's

business practices and internal controls in order to gain comfort in the reported numbers. Auditors are also concerned that only authorized transactions are transmitted and received. Further, they test to ensure that transactions are not duplicated, altered or lost during processing. Since there are fewer tangible pre-numbered documents to examine as in manual and legacy systems, auditors must instead examine the computer based system that has replaced the paper documents with electronic transactions. It is also possible that such an audit will be performed by another soft application, either stand alone or embedded intelligently (Kang & Han, 2003) within the transaction processes.

While it is premature to claim this as an alternative to the human auditor, there certainly is the possibility of providing continuous monitoring of the firm's transactions with ready 'red-flags' and 'exception reporting'. This kind of continuous monitoring is also known as continuous auditing (Vasarhelyi et al, 2002; Wright, 2002). E-commerce systems must use the latest encryption technology, digital signatures and certificates and secure server technology (Busta, 2002) to ensure that all information exchanged is secure. Thus independent verification must be used to ensure that all security controls adequately protect the organization, its suppliers, partners and customers from the risk of security breaches (Elifoglu, 2002) The accounting firms either have or are in the process of redesigning their audit process to deal with the evolution to integrated enterprise information systems. In redesigning the audit, the auditors place a much heavier emphasis on the business processes.

### **SAS-94 & Its Effect on the Audit Process**

SAS-94 is a framework standard that resulted from the growth and influence of IT on business systems. Auditors must prove equal in comprehending these IT

developments. The ASB issued SAS-80, in December 1996, entitled Amendment to Statement on Auditing Standards No. 31, Evidential Matter, in order to address questions about the validity, completeness, and integrity of electronic evidence. When entities transmit process, maintain, or access information electronically, it may be impractical or even impossible to reduce detection risk to an acceptably low level by performing only substantive tests for one or more financial statements. Furthermore, SAS 80 concluded that tests of controls, in conjunction with substantive tests, should be sufficient to support an audit opinion (Helms & Lilly, 2000). Auditing Procedures Study (APS) also describes electronic evidence and associated evaluation issues. Prior to the release of SAS 94, although some guidance had addressed audit considerations in an IT environment, there had not been an update to the evaluation of controls and assessment of control risk since SAS 78. SAS 94 filled this gap. SAS 94 is intended to fulfill certain specified objectives. Recognizing the importance of IT, SAS-94 amended SAS-55. SAS-94 does not change the basics of SAS-55, and its importance in the audit-risk model, but it addresses the effects of IT on the professional standards process. When significant evidence of an entity's initiation, recording, or processing of financial data exists only in electronic form, the ability of the auditor to obtain the desired assurance only from substantive tests is significantly reduced. SAS-94 still requires the performance of substantive tests for significant account balances and transaction classes. Basically the ASB took SAS-55 and modified it to include the effect of IT on internal control, the auditor's understanding of internal control, and the auditor's assessment of control risk. SAS-94 specifically requires that when obtaining this understanding of internal control, the auditor should consider how an entity's use of IT and manual procedures may affect controls relevant to

the audit. The extent and nature of these risks will vary, depending on the nature and characteristics of an entity's information system and the extent to which the information system affects the entity's internal control

SAS-94 provides guidance to help auditors in determining if professional possessing IT skills will be needed for an assignment. This person may be on the auditor's staff or may be an outside professional. To determine if a technology professional is needed, an audit planner is expected to consider these factors: Complexity and usage of the firm's systems; Significance of changes to existing systems; Extent of data sharing; Extent of the entity's participation in electronic commerce; Audit evidence available in digital form.

Many accounting firms, internal and external auditors, and state and federal agencies already are using some various types of software in the audit process. With SAS 94, a new era of auditing has arrived; and the CPA profession must keep up with technology advances or bear the consequences. Once a CPA uses, understands, and employs advanced IT techniques - such as data mining, digit analysis, and Benford testing - in the audit process, he or she often asks why such techniques were not used before. When it comes to advice on technology-driven audit tools and/or procedures, the ASB and the Public Oversight Board (POB) are not specific in their recommendations or requirements. Auditing can be influenced by technology in limitless ways, and how it eventually will be changed is subject to much conjecture. Imagine what would have happened if we had the ability to use continuous auditing to examine and report on various data sets immediately. The potential benefits include reduced overall audit risk, increased audit confidence, and

a timeliness that has never been achievable before. This shows where auditing will go as the profession embraces technology. SAS 94 notes that assessing control risk at the maximum and performing a substantive audit may not result in an effective audit because the audit evidence does not exist outside the IT environment. Furthermore, even when evidential matter allows an assessment of control risk below the maximum, there remains a need to perform substantive tests on significant amounts. Stated differently, an audit involves the assessment of control risk and the design, performance, and evaluation of substantive tests to reduce audit risk to an acceptably low level. Since the Auditing Standards Board (ASB) recognized that it is increasingly difficult for auditors to rely on traditional (paper) audit evidence to acquire sufficient competent evidence, they issued SAS-94.

Since an auditor focuses on controls pertinent to financial statement assertions-how the transactions are authorized, recorded, aggregated, and displayed in the financial statements-- when planning and performing an audit, it may not be necessary to obtain an understanding of the controls of operating units and business functions. Due to the extensive use of IT, SAS 94 cautions that its implications may need to be considered in evaluating the internal control. As Enterprise Resource Planning (ERP) systems have become more comprehensive, even small entities may have complex, highly integrated IT systems that share data and support all aspects of financial reporting, operations, and compliance.

Controls in IT systems consist of a combination of automated and manual controls. Manual controls may function independently of the IT system or use

information produced by the IT system to monitor the automated controls. The appropriate mix of manual and automated controls varies with the nature and complexity of the IT system. IT internal controls can provide only reasonable assurance regarding the achievement of an entity's control objectives. All internal control systems, regardless of their design, face certain inherent limitations that make absolute assurance impossible. In an IT system, errors can occur in designing, maintaining, or monitoring automated controls. SAS 94 repeats the requirement to obtain a sufficient understanding of each of the five components of internal control in order to plan the audit. An auditor could still determine that performing substantive tests alone would be effective and more efficient than performing tests of controls for assertions in some circumstances. In more complex situations with a large volume of transactions processed in a complex IT environment, performing tests of controls to assess control risk below the maximum level for certain assertions would be effective and more efficient than performing only substantive tests. SAS-94 requires tests of both the design and operation of controls in order to reduce the assessed level of control risk.

The knowledge gained from an understanding of internal controls should be used to identify the types of potential misstatements that could occur in financial statement assertions. The controls that are likely to prevent or detect material misstatements in specific financial statement assertions may relate directly to one or more of them, but their continued effective operation usually depends on general controls that are indirectly related to the assertions. Other automated tools could test the operating effectiveness of indirect controls, such as access controls. Specialized computer skills may be needed to design and perform the tests of controls. Ultimately, these situations call for an



assessment of the level of control risk for specific financial statement assertions. The assessed level of control risk (along with the assessed level of inherent risk) should determine the acceptable level of detection risk for the financial statement assertions. As the acceptable level of detection risk decreases, the assurance provided from substantive tests should increase. SAS-94 changes the documentation requirements for understanding and evaluating internal control. Consistent with the previous guidance of SAS-55 (as amended by SAS-78), the form and extent of this documentation depends upon the nature and complexity of the entity's controls. Generally, the more complex the internal control and the more extensive the procedures performed, the more extensive the documentation should be. The basis for the conclusions about the assessed level of control risk also requires documentation. Conclusions about the assessed level of control risk may differ by account balances or classes of transactions. For those financial statement assertions where control risk is assessed at the maximum level, the level should be documented but there is no need to document the basis for that conclusion. For those assertions where the assessed level of control risk is below the maximum, the basis for the conclusion that the effectiveness of the design and operation of controls supports the assessed level should be documented.

### References

1. Barrier, Michael, "The Crisis in Governance," *The Internal Auditor*, 59(4), (2002), pp.50-54.
2. Busta, Bruce, "Encryption in Theory & Practice," *The CPA Journal*, 72(11), (2002), pp 42-48.
3. Deshmukh, Ashutosh & Jeffrey Romine, "Accounting Software & e-Business," *The CPA Journal*, 72(11), (2002), pp.52-54.
4. Elifoglu, Hilmi I, "Navigating the Information Super highway," *Review of Business*, 23(1), (2002), pp.67-71.
5. Good, David & Roberta Schultz, "E-Commerce Strategies for Business-to-Business Service Firms in the Global Environment," *American Business Review*, 20(2), (2002), pp.111-118.
6. Helms, Glen L & Fred L Lilly, "Case Study on Auditing in an Electronic Environment," *The CPA Journal*, 70(4), (2000), pp. 52-54.
7. Helms, Glen L., "Traditional and Emerging Methods of Electronic Assurance," *The CPA Journal*, 72(3), (2002), pp. 26-31.

8. Kang, Namoo and Sangyong Han, "Agent-based e-Marketplace System for More Fair and Efficient Transaction," *Decision Support Systems*, 34:2, (2003), pp. 157-165.
9. Koldzinski, Oscar, "Cyber Insurance Issues: Managing Risk by Tying Network Security to Business Goals," *The CPA Journal*, 72(11), (2002), pp. 10-11.
10. Morgan, John & Stocken, Philip, "The Effect of Business Risk on Audit Pricing," *Review of Accounting Studies*, 3(4), (1998), pp. 365-385.
11. Ronen, Joshua and Cherny, Julius, "Is Insurance a Solution to the Auditing Dilemma," *National Underwriter*, 106(32), (2002), pp. 26-29.
12. Vasarhelyi, Miklos A; Kogan, Alexander; and Alles, Michael, "Would Continuous Auditing Have Prevented the ENRON Mess?" *The CPA Journal*, 72(7), (2002). pp.80.
13. Wright, Arnold, "Forum on Continuous Auditing & Assurance," *Auditing: A Journal of Practice and Theory*, 21(1), (2002), pp. 123.
14. Yusuf, Yahia Y; Little, David and Omuh, Spencer O, "Multiple Case Studies of Total Enterprise Integration Programs: Lessons & Benefits," *International Journal of Manufacturing technology & Management*, 4(3-4), (2002), pp. 283-302.