The Impact of Transactional E-Commerce on CPAs' Perception of Audit Risk: Preliminary Results

Steven T. Breslawski, State University of New York, College at Brockport, 350 New Campus Drive, Brockport, NY 14420, USA; E-mail: sbreslaw@brockport.edu

ABSTRACT

In this paper, we report results from a preliminary study designed to understand 1) the level, if any, at which transactional e-commerce systems are viewed as sufficiently substantive to have a material impact on audit risk, and 2) how the presence of a material transactional e-commerce system impacts auditors' perceptions of audit risk. The results provide motivation for a more extensive and detailed study that investigates how a material e-commerce presence impacts the individual components of audit risk specified in SAS 55 (AICPA, 1988).

INTRODUCTION

It is well understood that the development of computerized information systems has long spawned challenges for accounting professionals charged with auditing financial statements. In particular, numerous authors and texts have discussed the problem of "auditing around the computer." The problem, in essence, occurs when information systems are either sufficiently complex or opaque as to render it impossible for auditors to efficiently and effectively conduct an audit. In these situations, there may be an increase in audit risk.

Audit risk is the risk that the auditor will fail to detect one or more material errors in the financial statements. Audit risk is espoused to have thee components: Inherent Risk, Control Risk, and Detection Risk. The basic audit risk model framed in *Statement on Auditing Standards 55* (SAS 55) is as follows:

Audit Risk = Inherent Risk * Control Risk * Detection Risk

Inherent Risk is the risk that an assertion made in a financial statement contains a material misstatement, assuming the absence of controls that might detect the misstatement. Inherent risk varies by financial statement assertion, type of business, and complexity of the business environment. *Control Risk* is the likelihood that controls established by a business fail to prevent, detect, and correct a misstatement. Inherent and control risk are assessed by the auditor, but are not directly under their control (although the auditor might make recommendations that will influence future levels of control risk). *Detection Risk* is the risk that an auditor fails to detect a material misstatement in the financial statements that has evaded detection by internal controls. Detection risk is controllable by the auditor and is a function of nature, timing, and extent of audit procedures applied.

As information technology has become more complex and ubiquitous, the challenge facing auditors has grown correspondingly. The accounting profession has responded with more guidance to auditors (embedded in professional standards), automated auditing software, better educated and more technically savvy audit professionals, and the use of information technology specialist on audit teams. However, despite the responsiveness of the accounting profession, the exponential growth in the scope and sophistication of new information systems technologies threatens to outpace and overwhelm the responses of the auditing profession, almost like a fire that is growing faster than firefighters can extinguish it.

While the information technology (IT) environment continues to challenge auditors' ability to effectively and efficiently test information systems controls or verify the integrity of transactions, recent changes in regulations and professional standards, most notably the Sarbanes-Oxley act of 2002 (henceforth SOX) (SEC, 2002) and SAS 94 (AICPA, 2001), compel auditors to be more aggressive, thorough, and efficient in this regard. The overarching consequence of SAS 94 and SOX is that managers and auditors can no longer simply assess control risk at its maximum level and assert that the effectiveness of IT controls can not be assessed. They are now compelled to develop a detailed understanding of the controls and the associated control risk.

Specifically, section 404 of the Sarbanes-Oxley act (SOX) requires the senior management of publicly traded companies to establish and maintain adequate internal controls for financial reporting as well as annually assess the effectiveness of said controls. The law also establishes attestation requirements auditors to assess management's certification of the effectiveness of its internal controls over financial reporting. Section 404 went into effect in November 2004; see Geiger and Taylor (2003) for a review of section 404.

SAS 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit* requires the auditor to test the automated IT controls embedded in computer programs by using computer-assisted audit techniques. Auditors are obliged to respond in this fashion when the IT environment is complex and it is not practical to reduce detection risk to acceptable levels through the use of substantive tests alone. Further, SAS 94 requires tests of both the design and operation of controls in order to reduce the assessed level of control risk. While SAS 94 focuses on the control risk component of audit risk, threats to inherent risk are implied as well. SAS 94 identifies various IT-related threats that render certain asset classes inherently more risky. These include reliance on systems that incorrectly process data, the processing of inaccurate data, unauthorized access to data, destruction or modification of data resulting from unauthorized access, recording of unauthorized or nonexistent transactions, unauthorized changes to systems and programs, and unauthorized manual intervention. A number of authors have discussed the correlation between control and inherent risk; see for example Cushings and Loebbeck (1983) and Waller (1993).

The issues addressed in SAS 94 are not entirely new to auditors, as SAS 94 amends on guidance provided earlier in other professional standards, including SAS 47 (Audit Risk and Materiality), SAS 55 (Internal Control in a Financial Statement Audit), SAS 73 (Using the Work of a Specialist) SAS 78 (Internal Control: An Amendment to SAS 55), SAS 80 (Electronic Evidence). SAS 94 does not, however, change the basic audit risk model described above and specified in SAS 55.

RESEARCH QUESTIONS AND FOCUS

SAS 94 and SOX both compel auditors to pursue enhanced vigilance in the face of existing and emerging IT environments. Two general questions for researchers are:

1. To what degree, if any, do auditors perceive that various IT environments and technologies change audit risk and, therefore, audit practice?
2. At what scope of adoption do various IT environments become a material concern in the assessment of audit risk?

While these questions can be asked for many of the exciting IT technologies embraced by business in recent years, our focus in this paper will be transactional e-commerce. We define transactional e-commerce as *the process of conducting*

transactions, including buying, selling, purchasing, and payment using the internet or other computer networks connecting two or more organizations. Transactional e-commerce (TEC) has had a profound impact on business practice and the degree to which TEC has become ubiquitous suggests that its impact on audit risk is relevant to many in the audit profession. Further, transactions are perhaps the most fundamental inputs to the financial reporting process and are therefore key to the consideration of how technology impacts audit risk.

A priori, it is difficult to predict how a material transactional e-commerce presence impacts audit risk. Traditionally, transactional e-commerce has taken the form of highly structured electronic data interchange (EDI) transactions supported (and recorded) by a third party value added network (VAN) using dedicated, private, and secure communications links. EDI has evolved into a highly structured and mature technology, benefiting from international standards such as EDIFACT and ANSI X12 (see, for example, OECD, 1995). It can be argued, for example, that traditional EDI systems lend themselves to perpetual auditing approaches and would therefore result in a corresponding reduction in audit risk; see, for example, Helms (2002) and Write (2002). Because there are substantial costs involved, EDI has been adopted primarily by large organizations that often have highly trained IT staff and internal audit staff, also suggesting reduced audit risk.

Compared to traditional EDI, web-based TEC is much less mature as a technology and much less standardized. Consider, for example, that web-based TEC has grown from virtually zero in 1995, in terms of number of companies impacted and volume of sales, to billions of dollars in sales and thousands of companies involved. Traditional EDI is rapidly being replaced or augmented by internet-based solutions that are often less secure, standardized, and robust in their designs than traditional EDI implementations. Adopters of web-based transactional e-commerce include smaller firms with more modest IT and internal audit staffs. In this new environment, we might expect audit risk to increase.

Consider also that e-commerce technologies have facilitated accelerated fracturing of the business value chain. As companies outsource nearly everything except their core competencies, it becomes more and more difficult for auditors to confirm the existence of management and software application controls; it is not unusual for those controls to reside with other companies. As paper trails, legacy systems, and programming staff are replaced with vendor-based and outsourced IT solutions, institutional knowledge of the details underlying software controls becomes increasingly scarce. See Pathak and Lind (2003) for a good discussion of possible ways that IT might impact audit risk.

This paper represents the initial stages of inquiry regarding the relationship between a transactional e-commerce presence and audit risk. Our long-term goal is to develop a detailed understanding of whether changes in perceived overall audit risk, related to the IT environment, are directly related to changes in the auditor's perception of inherent, control, and detection risk as suggested by the SAS 55 audit risk model. However, we first begin by determining whether audit professionals can even respond to questions concerning the impact that transactional e-commerce has on audit risk. As such, our immediate goal in this study is to explore the following questions:

1. From an auditor's point of view, what is a material e-commerce presence? That is, at what point does a transactional e-commerce presence become enough of an issue as to impact perception of audit risk and, therefore, the conduct of an audit?
2. How does a material e-commerce presence impact audit risk and, consequently, audit costs?
3. Are the components of audit risk (inherent, control, and detection risk) impacted by a material e-commerce presence?
4. Does the amount of experience of the auditor, in the e-commerce environment, impact perceptions of changes in audit risk?

While some, most notably Pathak and Lind (2003), have discussed the relationship between audit risk, audit practice, and IT, we are unaware of any research that seeks to solicit the perception of auditors on these issues.

SURVEY INSTRUMENT AND RESULTS

This inquiry is based on analysis of responses of fifty CPAs who agreed to complete a brief survey. The fifty participants, identified from the American Institute of Certified Public Accountants (AICPA) database, worked for large firms and indicated auditing as an area of interest. We hoped to identify individuals who had experience auditing in a TEC environment as well as individuals who had little or no experience, in order to understand how perceptions between the two groups differed.

Prior to administration of the survey to the target population, a pilot survey was administered to 12 local CPAs for the purpose of investigating clarity in the wording of survey instructions and questions. Survey questions are prefaced by instructions, to participants, that include a brief description of the audit risk model and the definitions of inherent, control, and detection risk. A definition of the phrase *transactional e-commerce* is also provided.

Results - Question 1: What is a material transactional e-commerce presence? Participants were asked to define a material transactional e-commerce presence in terms of percent of total sales and percent of total purchases. Results appear in Exhibit 1.

Exhibit 1. Material transactional e-commerce presence defined in terms of sales and purchases

A material transactional e-commerce presence is defined as….			
Sales		**Purchases**	
Response	**% of Respondents**	**Response**	**% of Respondents**
Sales exceed 10%	34%	Purchases Exceed 10%	24%
Sales exceed 20%	52%	Purchases Exceed 20%	70%
Sales Exceed 30%	14%	Purchases Exceed 30%	6%
More than 40%	0%	More than 40%	0%

Exhibit 2. Impact of material transactional e-commerce on audit risk and costs

A material transactional e-commerce presence results in….		
Response	**Impact on Audit Risk**	**Impact on Audit Cost**
Increases significantly	46%	22%
Increases, but not significantly	54%	62%
Does not increase/decrease	0%	16%
Decreases, but not significantly	0%	0%
Decreases significantly	0	0

Exhibit 3. Impact of material transactional e-commerce on audit risk components

What is the impact of a material e-commerce presence on…			
	Inherent Risk	Control Risk	Detection Risk
Significant Decrease	0%	0%	0%
Moderate Decrease	0%	4%	0%
No Meaningful Impact	12%	22%	14%
Moderate Increase	74%	40%	70%
Significant Increase	14%	34%	16%

The results suggest that a fairly modest e-commerce presence is considered to be material with regard to audit planning and risk.

Results - Question 2: How does a material transactional e-commerce presence impact audit risk and, consequently audit costs. Responses appear in Exhibit 2.

The auditors uniformly perceived an increase in overall audit risk, with about one-half perceiving a significant increase in risk. Interestingly, only about twenty-five percent thought that the increased risk would result in significant increases in audit costs while the remainder predicted little or no impact on costs. Ninety-four percent believed that increased costs would *not* be passed along to the client.

Results - Question 3: Are the components of audit risk (inherent, control, and detection risk) impacted by a material e-commerce presence? We asked auditors to provide "overall and general[1]" perceptions concerning the impact of a material e-commerce presence on inherent risk, control risk, and detection risk. Results appear in Exhibit 3 below.

Only two of the fifty participants suggested a decrease in any of the risk components (control risk). Auditors are most concerned with significant increases in control risk, consistent with the focus of SAS 94.

The results suggest that the perceived change in overall audit risk, shown in Exhibit 2, is associated with changes in the components of the SAS 55 model. However, since we measured the changes in a qualitative rather than quantitative fashion, the exact nature of the relationship AR = IR * CR * DR cannot be explored. In future research, we will determine whether CPAs are able to articulate percentage increases/decreases so that the relationship can be explored more completely.

Results - Question 4: Lastly, we were interested in whether the amount of experience one has in auditing in an e-commerce environment would influence perceptions of changes in audit risk. Of the fifty participants, thirty-two percent claimed "substantial" experience auditing in an e-commerce environment, thirty-six percent claimed "moderate" experience, twenty-six percent claimed "little" experience and six percent claimed "none". We organized our subjects into two groups, whose experience was "substantial or moderate" and "little or none". Utilizing the categories shown in Exhibits 2 above, a chi-squared test of independence revealed no statistically significant difference (α=.05) in the responses of the two groups with regard to perception of changes in audit risk. As such, we conclude that perception is independent of level of experience.

SUMMARY AND CONCLUSIONS

Our goal was to begin an investigation of how an important type of information technology, specifically transactional e-commerce, is perceived by CPAs to impact audit risk and practice. A survey was used to determine whether auditors have salient opinions that can be expressed concerning the relationship between transactional e-commerce and audit risk. Not only were auditors able to express opinions on the relationship, the opinions were uniform in suggesting an increase in overall audit risk and in the individual components of risk. The results motivate further detailed study to see if the relationship between the components of audit risk, as specified in the SAS 55 model, can be substantiated, perhaps by asking auditors to express perceived changes in risk in numeric terms and at the account and management assertion level. A larger sample will facilitate the inclusion and analysis of additional control variables. For example, the differences in responses pertaining to traditional EDI systems and non-EDI web-based systems might be explored.

A majority of auditors suggested that some increase in audit costs would occur, suggesting (as anticipated) a change in audit practice. A more detailed analysis of changes in audit practice, resulting from the perceived increase in audit risk, could be pursued. This includes understanding whether increased costs are due to changes in procedures, changes in scope, changes in timing of procedures, or some combination.

REFERENCES

AICPA, Statement on Auditing Standards No. 55, "Consideration of Internal Control in A Financial Statement Audit," New York, (April 1988).

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

Cushings, B. E. and Loebbecke, J. K. "Analytic Approaches to Audit Risk: A Survey and Analysis," *Auditing: A Journal of Practice and Theory*, 3(), (Fall 1983), pp. 23-41.

Helms, Glen L. "Traditional and Emerging Methods of Electronic Assurance," *The CPA Journal*, 72(3) (2002), pp. 26-31.

OECD (Organization for Economic Cooperation and Development), "The development of ANSI X12 and EDIFACT," *The OECD Observer*, (Oct/Nov 1995).

Geiger, M. and Taylor, P. "CEO and CFO Certifications of Financial Information," *Accounting Horizons*, 17(4) (2003) pp. 357-368.

Pathak, J. and Lind, M. R., "Audit Risk, Complex Technology, & Auditing Processes" (March 2003). Available at Social Science Research Network: http://ssrn.com/abstract=397321

Securities and Exchange Commission, Public Company Accounting Reform and Investor Protection Act of 2002 (commonly known as Sarbanes-Oxley Act of 2002), Pub. L. No. 107-204, 166 Stat. 245.

Waller, W. S. "Auditor's Assessment of Inherent and Control Risk in Field Settings," *The Accounting Review*, 68(4), (October 1993), pp. 783-803.

Write, A. "Forum on Continuous Auditing and Assurance," *Auditing, a Journal of Practice and Theory and Practice*," 21(1), (2002), pp. 123.

ENDNOTE

[1] The qualifier "overall and general" is required because these risk factors should be assessed for each account classification (e.g. accounts receivable) on the financial statements and for each management assertion made for the account. Under SAS 55, the assertions are completeness, existence, ownership, valuation, and disclosure.