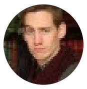
Remote Audit: A Research Framework

ARTICLE *in* SSRN ELECTRONIC JOURNAL · SEPTEMBER 2010

DOI: 10.2139/ssrn.1668638



Ryan Teeter
University of Pittsburgh

Michael G. Alles
Rutgers, The State University of New Jersey

Miklos A. Vasarhelyi
Rutgers Business School

Remote Audit: A Research Framework[1]

Ryan A. Teeter, Rutgers University, teetery@rutgers.edu
Michael G. Alles, Rutgers University, alles@business.rutgers.edu
Miklos A. Vasarhelyi. Rutgers University, miklosv@andromeda.rutgers.edu[2]

SUMMARY: Audit practitioners have been progressively adopting communications and analytic technology to extend the scope, change the timing, and reduce the costs of audit processes. These efforts have been mainly ad hoc, lacking an integrative theoretical positioning. This paper redefines the concept of the "remote audit" as the process by which internal auditors couple information and communication technology (ICT) with analytical procedures to gather electronic evidence, interact with the auditee, and report on the accuracy of financial data and internal controls, independent of the physical location of the auditor. Building on research on virtual teams and an analysis of internal audit activities, we present a research framework identifying areas where ICT and automated audit analytics enable auditors to work remotely, reduce travel costs and latency, and increase efficiency and coverage.

Keywords: audit innovation, remote audit, continuous auditing, internal auditing, communication, evidence, virtual teams

[1] The authors are appreciative of the numerous comments received at the Rutgers Accounting research Forum and the SET research workshop at the National Meeting of the AAA in san Francisco, July 2010. Also, the comments from Jim Littley of KPMG, Rod Brennan from Siemens ,Don Warren from University of Hartford, and J.P. Krahel from Rutgers were invaluable in the completion of this paper.
[2] Corresponding author.

I. Introduction

Discussing the implementation of a continuous auditing system by internal auditors at Siemens Corporation, Alles et al (2006, p. 140, emphasis added), state: *"Siemens has SAP installations spread throughout the United States that need to be audited on a regular basis. The SAP IT audit process is comprehensive across major SAP modules, is performed online, but essentially manual and obviously episodic.* ***The end to end process takes nearly 70 person days for a single SAP system and involves a great deal of traveling by the audit staff.*** *The ability to automate some audit checks was considered to potentially lead to large cost savings, even leaving aside any increase in effectiveness."*

Since that pilot implementation, internal auditors have increased their use of technology with the goal of automating the internal audit process and making it more cost-effective (Alles et al 2008, 2010). Much of the research literature has focused on audit automation, but less attention has been paid to one of the major benefits of technology in auditing: the ability to reduce the amount of onsite audit work and to shift that work to remote team members. While continuous auditing extends the scope of an audit, by enabling ongoing and on demand procedures (Alles et al 2002), remote auditing expands the location requirement for auditors, allowing them to divide the audit tasks between onsite and remote audit team members. The addition of a remote internal audit component is not simply a side benefit of audit automation; it is a driver for technology use and presents an opportunity to rethink the way an audit is performed.

The objective of this paper is to examine how technology is facilitating reengineering of internal auditing through remote auditing. This complements the literature on audit automation by examining auditing processes where information and communication technology (ICT) and analytics enable internal auditors to interact with other business process owners and team members, as well as gather and analyze data. In this paper we focus on these two areas of that transformation, interpersonal communication and data analytics, and attempt to identify specific areas where future research may offer insight into this reengineering paradigm.. The desired outcome is a location-independent audit where audit tasks can be performed by any auditor with a network connection, whether they are onsite or working remotely.

While certain aspects of internal auditing tend to require physical proximity, the notion that internal auditors need to be physically present to conduct an entire audit no longer applies. Many audit tasks can now be led by virtual audit teams and technology facilitates a reengineering of what internal auditors do and how they do it. For example, videoconferencing replaces travel to an audit location when auditors must simply follow up with process owners, and internal controls in online enterprise resource planning (ERP) systems are evaluated using an online dashboard. We attempt to identify some of these tasks and examine how electronic evidence facilitates a remote audit.

The paper is organized as follows: Section II discusses our vision of the remote audit and presents a research framework for internal auditing activities and virtual teams. Section III examines ICT literature from various domains and identifies how it may apply in a remote audit. Section IV evaluates the impact of automated evidence collection and analytics. Section V offers concluding remarks.

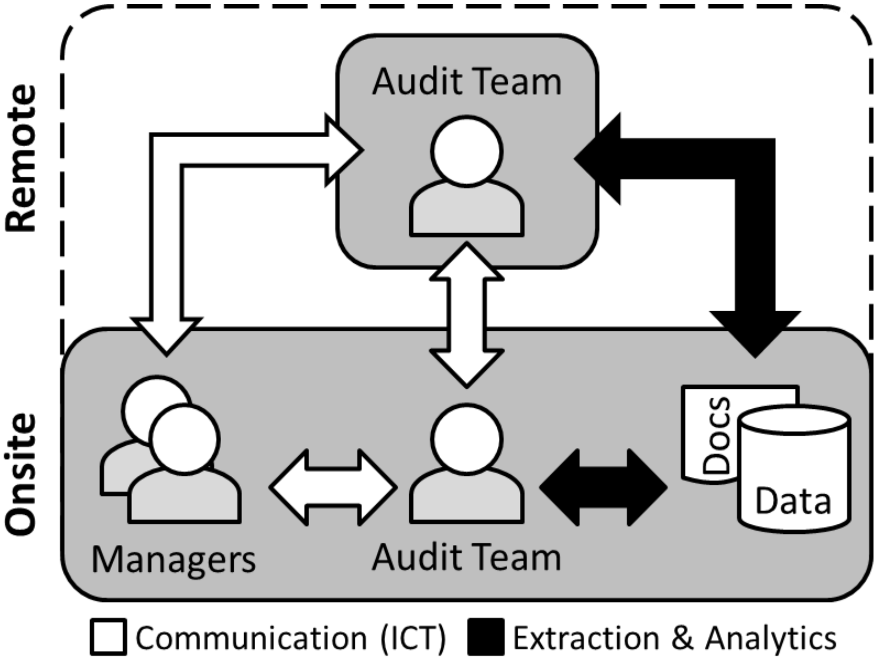
II. The Remote Audit

We define the term remote auditing[3] to mean: *the process by which auditors couple information and communication technology with data analytics to assess and report on the accuracy of financial data and internal controls, gather electronic evidence, and interact with the auditee, independent of the physical location of the auditor*.

The two primary enabling elements of the remote audit, ICT and analytics, provide the framework for future research into the technical and behavioral aspects of a remote audit. Figure 1 illustrates these elements. Both the onsite and remote members of the audit team use ICT to interact with both process managers and one another. The auditors also use automated tools to extract and analyze data from the auditee's systems to test internal controls and transactions.

Figure 1: Components of Remote Auditing

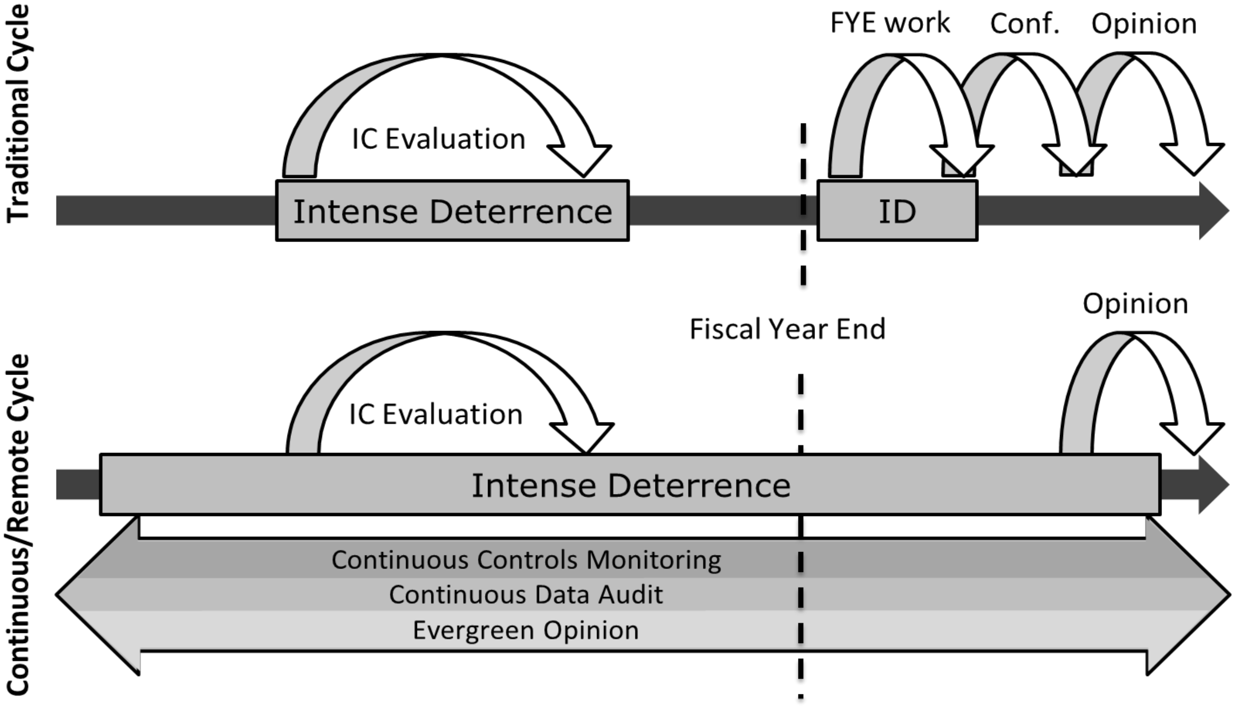
[3] We attempt to differentiate this term from its use in computer science for the remote monitoring of distributed PCs and other equipment in a computer network, see http://www.emco.is/products/network-inventory/features.php



As the cost of technology and online access continues to decline and budgetary pressure increases, more and more internal audit teams are using technology needed for the remote audit. Some primary motivators for organizations embracing a remote audit include improved audit quality, extended client contact time, increased perceived contact time, expanded audit coverage, and reduced travel and entertainment expenses.

Open research questions facing a remote audit component include both technical design and behavioral effects. For example: How much of the audit process can be expanded by ICTs? How would auditors form their "virtual" teams? Would employees be deterred from committing fraud if they knew remote auditing was in place? For the latter issue, we expect to see an expanded intense deterrent effect when remote auditing is coupled with continuous assurance, as shown in Figure 2, comparable to that experienced when retail stores have installed closed circuit video cameras.

Figure 2: The expected deterrent factor of remote auditing

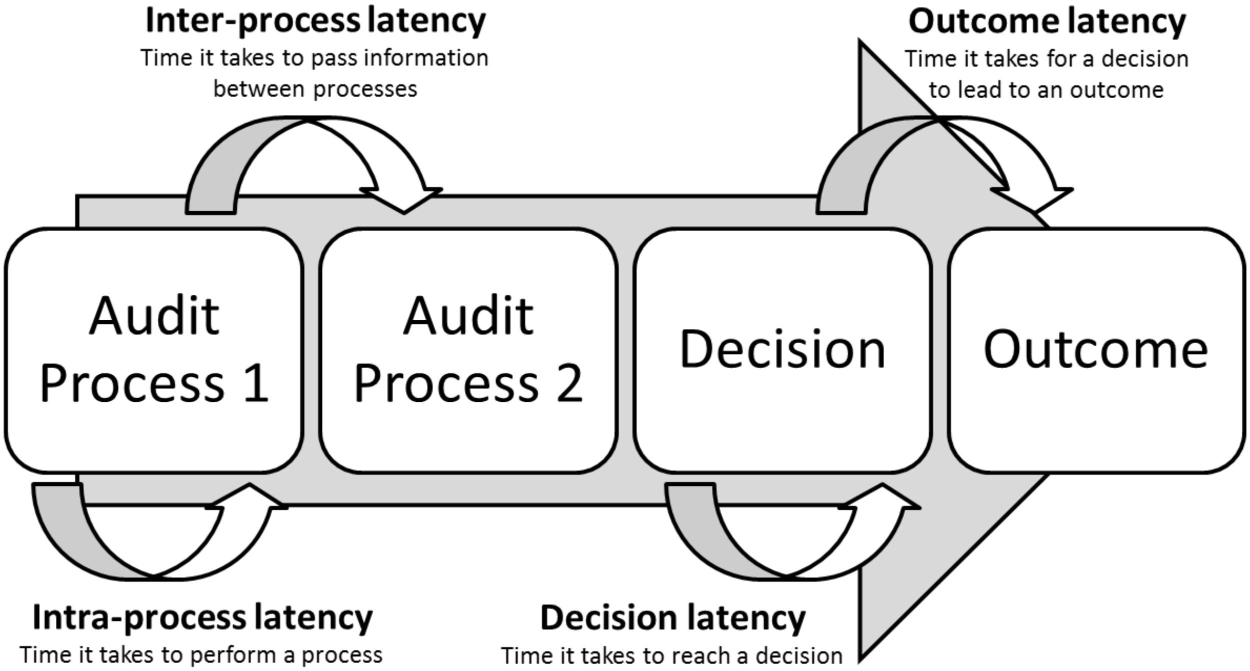


Just as General Motors' OnStar™[4] system enables vehicle monitoring and assistance in between garage visits, the remote audit enables auditors to monitor transactions and communicate with business process owners throughout and subsequent to formal audit engagements. In a similar manner, when continuous auditing systems alert auditors to potential internal control weaknesses, fraud or error, the auditors can respond remotely to help management resolve those issues..

Other potential benefits of remote auditing have been discussed previously. Audit efficiency can be achieved through the reduction of latency, which occupies labor and capital (Hoitash et al. 2006; Vasarhelyi, Alles and Williams, 2010). Latencies occur in all business processes, particularly the audit process, as shown in Figure 3. Engagement procurement, audit planning, internal controls evaluation, internal controls compliance, and substantive testing all experience significant intra- and inter-process latencies during audit task performance and auditor meetings. Audit decisions and reporting face decision and outcome latency as auditors work with managers to address and resolve issues. Latency reduction for any of these sub-processes can free up resources, especially auditor labor, to be utilized elsewhere.

[4] A similar analogy is found in the medical profession with the remote monitoring and intervention of cardio pacemakers (Jung et al, 2008)

Figure 3: Audit Process Latencies[5]


Inter-process latency
Time it takes to pass information between processes
Outcome latency
Time it takes for a decision to lead to an outcome
Audit Process 1
Audit Process 2
Decision
Outcome
Intra-process latency
Time it takes to perform a process
Decision latency
Time it takes to reach a decision

Internal auditors will ultimately determine the benefits received from remote auditing, whether they lean toward the onsite end of the continuum or conduct more procedures through telework and virtual teams, utilizing a larger number of automated and continuous auditing tools. While we limit the scope of this paper to internal auditors, many of these principles also apply to external auditors.

Virtual teams

Virtual teams are generally defined as "*groups of geographically and/or organizationally dispersed coworkers that are assembled using a combination of telecommunications and information technologies to accomplish a variety of critical tasks*" (Townsend et al. 1998: 17). These specialized teams consist of individuals who are linked by ICT and form dynamic relationships to coordinate and delegate responsibility (DeSanctis and Monge, 1999). Increasingly, virtual teams are formed within organizations that seek to streamline business processes and promote collaboration among employees, such as software developers and risk and position traders. They allow an efficient use of geographically dispersed expertise and provide economic advantages such as a 24-hour work day.

[5] Adapted from Vasarhelyi, Alles and Williams (2010)

Internal auditors already collaborate and coordinate with team members across (potentially) long distances to complete an audit. In cases where the internal audit function is outsourced or is being performed within a large, global company, virtual audit teams become more of the norm in an effort to reduce transaction costs and increase efficiency (Widener and Selto, 1999). There is a vast literature that studies the dynamics of virtual teams and organizations and addresses issues such as trust (Handy, 1995; Holton, 2001; Jarvenpaa et al, 1998; Jarvenpaa and Leidner, 1999; Ridings, 2002; Meyerson et al, 1996) and communication (Jarvenpaa and Leidner, 1999; DeSanctis and Monge, 1999; Wiesenfeld et al, 1999)[6].

Virtual teams are an important antecedent to the remote audit. In a remote audit environment, the virtual team coordinates auditing activities among auditors who are physically present at the audit site and auditors who are located in other locations, such as corporate headquarters. Cooperation between the virtual team and business process owners ensures that the audit is completed in a timely fashion. While trust and communication are key elements of virtual teams, the audit environment may present unique challenges, such as the role of professional skepticism that is needed for objectivity and the level of communication necessary to provide assurance on internal controls. What are the tradeoffs of trust and skepticism during a remote audit? Would incomplete trust increase the scope of the audit? Will auditors working remotely experience the increased volume of ambiguous communication shown in virtual teams? How would they process the excess information?

Shifting the audit team from an entirely onsite, periodic operation to a combination of onsite and remote team members will require increased use of and competence with ICT as well as training in technology usage, group processes, and in some cases cross-cultural awareness (Blackburn et al. 2003; Rosen et al, 2006). In many cases, technology will provide opportunities to reengineer the audit process itself to enable greater efficiency and coverage. Understanding the impact technology has on developing and using the audit procedures will need further research.

Auditing activities

The remote audit provides an opportunity to innovate the internal audit process. Internal auditors are charged with providing "*a systematic, disciplined approach to evaluate and improve*

[6] For an extensive list of references to studies on virtual teams, see Kirkman and Mathieu, 2005

the effectiveness of risk management, control, and governance processes" (IIA, 2010b). Internal auditors develop new methods for combating fraud and error, monitor internal controls, test process effectiveness, and consult with management to help improve business operations. They conduct financial, operational, compliance, investigative, fraud, information systems, and other miscellaneous audits in order to determine how well their organization and its systems are functioning. Placing the audit into a communication and analytics framework enables us to understand which aspects of the audit can indeed be performed remotely and how they can be done.

Currently, most internal auditors work onsite. Videoconferencing can replace many routine face-to-face audit meetings but not those where all the subtlety and nuance of a conversation must be analyzed, such as an interview with someone suspected of committing fraud or interactions aimed at reducing auditor-client stress.

Table 1 illustrates how different audit activities may be performed onsite and remotely. In practice, we expect there to be a continuum between entirely onsite and entirely remote methodologies, and auditors will have to determine which methodology is appropriate for their circumstances. Further investigation should provide insight into how closely this matches practice.

Table 1: Internal Audit Activities[7]

Audit Activity	Onsite Methodology	Remote Audit Methodology
Engagement procurement	Auditors have lunch meetings and make office visits.	Auditors use e-mail and telephone to arrange audits and meet with management in web conferences and follow up with e-mail.
Audit planning	Audit teams meet physically to outline audit goals and delegate tasks.	Virtual audit teams meet in web conferences to discuss details of the audit. Tasks are assigned automatically in an electronic workpaper system.
Internal control evaluation & compliance	Auditors interview process owners, evaluate paper and digital documentation, run test control settings or evaluate data on their laptop.	Auditors interview process owners via videoconferencing, connect to the client system over the network and run analytical tests through a terminal. They also check audit logs.
Substantive testing	On a laptop, auditors pull sample transactions locally and test for anomalies.	On a laptop, auditors pull sample transactions over the network and test for anomalies. In a continuous setting, automated systems do full sample testing and

[7] Based on Vasarhelyi and Greenstein (2003).

		provide a list of exceptions for the auditor to follow up with.
Audit decisions & reporting	Auditors meet with process owners for follow up. Report to management, audit committee, and/or external auditors.	Same, but via web conferencing.

As the remote audit encourages the creation of virtual teams, an evaluation and reformulation of audit procedures will help audit managers delegate responsibilities to onsite and remote team members and determine the technology and audit methodology needed to coordinate their efforts. Many procedures will necessarily be reengineered so that remote auditors can take on the role of a persistent proctor, notifying the auditor when failures occur within or outside of the scope of the periodic audit.

III.Information and Communication Technology

ICT has already significantly impacted the way businesses and auditors operate and has enabled decentralization. A vast number of firms use e-mail, web conferencing, online document storage, real-time collaboration tools, and telepresence to develop new products and interact with counterparts in other locations. To a great extent, auditors use some of these tools to coordinate with each other as well (Vasarhelyi and Kuenkaikaew, 2010).

The remote audit embraces ICT to create a rich audit experience. However, Vasarhelyi and Kuenkaikaew (2010) observe that internal audit departments generally use enabling technology to simply replicate procedures that already exist, rather than adapting technology to provide better assurance for newer streams of data and information. An auditor may use a spreadsheet to visually evaluate a sample, a macro to run an analysis, e-mail to receive information from an auditee, or a laptop to store audit evidence, but if she must travel from Atlanta to Dayton to perform her tests when the data is readily available online, she is not taking full advantage of the available technology to enable a more interactive audit, such as that aided by monitoring platforms and collaboration tools.[8] This reflects the argument of Hammer (1990)

[8] Alles et al (2006) point out that the data used in the pilot continuous auditing system developed by Siemens was in fact the same digital data that auditors had been relying on when they conducted the onsite IT audit.

that process reengineering should be the result of a new conceptualization of the process rather than simple automation.

ICT enables enhanced interpersonal communication, knowledge sharing, and project management, particularly within virtual audit teams. In this section, we discuss interpersonal interaction and electronic working papers (EWP) as two areas where ICT can directly impact the audit. Ideally, applying ICT in these cases would lead to process reengineering and audit innovation, rather than simply changing the channel.

Interpersonal interaction

Throughout the evidence collection process, interpersonal interaction impacts the effectiveness and outcome of the audit. As with virtual teams, the remote audit has the added challenge of limited sensory perception when the auditor is not physically present to conduct tests, interviews, etc. The influence of trust and collaboration on virtual teams is well documented (DeSanctis and Monge, 1999; Holton, 2001) and provides the foundation for the use of ICT to enable electronic communication.

In order to enable the remote audit, currently used ICTs (such as e-mail) will need to be expanded to include additional technology that facilitates remote communication, centralized evidence gathering, and coordination within the audit team[9]. These are the primary concerns of web conferencing and telework.

The concepts of web conferencing and telework are designed to *"assist groups in communicating, in collaborating, and in coordinating their activities."* (Ellis et al, 1991). Ellis et al (1991) identify the basic philosophy of groupware to enhance group communication over the spread of time and space. Starting with message systems, they expand to discuss computer conferencing, intelligent agents, and coordination systems that were precursors to our modern scheme of e-mail, videoconferencing, artificial intelligence, and planning applications that apply to remote auditing.

Many organizations' IT departments have implemented web conferencing tools to help managers and process owners communicate with vendors and customers. Depending on the security policy of the organization, many of these services can now be accessed directly from a Web browser. These services provide computer-mediated communication, enhancing voice with

[9] For example, e-mail can be used by auditors to submit electronic evidence to an EWP system or for the system to alert auditors when new evidence has been collected automatically.

visual cues (via live multi-directional video streams) and co-browsing of information (via screen and application sharing). Two challenges to adoption of these technologies are the uncertainty intrinsic to the use of new technology and the need to change processes to better use technology.

From a behavioral perspective, the remote audit can be understood by looking at the prevalence of telework, where employees may choose from several physical work locations and use electronic communication to complete their tasks (Hunton and Harmon, 2004; Hunton, 2005; Campbell and McDonald, 2009). Many of the same issues of motivation and productivity found in telework apply to remote interaction between internal auditors and business process managers. We identify several of these open behavioral research issues in Table 2.

Table 2: Selected Behavioral Issues of the Remote Audit

Auditor	Auditee
• Motivation to complete audit tasks • Efficiency of collecting and processing data • Information overload • Technical skills and ability • Trust and professional skepticism	• Continual auditor presence • Ability to hide fraud • Prolonged contact • Resistance to change • Trust

Behavioral issues, if left unaddressed, cloud the potential benefits of a remote audit. For example, ICT is beneficial only if the auditor is trained, feels competent and works efficiently to complete her tasks. Inadequate use may also provide the auditee with motivation to hide fraud, deflect the threat of monitoring or distrust the auditor. In future research should address the extent to which these issues exist and affect the adoption of remote auditing.

Online electronic working papers

Electronic working papers (**EWP**) are designed specifically with the audit in mind. EWP systems build on electronic document management systems (EDMS) and contain tools and workflows that aid in the capture and analysis of audit data. In a remote audit setting, EWPs contain evidence collected on demand by the auditor along with transaction-relevant data extracted and generated by an automated system.

Many accounting firms have adopted more complex database-oriented systems with varying degrees of success (Bierstaker et al, 2001; Bedard et al, 2007). Still, the current state of systems is designed to mimic the history-oriented audit, not to create a real-time snapshot of how internal controls are working. Furthermore, many internal audit departments and some large CPA firms limit themselves to the capabilities of desktop productivity software and forego the tremendous potential value of a modern EWP. As data is increasingly linked together in EWPs, incorporating technology such as process mining (Jans et al, 2010) will not only provide context for that data, but also help auditors gain better insight into failures from any networked device.

Online EWPs facilitate the centralized collection of data during an audit. Specific monitoring events could trigger the automatic collection of data from ERP systems or EDMSs so auditors can focus their effort on following up with the issue, rather than manually collecting the evidence. Where online EWPs are centralized and synchronized, anyone on the audit team can access and review the work of the audit team, thereby reducing data and effort duplication.

There are limitations to implementation of online EWPs, including restrictive security and privacy policies (Prosch, 2008). The location of the data store also has legal implications as some countries don't allow data to leave their physical jurisdiction. These limitations provide interesting research opportunities as well. We expect EWPs to facilitate group decision making, coordination between auditors, enhanced audit logging, and provide a host of other tools and features needed to provide a central audit hub.

Adoption of EWPs for virtual audit teams requires both investment in a software platform or service, and updating evidence collection and storage protocols. Auditors will need a more group sharing-oriented mindset in order to allow a system to take hold and be used effectively. Research on the development of a remote audit-centric EWP system would provide insight into the underlying structure of auditor collaboration.

IV. Continuous Evidence & Analytics

Enterprise resource planning (ERP) systems allow authorized users to collect and analyze disaggregated data and provide reports on many issues ranging from key performance indicators to the behavior of their customers. While evidence has traditionally been static and laborious to collect, the progressive availability of real-time data now enables automation of audit analytical procedures, continuous process monitoring, and automatic evidence collection across all business processes, customers and suppliers (Alles et al, 2010). Financial and non-financial data are progressively available continuously, enabling internal auditors to expand the scope of their tests to include the full population of current, relevant transactions.

This can include alarms generated by controls failures and the resulting reactions by management and auditors (Vasarhelyi & Halper, 1991). In many cases, internal auditors work with IT departments, management, and consultants to determine the amount and types of evidence that should be collected (Vasarhelyi and Kuenkaikew, 2010; Teeter et al, 2010). Based on Statement on Auditing Standards No. 106 (AICPA, 2006), Table 3 presents examples of onsite and remote audit methodologies that may be used to obtain data for certain audit procedures.

Table 3: Audit Procedures for Obtaining Audit Evidence[10]

Procedure	Onsite Methodology	Remote audit Methodology
Inspection of Records or Documents (e.g. authorization)	Pull a sample of purchase orders and verify authorized signature exists and matches authority list	Evaluate entire purchase order population in ERP and verify POs passed through approval workflow and possess authorized user stamp
Inspection of Tangible Assets (e.g. physical inventory count)	Print a list of inventory, walk through warehouse, open boxes, etc.	Employ closed circuit video monitoring, scales, other metrics
Observation (e.g. watching someone complete a process)	Shadow a worker and observe procedure	Use process mining to identify transactions that do not follow a standard workflow
Inquiry (e.g. written or oral interviews)	Communicate electronically or in person as part of traditional audit	Monitor processes/controls. Automatically identify process owner when exceptions occur
Confirmation (e.g. verify account balances)	Send letters or e-mail to banks, suppliers, etc.	Evaluate linked data streams from financial institutions, other businesses through IDE, etc.
Recalculation (e.g. using CAAT to recalculate figures)	Manually extract data, run CAATs	Monitor transactions, run calculations automatically at standard intervals, perform process integrity reviews, monitor changes in processes
Reperformance (e.g. aging of accounts receivable)	Manually extract data, run CAATs	Monitor accounts, run calculations automatically, replicate transactions
Analytical Procedures	Extract data, scan for anomalies based on auditor	Filter real-time data through continuity equations, ratio

[10] Based on Statement of Auditing Standards No. 106 (AICPA, 2006).

(e.g. scanning and statistics)	judgment	analysis

Inspecting paper documents, for example, requires an auditor to physically pull a sample of authorized forms and verify that signatures are present and match authority lists. While many businesses are progressively implementing electronic documents and signatures, the remote audit is dependent on access to the electronic data this reengineering process enables. In the case of documents such as invoices and credit profiles, reengineering would involve implementing devices and procedures for document scanning, character and signature analysis, and online storage, and/or the design and implementation of a module in the ERP system that enables direct online form entry and requires an approval workflow. In their consultant capacity, internal auditors would work with business process owners where reengineering is necessary.

To demonstrate the possibilities of a reengineered electronic evidence environment, the internal audit team at Siemens implemented a methodology of continuous control monitoring as a means to gather evidence of IT controls operation (Alles et al, 2006; Teeter et al, 2010). Siemens converted the existing audit methodology that was typically performed once every 18 to 24 months and supplanted it with a stream of control assurance evidence drawn daily. This system provides an online dashboard that auditors can evaluate periodically and configure to send e-mail alerts when internal controls fail.

Working remotely, internal auditors evaluate continuous evidence, in the form of documentation and data, using computer assisted auditing techniques (CAATs) and continuous auditing (CA) systems, comprised of continuous controls monitoring (CCM) and continuous data assurance (CDA) tools. With the resulting distilled information, auditors can work in virtual teams to help managers evaluate and address internal controls and other assurance issues on demand.

Documentation

Documentation plays a central role in both communicating business processes and evaluating the integrity of an audit (Sprague, 1995). For an auditor, documentation can include a set of audit procedures, a spreadsheet of extracted information, a transcript from an interview, or a combination of different media elements. For a process owner, documentation details the standard operating procedure that workers should follow to complete their process objective.

From the line worker to the auditor, documentation ensures that all parties understand their precise tasks and provides a reference for new employee training. Properly configured systems also create logs that function as "paper" trails of economic transactions and user activity within the system.

Electronic document management systems (EDMS) provide the infrastructure to centrally store and access relevant information. EDMSs provide the backbone for the different types of documentation used within an organization and deliver an added layer of user access control and audit logging. They also supply a platform for auditors to gather and store evidence in an online, collaborative environment.

EDMSs are far more than simple file cabinets for static documents. They are collaborative platforms where users can contribute to the existing collective knowledge of the organization (Cho, 2010). Low storage costs and online access allow organizations to create massive information repositories while enforcing ownership, document versioning, and retention policies (Sprague, 1995). Borrowing from the Internet model, documents within these systems can be tagged with metadata (e.g. descriptive keywords, summaries, and date stamps) and hyperlinked to provide context and flexibility (DeYoung, 1989; Dourish et al. 2000). Most systems index the titles, contents, and metadata of these documents and enable simple search and navigation capability. Increasingly, employees can access and update documentation within a "cloud", or Internet-connected service, through a Web browser on their computers or mobile devices (Armburst et al, 2009). The universal access and scalability of cloud computing makes it attractive to companies that are spread out geographically or have a mobile workforce.

Documentation currently provides a significant hurdle to the remote audit. Many organizations continue to have a substantial amount of data generated by paper documents; conversion of these documents into digital form is prone to manual entry errors and potential falsification. Where EDMSs are not comprehensive or existent, auditors continue to perform a significant amount of manual document checking, comparing signatures to decision authorities and looking for evidence of tampering. Auditors may fulfill their consultant role by working with process owners to reengineer document generation and collection procedures. In order to aid the digitization process, auditors will need to possess adequate knowledge of these systems and build controls around them.

With the expansion of digital evidence, auditors will be able to more quickly assess the existence and validity of documentation. Alerts, activity and change logs, and other monitoring techniques become the new indicators for auditing documentation. In specialized cases, light semantic processing and text mining techniques allow auditors to determine who created, accessed, and may have changed a document.

As with any access control system, challenges still arise in an electronic environment. For example, someone may alter a document using another user's credentials, or someone with super user privileges may remove evidence without detection. As they work to reengineer the documentation, auditors must consider these and other challenges when helping develop the controls and audit procedures for evaluating electronic documentation.

Computer Assisted Auditing Techniques

Computer Assisted Auditing Techniques (CAATs) are used to interrogate databases and other data sources and perform analytical procedures, transaction tests and other audit tests in real-time systems (Sayana, 2003) with or without an onsite auditor. Internal auditors employ numerous CAATs to facilitate evidence collection and analyze data using techniques such as financial accounting ratios (Deakin, 1978; Tabor & Willis, 1985; Stringer & Stewart 1986) and advanced statistics like Benford's Law (Nigrini and Mittermeier, 1997) and continuity equations (Vasarhelyi et al. 2004). In a continuous audit, CAATs provide the basis for automated auditing tools (Zhao et al. 2004; Alles et al, 2006).

The extent to which auditors employ CAATs varies depending on tool complexity and auditor expertise. Debreceny et al (2005) evaluate the use of CAATs within a banking environment and find that while internal auditors generally use audit software, they appear to be inconsistent in their application of these tools. In some cases, auditors perceive these audit tools as necessary for fraud investigation or special instances, but not for mainstream substantive testing procedures. Likewise, while auditors seem to appreciate the benefits of CAATs, they lack the expertise and training necessary to understand and use them more effectively (Braun and Davis, 2003; Janvrin et al. 2008). As auditors evaluate the use of CAATs as remote audit tools, this learning gap will need to be addressed.

Most CAATs are already designed to be run on computers and access networked data. Moving these tools to a remote environment is a trivial task, assuming auditors have a secure remote connection to the data they are accessing[11]. When evaluating which tools to use and develop for the remote audit, auditors can use existing CAATs as a foundation, expanding them to enable real-time data assessment and automatic evidence collection.

Continuous auditing

One of the key developments in modern audit analytics is the concept of continuous auditing (CA). CA is based on the formalization of audit procedures and automation of CAATs and other tasks from the audit plan. A remote audit would rely heavily upon the existence of automated monitoring devices that direct the auditor's attention to high-risk transactions and controls failures on a real-time basis. Internal auditors already receive guidance on the use of continuous auditing and monitoring systems (COSO, 2008).

Multiple models for continuous auditing have been proposed (Rezaee et al, 2002; Woodroof and Searcy, 2001), each delineating requirements of data availability and auditor interaction. The two main components of continuous auditing are continuous controls monitoring (CCM) and continuous data assurance (CDA). CCM is a platform for evaluating internal controls settings within an ERP system and notifying auditors when a failure occurs. CDA assesses the underlying data within those systems to ensure that the data is valid and had not been tampered with. Together CCM and CDA ensure that data pulled from a company's ERP system accurately reflects the functioning business processes.

Brown et al (2007) provide an overview of CA research, identifying the trends of auditors to increasingly utilize monitoring and other audit automation technologies (Glover et al. 2000; Rezaee et al. 2002). In addition to enabling auditing by exception, CCM has the potential to deter management from taking unnecessary risks. For example, Hunton et al (2008) examine CCM from the manager's perspective and find that where monitoring is in place, incentives to smooth income or make high-risk investments are decreased. These and other behavioral effects of implementing auditing analytics should be examined in future research.

CA theory is now approaching maturity, with the technological infrastructure necessary for its effective implementation, particularly ERP systems and the awareness of the CA becoming ubiquitous among internal auditors (Vasarhelyi et al 2010). The platform provided by

[11] Many IT departments deploy Virtual Private Networks (VPNs) for workers to connect remotely (e.g. when traveling) through an encrypted channel.

CA eliminates much of the manual internal audit work, while providing remote auditors with comprehensive monitoring and real-time analysis of company data.

Because of the time shift created by CA, auditors can work remotely to address issues within a business process as they occur, rather than waiting for the periodic audit. This facilitates the prolonged intense deterrence by auditors, while changing the function of the remote audit team to that of a perpetual proctor, facilitating more timely and continuous interaction with the auditee.

There are many examples of implementation of remote-audit enabling CCM technology (Alles et al. 2006; Alles et al, 2008; Murthy, 2004; Nelson, 2004; Rose and Hirte, 1996; Turoff et al, 2004; Vasarhelyi & Halper, 1991). Each of these papers evaluates specific issues within these organizations, and outlines the reengineering process of evaluating traditional audit methods, developing new or analogous tests, and comparing the automated procedure to the manual one. Coupled with ICT, CA and other analytics provide the toolkit that auditors need to work remotely.

V. Conclusions and Directions for Future Research

Remote auditing presents an opportunity for internal auditors to leverage technology and adapt to a changing information environment. While CA removes the timing constraint of the audit, remote auditing removes the location constraint. Implementing remote auditing may cause auditors to fundamentally rethink the way an audit is carried out and the way the audit team is formed and managed.

In addition to the demand, motivation, and technology needs of the remote audit, reengineering of the audit processes plays a central role. From rebalancing and reassigning auditing activities to implementing more comprehensive analytics, many issues persist regarding the audit reengineering process. In some cases, the remote audit is also dependent on the reengineering of business processes themselves. It is unlikely that auditors will drive the change, but they must work with managers to deal with new streams of data and evidence.

Figure 4: Components of Remote Auditing

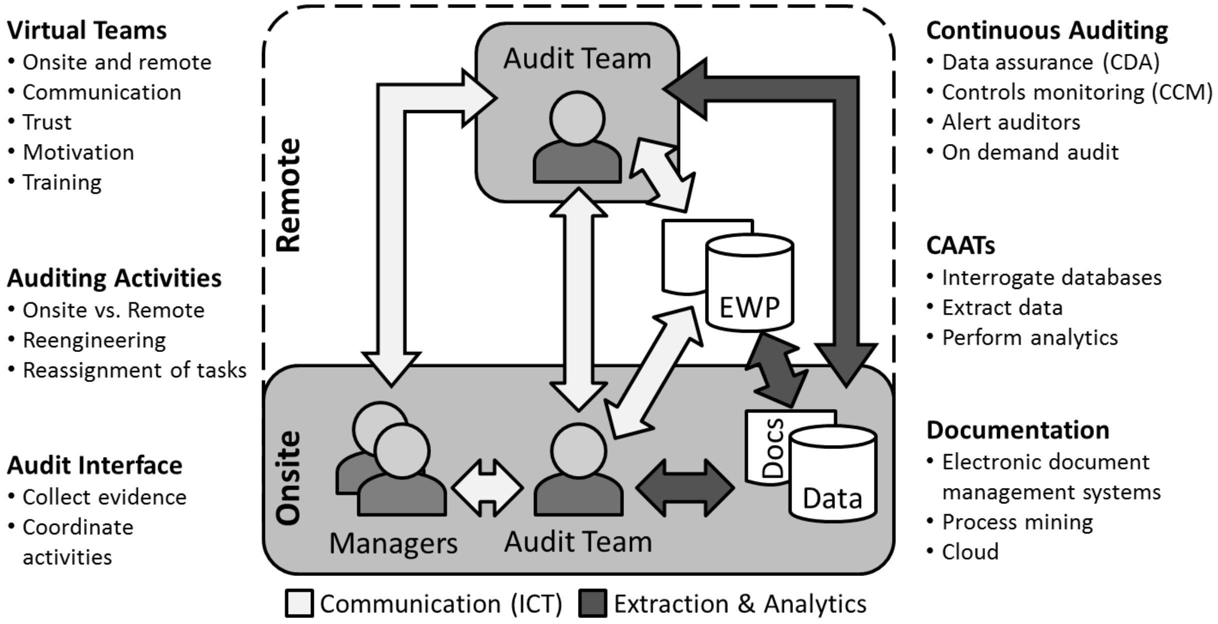


Figure 4 summarizes the remote audit function described in this paper and identifies the needs and features of remote audit teams, activities, communication, documentation, and analytics. It is those communication tools and analytic techniques that underlie and facilitate the remote audit, and there is much research that needs to be undertaken to gain insight into the development and application of these components to internal auditing. Moreover, the drivers (and barriers) of remote auditing are not only technological, but extend to the behavioral realm. These factors will determine the comfort level of auditors providing assurance based on evidence obtained and analyzed remotely, and the potentially changing trust relationships between virtual audit teams and auditees.

In this paper, we have developed the concept of a remote audit and provided a framework for understanding the reengineering needed in the audit process to enable such a vision.. For future research, there remain several important questions that must be addressed if this vision is to become a reality, including conceptual, technical, and behavioral.

Conceptually, the internal audit objectives and goals need to be evaluated to identify those that are still relevant, those that are no longer applicable, and those that have not yet been identified in the real-time environment. Field studies of different types of organizations and mapping data flows would provide insight into these questions.

From a technical standpoint, IT, AIS, and OM research have identified several uses of databases, clouds, and other mechanisms for storing and accessing data. Developing and simulating auditing systems that reduce latency, improve security and reliability, and protect privacy is essential to remote auditing.

In Table 2, we identify some outstanding behavioral issues related to reengineering audit processes for a remote environment. Understanding how the dynamics of virtual audit teams (including formation, trust, and communication) differ from other types of virtual teams would be valuable in informing both auditors and managers. Insight into how auditors use or would use technology within their organizations could be gathered through experimental research.

In our own future research, we hope to explore some of these open issues and work with several organizations to develop pilot implementations of remote auditing. Through those we hope to further answer many of the conceptual, technical, and behavioral questions introduced in this research framework.

References

Alles, M.A., G. Brennan, A. Kogan, and M.A. Vasarhelyi. 2006. Continuous monitoring of business process controls: a pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems* 7(2): 137-161.

--------, A. Kogan, and M.A. Vasarhelyi. 2002. Feasibility and economics of continuous assurance. *Auditing: A Journal of Practice and Theory* 21 (1): 125-138.

--------, A. Kogan, and M.A. Vasarhelyi. 2008. Putting continuous auditing theory into practice: lessons from two pilot implementations. *Journal of Information Systems* 22(2):195-214.

--------, A. Kogan, and M.A. Vasarhelyi. 2010. Principles and Problems of Audit Automation as a Precursor to Continuous Auditing, working paper. *Working paper*, Rutgers Accounting Research Center, Rutgers Business School.

American Institute of Certified Public Accountants (AICPA). 2006. Statement on Accounting Standards (SAS) No. 106. *Audit Evidence*. New York, NY: AICPA.

Armbrust, M., A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, et al. 2009. Above the clouds: a Berkeley view of cloud computing. *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28*, 07-013.

Bedard, J.C., M.L. Ettredge, and K.M. Johnstone. 2007. Using electronic audit workpaper systems in audit practice: task analysis, learning, and resistance. *Advances in Accounting Behavioral Research* 10(1): 29-53.

Bierstaker, J.L., P. Burnaby, and J. Thibodeau. 2001. The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. *Managerial Auditing Journal* 16(3): 159-164.

Blackburn, R.S., S.A. Furst, and B. Rosen. 2003. Building a winning virtual team. *Virtual teams that work: creating the conditions for virtual team effectiveness.* 95-120

Braun, R.L. and H.E. Davis. 2003. Computer-assisted audit tools and techniques: analysis and perspectives. *Managerial Auditing Journal* 18(9): 725-731.

Brown, C. E., J.A. Wong, and A.A. Baldwin. 2007. Research streams in continuous audit: a review and analysis of the existing literature. *Journal of Emerging Technology in Accounting*. 4(1): 1.

Cho, V. 2010. A study on the impact of organisational learning to the effectiveness of electronic document management systems. *International Journal of Technology Management* 50(2): 182-207.

Campbell, J. and C. McDonald. 2009. Defining a conceptual framework for telework and an agenda for research in accounting and finance. *International Journal of Business Information Systems* 4(4): 387-402

Committee of Sponsoring Organizations (COSO). 2008. Guidance on monitoring internal control systems.

Curtis, M.B., and E.A. Payne. 2007. An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. *International Journal of Accounting Information Systems* 9(2): 104-121.

Deakin, E. 1976. Distributions of financial accounting ratios: some empirical evidence. *Accounting Review* 51(1), 90–96.

Debreceny, R.S., S. Lee, W. Neo, and J. Toh Shuling. 2005. Employing Generalized Audit Software in the Financial Services Sector: Challenges and Opportunities. *Managerial Auditing Journal 52*(4): 813-618.

DeSanctis, G., and P. Monge. 1999. Introduction to the Special Issue: Communication Processes for Virtual Organizations. *Organization Science* 10(6): 693-703.

DeYoung, L. 1989. Hypertext challenges in the auditing domain. *Proceedings of the second annual ACM conference on hypertext.* 180.

Dourish, P., W. Edwards, A. LaMarca, J. Lamping, K. Petersen, M. Salisbury, M., et al. 2000. Extending document management systems with user-specific active properties. *ACM Transactions on Information Systems* 18(2): 170.

Ellis, C.A., S.J. Gibbs, and G. Rein. 1991. Groupware: some issues and experiences. Communications of the ACM 34(1):39-58.

Glover, S.M., D. Prawitt, and M.B. Romney. 2000. The software scene. *Internal Auditor* 57(4): 49-57.

Hammer, M. 1990. Reengineering work: don't automate, obliterate. *Harvard Business Review 68*(4): 104-112.

Handy, C. 1995. Trust and the virtual organization. *Harvard Business Review 73*(3): 132-142.

Hoitash, R., A. Kogan, R. Srivastava, and M.A. Vasarhelyi. 2006. Measuring information latency. *The International Journal of Digital Accounting Research* 6(May).

Holton, J.A. 2001. Building trust and collaboration in a virtual team. *Team Performance Management* 7(3/4): 36-47.

Hunton, J.E. and K. Harmon. 2004. A model for investigating telework in accounting. *International Journal of Accounting Information Systems* 5(4): 417-427.

Hunton, J.E. 2005. Behavioral Self-Regulation of Telework Locations: Interrupting Interruptions! *Journal of Information Systems* 19:111.

-------, J.E., E.G. Mauldin, and P.R. Wheeler. 2008. Potential Functional and Dysfunctional Effects of Continuous Monitoring. *The Accounting Review* 83(6): 1551.

Institute of Internal Auditors. 2010b. What is internal auditing? http://www.theiia.org/theiia/about-the-profession/internal-audit-faqs/?i=1077. Accessed May 4, 2010.

Jans, M., M. Alles, and M.A. Vasarhelyi. 2010. Process mining of event logs in auditing: opportunities and challenges. Working paper. Hasselt University. Belgium.

Jarvenpaa, S. L., K. Knoll, and D.E. Leidner. 1998. Is anybody out there?: antecedents of trust in global virtual teams. *Journal of Management Information Systems* 14(4).

Jarvenpaa, S., and D. Leidner. 1999. Communication and trust in global virtual teams. *Organization science* 10(6): 791–815.

Janvrin, D., D.J. Lowe, and J. Bierstaker. 2008. Auditor acceptance of computer-assisted audit techniques. *Working Paper*, Iowa State University.

Jung, W., A. Rillig, R. Birkemeyer, T. Miljak, and U. Meyerfeldt. 2008. Advances in remote monitoring of implantable pacemakers, cardioverter defibrillators and cardiac resynchronization therapy systems. *Journal of Interventional Cardiac Electrophysiology* 23(1): 73-85.

Katz, M.L. and C. Shapiro. 1986. Technology adoption in the presence of network externalities. *The Journal of Political Economy* 94(4): 822-841.

Kirkman, B.L., and J.E. Mathieu. 2005. The dimensionalities and antecedents of team virtuality. *Journal of Management* 31(5): 700-718.

Meyerson, D., K.E. Weick, and R.M. Kramer. 1996. Swift trust and temporary groups. *Trust in Organizations: Frontiers of Theory and Research*. R.M. Kramer, T.R.Tyler, eds. Thousand Oaks, CA: Sage Publications. 166-195.

Murthy, U.S. 2004. An analysis of the effects of continuous monitoring controls on e-commerce system performance. *Journal of Information Systems* 18(2): 29-47.

Nelson, L. 2004. Stepping into continuous audit. *Internal Auditor* 61(2): 27-29.

Nigrini, M.J. and L.J. Mittermaier. 1997. The use of Benford's Law as an aid in analytical procedures. *Auditing: A Journal of Practice and Theory* 16(2): 52-67.

Prosch, M. 2008. Protecting personal information using generally accepted privacy principles (GAPP) and continuous control monitoring to enhance corporate governance. *International Journal of Disclosure and Governance* 5(2): 153-166.

Rezaee, Z., A. Sharbatoghlie, R. Elam, and P.L. McMickle. 2002. Continuous auditing: building automated auditing capability. *Auditing: A Journal of Practice and Theory* 21(1): 147-163.

Ridings, C. 2002. Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems* 11(3-4): 271-295.

Rose, W. C. and B. Hirte, B. 1996. Carolina Power and Light: smart auditing. *In Enhancing Internal Auditing Through Innovative Practices*, edited by G. L. Gray, and M. J. Gray, 47–57. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Rosen, B., S. Furst, and R. Blackburn. 2006. Training for virtual teams: An investigation of current practices and future needs. *Human Resource Management* 45(2): 229-247

Sayana, S. 2003. Using CAATs to support IS audit. *Information Systems Control Journal* 1*:* 21–23.

Sprague Jr, R. 1995. Electronic document management: Challenges and opportunities for information systems managers. *MIS Quarterly* 19(1): 29–49.

Stringer, K.W., and T.R. Stewart. (1996). *Statistical techniques for analytical review in auditing.* Second edition. New York, NY: John Wiley & Sons.

Tabor, R.H. and J.T. Willis. 1985. Empirical evidence on the changing role of analytical review procedures. *Auditing: A Journal of Practice & Theory* 4(2): 93-109.

Teeter, R.A., G. Brennan, M.G. Alles, and M.A. Vasarhelyi. 2010. Aiding the audit: Using the IT audit as a springboard for continuous controls monitoring. *Working paper*, CarLab, Rutgers Business School.

Turoff, M., M. Chumer, S.R. Hiltz, R. Klashner, M.G. Alles, M.A. Vasarhelyi, and A. Kogan. 2004. Assuring homeland security: continuous monitoring, control & assurance of emergency preparedness. *Journal of Information Technology Theory and Application* 6(3): 1-24.

Vasarhelyi, M.A., and F.B. Halper. 1991. The continuous audit of online systems, *Auditing: A Journal of Practice and Theory* 10(1): 110-125.

--------, and S. Kuenkaikaew. 2010. Continuous auditing and continuous control monitoring: case studies from leading organizations. *Working paper*, Rutgers Accounting Research Center, Rutgers Business School.

--------, and M. Greenstein 2003. Underlying principles of the electronization of business: a research agenda. *International Journal of Accounting Information Systems* 4(1):1-25.

--------, M.G. Alles, and A. Kogan. 2004. Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting* 1(1): 1-21.

--------, M.G. Alles, and K.T. Williams. 2010. Continuous assurance for the now economy. *A Thought Leadership Paper for the Institute of Chartered Accountants in Australia*, forthcoming May.

Widener, S., and F. Selto. 1999. Management control systems and boundaries of the firm: why do firms outsource internal auditing activities? *Journal of Management Accounting Research* 11: 45-73.

Wiesenfeld, B., S. Raghuram, and R. Garud. 1999. Communication patterns as determinants of organizational identification in a virtual organization. *Organization Science*, 10(6): 777–790.

Woodroof, J. and D.W. Searcy, 2001. Continuous audit: model development and implementation within a debt covenant compliance domain. *International Journal Of Accounting Information Systems* 2(3): 169-191.

Zhao, N., and D. Yen. 2004. Auditing in the e-commerce era. *Information Management & Computer Security* 12(5): 389-400.