ESSAYS ON THE ENHANCED AUDIT

by

RYAN ANTHONY TEETER

A Dissertation submitted to the

Graduate School-Newark

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Management

written under the direction of

Miklos A. Vasarhelyi, Ph.D.

and approved by

_____

_____

_____

_____

_____

Newark, New Jersey

May 2014

Copyright page:

©2014

Ryan Teeter

ALL RIGHTS RESERVE

ABSTRACT OF THE DISSERTATION

Essays on the Enhanced Audit

By RYAN A. TEETER

Dissertation Director:

Miklos A. Vasarhelyi, Ph.D.

Automation, remote access, and continuous access to enterprise data provide opportunities for internal auditors to improve and enhance their ability to provide assurance that their firms' business processes are compliant and well-controlled. This dissertation documents the efforts by researchers working with two internal audit organizations as they develop and implement enhanced auditing procedures.

Field studies at these two sites provide insight into the adoption of enhanced audit procedures, and provide discussion on technology dependence and auditor competence. Analysis of these organizations' audit plans and effort also guides the definition of a standard framework for audit evidence classification that synthesizes various approaches to the enhanced audit and provides a tool for auditors' evaluation of their own audit plan.

The first essay (Chapter 2) investigates the implementation of a comprehensive continuous controls monitoring (CCM) platform for evaluating internal controls within a highly formalized and well-controlled enterprise resource planning environment.

Utilizing the IT audit plan as a template, auditor expertise as a guide, and manual audit output as a validation tool, this field study examines the process of audit formalization and implementation of CCM at a software division of a large, multinational corporation.

The second essay (Chapter 3) identifies two different approaches to audit reengineering and the experience of the auditors in attempting each method at a large consumer goods company with a highly manual, paper-based environment. Similarly, the third essay (Chapter 4) presents a conceptual framework for the remote audit. Following an introduction to virtual teams, information and communication technology and data analytics, this essay presents the analysis of the revenue audit program.

The enhanced audit classification model (EACM) presented in Chapter 5 joins three concepts found in the assurance literature that link directly to the enhanced audit. These concepts include audit automation, remote auditing, and continuous auditing. The EACM provides auditors and researchers with a framework for identifying opportunities for audit innovation based on the characteristics of the underlying evidence used in the assurance process.

ACKNOWLEDGEMENT

There are numerous individuals without whose insight and direction I would never have completed this work. At Maritis, Rod Brennan championed the implementation effort while David Walther helped me navigate the complex world of the IT audit along with the auditors Rolf Haardoerfer and Jens Klingen. At Nouant, David Levin, Terry Hickman, Mamuka Murjikneli provided overall guidance while Brandy Stracener and Jeanette Bredestege worked behind the scenes to provide data and institutional knowledge.

I would like to invaluable feedback I received from members of the Strategic and Emerging Technologies section of the American Accounting Association. Amelia Baldwin provided editorial guidance on my first papers, Greg Gerard and Roger Debreceney provided critical comments that made this dissertation stronger. Also participants at the ISAR and CONTECSI conferences provided insightful feedback.

Harry Evans and Nandu Nagarajan helped with the final push, JP Krahel and Erin Starks-Teeter were there with encouragement and editing help. I would like to recognize the incredible patience of my committee members, Michael Alles, Alex Kogan, Don Warren, and Ted Mock. Finally, I will be ever grateful to Miklos Vasarhelyi, my dissertation advisor, who worked tirelessly to help me through to the end.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1. INTRODUCTION AND RESEARCH OBJECTIVES

Introduction

The audit environment is continually evolving. New strategic and emerging technologies allow auditors to take advantage of the automation and monitoring tools that management has made possible through business process reengineering efforts over the past few decades. These new systems and information technology have generated large amounts of data throughout the information supply chain. Used properly, these data can provide insight into how operations work, help auditors and managers identify levels of risk within business processes, and provide timely notification of process failure.

The prevalence of digital data and complex networks of information systems presents unique challenges to auditors, whose primary purpose is to provide assurance to shareholders and help maximize shareholder value. As a part of this role, they verify the reliability of the information generated by these systems and present useful analyses to facilitate the decision-making process. Contemporary assurance demands that auditors be not only familiar with emerging technology, but also be able to objectively assess the quality of data generated by these systems, and explore new ways to extract meaning from these new sources of data.

The quality of data in these systems impacts management's ability to make informed decisions as well as the confidence of stakeholders. For this reason, researchers continuously investigate ways to improve the data quality so that it can help improve the decision-making process. Wang and Strong (2006) make the case for "high-

quality data to be intrinsically good, contextually appropriate for the task, clearly represented, and accessible to the data consumer." For this reason, auditors must work with management to ensure that they are using high-quality data to validate management's assertions.

Information technology use has increased dramatically in recent years, producing a multitude of information systems and underlying databases. The diverse number of users and implementations of this technology have generated terabytes of data, some of which is incomplete or inaccurate. Hong and Kim (2002) note that as organizations have adopted commercially available ERP systems, a high number of those adoptions have failed because they do not fit the organization's strategic goals and structure. These systems continually face threats of data loss, privacy breaches, and manipulation by users. More significantly, poorly-controlled implementations are more likely to produce inaccurate information and misrepresent the operations of the company (Bisbal, Lawless, Wu, & Grimson, 1999; Prosch, 2008). If management and stakeholders are to rely on data generated by these systems, it is essential that they be well controlled, protected, and insulated from the greatest risks, including intentional or accidental manipulation (Pitt, Watson, & Kavan, 1995).

While management has actively embraced enterprise data to extract business intelligence and gained insight into hidden relationships, auditors appear to be reluctant or unable to do likewise. Gonzalez, Sharma, & Galetta (2012) surveyed members of the Institute of Management Accountants and note that while awareness of continuous auditing is on the rise, actual adoption of the technology is low compared to the high

level of expressed interest in using this technology found in surveys from public accounting firms (PricewaterhouseCoopers, 2012). This apparent disconnect is attributed to a number of factors including increased litigation risk in the United States (Janvrin, Loudder, & Bierstaker, 2008b), lack of proper incentives (DeAngelo, 1981), and reluctance to adopt new technology (Gonzalez et al, 2012). Audit executives observe that while auditors have good professional skills, such as judgment and skepticism, they lack the technical skills needed to either produce advanced analytical procedures or participate in audit reengineering efforts (Braun & Davis, 2003; Gonzalez et al, 2012; Gupta, 2001). In other cases, they are reluctant to invest in approaches that cause auditors to over-rely on computerized systems at the expense of auditor judgment (Dowling & Leech, 2007). Finally, anecdotal evidence from the research presented in the following chapters suggests that organizational barriers prevent auditors from having timely and appropriate access to the company data needed to evaluate management's assertions.

The objective of this dissertation is to develop an understanding of the data and evidence auditors collect, identify opportunities for an enhanced audit through automation, remote auditing, and continuous auditing procedures and tools, and observe internal auditors' response to these opportunities. This understanding is achieved through the study of the internal audit departments at two large multinational corporations, whose insights help explain the successes and challenges of enhancing audit plans and using more efficient enhanced audit procedures.

Value Proposition

Each company has unique audit needs and expectations within the audit and control framework. A highly manual business process in one company may match the highly formalized and digitized workflow in another. The choice of business processes is largely determined by the nature of the business and decisions made by management (Aral & Weill, 2007). Management attempts to adopt systems that fit the organization's objectives. The types of approaches employed by auditors should also match the client's environment and needs, though auditors tend to prefer traditionally manual procedures that rely more on the auditor's judgment over computerized analysis and decision support (Dowling & Leech, 2007).

Meanwhile, stakeholders expect auditors to provide sufficient assurance at the lowest cost. The desired level of effectiveness and efficiency challenges auditors to continually reevaluate their audit plans and optimize their effort. In many cases, resulting in a risk-based approach where some procedures are dropped so auditors can focus their energy on the highest risk areas. Adoption of enhanced audit techniques allows both: auditors reduce overall effort by automating repetitive tasks and communicating with remote team members while improving stakeholder confidence in their judgments.

The enhanced audit allows audit organizations to reduce the costs associated with auditor travel (in the case of a remote audit), decrease the frequency of audit visits (where continuous assurance is in place), focus auditors' efforts on areas of high operational risk, and allow them to utilize greater judgment. As audit managers seek

short-term investment for the development of enhanced auditing techniques, they often cite a reduction in long-term operating (travel and entertainment) cost as one of the primary objectives (Alles, Brennan, Kogan, & Vasarhelyi, 2006; Rezaee et al., 2002).

There are other ways that an enhanced audit approach can improve audit effectiveness. Automation reduces auditor effort while providing greater coverage through full population or targeted sampling testing (Coderre, 2008; Stark, 2009). Remote auditing allows members of audit teams be distributed geographically and take advantage of knowledge concentration (Zaheer & Manrakhan, 2001). Continuous auditing permits more timely evaluation and detection of data anomalies and potential fraud. This also reduces the auditors' disruptive impact on line workers and provides sustained deterrence to fraud (Langford, 2010; Vasarhelyi, Alles, & Williams, 2010).

Pressure and Access

Auditors are aware of the ability of technology to enhance assurance, and they express a commitment to use some tools and techniques such as continuous auditing, but actual adoption of these techniques in recent years has been incremental and inadequate (Gonzalez et al, 2012; PricewaterhouseCoopers, 2012; Vasarhelyi & Kuenkaikaew, 2011). Auditors are constrained in their audit reengineering efforts by external political pressures, such as budgetary and organizational pressure as well as incompatibility of audit evidence.

Some pressures are external. For example, auditors are reluctant to modify client systems to enable full-population testing because of the risk of litigation (Hunton, Wright, & Gerard, 2003). Kuhn and Sutton (2010) state that the "threat of litigation …

would likely be sufficient to cause many public accounting firms to refuse to undertake continuous auditing of client systems." While litigation risk isn't as prevalent for internal auditors, reengineering the audit process typically requires changes to be made to underlying systems, which can face political and organizational hurdles. Because internal audit is a cost center, upfront investment in enhanced auditing development may not allocated without a strong argument for longer term cost savings. In general, only specialized (typically IT) auditors are trained in enhanced auditing techniques, so the learning curve on unfamiliar technology and current techniques such as advanced analytics, data mining, and visualization is steep and costly.

Restricted access to data also limits auditors' attempts to provide more real-time auditing capability. In the course of a normal audit, both external and internal auditors make multiple requests for data from IT personnel in order to find sufficient support and evidence to test management's assertions. While IT is obligated to meet these requests, anecdotal evidence suggests that there is often significant time delay between requests and delivery. This is partly due to the burden placed on the IT staff to write scripts and produce data for a process that ultimately doesn't generate revenue, not to mention the perceived threat of auditors. Often, the data provided by IT don't always meet the auditors' needs, and multiple requests are made to gather the appropriate data. Auditor access to complete, timely data that is in the correct format for the tools they use is an important prerequisite for the enhanced audit.

Finally, a major factor limiting the adoption of enhanced audit techniques is a lack of modernization in the business processes themselves. For example, some business

processes do not generate digital data (e.g. sales recorded in emerging markets or requirements for physical signatures on documents). Unless the data are converted into some digital form through data entry or electronic filing, the scope of automation and remote auditing is very limited. Without digital data and remote connections, adding a timing component necessary for continuous auditing is likewise impossible.

Research Objectives

Transformational change through the process of implementing continuous assurance and increased reliance on more frequent automated monitoring is a necessary step in the modernization of business processes (Alles et al., 2006; Elliott & Jacobson, 2002; Hunton et al., 2003; Vasarhelyi & Halper, 1991). Auditors have moved their audit working papers online and a limited number of firms have experimented in audit analytics and automation (Brown et al., 2007; Gupta, 2001; Janvrin, Bierstaker, & Loudder, 2008a;). Yet given the apparent benefits, progress in the actual formalization of the audit effort has fallen short of expectations (PricewaterhouseCoopers, 2012; Vasarhelyi & Kuenkaikaew, 2011).

As business processes have evolved from manual systems to incorporate more automated real-time systems, auditors continue to use highly manual, periodic testing and procedures to provide assurance, albeit enhanced by job aids and decision support tools. This has perpetuated a disparity between these two important processes. Most of the audit procedures do not match the interactivity, frequency, and location of the underlying data found in the enterprise system. Internal auditors' efforts to better align their audit effort to the audit data is the focus of this dissertation and is presented and

analyzed herein. Automation can reduce internal audit effort, continuous auditing can reduce audit lag, and remote auditing procedures can enable a more dynamic, on-demand audit while increasing auditor efficiency and placing audit procedures closer to the source data. However, attempts at internal audit reengineering are not always successful, as illustrated in the field studies presented in this dissertation.

Because there are limited examples of internal audit reengineering that focus on automation and digitization of the audit process, there is an opportunity to expand the literature with field research that demonstrates new methodologies, provides insight into the advantages, disadvantages, successes, and challenges of those methods, and better defines the role of enhanced assurance in all types of firms.

The findings presented in this dissertation focus primarily on the technical feasibility of internal audit reengineering. Some behavioral and non-technical elements that limit implementation are discussed. Many of these issues have been identified before. They generally relate to barriers to technology adoption (Curtis & Payne, 2008; Parente & Prescott, 1994), resistance to change in the audit process (Lapointe & Rivard, 2005), the role of champions in technology adoption (Beath, 1991), and auditor incentives (Curtis & Payne, 2008). The nature of audit automation and continuous auditing as a radical technological change encounters similar barriers (Gonzalez et al, 2010; PwC, 2012) Anecdotal evidence collected during the field studies presented here provides support and insight into some of these theories.

This dissertation expands the assurance and audit technology literature by documenting the approaches taken by internal auditors to enhance their audit plans. It

also examines the technical feasibility of audit automation, remote auditing, and continuous auditing, and proposes generalized methodologies. Specifically, it addresses the following general overarching research objectives:

1. Determine the theoretical and practical extent of audit reengineering to incorporate continuous, automated, and remote procedures;
2. Understand the approaches auditors and researchers take to implement technology as part of internal audit reengineering; and
3. Develop a systematic framework for identifying opportunities for enhanced audit procedures.

Insight into these questions is documented in the work of auditors, researchers, and support staff at two firms as they actively attempt to implement some elements of automated, continuous, and remote auditing and assurance. The enhanced audit effort consists of identifying the source of data, analyzing opportunities in the existing audit plan, and identifying the types of procedures that are good candidates for automation, synchronization, and coordination. The resulting audit plan consists of a mix of traditional, periodic manual procedures and modern, continuous automated procedures.

In the scope of this research, internal auditors and managers are the primary beneficiaries of a reengineered audit. Internal auditors utilize technology to identify inefficiencies and error within their company's business processes, and management can identify opportunities to monitor and evaluate firm performance and any number of metrics. Thus internal auditors are likely to promote enhanced assurance as a way to

reduce audit cost and increase information value (Elliott, 2002). Auditing Standard No. 5 allows external auditors to become secondary beneficiaries, as they now can rely on the work of internal auditors and their systems while supplementing them with their own set of procedures. The procedures generated at the firm level allow the external auditors to take advantage of the benefits of continuous assurance while minimizing the risk of litigation they would face in the United States if they were to over-rely on advanced analytics and conduct full-population testing themselves.

The remainder of the dissertation is organized as follows. Chapter 2 documents the process of automating the IT audit within a highly formalized operating environment at a software division of Maritis Corporation. Chapters 3 and 4 record the process of enabling automated and remote audit procedures for the revenue cycle within the heterogeneous and highly manual environment of a large consumer goods firm. Chapter 5 joins the key insights from both field studies and provides a framework for identifying opportunities for an enhanced audit based a classification of audit evidence. (Hammer & Champy, 1993; Keenoy, 1958) presents the summary and conclusion section with discussion of the implications of this process.

Summary of Research Sites

The field studies presented in this dissertation are based on extensive documentation related to the audit plan, access to internal auditors, and audit output from the manual IT audit performed at a division of Maritis Corporation, and the periodic order-to-cash audit at Nouant Company. Both companies are considered leaders in technology acceptance and use.

Maritis Product Lifecycle Management

The internal IT auditors at Maritis selected a recently acquired division for implementation of a continuous monitoring platform. Product Lifecycle Management, like most of the other Maritis divisions, runs SAP for production services, human resources, and customer relationship management, and has similar controls settings. The automation project allowed auditors to give their initial evaluation of the newly adopted controls settings mandated from Maritis headquarters while providing the initial test and structure that would eventually guide implementation of a companywide monitoring solution.

In 2008, Maritis had approximately 70,000 employees, and generated $20 billion dollars in annual sales across a variety of business sectors in the United States. In the US, the IT Internal Audit department of Maritis Corporation provides IT audit services for each company division, including annual IT audits and system certifications. Maritis used SAP R/3 for its enterprise resource planning.

The implementation at Maritis' software division provides insight into challenges and features of using continuous monitoring software platforms available from third-party vendors to automate the existing internal audit plan. A byproduct of the automation process of particular interest to Maritis Corporation is the ability to take the automation concepts and rulebooks that were created parallel with the IT audit and apply them to other divisions that have similar systems and analogous audit and monitoring requirements. This section provides additional insight into practical application of CCM.

This case follows an initial pilot study on continuous monitoring of business process controls (CMBPC) presented in Alles et al (2006), which examines the feasibility of the underlying technology and methodology needed to automate auditing procedures. The authors conclude that while the existing audit procedures could be easily formalized and implemented into an online system, a certain degree of reengineering of the audit is necessary. This study provides an important benchmark for the proportion of auditing procedures that benefit from automation.

Nouant Company

This firm provides consumer goods globally. Expansion for the company comes in part from organic growth, but also through acquisition of other companies. Unlike Maritis, Nouant operates multiple heterogeneous information systems, due to legacy systems and systems integrated through acquisitions. Different geographic locations have different control objectives, and a large amount of evidence generated by the business processes is paper-based. The auditors are directed from corporate headquarters

The internal audit team rotates through each of the geographic divisions on an 18-24 month cycle. Most of the audit tasks related to the order-to-cash cycle are performed onsite. Enabling remote collection and analysis of the audit evidence would enable internal auditors to restructure their teams so that fewer auditors would need to travel to the division site while providing greater audit coverage and more frequent monitoring.

The internal auditors considered automation of their audit procedures as an exploration exercise that would allow them to identify opportunities for formalization and automation of their procedures. While initially focused on developing highly formalized controls within IT systems, they shifted their focus to enabling remote and automated audit procedures in the order-to-cash business cycle, which constitutes a significant portion of their internal audit effort.

CHAPTER 2. AUTOMATING THE IT AUDIT

Introduction

In May 2007, Maritis acquired a product lifecycle management software company for $3.5 billion to enhance their Automation and Drives group (Maritis, 2007). The acquisition was designed to expand Maritis' "technology leadership" across manufacturing and process industries as well as bring new leadership to Maritis. In the year following the acquisition, management at the new Maritis software division worked hard to integrate their systems and processes to meet the requirements of their new owner. This integration effort included harmonization of their SAP systems to comply with Maritis' controls. The first SAP certification audit (an IT and compliance audit) of Maritis' software division took place from January to March 2008. The director of IT audit for Maritis' US division at the time saw audit this as a good opportunity to build and test a series of automated audit tests, with the expectation that those tests would become part of a continuous monitoring program for Maritis globally.

This study identifies the characteristics and features of the large-scale automation of Maritis' SAP certification audit and proposes a framework for attempts by similar large, highly formalized enterprises. The results of this study provide evidence that supports the assertion that automation greatly reduces audit effort subsequent to implementation, provides more frequent and continuous monitoring capabilities, and exposes some of the control weaknesses inherent in enterprise resource planning (ERP) systems.

The design and implementation of automated procedures presented in this paper build upon a pilot study (Alles et al, 2006). In that study, researchers formalize a sample of 12 audit action sheets (representing 5% of the population) from Maritis' SAP certification audit and develop scripts for automated equivalents that monitor those controls and notify the internal auditors promptly following a control failure. This paper expands that study to include the population of 368 audit action sheets from Maritis' SAP certification audit, provides classification of those tests, and documents the creation and testing of an automated rule book using commercially available monitoring software.

While this paper focuses on the automation effort within a single division of Maritis, the majority of Maritis' divisions run SAP with a similar set of business processes and internal controls. This allows for scalability and transferability of the implementation process and formalized rules detailed here to other divisions within the organization with minimal effort. This was one of the stated goals of Maritis management and auditors. The project validates the technical feasibility of audit automation. However, the subsequent failure to expand the specific automation program to other divisions of the company emphasizes the significant political and legal hurdles that large-scale audit automation projects face despite the suitability of the technology.

This essay is arranged in four remaining sections. In the first section, the theory behind internal controls within enterprise systems and automation of auditing procedures is introduced. A review automation literature identifies the primary candidates for formalization and examines the concepts of audit process latency and the

phenomenon of prolonged intense deterrence. In the second section, the research methodology and approach to the automation project are described. The third section introduces the context of the ERP certification audit at Maritis and the field study undertaken at the software division. The fourth section outlines the main findings of the study and its contribution to audit automation and continuous monitoring theory.

The observations and evidence presented in this field study confirm the hypothesis proposed by Alles et al (2008a) that the majority of the firm's existing IT audit procedures are convertible into automated continuous monitoring tasks. It also proposes that auditor expertise and feedback from a concurrent manual audit provide the necessary measures of quality and validity of the automated procedures. Finally, the study emphasizes the need for more formalized and simplified audit plans.

Theoretical Background

Audit automation is the process of formalizing manual audit procedures and adopting tools and techniques that generate support for management assertions. Demand for automated audit procedures has been driven by the push by large enterprises to automate general business processes (Hammer & Champy, 1993; Keenoy, 1958) and realign auditor expertise (Coderre, 2008; Janvrin et al., 2008a). As advances in technology allow accounting information systems to provide real-time financial data, the demand by management to evaluate risks and resolve controls weaknesses as they happen, rather than solely at periodic intervals, has led to the development of robust continuous controls monitoring (CCM) platforms and tools (Alles, Kogan, Vasarhelyi, & Wu, 2010b; Brewster, Gal, Rosen, & Zubenko, 2007; Brown et al., 2007).

When implemented and functioning properly, CCM "can enhance the efficiency and effectiveness of the whole internal control system" (COSO, 2009). Additionally, in the model proposed by Alles et al (2004), CCM plays an important part of continuous assurance, providing the tools necessary for evaluation of business process effectiveness. External auditors also benefit from CCM as they may rely on the output of CCM systems to provide evidence for their own audits, as permitted by Auditing Standard 5 (PCAOB, 2007).

Internal controls in enterprise systems

Audit automation builds on the audit of existing controls within an ERP system. The internal controls employed by enterprises, such as Maritis, include policies and procedures that are designed to provide management with reasonable assurance that the objectives and goals of the company are met. More specifically, the internal controls over enterprise data provide assurance that master data and transaction records within the enterprise system represent actual economic events, were created and maintained by authorized users, and have not been recorded erroneously or fraudulently manipulated. Within this system, controls are also designed to prevent users from accessing unauthorized forms or tables by granting limited access to only the functions needed by each user, keep user activity within predefined limits, ensure that data are input correctly, prevent unauthorized changes to the system configuration and settings, etc. Properly designed and functioning controls help ensure high quality enterprise data and provide accurate reporting and information to decision makers. Some common internal controls for enterprise systems are presented in Table 2.1.

Table 2.1: Common SAP controls

Control Type	Description
Authorization	Identify authorized users within the system; block unauthorized users from performing functions.
Separation of duties	Assign users to specific roles; prevent users from accessing related conflicting functions.
Configuration	Static settings within the ERP that require logs
Transaction	Limit acceptable values to specified ranges.
User Activity Insight	Log user workflows; monitoring for prohibited transactions
Baseline	Compare subsequent values to previously recorded values.
Manual	Documentation; interviews; processes

Authorization controls restrict user activity within the ERP system. System-defined access control ensures that users are given authority to perform certain transactions and reports while restricting access to others. An authorization matrix lists each of the user roles available and what each role can do, including read, write, and update functions. Users are assigned to these limited roles in order to perform their job function. Properly functioning access controls prevent users from committing common types of fraud, such as creating fake vendors and approving payment of invoices to those vendors. See Table 2.3 for examples of thee controls at Maritis.

Because of the large risk associated with unauthorized users, a large portion of the IT audit effort is used to ensure that access controls are not circumvented. These controls tests function by validating specific users' ability to access certain functions. More robust versions of these tests can evaluate user behavior, analyze audit logs, and identify access from multiple locations.

Authorization tests verify which users currently have access to certain functions or screens in the ERP system. In results from these tests it is normal to see an appropriate

number of users, based on their roles in the system. For example, a rule is created to see which users have authorization to maintain customer master data, checking any of a series of transaction codes in SAP, such as XD01 (create customer), and create and edit attributes, such as activity 01 and 02.

Likewise, *Separation of Duties* controls ensure that users don't have access to simultaneously create and update records, according to company policies. For example, a user should not be able to create a purchase order and have permission to approve that order within the system. Separation of duties tests evaluate the user roles table for conflicting authorizations.

Configuration controls are generally binary settings that enable logging of activity and availability or restriction of features within the system. Tests for configuration controls often query the system to validate those binary settings (e.g. on or off, checked or unchecked) that reflect the firm's policies. For example, checking that the production client is locked to changes (In SAP, Table T000 contains the client configuration, the value in field CCCORACTIV should be set to 2 to indicate locked status).

Transaction controls limit the data that can be recorded within the system. For example, orders would not be allowed before a customer's credit was verified. Transaction tests are applied to see if the data are appropriate and also to check the distribution of transaction items. For example, a transaction test may verify that one-time customers have an "X" in a specific field. Transactional tests may require verification as to what transactions are normal and expected for a particular function.

User activity insight controls ensure that users follow workflows in their proper order. These should identify whether prerequisites exist and generate logs with timestamps that may be audited for compliance. Tests check for timeliness and correctness of ERP functions. UAI tests generate reports for user activity that is suspicious or prohibited, such as attempts to access restricted functions within the system.

Baseline controls provide a snapshot, hash, or predicted value for certain data values, such as a company code or controlling area value. Baseline tests compare actual values to expected values and report mismatched values.

Manual controls consist of the procedures and documentation that are in place to ensure employees follow their prescribed jobs. To test manual controls, auditors conduct interviews and review documentation to verify that outlined procedures are adhered to. The hands-on nature of these tests restricts them from formalization and automation, although decision support systems are generally available to aid the testing process and aid auditor judgment. The size and complexity of ERP systems warrants extensive use of automated internal controls within those systems.

Audit automation

Despite advances in data access and analytical procedures available to auditors, audit processes remain highly manual labor intensive. This was observed Vasarhelyi (1983) and most advances in practice continue in this state. The most visible changes to computerized auditing in practice appear in the form of decision support systems (Dowling & Leech, 2007; Turban, Sharda, & Delen, 2010), XBRL and data tagging (Bonsón,

Cortijo, & Escobar, 2009; Brown et al., 2007; Debreceny & Gray, 2001), and computer-assisted auditing techniques (CAATs) (Sayana & CISA, 2004; Braun & Davis, 2003; Coderre, 2005). Many of these tools continue to be used in conjunction with the periodic audit.

By its very nature, an IT audit evaluates data that exists within the ERP system. It evaluates users' attempts to access databases and reports, validates the configuration settings, and tests audit logs for other behavior. The majority of the data queried and compared in the IT audit resides in digital form that is automatically generated whenever a specific event takes place. This data is typically maintained on remote servers and is updated constantly. Auditing procedures should identify the specific data points to be audited, defining acceptable or unacceptable parameters to evaluate, and generating evidence for the auditors.

A typical audit plan will consist of a series of well-documented procedures that direct the auditors to perform some tasks step-by-step. Because humans perform these procedures, each step identifies audit objectives, tools to use, data to collect, and observations to record. Automation and reengineering of the IT audit consists of extracting the steps that can be formalized and translated into generalized non-interactive computer-readable models.

For example, in a typical manual separation of duties procedure an auditor would query a list of users within the ERP system and a copy of the authorization matrix, select a sample of 25 users and validate that each of those users can either access the form to

add or create a purchase order (transaction code ME25, action 01 in SAP), the form to release or approve a purchase order (ME28, action 02) or neither.

One common method for generating audit alarms is through the use of rule-based expert systems. In highly formalized systems, these rules correspond with the steps outlined in the audit plan. Generally, these steps tell the auditor what data to collect and may aid in the decision-making process. The process described in the previous paragraph could be formalized into a simple rule-based mechanism such as this:

IF user IS active AND can execute t-code ME25/01 AND user can execute t-code ME28/02 THEN generate audit alarm

This means that if the user is authorized to execute both transactions (ME25/01 and ME28/02) then the separation of duties internal control is weak and the auditors should investigate, assuming this represents a significant risk. The formalized procedure actually follows a series of questions in the algorithm, simplified below, and will continue until it receives a false response.

1. Is the user active in the system?
2. Can the user execute ME25/01?
3. Can the user execute ME28/02?
4. Generate alarm.

If this rule were input into a spreadsheet, this algorithm would be translated into the following If…Then function:

=IF(USER.ACTIVE=TRUE,(ME25/01.EXECUTE=TRUE,(ME28/02.EXECUTE=TRUE,ALARM,END),END),END)

In a monitoring system, each user's authorization schema would automatically pass through this and other rules and only those users who meet all of the criteria would have an alarm generated. The low complexity and high processing speed of the monitoring system would be able to evaluate the entire population of user records in a few moments. The auditors could then focus their effort on following up on specific exceptions rather than spending time manually checking a small sample.

Audit procedures that have been formalized and automated in online systems provide auditors with greater flexibility in formulating and executing their audit plans. The very nature of online systems allows the data to be portable and accessible from any network-connected device. Auditors have the choice to execute the automated procedures on demand and then process results from a specific point in time or to place the procedure into a system that will automatically execute the procedures at specific intervals on a continuous basis.

Continuous controls monitoring

Continuous monitoring favors the latter approach. With CCM, internal controls are evaluated on a daily, weekly, monthly, or lengthier basis, depending on the timing of data changes. A control state that should constantly have one value might be evaluated daily to ensure that the controls aren't modified. CCM becomes a tool for three major stakeholders. These include internal auditors, management, and external auditors. Internal auditors will use these tools obviously to supplement their audit plans. This changes the dynamic of their work by allowing them to focus their cyclical audit on the manual procedures, while keeping an eye open for control failures.

Management already monitors multiple streams of enterprise data as they track sales performance and other financial and non-financial measures. By incorporated continuous controls monitoring to their toolset, management can provide an additional level of assurance that their systems are functioning properly. Control failure can be brought to the attention of management more quickly and directly, ensuring that the control is fixed in a more timely fashion.

To take advantage of the audit innovation that is typically initiated by the internal auditors, the PCAOB adopted Auditing Standard 5, which provides guidance on the audit of management's assessment and tests of effectiveness of internal controls over financial reporting (PCAOB, 2007). It also identifies audit procedures performed by internal auditors that external auditors can rely on in an effort to minimize redundancy (Sections 16-19). Because of this specification, external auditors also benefit from internally generated monitoring programs as they minimize the work needed to directly test the controls and increase coverage.

Data

The audit automation project at Maritis' software division occurred from December 2007 to March 2008. Preliminary background and proof-of-concept work was completed prior to December 2007 and is documented in Alles et al (2008a). The automation project was designed to monitor the systems themselves (or a data warehouse equivalent) for changes in controls and build the analytics directly into the monitoring system. This would increase audit confidence, reduce the effort and duplication

problems, and allow the auditors to conduct an intensive manual audit less frequently than the 12-18 month rotation.

At Maritis' software division, a team of three researchers and two internal auditors, working alongside two principal internal IT auditors from Maritis Corporation who were conducting the manual IT audit, created and implemented rules and reports that would be used to perform CCM at software division. Once again, the objective of Maritis Corporation was not only to provide CCM for the software company they had acquired one-year prior, but also to create a universally-adaptable set of rules and control tests that could aid future audits and be easily implemented at other subsidiaries and divisions of the company.

Throughout the automation process researchers retained e-mail exchanges with the auditors and IT staff, collected source documents, and maintained a spreadsheet documenting the progressive implementation. The data collected includes the complete SAP certification audit plan and decision aids as well as extracts of the source code of the completed rule in XML format. The initial and subsequent classification, attributes, and comments were captured in a series of spreadsheets that document the automation process observations. This documentation includes the following:

SAP certification audit plan: The audit plan was comprised of audit action sheets (AASs) containing 284 IT controls, illustrated in Figure 2.1. Each AAS was organized by audit field matching a SAP module (e.g. Basis), and audit area containing a risk area (e.g. user authentication), and an audit task (e.g. system parameters for SAP). Additionally, each AAS is given a priority level of Low, Medium, or High and a subjective auditor rating

score from 0-4. The body of the AAS contains step-by-step procedures that the auditors follow in performing the audit tests and provide a more verbose description of the control objective and audit risk. Importantly, the AASs detail specific tables, fields, and reports within SAP that auditors should evaluate to determine their rating. The audit plan provides the base for the automated rules. These tests were developed with the help of a large public accounting firm. The controls cover seven SAP modules, which were designed to match Maritis' business cycles. Of those controls, approximately 24% tested user authorization within SAP, as shown in Table 2.2.

Figure 2.1: Sample audit action sheet

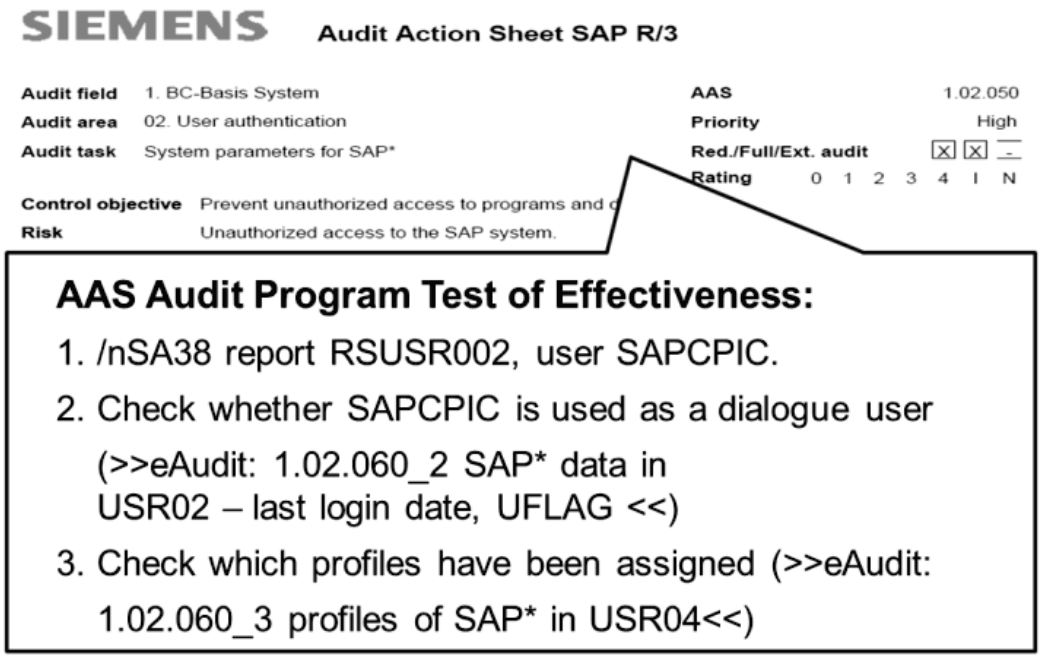


Table 2.2: Breakdown of IT audit control tests at Maritis

Module	Total Controls	Authorizations Controls	Business Process Controls
Basis System (BC)	104	20	84
Financial Accounting (FI)	55	8	47
Asset Accounting (AA)	26	4	22
Sales and Distribution (SD)	21	5	16
Materials Management (MM)	32	8	24
Project System (PS)	32	9	23
Human Resources (HR)	14	14	N/A
Total	284	68	216

Audit working papers: As the auditors completed the tasks outlined in the AASs, they would extract and compile evidence of functioning and failing controls. These extractions were generally raw spreadsheet files pulled from SAP and filtered using standard audit software. The audit working papers also included the notes and scores assigned by the auditors for each AAS. The filtered files were used as a benchmark for comparing the automated tests.

Project log: At the beginning of the project, a spreadsheet file was maintained to capture critical values from the AASs, illustrated in Table 2.3. The project log included a reference to the original AAS, a control classification and a short description extracted from the audit area of the AAS. A description of the automated rule to be created was then compiled outlining transaction codes, tables, fields, and expected values in SAP. The conditions and additional parameters used in the original test were also extracted

Table 2.3: Project log sample from Maritis' audit action sheets

AAS Ref #	Control Type	Short Description	Description of rule to be created	Conditions used	Status
1.02.X	Authorization	Unauthorized access to SAP system – emergency user concept	Test these authorizations: 1. S_TCODE=SM18, S_ADMIN_FCD=AUDA 2. …	AI rules	Rule Built 1.02.X
1.02.X	Configuration	System admin/completeness verification	Set up 3 rules to test the following: 1. parameter rdisp/vbdelete=0 2. parameter rdisp/vbreorg=0 3. …	Parameters are listed in report RSPFPAR	Rule Built 1.02.X
5.06.X	Separation of Duties	Particular authorizations in SAP are only granted to appropriate personnel - Posting and master data maintenance authorization	Maintain conditions, invoices, and central data	V_KONH_VKS Act 01 OR 02; V_VBRK_FKA Act 01 OR 19;…	Rule Built 5.06.X
5.04.X	Transaction	Use of one time customers	Look in vendor rule set for one time customers	Table KNA1 and Field Name XCPDX. Value equaling "X" indicated one time customer	Rule Built 1.02.X
7.01.X	User Activity Insight	Report Analysis	Determine the reports available, the frequency of use, and whether the reports contain all the necessary information in order to manage projects.	Reports used (t-code used for each report): 1. Y_D01_1400014X - CSS Proj Fin Related Info GRP Currency 2….	Rule Built 7.01.X
7.20.X	Baseline	Project profiles	Configure the system to provide a notification if any changes are made to existing project profiles, or if new project profiles are created, or existing ones are deleted.	Table TCJ4X Baseline	Rule Built 7.20.X
1.02.X	Manual	System parameters for SAP*	Involves interviews and understanding. Interviewing the company, determining how passwords are assigned, etc. are manual and must still be performed.	N/A	N/A No rule required

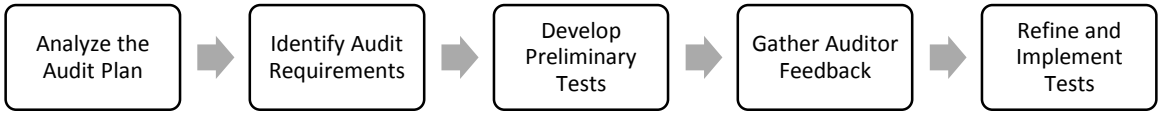
from the AAS. Finally, the log included comments from members of the audit and research team and rule status. The project log was updated daily to reflect progress made in the automation of the original rules.

E-mail exchanges: Throughout the project, e-mail was the primary tool used for communicating between the researchers and the auditors and IT staff. This was necessary because the researchers were on site only part of the time. These e-mail exchanges typically included requests, questions, concerns and additional insight.

Method and Implementation

The researchers played an active role in the development and implementation of the automated audit methodology and rules alongside the internal auditors. This section provides details about the data collected and the process followed to classify and design automated audit rules. The audit automation process consisted of five primary steps, shown in Figure 2.2 and discussed in depth in this section.

Figure 2.2: Method for developing automated auditing procedures



Analyze the audit plan and identify audit requirements

Prior to and during the implementation of the CCM rulebooks, an evaluation was conducted to determine which audit processes found in the AASs could be formalized and automated (see Alles et al., 2006). This was a particularly involved process for the automation team as some processes lent themselves to simple formalization, while others were not straightforward. A spreadsheet was maintained that identified each

audit requirement and had comments as to whether it was automatable and what needed to be done to create a rule for that requirement. This evaluation was important to identifying trivial automation concepts, partially automatable tests, rules requiring a degree of reengineering, and non-formalizable manual tests. Tests used in the Maritis audit program generally fit into one or more of the following categories: authorization, configuration, separation of duties, transaction, user activity insight, baseline, or manual.

Develop preliminary tests based on the existing audit plan

The controls tests that were already highly formalized were analyzed first. These tests included authorization, configuration, separation of duties and UAI tests. Using the CCM platform's Web interface, creating these rules required selecting transactions from pull-down menus and entering values to be checked in the text boxes that appeared. In the system, rules were assigned numbers and names corresponding to the objectives found on the audit action sheet. Rules were also grouped into "rulebooks" based on the module they were part of. Once all of the rules for a module were completed, the entire rulebook would be executed and the results would be compared to the results from the manual audit.

More complex controls tests would be evaluated and, in most cases, partially automated. Baseline rules, for example, were created using the vendor's add-on tools, because the CCM platform didn't provide automatic functionality for this type of rule. A number of the controls tests in the program were duplicated in other modules. In these

cases, it was not necessary to recreate additional rules, but to identify the existing rule on the AAS so that the auditors could test it.

At the request of the Maritis IT auditors, descriptions of the rules were also added, based on the description of the audit requirement outlined on the AAS. This provided the auditors with an easy way to identify which functions the rules were testing so they could minimize their own report creation. For convenience in adding the descriptions, rules created in the CCM platform were exported and converted to a spreadsheet file. This made adding additional attributes significantly easier than clicking through each rule a number of times in the Web interface.

Identifying all of the related tables and transaction codes posed a challenge to creating rules within the CCM platform. For example, some of the objectives on an AAS would identify a transaction code for a form that was accessed using a different code within the company. As a result, the original transaction code would not show any user instances, but a different transaction code would at this particular site. The rules, therefore, were adapted to look for both transactions.

Gather auditor feedback

Throughout the automation process, the research team continuously evaluated the audit action sheets to see if they could be effectively automated, reengineered, and whether they applied to the IT audit. Once all of the tests were formalized in a module, the research team created the monitoring rules and tested them on exported sample data. Reports showing results from the automated rule were then checked against the

manual evaluation results provided by the Maritis auditors. This process provided insight into the reliability and performance of the rules in detecting anomalies.

In the cases where the automated results and manual results did not match, the research team re-evaluated the rules, made necessary changes and the re-tested the new rulebook. In many cases, the research team spent significant time troubleshooting the rule, platform, and settings to discover why results were inconsistent. This was also helpful in determining limitations in the platform itself and providing feedback to the vendor.

Due to the importance of this implementation, support staff from the CCM platform vendor worked directly with the audit team on multiple occasions to provide training and workarounds for many of the custom rules. Based on the auditors' feedback, the research team sent platform feedback on these limitations to the developers to be addressed into future releases of the software. In many cases, however, unaddressed bugs prevented rule creation until the new update was released. These instances of incomplete software became a source of frustration for the audit team.

Refine and implement tests

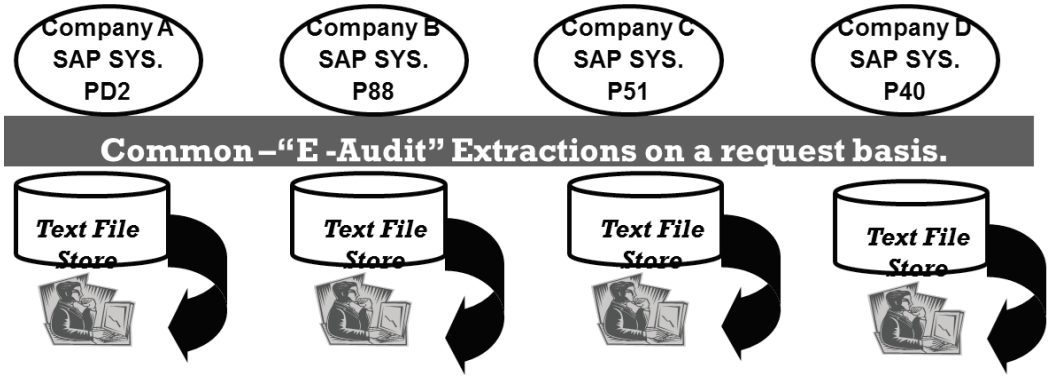
At the beginning of the automation process, the research team focused its efforts on the easily automatable objectives. Once those rules were created and tested, work shifted to reengineering of controls tests. Reengineering was essential to shift the focus from subjective controls tests that require auditor interpretation to objective tests that can be automated and produce reports that are useful to management. For example, a manual control may look like this: "Gain an understanding of X process. Verify Y function

isn't allowed." The team would build a rule for the second half of the test based on a manual investigation of the first part of the test.

Subsequently, the research team evaluated each of the "manual" tests for possible automation. In some cases existing rules provided the validation necessary. In other cases, limitations in the CCM platform would allow a rule to be created but the results would not be correct, so the rule was scrapped. The status of each rule was then updated in the spreadsheet. By the end of the automation project, the research team had compiled a complete list of automated and manual rules for each module from that spreadsheet.

Maritis previous audit program included "E-Audit" procedures, which required auditors to make specific data extraction requests from the IT manager at each of the divisions it visited. As illustrated in Figure 2.3, a set of text files was generated for each SAP instance and stored locally on the auditor's computer. The auditor would then complete a series of analyses on the extracted data and form their opinion on compliance, etc. The auditors indicated that this task as "tedious" and caused significant data duplication.

Figure 2.3: Maritis' previous SAP audit model



Install the monitoring platform

Software vendors have emerged and developed solutions to make it easier to create rules that perform the tests. These platforms provide user-friendly interfaces for tools that perform complex SQL database queries. Development by these third-party vendors has also been limited as large public accounting firms restrict the use of outsourced controls monitoring. While many large accounting firms develop CCM platforms and solutions internally, these solutions cannot be sourced to audit clients, but are often sold to non-audit clients and many of the third-party vendors directly (Alles, 2006).

Internally developed legacy auditing tools (Maritis uses a tool called E-Audit) may work well in aiding the periodic audit, but are not designed to take advantage of the real-time environment. Some automated tools created by academic researchers suffer from performance issues (see Alles et al., 2006). Thus, choosing a monitoring platform that can handle CCM and provide the analytics that match the audit program is essential.

Maritis auditors looked for CCM tools and platforms that could be used to analyze large snapshot databases of the current ERP system. These tools function as part of a monitoring and control layer as performance and access considerations limit access to the production server (see Alles et al., 2004). While most vendors tout their benefits of regulatory compliance and fraud detection, these tools vary in their applicability and implementation of CCM. Current tools and platform can be classified into three types: system-specific, modular and mapping, and custom. These systems tend to be

distributed, intermediate, monitoring and control layer platforms (see Alles, Kogan, & Vasarhelyi, 2010a) and rely on data warehouses, which contain periodic (generally daily) snapshots of the enterprise data.

System-specific platforms provide comprehensive analysis of controls based on specific systems, such as SAP. These tools translate codes and tables from specific systems into a user-friendly interface that allows creation of system-specific rules for control checks. Rules created with these platforms can only be used on the systems for which they were created. While these tools are helpful in homogenous ERP environments, distinct instances and rules must be created for heterogeneous systems.

Modular and mapping platforms provide different CCM modules for business processes that meet specific business control objectives. Modules may follow supply chain cycles, such as Procure-to-Pay or Order-to-Cash. These monitoring platforms check for standard controls, based on widely accepted risk frameworks, such as the one provided by COSO (1992). These modules are standardized to evaluate control objectives across different systems and data stores. By mapping existing systems to a common data model, universal rules and analyses are performed on the system. Custom libraries can also be developed, but they are generally platform-independent. In some cases, ERP vendors incorporate limited monitoring modules into newer releases of their systems.

Custom platforms, such as Maritis' E-Audit, are typically developed in-house to meet specific controls objectives. Consulting firms may provide planning, implementation, and deployment of custom solutions. These platforms are particularly

useful in environments where the ERP system is hybrid and requires a great deal of customization to allow sufficient control risk assessment.

A default installation of each of the different platforms provides the ability to create generic controls tests that can be applied to existing transactions. Because of the focus by vendors on SOX 404 compliance and the COSO control risk framework, many of these solutions provide monitoring functionality in the form of alarms and generic reports.

After the tests from the AASs were classified and identified and manual or automatable, creating the actual rules in the CCM platform was fairly straightforward. Prior to implementing CCM, Maritis auditors relied on their proprietary e-Audit tool to analyze some of some of the controls and return results corresponding to tests found on the AASs. While this tool was helpful during the periodic audits, it was not robust enough to continuously analyze thousands of transactions and report anomalies. The large-scale CCM implementation drew from the experiences in the pilot study, and an instance of the CCM platform was installed alongside the SAP R/3 production and human resources servers at Maritis' software division. The CCM server stored daily snapshots of the production and HR servers and allowed rule creation and report testing via a Web interface. Because the CCM platform used at software division is a monitoring and control layer, analytics run on the server had no impact on performance for the production servers.

Classification, installation, formalization and feedback

Before the CCM could be implemented, the audit requirements in the existing AASs were evaluated and classified into degrees of automation, defined in the next section.

Later, creation of automated rulebooks based on those requirements, and reengineering manual controls into automatable controls was performed. Throughout the entire process, feedback was solicited from management, the auditors, and other researchers so that the rules created would produce reliable and accurate results.

At the time of this study, the IT audit (also known as an ERP certification audit) at Maritis was performed periodically to provide risk assessment and test the controls of ERP systems, such as SAP, Oracle, and other hybrid or legacy systems. The IT audit specifically tests controls that exist in the current business processes for the firm. Alles et al (2006) determine in a CCM pilot that approximately 50% of the controls tests in their IT audit program are automatable with little or no alteration of the existing audit plan. An additional 25% of the tests have potential to be normalized and audited, but require significant reengineering in order to verify the functionality of the controls. Using the existing audit program as a base, experienced auditors can prioritize controls risks and directly test the CCM rules against typical and expected results from the periodic IT audit.

Where an IT audit may require evaluation of division- or company-specific transaction codes that must be explicitly evaluated, some automation tools provide support for variables and parameter lists, which can be used to create “generic” rules for use across multiple divisions or companies. When the rules are implemented elsewhere, the auditor need only enter the company-specific values into the parameter lists. While convenient, these parameter lists are a source of potential control weakness themselves.

In addition to preset mapping of common ERP tables and codes and standard controls tests, many automation tools allow for customization. Some software vendors provide add-on tools that allow auditors greater ability to create customized controls that are more complex and/or specific to the firm's needs. This customization ability can extend the system to scale the CCM platform over multiple systems and aid in the control test reengineering process.

A significant issue that faces off-the-shelf software solutions is limitations and bugs are released with each version. Even with open source solutions, programmers may not be able to anticipate all of the scenarios that a client may face. Incompleteness may include missing functionality, which will not allow full automation of an audit plan. Most current software platforms suffer from incompleteness and minor, yet significant, deficiencies in functionality, which were observed during this study. As more firms implement these software platforms, many of these flaws are being discovered, giving vendors an opportunity to address these issues in future revisions of their respective platforms.

In addition to platform limitations, current audit plans are ultimately subject to non-formalized tests, such as auditor interpretation. As a result, sets of rules may not supply sufficient information for an automatic control evaluation without significant reengineering of the audit plan itself. For example, with Maritis' audit plan, evaluation of the AASs was provided with a value on an ordinal scale of 0-2. While 0 and 4 could be easily evaluated based on some threshold limit or other easily identifiable indicator,

determining intermediate values is more subjective. An altered audit plan would possibly require additional rules or a separate evaluation of multiple rules at once.

After the tests from the AASs were classified and identified and manual or automatable, creating the actual rules in the CCM platform was fairly straightforward. Prior to implementing CCM, Maritis auditors relied on a proprietary tool to analyze some of some of the controls and return results corresponding to tests found on the AASs. While this tool was helpful during the periodic audits, it was not robust enough to continuously analyze thousands of transactions and report anomalies. The large-scale CCM implementation drew from the experiences in the pilot study, and an instance of the CCM platform was installed alongside the SAP R/3 production and human resources servers at Maritis' software division. The CCM server stored daily snapshots of the production and HR servers and allowed rule creation and report testing via a Web interface. Because the CCM platform used at software division is a monitoring and control layer, analytics run on the server had negligible impact on performance for the production servers.

Figure 2.4: Sample rules in the monitoring platform's interface

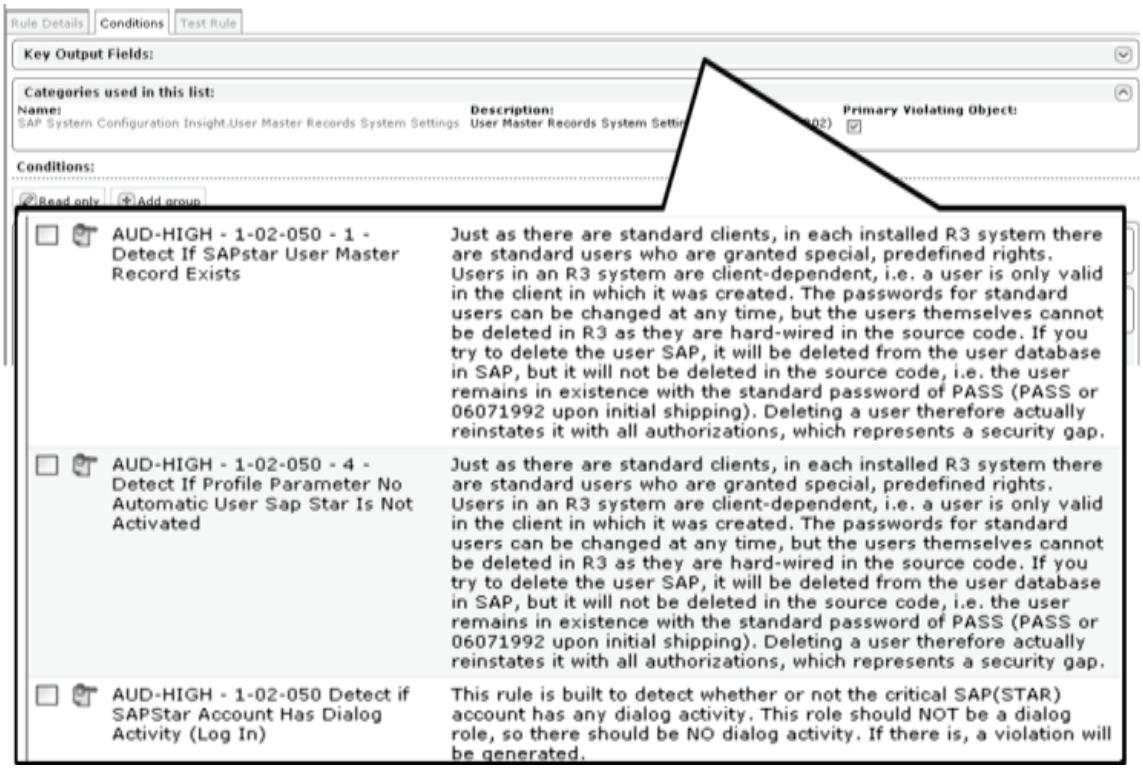
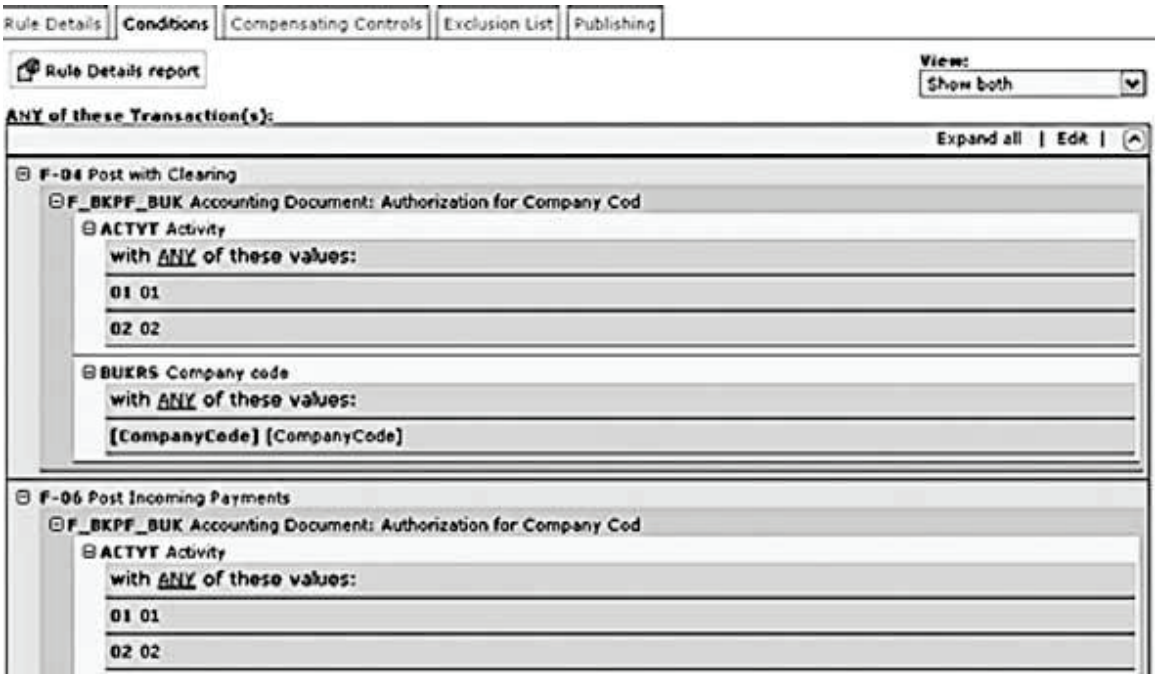


Figure 2.5: Sample from monitoring platform with fields and rules



Reengineering audit processes

For some of the audit tests, formalization of the existing audit process was not readily apparent. This was the case for rules that require manual verification of documentation, calculations, or authorizations. To monitor these controls, the auditors needed to determine whether there was some alternative or partial automated procedure that would proxy for the original rule. For example, to gain an understanding of one process, the auditor would verify that an alternative function is or isn't allowed. In some cases, the insight gathered from an existing test provided the necessary assurance that the control is functioning.

The monitoring platform allows the creation and scripting of custom rules that don't fall within the templates available within the system. Maritis' IT auditors worked with a consultant from the vendor to determine the additional scripts that could fill gaps in the monitoring coverage. These scripts were often combinations of existing control tests or partial automation of manual controls. For example, in order to gain an understanding of X process, the program would verify that Y function isn't allowed.

Results and Discussion

Of the 284 total controls, 180 were fully automated, as shown in Table 2.4 by SAP module. Controls over user authorization, which include checking for separation of duties and logical access to specific screens in the SAP system, were fully automated. These authorizations make up 23% of the total controls, and this result is consistent with Alles et al (2006), which showed that approximately 25% of the controls could be automated with little additional formalization needed.

Table 2.4: Results of the IT audit automation at Maritis

	Total	Authorizations		Business Process		
Module	Controls	Controls	Percent Automated	Controls	Percent Automated	Overall Percent Automated
Basis System (BC)	104	20	100%	84	44%	55%
Financial Accounting (FI)	55	8	100%	47	51%	58%
Asset Accounting (AA)	26	4	100%	22	64%	69%
Sales and Distribution (SD)	21	5	100%	16	50%	62%
Materials Management (MM)	32	8	100%	24	54%	66%
Project System (PS)	32	9	100%	23	70%	78%
Human Resources (HR)	14	14	100%	N/A	N/A	100%
Total	284	68	100%	216	52%	63%

Table 2.5: Audit action sheets targeted for automation.

Module	AAS Referenced	Manual Count	Manual %	Partial Count	Partial %	Full Count	Full %	Partial + Full	Partial + Full %
Basis System (BC)	23	1	4.3%	0	0.0%	22	95.7%	22	95.7%
Financial Accounting (FI)	39	13	33.3%	11	28.2%	15	38.5%	26	66.7%
Asset Accounting (AA)	17	6	35.3%	4	23.5%	7	41.2%	11	64.7%
Sales and Distribution (SD)	18	6	33.3%	4	22.2%	8	44.4%	12	66.7%
Materials Management (MM)	12	3	25.0%	3	25.0%	6	50.0%	9	75.0%
Project System (PS)	16	2	12.5%	0	0.0%	14	87.5%	14	87.5%
Human Resources (HR)	24	8	33.3%	5	20.8%	11	45.8%	16	66.7%
Total	**149**	**39**	**26.2%**	**27**	**18.1%**	**83**	**55.7%**	**110**	**73.8%**

These action sheets were targeted for automation based on manual analysis of the AASs. The research team looked for key elements including references to the SAP tables and fields, and key data manipulation words such as “analyze”, “verify”, “extract”, and “join”.

Of the 149 AASs referenced by the research team, 83 (55.7%) were fully automated with corresponding rules, 27 (18.1%) were partially automated where one or more steps had a corresponding rule but the remaining steps required manual intervention, and 39 (26.2%) could not be automated at all. Overall, 110 (73.8%) of the AASs were at least partially automated, as shown in Table 2.5.

Table 2.6: Rules created for the applicable tests in each module (excluding not-applicable and redundant tests)

Module	AAS Referenced	Total Tests	Applicable Tests	Applicable %	Rules Built	Test Automation Percentage
Basis System (BC)	23	62	30	48.4%	25	83.3%
Financial Accounting (FI)	39	79	66	83.5%	42	63.6%
Asset Accounting (AA)	17	47	45	95.7%	36	80.0%
Sales and Distribution (SD)	18	40	25	62.5%	23	92.0%
Materials Management (MM)	12	71	33	46.5%	33	100.0%
Project System (PS)	16	40	37	92.5%	24	64.9%
Human Resources (HR)	24	37	19	51.4%	19	100.0%
Total	**149**	**376**	**255**	**67.8%**	**202**	**79.2%**

Within Maritis' 149 AASs, there were 376 specific controls tests. Of these, 255 (67.8%) were applicable to the certification audit at software division, meaning they covered systems implemented at software division and were not duplicated within other modules. Of the 255 applicable tests, 202 (79.2%) were successfully translated into automated rules in the CCM platform. The auditors produced their final report on February 26, 2008. Their findings outlined each of the AASs that failed with an explanation of the reasons for failure (e.g. "AAS 1.03.090: 36 accounts are configured with SAP_ALL and SAP_NEW authorizations which is a strong violation of Maritis policies and guidelines."). The overall number of failed AASs resulted in an audit score that

determined whether the module passed (80 or above) or failed (below 80). By analyzing the failed AASs presented by the auditors, the researcher team determined that nearly half of violations could have been detected by the rules implemented in the CCM, as shown in Table 2.7 and detailed in Table 2.8.

Successes

As indicated previously, the rulebooks created during the IT audit at software division provided evidence for approximately 63% of the audit action sheets. Throughout the audit, alarms were set for most of the rules, providing one of the key benefits of CCM by allowing management to quickly see controls violations and instances. The IT auditors indicated that these rules produced sufficiently reliable output for the IT audit objectives. With some additional work in the future, these rulebooks can be refined and generalized even further so they can be used universally at other Maritis divisions. The auditors also need to work with management to determine the priority of each control and refine alarms to address the volume of alarms generated by the system.

It is yet to be seen if the cost savings identified by Alles et al (2006) will be realized as they predicted, but there the IT auditors felt that having the CCM rulebooks will significantly reduce the time required for their next IT audit. One of the key cost benefits expected by Maritis of the automated system was a reduction in the audit staff time and travel expense needed. While some of these savings are expected in the future, the auditors made an interesting observation. With the creation of rulebooks,

Table 2.7: Results from Maritis' first manual SAP certification audit (Feb 26, 2008)

Module	Audit score (out of 100)	AAS failed	Detected with rules	Percentage of failed AAS detected with rules
Basis System (BC)	64	27	7	25.9%
Financial Accounting (FI)	87	11	8	72.7%
Asset Accounting (AA)	92	4	1	25.0%
Sales and Distribution (SD)	82	7	4	57.1%
Materials Management (MM)	82	8	5	62.5%
Project System (PS)	99	1	0	0.0%
Human Resources (HR)	81	7	4	57.1%
Total		65	29	**44.6%**

Table 2.8: Analyzed auditor report, financial accounting module, emphasis added (Feb 26, 2008)

Violated Audit Action Sheet	Auditor Comments	Detectable by automated rule?
AAS 3.01.000:	A formal system customization and configuration documentation reflecting the current settings for the FI module was not observed.	No
AAS 3.01.000:	Company ICNA is not listed in the documentation of company codes	No
AAS 3.01.010:	**Entries for business areas (table TGSB) and functional areas (table TFKB) are not current and/or consistent.**	**Yes**
AAS 3.02.000:	**SAP report SAPF190 is not used for monthly closing as outlined in the AAS.**	**Yes**
AAS 3.02.010:	**SAP reconciliation reports RFHABU00, RFSSLD00, RFKSLD00, and RFDSLD00 are not used for month-end closing as outlined in the AAS.**	**Yes**
AAS 3.02.020:	**SAP reconciliation report SAPF070 is not used for month-end closing as outlined in the AAS.**	**Yes**
AAS 3.02.080:	**Year-end reclassification of debit balances in A/P and credit balances in A/R is not done via build-in functionality in SAP.**	**Yes**
AAS 3.02.120:	Formal documentation reflecting the software division specific processes/activities for monthly uploading of financial data to ESPRIT with a clear definition of roles and responsibilities not observed.	No
AAS 3.03.010:	**Changes to tables T030E and T030HB are not logged**	**Yes**
AAS 3.06.040:	**Special G/L Analysis for CoCd 5000 via OBL4 reports errors**	**Yes**
AAS 3.09.000:	**GR/IR account (account 2001) not set to allow only automatic postings**	**Yes**
AAS 3.11.060:	Authorization checks/reports for FI contain a large number of batch, communication and service user accounts. The accounts in question also violate SoD requirements.	No
RESULT	PASSED (87%)	

they argued that there would be a shift from an audit of the controls via querying and transaction testing to an audit of the rules themselves. The cost savings, therefore, may be as significant as previously predicted as the audit effort is redirected, rather than simply reduced.

Challenges

Most of the challenges that were identified along the course of the CCM implementation at Maritis' software division can be classified into three main issues: audit priority, platform bugs, and properly functioning basic controls. As the research team developed and implemented the CCM rules, the main priority of the IT auditors was to complete the audit of software division's systems. Because of this focus, some rules that were not applicable to the site were ignored by the auditors and not given adequate attention due in part to the time constraints on the actual audit. These rules will need to be developed at a later time for other sites that deal with applicable line items, such as physical inventory, which have specific controls to be tested.

One of the primary challenges that existed as the research team worked alongside the IT audit turned out to be bugs in the CCM platform itself. For example, when results from one rule were compared to the manual results of the auditors, users who were locked and/or inactive in the company did not appear on the automated list. The response from the vendor was that that functionality had not been seen as a risk issue, but that the problem would be addressed in the next update to the software.

Many of the issues that were found in the software code had been identified as issues that would be resolved in the upcoming release. This brings up an important

concern with any implementation of CCM as well as the development cycle of the CCM platform. During the implementation, the client firm may either alter the audit plan to create workaround rules to adapt for the shortcomings or ignore rules altogether. When vendors release bug fixes or new platform versions, the changes may fundamentally alter the results of some CCM rules. When the time comes to audit the CCM tests themselves, it is likely that greater expense will be incurred to reevaluate rules affected by changes in the platform architecture. The differences in ERP installations across firms create a challenge for vendors to address all of the control issues across firms.

Multiple SAP tables used by software division were not available in the monitoring platform by default. This meant that the internal auditors had to work with the vendor to create 61 additional connections, across 11 separate requests, shown in Table 2.9.

Table 2.9: Requests for additional connections to SAP objects.

Module	Requests	Additional Tables/Objects Requested
Basis System (BC)	1	4
Financial Accounting (FI)	3	11
Asset Accounting (AA)	1	18
Sales and Distribution (SD)	2	6
Materials Management (MM)	2	15
Project System (PS)	2	7
Human Resources (HR)	0	0
Total	11	61

As mentioned previously in this chapter, identifying platform weaknesses and bugs required significant troubleshooting and verification with the vendor. Most were identified after automated and manual results were compared and rules were fine-tuned. Fortunately, the ability to compare results and receive feedback is a primary

benefit of implementing an effective CCM alongside the traditional IT audit. Such an issue is common in software implementing state-of-the-art process improvements. As classes of software mature, they are likely to become more reliable, bug-free, and easier to use.

Finally, functioning basic controls play an important part in successful implementation of continuous controls monitoring. From the controls and settings that must be observed manually, control failure in these areas leads to lack of support for the auditors and potentially failure of the audit itself. At the end of the implementation, the auditors discovered one control weakness that significantly impacted the reliability of the results of the audit, as well as many of the CCM rules the research team had created.

Time and resource commitments

For this implementation effort and research case, the research team consisted of two professors and two graduate students working part time, one full-time internal auditor, one audit manager, and one support person from the CCM platform vendor, who helped out on a needs basis for rule development and platform support. The research team worked alongside two full-time internal auditors, who were also brought on-site to conduct the manual IT audit. Cost considerations for Maritis included transportation and lodging for off-site researchers who worked part-time on the site, as well as salaries for those performing the audit and working on the CCM implementation.

The IT audit was performed in a little less than 70 days. Prior to the audit being performed, evaluation of the existing audit plan had been extensively conducted by the

IT audit head, three professors, and two doctoral students from Rutgers. The bulk of the evaluation had been conducted in the three months leading to the actual audit, although preliminary work preceded the audit by more than a year. Other resources included in the CCM project included support staff from the IT department at software division, two CCM platform installations (one for the production server and one for HR).

Additional observations

There were a number of attributes that made for a smooth implementation of the automated rulebooks. First, it was mentioned by one of the auditors that software and technology firms generally implement better tools and controls procedures from the get go because they have knowledgeable management, auditors, and IT developers.

One auditor noted that most companies acquired by Maritis fail the IT audit the first time around. This is partly due to differences in each firm's ERP systems and business processes going into the acquisition. For Maritis, software division was a particularly good candidate for passing the initial IT audit because it was heavily SAP-centric before the acquisition matched a significant number of controls similar to those at Maritis were already in place.

These firm characteristics are particularly relevant to the objectives of Maritis to create a comprehensive CCM and automated audit program. At the same time, the degree of success in implementing CCM at single-unit firms may be dependent on the amount of IT systems and support available.

Auditor contribution

As anticipated, the auditors working on the manual IT audit provided valuable feedback throughout the automation process. The research team ran into the same issue with human judgment and bias issues discussed by Alles et al (2010a). As mentioned in the previous section, the research team faced occasional challenges working with the IT auditors due to their audit priority and importance of particular controls. However when it came time to test the controls, they were very helpful in providing the necessary feedback for the research team to alter rules so they were more complete. Additionally, in comparing results the research team was able to discover limitations and bugs in the third-party monitoring platform.

Conclusion

Based on the experience at Maritis' software division and previous theoretical models presented in the literature, the IT audit proves to be a feasible starting point for implementation of CCM at a firm. This existing plan for an audit of business process controls provided by the IT audit, the feedback provide by experienced auditors, and real-time performance comparison and testing of automated controls tests contributed to the success of the implementation. These three elements facilitate the implementation of CCM, aid in creating a powerful tool for periodically evaluating internal controls, and potentially provide considerable cost and time savings for internal IT auditors.

The progress made in this project with Maritis reveals several of the key benefits of CCM as an aid to the audit itself and as a springboard for implementing a platform for

CCM. The implementation presented here is not, however, without weaknesses. Auditors' higher priority for the onsite audit, missing system functionality, and weak controls posed challenges to creating a complete set of rules that can be used throughout Maritis Corporation by the end of the audit. However, the bulk of the work has been completed and is functional for the installation at Maritis' software division. A revision of the rules to fit the broader scope of the corporation as a whole appears to be a worthwhile, yet potentially time-consuming process.

Although not evaluated in this study, weighting the automated rules may provide additional insight into controls effectiveness. Weighting has the potential to focus management on more important risks while not abandoning "lesser" weaknesses. The creation of a theoretical basis for attributing weights to controls and methods of control combination are very important issues that have been extensively examined in the literature using reliability theory and other methods (Cash, Bailey, & Whinston, 1977; Cushing, 1974; Vasarhelyi, 1980). These issues now with Sarbanes-Oxley Section 404 and this class of automation tools become crucial. This may also aid in the reengineering process by helping redefine, combine, or eliminate some manual controls checks.

From the audit perspective, evaluating the time investment required to perform the remaining tests would be valuable. One very important insight gained from this CCM implementation came at the very end of the audit. While the automated controls allowed the firm to take advantage of cost savings by limiting the number of audit engagements, there will very likely be a shift of focus from testing controls to evaluating the sets of rules used to test the controls. Additional audit requirements will be required

to evaluate authorization controls to the CCM platform, appropriate access, alteration of rules and reports, etc. Platforms that utilize parameter lists will have to be evaluated on a site-by-site basis to determine if the correct parameters are used. Alteration of these parameters can affect the outcome of the rules without requiring a change to the rule itself.

Future research into CCM and continuous audit implementation will provide additional insight, including an evaluation of the effectiveness of the revised IT audit program and a closer estimate of the amount of the cost savings realized. Of particular interest is the portion of cost savings that will be reallocated to evaluating and "auditing" the CCM platform itself.

CHAPTER 3. LIMITS TO AUDIT AUTOMATION IN MANUAL ENVIRONMENTS

Introduction

Firms spent a great deal of time and effort in incremental business process reengineering in the late 1990's and early 2000's that has allowed them to take advantage of vastly improved processing power and networked systems. While this change process has been more evolutionary than revolutionary (Hammer and Champy, 1993), the improved access to online systems and large amounts of enterprise data have presented opportunities for auditors to improve their procedures and provide better assurance for their stakeholders. Internal auditors, in particular, are tasked with improving the efficiency and effectiveness of their operational, information technology, and compliance audits as a way of adding value to the firm. In recent years, this has been accomplished through audit process reengineering and automation (Brown et al., 2007; Gupta, 2001; Manson, McCartney, & Sherer, 2001).

Recent documented audit automation projects found in academic and trade articles rely on proprietary expertise and anecdotal evidence and thus are difficult to generalize (Alles, Kogan, & Vasarhelyi, 2008b; Teeter, Brennan, Alles, & Vasarhelyi, 2008, Lombardi et al, 2012). This is primarily due to the customization of each firm's audit process and the variety of enterprise systems used. Even firms that claim to have standardized and homogenous enterprise resource planning systems often use those systems in unintended ways. Businesses that fundamentally rethink their business processes as they implement ERP systems are much more likely to have successful transitions whereas systems that are implemented without this radical rethinking are more likely to

fail or be implemented improperly (Karimi et al, 2007). This also affects business process reengineering where proprietary expertise is attributed to the researchers and practitioners in individual cases rather than developing a systematized strategy (Grover et al, 1995). The expectation for a “canned” or “structured” methodology to audit reengineering is problematic if the organization is unwilling to reflect on the fundamental changes that are necessary (Gupta, 2001, p. 61). The study presented in this essay continues this trend by reporting on the unique characteristics of a single company. However many firms experience similar obstacles to successful development and adoption of automated audit procedures. Indeed, many of the obstacles observed by Gupta (2001, p. 119) were present throughout this field study, including management skepticism, lack of clear vision, and technical challenges.

Recent research on successful automation efforts has also revealed a self-selection bias. Firms such as Maritis and Telecris possess highly formalized processes and access to large amounts of data within their centralized ERP systems (Alles et al, 2008; Teeter et al, 2008; Lombardi et al, 2012). Automation and other data analytics in these firms fit naturally with the strategic direction of the company's management and are supported by the streamlined information technology. Additionally, they demonstrate clear prerequisites to change management including clear objectives, management initiative, and system support (Grover et al, 1995).

Yet as with business process reengineering, many audit automation efforts fail and the results are not reported (Kuhn and Sutton, 2010). These failures tend to be the result of deviation from best practices for change management. Understanding the

reasons why these projects fail provides valuable insight, particularly as the number of automation and continuous auditing efforts is on the rise (PwC, 2012).

This essay investigates the failed attempt of researchers and internal auditors to develop and implement automated audit procedures at a multinational consumer goods firm. While auditor and researcher expectations were optimistic going into the project, they quickly became misaligned. Specifically, the automation process appeared to be only incremental to the auditors and management (who expect more radical change and thus view the impact as inconsequential), and the underlying systems and business processes didn't support the type of changes needed to enable effective automation. Analysis of this effort reveals these limitations and explains how systems and processes that are largely manual and heterogeneous create significant hurdles to audit automation efforts. It also elucidates the need for fundamental changes to the business processes that will benefit auditors and management alike.

The analysis of the limits to automation in this case provides insight into the following questions:

1. What prompts auditors to pursue automation projects?
2. What prevents successful adoption of automated auditing procedures?
3. How could these obstacles to audit reengineering be mitigated?

Answers to these questions should provide auditors and researchers with tempered expectations for automation efforts. Following a discussion of change management and process reengineering from existing literature, this essay presents a description of the proposed methodology for the automation project. Then, the exploration of the

successive failures of alternative approaches is documented. Finally, the paper concludes with commentary on the significant impediments to audit automation in general.

Drivers and Obstacles to Audit Reengineering

Gupta (2001, p.49) defines internal audit reengineering as:

> *Optimal restructuring* of the internal audit function to re-relevance its *core and support business processes* to help organizations achieve their *business objectives* in *risk intelligent* ways. [Emphasis from original]

Contrasting with Hammer and Champy's (1993) model for business process reengineering, Gupta indicates that reengineering of the internal audit function includes fundamental rethinking of the internal auditor's role, reestablishing the internal audit function's focus, adopting process-oriented approaches, redesigning the internal audit department's structure to promote innovation, and operating internal audit as a business itself rather than a support function (p.50). An internal audit department must continue to protect shareholder value (provide oversight) while also improving shareholder value (adding value to the organization) (Deloitte and Touche, 1998).

Enablers of internal audit reengineering include the perception of the internal audit function as a value-added partner, and senior audit management's vision and passion for reengineering (Gupta, 2001, p. 115). Information technology is an important enabler or reengineering, but not the only critical factor. Without development of an internal audit business model and strategic plan, significant improvement, let alone radical change, is unlikely to occur.

Significant obstacles also lead to many false starts in internal audit reengineering. In a survey of leading firms' audit reengineering efforts, Gupta (2001) finds that 66% of the respondents encountered serious obstacles that have very little to do with technical capability, including lack of management understanding (34%), resistance by internal audit staff (28%), and resistance by the senior internal audit manager or director (23%) (p. 119). Nearly half of those organizations (46%) faced three or more major obstacles to their reengineering efforts.

Reengineering business processes

In an ideal environment, business processes would exist that provide ready access to transactions, documentation, and other support that auditors could use to provide assurance that systems are functioning correctly and that minimize overall audit risk. In the real world, however, this is not generally the case. Even in highly formalized environments, existing business processes do not provide a complete set of data upon which auditors can rely.

In cases where data doesn't exist, auditors have an opportunity to work with management to develop and implement more formalized, reengineered systems. Business process reengineering requires managers to completely rethink and redesign the way business processes work so that the organization can improve performance measures, such as cost, quality of service, and speed (Hammer & Champy, 1993). However managers tend to resist or underestimate these changes. Reengineering project implementation tends to be more complex, lack support, and not be very well defined (Grover et al, 1995).

Earl et al (1995) identify a model for business process reengineering which requires an analysis of process, strategy, information systems, and change management and control. Each of these aspects of the business process reengineering effort adds a level of complexity that managers are unlikely to tackle if the outcome is adding a checkbox for auditors to monitor.

If business process reengineering is essential to enable audit automation, the internal auditors must frame the change not from the audit perspective, but rather from the business value side. For example, auditors must highlight business efficiencies gained through reengineering, such as reduced costs or increased timeliness, if they are to receive any support from management.

Audit process reengineering

Where audit tests are highly manual or data do not exist in the business supply chain, new audit procedures must be developed to enable an automated audit. Gupta (2001) identifies how reengineering affects the internal audit function generally:

- Fundamentally rethink the internal audit's role in the organization
- Reestablish the internal audit's focus
- Redesign the internal auditing processes to align them with the new role and focus
- Redesign the internal audit department's structure

In the audit automation process, it is more likely that auditors will encounter success by adapting their auditing tests to fit the existing business processes rather than the other way around. From a practical perspective, this means evaluating the

overarching goal of a specific audit test and developing some proxy measures that will verify that that audit objective is being met.

Audit process reengineering also results in audit efficiency by reducing latency, which occupies labor and capital (Hoitash, Kogan, Vasarhelyi, & Srivastava, 2006; M. A. Vasarhelyi et al., 2010). Latencies occur in all business processes, particularly the audit process. 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. A result of audit automation, latency reduction for any of these sub-processes can free up resources, especially auditor labor, to be utilized elsewhere.

Rather than preferring Hammer's "radical redesign of the processes," a survey by the Institute of Internal Auditors reveals that internal auditors think of internal audit reengineering as "the fundamental rethinking of internal audit's role in the organization in light of the organization's vision, mission, goals, and objectives" (Gupta, 2001, p. 179). In that same survey, the auditor management focuses on vision, opportunity, and threats as major drivers for change efforts, but feel their audit staff are often underprepared and inadequately trained in change management, knowledge of alternative business controls, familiarity with information technology, and risk management (p. 180). A combination of these elements leads to significant impediments to successful reengineering efforts.

Tradeoff

From the auditors' perspective, the most straightforward approach to audit automation begins with existing control tests. These control tests identify precise indicators or controls that auditors would evaluate in a completely manual audit. Where audit control tests are highly formalized, meaning they identify specific locations of data and testing criteria within some accessible digital system, and business processes automatically generate the data to be tested automation is relatively trivial and very little reengineering is needed on either the audit or business process side. On the other hand, where control tests rely on the collection and evaluation of manually generated data, such as paper documents, significant reengineering of that data generation on the business process side is required if the audit test is essential and inflexible. This business process reengineering may include the addition of an e-filing system for paper documents or direct data entry into an ERP system.

In most cases, the audit test is not necessarily as rigid and important as the overarching control activity, particularly if the business process providing the data cannot be altered. For control tests that cannot be automated outright, an auditor would evaluate the control activity and determine if a modified test would provide similar assurance or if a complete revamp is necessary.

In cases where audit tests and activities aren't formalizable or rigid, auditors can reevaluate the control objectives and develop a risk-based audit plan that validates controls over areas where electronic data is readily available from the business process. The rigidity of business processes and flexibility of control tests and activities

determines how far up the hierarchy of the audit plan to go. Defining automated audit procedures at levels with lower granularity require higher levels of audit reengineering effort but allow you to work in environments where radical business process reengineering is not an option.

Developing Automated Audit Procedures

The audit automation project began at the request of the internal audit innovation group of a large North America-based consumer goods firm. The firm operates globally and has multiple geographic regions that manage local brands and consolidate with the North America headquarters. While the firm outsources its IT infrastructure, its general ledger reporting is maintained in SAP. The firm has expanded in the past several decades through acquisition of other major companies. In lieu of requiring standardization on SAP, most of these acquired subsidiaries maintain their existing systems. This has resulted in a heterogeneous enterprise system with very complex consolidation procedures, authorization matrices, and reporting structures.

Internal auditors conduct periodic financial and compliance audits in each of its geographic regions. This requires a team of two auditors to travel onsite for three workweeks and complete a prescribed set of audit procedures for each of the major business modules (e.g. procure-to-pay, order-to-cash, etc.). Before the auditors arrive, business process owners complete an internal control self-assessment, which helps auditors plan and prioritize their audit efforts. The procedures found in the internal control self-assessment and the audit plan are identical.

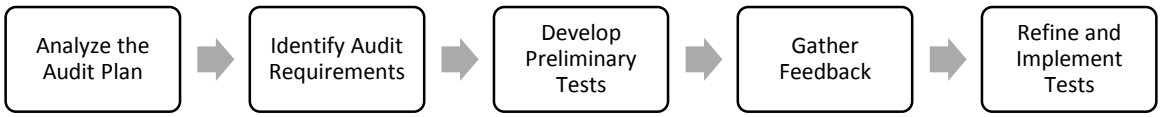
Because many of the audit procedures begin with the selection of a random sample of transactions found in the SAP consolidated accounts, audit automation would have the most impact in the selection of better samples (e.g. identifying high-risk transactions). This would allow auditors to focus their efforts on areas of higher risk as well as provide a mechanism for management to monitor and track control weaknesses in between the periodic audits. These procedures could also be used to automatically analyze the supporting documentation in regions and subsidiaries where that source data is captured in online systems.

At the start of the automation project, internal auditors provided researchers with the internal audit procedures and internal control self-assessment for the revenue (order-shipping-billing and accounts receivable) cycle. These procedures identify control objectives, activities, and tests that guide the auditors (and managers) through the collection and analysis of evidence generated by the revenue process. Similar to Maritis' IT audit action sheets (described in Chapter 2), the firm's audit procedures identify the controls that are expected to be operational, and the methodology to be used by the auditors. In some cases, they also contain job aids, which provide step-by-step interaction with the online systems.

This field study represents exploratory research with the expected outcome of implementation of a series of automated audit tests. The methodology described in Chapter 2 and presented in Figure 3.1 guided this approach. Once that methodology was tested, the automation objectives were expanded as alternative approaches to the

original audit tests were explored. The results of this effort are presented in the following section.

Figure 3.1: Maritis audit automation methodology



Analyze the audit plan and identify audit requirements

The first step involves analysis of the audit plan. The key descriptive elements were extracted from the audit tests and compiled into a spreadsheet. Tests that involved more than one step were treated as separate procedures. The scope of the automation exercise allowed researchers and auditors to attempt automation for any portion of the audit test as these can be developed into computer-assisted auditing tools (CAATs). The classification step involves determining the extent to which the audit procedures may be automated (through the use of scripting or monitoring software). Other descriptive elements including comments, interpretation of key attributes, data location, and parameters were compiled in the spreadsheet to facilitate development of the automated procedures once they had been identified, shown in Table 3.1.

Table 3.1: Sample documentation and classification of the audit plan.

CO	CA	CT	Description	Key Attributes	Preliminary Classification	Prerequisites	Data Location	Table/Field/ Transaction Code	Parameters
1			RE3010 Orders are only processed within approved customer credit limits. (Operational)						
	1.1		The Order/Shipping/Billing System is configured to automatically put an order on hold when the customer exceeds his credit limit or fails the established credit verification criteria						
		1.a	Compare system settings with the global standard for risk categories.	Verify that all active customers have a risk category assigned in the system. In addition, retrieve all customers that have a risk category "exempt" or "pre-approved" and obtain justifications from management for these.	B	Credit Control Areas used at site (e.g. CN00, PH00)	Local OSB (e.g. ASP, F5P. L5P)	OVA8	
	1.2		Credit held an independent person following approval in line with the organization's local Decision Authority guidelines releases orders.	• The person responsible to execute the credit hold release in the Order/Shipping/Billing system does not have access to order entry and master data transactions (or sufficient compensating controls are in place). • Organization specific local Decision Authority guidelines (Credit Hold releases are not governed by global DA) for the release of credit held orders exist. • All credit held orders are released as per the organization's local DA guidelines, prior to the order release in the system. • Supporting documentation showing the reason for the release (e.g. proof of money in transit) are retained for at least one year.					
		1.c	Generate the list of all orders that have been released from credit hold for a specific time frame.	Obtain a sample of 25 orders on credit limit hold or financial hold over the current fiscal year/period and verify the following key attributes: • Approvals of the releasing of credit held orders were in accordance with the organization's local Decision Authority guidelines. • Reasons for releasing the order and supporting documentations exist and are filed (release sheets, proof of money in transit, etc.). A person who does not have access to either order entry or master data maintenance has released • The order.	A	1) Particular time frame for testing (based on audit review period) 2) Credit control Area 3) Company Code	Local OSB (e.g. ASP, F5P. L5P)	ZVCR	KNKK_ID = "D"

A preliminary classification based on the perceived opportunity for automation each step was used to identify opportunities for automation. Procedures that involved querying SAP tables or testing system controls were classified as fully automatable (A). Procedures that involved querying the system but required auditor intervention to filter or aggregate the results were classified as partially automatable (B). Procedures that were deemed automatable if the audit procedure were altered or reengineered were classified as reengineerable (C). Procedures that involved no systems (or documentation that was not found in electronic document management systems) were classified as manual and non-automatable (D). These classifications were based on the assumption that the business processes adequately recorded and stored the data necessary for the audit.

Develop preliminary tests

Once the classification and related documentation were compiled, preliminary automated procedures were proposed. For example, one test validates that credit holds (customers who exceed their credit limit or don't already have established credit) are released by authorized credit managers once credit has been extended or denied. In SAP, credit holds are recorded in table VBUK field CMGST with a value of "D." Changes to credit holds are recorded in table CDPOS where TABNAME="VBUK", FNAME="CMGST". Releases of credit holds would show in records where VALUE_OLD="D", and VALUE_NEW<>"D". The username of the credit manager who recorded the change is found in CDHDR where USERNAME={Users assigned to credit manager role}.

Automation of the credit release hold audit test would include a script that joins tables CDPOS and CDHDR, filters the records to only show those that include a change from "D" to something other than "D", where the username doesn't match those found in a set of authorized users (called a decision authority). If the control were functioning properly, auditors would expect to see zero results. However, if any records appeared as a result of this script, auditors would identify a control weakness and follow up with the business process owners.

Subsequently the auditors would evaluate the supporting documentation for a statistical sample of 25 released credit holds to determine whether appropriate procedures were followed. Naturally, this step requires manual evaluation and automation will not provide a useful benefit.[1]

Gather auditor feedback

After the scripts and queries are developed, auditor and IT managers test the procedures and compare the output from the automated test to output generated manually by the auditors. If the results are substantially the same or better (based on the auditors' judgment call), they are included in the new set of automated procedures to be implemented in the future. If the results are less accurate than the manual procedure, the automated tests are refined using the auditor and IT manager feedback until they are deemed an adequate substitute for the manual procedures. If the auditors

[1] For discussion on how remote auditing would be beneficial in this instance, see Chapter 4.

implement continuous auditing or monitoring, a subset of the procedures would be added to the monitoring application and scheduled to execute at a predefined interval.

Once the audit tests have been evaluated and automated procedures have been developed and tested, the auditors would follow traditional change management (approve, unfreeze, change, refreeze) to implement the automated audit procedures. For research and evaluation purposes, the count of automated rules is compared to the predicted count and evaluated further.

Two Attempts at Audit Automation and Reengineering

The research team began their analysis of the revenue audit plan following the methodology presented in the previous section. The accounts receivable portion of the revenue audit represents approximately 30% of the audit effort, according to the auditors. Successful automation in this area was thought to have the largest immediate impact on the auditors' time commitment.

Each audit procedure identifies the overarching control objective, control activity, and control test used to verify each control, shown in the example in Figure 3.2. The accounts receivable portion of the firm’s audit plan contains nine control objectives, 25 control activities, and 40 control tests, summarized in Table 3.2.

Figure 3.2: Sample audit control test

Control Objective

1 Orders are only processed within approved customer credit limits. (Operational)

Control Activity

1.1 Credit held orders are released by an independent person following approval in line with the organization's local Decision Authority guidelines.

Key attributes:

- The person responsible to execute the credit hold release in the Order/Shipping/Billing system does not have access to order entry and master data transactions (or sufficient compensating controls are in place).
- The person executing the credit hold release is authorized and within the organization (AR, OM, authorized third party, etc.).
- Organization specific local Decision Authority guidelines (Credit Hold releases are not governed by global DA) for the release of credit held orders exist.
- All credit held orders are released as per the organization's local DA guidelines, prior to the order release in the system.
- Supporting documentation showing the reason for the release (e.g. proof of money in transit) exists and are filed (release sheets, proof of money in transit, etc.).

How do the processes in place in your organization meet the above Control Objective, Control Activities and Key Attributes?

<u>Test 1.a (Control Activity 1.1)</u>

Generate the list of all orders that have been released from credit hold for a specific time frame. Obtain a sample of 25 orders on credit limit hold or financial hold over the current fiscal year/period and verify the key attributes using the attached template and job aid.

Provide a summary of test results including: 1. Sampling methodology, 2. Test Results, 3. Supporting Attachments, and 4. Conclusion

Table 3.2: Composition and description of the accounts receivable audit plan

Category	Count	Description	Example
Control Objective	9	Overall expected control	Credit notes are issued for all goods returned in accordance with the organization policy.
Control Activity	25	Specific expected control	Documented procedures for all returns and refusals and adjustments to customer accounts exist and are approved.
Control Test	40	Procedure for testing control	See control test steps
Multistep Control Test	15	Control tests with multiple distinct steps	See control test steps
Control Test Steps	71	Sub step of control tests	Obtain and examine a copy of documented procedures on returns and refusals and verify the following: a. Important provisions (refer to key attributes in the Control Activity 5.1.) are present in the procedures
Job Aid	27	Instructions used to collect evidence	In SAP, enter t-code GUNNR. Export table to file.
CAAT	2	Scripts used to collect evidence	Run attached script to calculate aging of outstanding accounts receivable.

The overall control objectives define what should happen if the business process controls are functioning properly. These form the basis for the control activities and control tests that will evaluate the accounts receivable process, and are summarized in Table 3.3, grouped by operational, compliance, and financial activities:

Table 3.3: Control objectives for accounts receivable

Audit	No.	Control Objective
Operational	1	Orders are only processed within approved customer credit limits.
Compliance	2	Cash receipts are handled in accordance with external Money Laundering Avoidance (MLA) requirements.
Financial	3	Cash receipts are recorded in the period in which they are received. All cash receipts data is entered for processing accurately, and only once.
	4	Cash discounts are accurately calculated and recorded.
	5	Credit notes are issued for all goods returned in accordance with the organization policy.
	6	All credit notes and adjustments to accounts receivable are accurately calculated and recorded in the appropriate period.
	7	Accounts receivable reflect the existing business circumstances and economic conditions in accordance with the accounting policies being used.
	8	Journal entries are independently reviewed, validated, authorized, and properly recorded in the appropriate accounting period.
	9	Reconciliations for all significant accounts are performed properly, prepared on a timely basis, and independently reviewed. Issues identified are resolved and recorded in the general ledger on a timely basis.

From this audit plan, all of the key data from each audit test was compiled in a tracking spreadsheet (refer to Table 3.1 in the previous section for an example). Once all of the critical data was compiled, the following attempts were made to identify and develop automated procedures.

Attempt 1: Automation of existing audit procedures

The classification of the audit tests continued into more detail, where each sub step was identified and then evaluated to determine whether it had the characteristics needed for automation. 23 of the steps included words like “query” or “extract” or “sample” or included calculations and CAATs and were classified as fully automatable (A). 8 steps required auditor input or additional work before they could be executed and were classified as partially automatable (B). 3 steps were identified as reengineerable (C) as the procedure could be altered to enable automation. The remaining 6 steps required reviewing documentation, interviews, or other non-systems procedures and were classified as manual (D).

The count of tests found in each classification of the accounts receivable audit program is shown in Table 3.4. The principle analysis and classification of the accounts receivable audit procedures suggested that nearly three quarters of the tests could be partially or fully automated. Auditors reviewed the preliminary classifications and confirmed that they were generally in line with their expectations.

With the preliminary analysis complete, the source and location of the evidence used to validate the controls was identified. The evidence refers to the values on the paper source documents, and tables and fields in SAP. Once the data were identified,

development of the automated test prototypes could proceed. It was at this stage, however, some severe problems in the automation exercise were encountered.

Table 3.4: A priori classification of revenue audit procedures

Classification	Count	Percent
Fully automatable (A)	23	57.5%
Partially automatable (B)	8	20%
Reengineering required (C)	3	7.5%
Manual (D)	6	15%
Total	40	100%

Because of the way that the Nouant implemented and used SAP to compile the transactions from the various systems in place among their different divisions, many of the transactions and tables were used in non-traditional ways. For example, individual managers would release credit holds in the system, but SAP would record the change using a batch process. This meant that the user id would be that of the batch process and not the individual manager. An automated analysis of the user IDs to determine whether an authorized user recorded the status change (or to identify unauthorized changes) would not produce results because each change was made by the one user account in SAP. Additionally, an attempt to use a script to extract and join tables (such as the heading table CDHDR and the line item CDPOS) proved resource intensive and complex due to the volume of records.

The process and technical limitations were compounded by the fact that the internal audit manager was uninterested in tools that would create “better” samples. Rather, it became apparent that he was interested in more radical reengineering of the audit plan than he had previously indicated which also involved more of a “push button” audit approach. The reason for this shift in expectations was not determined

Further analysis of the SAP system and the business processes revealed that key audit evidence was not automatically recorded or updated in the system. Even though SAP was used as the primary repository for the organization's transaction records, simple automation procedures could not be developed because there was significant deviation from its intended use. For example, auditors would need to use the samples they had selected to validate the critical piece of data (such as a signature) that could only be found on the original source document. As the system was used currently, automation beyond the two existing CAATs was not going to yield the efficiency benefits that the organization desired. Some significant reengineering would be required in order for the system to capture critical audit data elements.

As the project proceeded, both the lack of support from the audit manager and existence of incompatible business processes proved to be significant obstacles to this portion of the audit automation effort. Various proposals were suggested over a period of four months, but all of the attempts were rejected.

Attempt 2: Reengineered audit processes

At this stage in the project, the focus shifted from a direct automation of the existing procedures to a more radical view of alternative procedures. In order to propose alternative tests, existing tests were ignored and the focus shifted to controls that represented the highest risk to the revenue process. The given audit activities (one per audit objective) were summarized in order to understand what the overall goals of the audit program should be. They are listed here:

1. Review the credit review process and identify customers who consistently exceed limits
2. Review reconciliation of cash receipts (there should be none)
3. Review reconciliation of remittances, suspense accounts, and collections
4. Review manual general ledger entries and applied prompt payment discounts
5. Review credit/debit notes
6. Analyze aging, allowances, rejected payments, referrals, and write-offs
7. Review revenue journal entries, unusual entries
8. Compare balance sheet receivables to subsidiary totals
9. Review procedures used for reconciliations

The highest risk was attributed to the collectability of the accounts (6), customers who were constantly reaching their credit limits (1), and a series of miscellaneous receivable that weren't attributed to specific customers (8). Additionally, the research team investigated interesting patterns and relationships between different data, such as comparing those customers who were exceeding credit limits with their payment history or possible circumvention of the process by recording their transactions as miscellaneous receivables.

Four approaches where automation could be used to analyze the firm's revenue data and help direct the auditors' attention to these areas of high risk were proposed, shown in Table 3.5. These activities looked at authorized users within the system (where they existed), linkages between account history and credit limits, and analyses of the

changes in customer credit. They also identified specific data that would be needed to complete the analysis both in SAP and the other existing enterprise systems.

Table 3.5: Proposed risk-based control activities and data requirements for automation

Proposed approach	Data requirements
Collectability (Aging & Estimates of Doubtful Accounts; 7.3) • Evaluate A/R transactions against the standard aging policy. • Test transactions against sales order & invoice date, and look for transactions that are outside the standard time lapse between the two dates (e.g. 7 days). • How are bad debts recorded (field in SAP?)	Aging output from existing CAAT • Credit account • Receivable amount • Sales order date • Invoice date • Paid date Aging policy (e.g. 30/60/90 days) How bad debts are determined (B.S/I.S.) Bad debt recording procedure
Credit Limits (1.1 & 1.2) • How many customers exceed credit limits? • Is there any way to bypass the set credit limits (e.g. super user access)?	Customer credit status Query with fields: • Credit Acct. • Credit limit Decision authority table: • Released by (authority id)
Miscellaneous A/R (8.1) • Query all miscellaneous A/R accounts together. • Look for duplicate entries. • Test aging of miscellaneous account transactions (follow up procedure) • Who is recording these? Is there an authority approval? Is follow-up recorded? Do the same people record numerous miscellaneous A/R? • Monitor balance levels. • Are misc. receivables added at creation, or part of end of month closing procedures?	Chart of Miscellaneous accounts A/R tables: • Credit acct. • Sales order date • Invoice date • Amount • Released by • Paid date Approval authority table: • Released by Disposition (removal) policy
Linkage • Credit limits to aging: do accounts with exceeded limits turn into bad accounts? • Credit limits to Miscellaneous: do accounts with exceeded limits have many transactions within miscellaneous accounts? • Approval authorities: do the same people who approve misc. A/R also have transactions with collectability issues?	See above

The audit manager appeared to be interested in these procedures and encouraged their development as they aligned better with his expectations. However, the underlying processes didn't support the proposed procedures. The next obstacle faced was getting access to the data from IT. Where the data didn't exist, these approaches

could not be implemented. Where they did exist, the research team's attempts to get access to the data in a format that would allow prototyping and testing of different automated tests was denied. In six months, several different requests for data were made but were ultimately unable to make progress because of miscommunication with the IT staff compounded by unavailable data. This supported the observation that lack of necessary IT resources and infrastructure was cited as a significant obstacle that firms face when attempting similar projects (7%) (Gupta, 2001, p. 119).

Discussion and Conclusion

Each of the approaches taken in selecting, categorizing, and creating conceptual automation rules was met with obstacles that the research team was not able to overcome. This failure to make progress, compounded by changes in the audit staff, resulted in the eventual abandonment of the audit automation project. The nature of the existing business processes did not lend itself to simple automation. Even in cases where the audit test could be restructured, the research team faced significant pushback from the internal auditors who preferred less "creative" solutions.

One reason for the failure to substantially automate the accounts receivable program was that the goals and outcomes of the researchers and the auditors were misaligned. Where the researchers wanted the automation to enable the delivery of exceptions, the auditors did not want audit sample creation. They were more focused on the idea of a push-button audit that would validate data directly and only output high-risk exceptions. Were business processes in place, this would likely have been possible.

The auditors were also reluctant to change their processes, and the idea of changing business processes was outside of their scope. When simple automation was not available, attempts at reengineering were thought of as “too creative” and dismissed.

In addition to the demand, motivation, and technology needs of the audit automation, 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 automated 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.

This chapter discussed the challenge of effective audit automation based on limitations in the business processes as well as misaligned expectation between researchers and auditors. The reengineering needed in the audit process to enable effective automation requires significant changes to the business processes and the systems that capture the enterprise data. 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.

There are also some outstanding behavioral issues related to reengineering audit processes for audit automation. Understanding more about auditors' expectations and limitations of technology within their organizations could be gathered through experimental research. Future research may address many of these open issues document future implementations of automated audit procedures.

Although the literature identifies clear steps and antecedents, audit automation within complex businesses can be nearly as complex. The audit plan at the consumer goods firm highly reflects the business environment and is consequently inherently manual and paper-based. Throughout the automation process, insight into the accounts receivable audit processes revealed some interesting findings. For example, the extent of manual involvement in the recording and validation of receivables transactions was substantially greater than anticipated. This led to inflated expectations of how the technology could simplify the audit effort compared with the reality of the business processes involved. Business process reengineering, including source document automation and process consolidation, would enable more straightforward and comprehensive automation procedures.

The audit automation project also provided support of audit reengineering model. Where straightforward automation of audit tests was not directly attainable, demand for business process reengineering was great. When those business processes could not be reengineered, the audit control tests provided the only opportunity for

reengineering. By moving up the audit hierarchy, the audit team identified some potential areas where an audit would be enhanced with automated auditing tools in the future.

CHAPTER 4. THE REMOTE AUDIT

Introduction

Discussing the implementation of a continuous auditing system by internal auditors at Maritis Corporation, Alles et al. (2006, 140) state:

> Maritis 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. (emphasis added)

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 on-site 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 reduces the location requirement for auditors, allowing them to divide the audit tasks between on-site 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 can enable the 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. This essay focuses on two areas of that transformation, interpersonal communication and data analytics, and attempts to identify specific areas where future research may offer insight into this reengineering paradigm. The desired outcome is a location-independent audit where any auditor with a network connection can perform audit tasks, whether they are on-site 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. Virtual audit teams can now lead many audit tasks, 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.

The audit environment often determines the extent to which audit procedures can be formalized, automated, and enhanced to meet the demands of real-time systems. The way that business processes function and generate evidence determines not only

the types of procedures that auditors can choose from, but also the structure and location of the audit team.

This essay details the efforts of researchers and internal auditors to explore remote auditing procedures. In contrast to the automation effort at Maritis (Chapter 2) this chapter identifies some of the major challenges auditors must deal with in large organizations that have diverse systems and processes. While run through SAP and a series of other legacy ERP systems, the business processes in place tend to be highly manual and paper-based. Analysis of the audit plan reveals that a large number of the analytical procedures require auditors to take random samples and validates the supporting documentation – a highly manual process.

The remainder of this essay is presented as follows. The next section provides a summary of relevant literature related the remote audit, including a discussion of virtual teams. This includes the tracking and documentation tools used by the auditors throughout the audit. The method section describes the field research processes and controls used to document and classify audit procedures to enable the remote audit. The results and discussion section contains insight gathered throughout the research process and describes limitations to the adoption of remote auditing capability. The conclusion provides a summary of the case and opportunities for future research.

Theoretical Background

Advances in network infrastructure and data portability enable auditors to perform audit tests from any networked location. Where a complete audit team previously needed to travel together and audit onsite, now auditors form virtual teams where a

smaller number of auditors travel to the audit site supported by audit analysts working remotely. As auditors perform their analyses from a distance and/or transmit data to other members of a virtual audit team, remote work has enabled more efficient use of company resources. One benefit of virtual audit teams is the ability to monitor business process and respond to internal control weaknesses with greater ease and flexibility.

Many different types of organizations show interest in continuous monitoring within the internal audit function. A recent survey by PricewaterhouseCoopers reveals that 81 percent of the organizations have either implemented or plan to implement some form of continuous monitoring (PricewaterhouseCoopers, 2007). What isn't clear is the extent to which roughly half of these organizations have implemented automated routines to analyze economic transactions and alert auditors to unusual variations, exceptions, or control violations nor the actual timing of these "continuous" audits. Many factors, including the design and implementation of the existing enterprise resource planning (ERP) system, structure of business processes, audit coverage, and risk assessment, can potentially affect the extent and timing of a monitoring function.

Continuous monitoring of ERP systems also provides a tool for internal auditors to gather and evaluate evidence remotely where proper controls over the monitoring function exist. With monitoring in place, internal auditors can work from a centralized location or in virtual teams to respond to exceptions and control violations, gather additional data that is available in digital form, and communicate with business process owners.

By definition, continuous monitoring relies on automated procedures. While automation of a highly formalized information technology (IT) audit is expected to be straightforward, automation of the audit procedures covering broader audit objectives, such as those controlling the revenue cycle within a company, presents a greater challenge. In the latter case organizational characteristics and information system utilization and use each play key roles in determining the extent of audit automation. Implementation of enterprise resource planning (ERP) systems varies greatly across organizations (Hong & Kim, 2002). Factors such as the degree of system homogeneity and digitization of business processes have been shown to positively affect the outcome of implementing ERP and monitoring solutions.

Within each organization, some audit procedures or business processes may not be formalized, have digital equivalents, or may be highly manual within the organization. Continuous monitoring of these types of procedures requires greater automation effort and in most cases some degree of reengineering or process redesign. Hammer (Hammer, 1990) suggests that these procedures should be redesigned completely with an eye to the monitoring environment. However, auditors may not have the influence or pull within the organization to have business processes change to accommodate a monitoring function and must therefore reengineer their own audit procedures in order to achieve the level of coverage they desire.

Finally, a significant challenge to audit automation is resistance to change by both auditors, who must alter audit procedures in some cases, and business process managers, who must incorporate greater degrees of digitization in other cases. This is

similar to the resistance to change facing ERP implementation (Aladwani, 2001). The role of the internal auditor as a consultant to management may play a greater role in less formalized yet progressive organizations that want to reap the benefits of continuous monitoring.

This chapter presents observations and results from a remote audit effort within a multinational consumer goods firm operating globally. This includes a model for audit and business process automation and reengineering. It then details the process for the accounts receivable function, notes the reactions from internal auditors, and describes the challenges and successes of shifting audit tests from in-person to remote. Additionally, areas where automation will aid a remote audit are identified and analyzed. This study provides evidence for one of the future research questions presented by Rezaee, et al (2002) by looking at the experiences within an organization attempting to incorporate continuous auditing and monitoring.

Internal auditors have increased their use of and reliance on technology to increase the coverage of the systems certification audit and improve its effectiveness (Alles, Kogan, Vasarhelyi, & Wu, 2010b; Vasarhelyi & Alles, 2008). Much of the research literature has focused on audit automation, but less attention has been paid to another major benefit of technology: the ability to connect to these systems remotely and reduce the cost of audit logistics. While continuous auditing extends the scope of an audit, by enabling ongoing and on demand procedures (Alles, Kogan, & Vasarhelyi, 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 essay is to examine how remote auditing technology is facilitating internal audit reengineering. 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. This chapter focuses 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 any auditor with a network connection can perform audit tasks, 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. Virtual audit teams can now lead many audit tasks 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. This chapter attempts to show empirically that in certain environments, auditors favor remote auditing techniques.

The theory of this chapter follows the outline in Teeter et al (2010). 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. This paper focuses on these two areas of that transformation, interpersonal communication and data analytics, and attempts to identify specific areas where future research may offer insight into this reengineering paradigm. The desired outcome is a location-independent audit where any auditor with a network connection can perform audit tasks, 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. Virtual audit teams can now lead many audit tasks 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. This essay attempts to identify some of these tasks and examine how electronic evidence facilitates a remote audit.

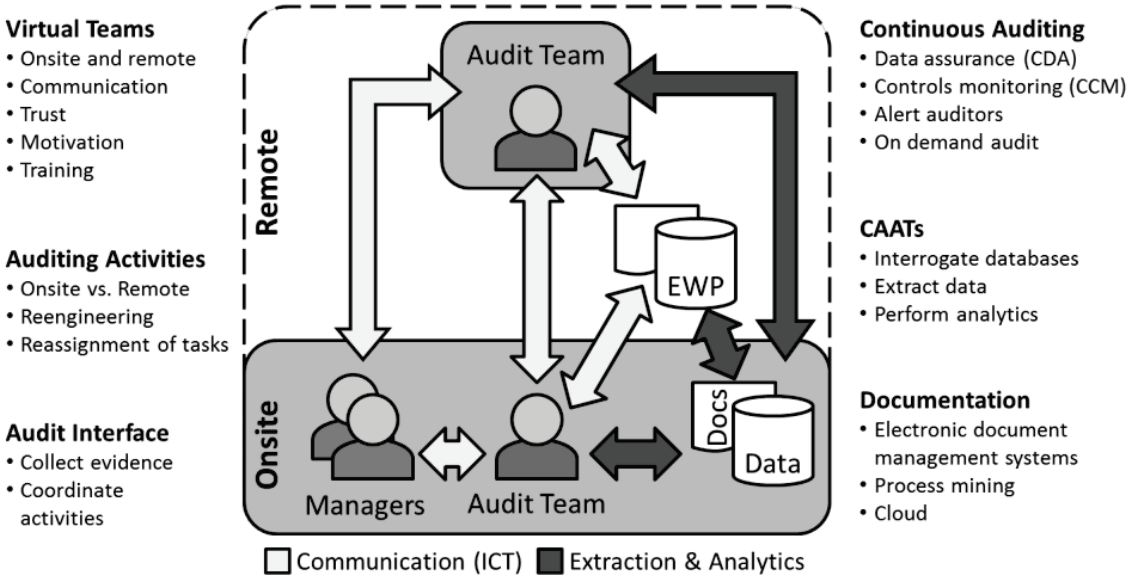
The remote audit

The term remote auditing means “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, information and communication technology (ICT) and data analytics, provide the framework for future research into the technical and behavioral aspects of a remote audit. Figure 4.1 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 audile's systems to test internal controls and transactions.

Figure 4.1: Components of remote auditing



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, it is expected that an expanded intense deterrent effect will be observed when remote auditing is coupled with continuous assurance, comparable to that experienced when retail stores have installed closed circuit video cameras.

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 the scope of this paper is limited 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, DeMarie, & Hendrickson, 1998) 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 workday.

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).

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.

Remote 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 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 auditors 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 4.1 illustrates how different audit activities may be performed onsite and remotely. In practice, it is expected that there will 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 4.1: Onsite and remote internal audit activities

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 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.

Information and communication technology (ICT)

ICT has already significantly impacted the way businesses operate and has enabled more decentralized and dynamic processes. 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 & Kuenkaikaew, 2011).

The remote audit embraces ICT to create a rich audit experience. However, Vasarhelyi and Kuenkaikaew (2011) 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. This reflects the argument of Hammer (1990) 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. This section presents a discussion of 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. 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 the modern utilization 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 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. Several of these open behavioral research issues in Table 4.2.

Table 4.2: Selected behavioral research issues of the remote audit

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

Data extraction and 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 Kuenkaikaew, 2010; Teeter et al, 2010). Based on Statement on Auditing Standards No. 106 (AICPA, 2006). Table 4.3: presents examples of onsite and remote audit methodologies that may be used to obtain data for certain audit procedures.

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.

Table 4.3: Audit procedures for obtaining audit evidence

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 (e.g. scanning and statistics)	Extract data, scan for anomalies based on auditor judgment	Filter real-time data through continuity equations, ratio analysis

To demonstrate the possibilities of a reengineered electronic evidence environment, the internal audit team at Maritis 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). Maritis 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

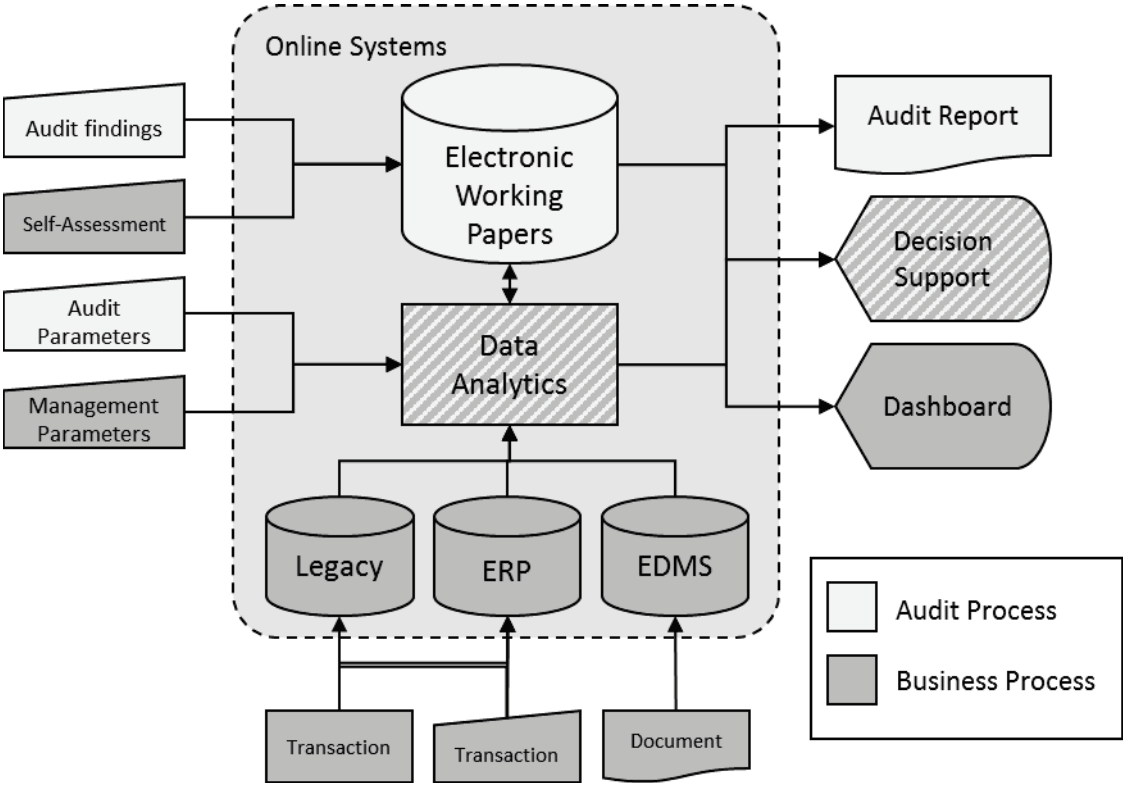
Documentation plays a central role in both communicating business processes and evaluating the integrity of an audit (Sprague, 1995). For an auditor, documentation can include a set of audit procedures, a spreadsheet of extracted information, a transcript from an interview, or a combination of different 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. Figure 4.2 illustrates function EDMS play within the audit evidence collection and processing.

Figure 4.2: Electronic working papers overview



During the course of regular business operations, transactions are processed and recorded in ERP and other legacy systems and key documentation is filed in the EDMSs. On the audit side, business process owners complete control self-assessment surveys while auditors collect evidence. The findings are all stored in the electronic working papers systems (a form of EDMS). At specified intervals, data analysis is performed on the enterprise data and audit data based on parameter specification by the managers and auditors. The results of the data analysis are returned to managers in the form of key performance indicators on a dashboard report and decision support. For the audit side, results may be returned to the EWP system and included as supporting evidence in the final audit report.

Throughout the process, documentation 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. For organizations without comprehensive EDMSs, 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 (Kogan et al 2011). 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.

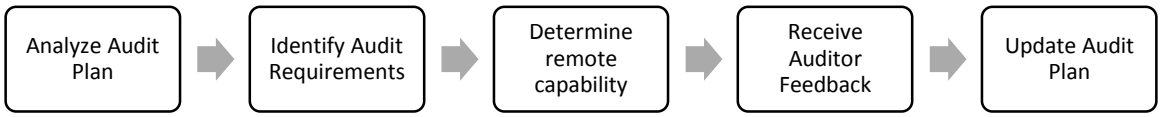
With some exceptions, most CAATs are run on computers and access data available in online systems. Assuming auditors have a secure remote connection to the data they

are accessing, running CAATs remotely requires little reengineering. 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.

Conceptual model

To determine how remote auditing procedures could be utilized in the audit process, researchers work with internal auditors to evaluate the audit plan and identify the location and format of the evidence needed for analysis. The approach presented in Figure 4.3 was used throughout this study. This follows a similar path to that of the automation effort with the focus on audit evidence rather than the audit test itself.

Figure 4.3: Steps for identifying the use of remote ICT capability



The initial analysis of the audit plan identifies the control tests and expected outcomes. Once an understanding of the audit tests has been obtained, the location and format of evidence needed to complete each test was identified. The evidence includes documents, files, tables, and observations. A preliminary classification is assigned to each test based on whether it could be reengineered to allow remote access to the data, shown in Table 4.4.

Analysis of an audit program

For each audit test, the auditors identified the control activity, and then examined the information and document needs. The information guided the auditors to the specific location of the documentation (such as policy guidelines or hard copies of sales orders) that would help support the audit. They then determined the tasks that could be performed remotely by a member of the audit team and those that needed to be conducted in person as part of the onsite audit. Because of the variety of operations and processes within each division, certain qualifications would have to be met in order for the auditors to work remotely. For example, paper files would need to be digitized and/or the ERP system would need the proper authorizations and transactions recorded.

The auditors finally assigned a classification assigned by the auditors was based on the ability of the auditors to collect the evidence from either the system where proper authorizations and other data exist, the business process owner through some form of e-filing, or the onsite audit team member through e-mail or other electronic communication.

Table 4.4: Selection of accounts receivable control activities with proposed remote tasks.

CA#	Control Activity	Information Needed	Document Needed	Class	Remote Tasks	Onsite Tasks	Qualifications	Proposed Change
1.2	Review credit limit held orders	Process Documents	-Approval for release of held order -Reason for release	**Partially remote**	- Pull released orders from SAP (code D) - Review fields for reason code and approval (efile or scan/e-mail to verify a sample)	- Pull held orders from local orders - Review supporting documentation for signature and reason	Remote if electronic approval exists and held orders are electronic process. Manual processes must be tested onsite. Supporting documentation showing the reason for the release is retained for at least one year.	N/A
2.1	Verify if customer payments are received in cash and limits	Process	-Local policy guidelines	**Remote**	Review current policy (efile or scan/e-mail)	Interview process owner	None	Phone conference interview
6.1	Review credit/debit notes	Process Documents	-Open and cleared debit and credit notes posted to customer accounts -Supporting documentation (customer claim, evidence of DC receipt) -Approval documentation -Original invoice	**Partially remote**	-Download CN/DN list from SAP -Verify authorization and invoice in SAP -Review electronic documentation (efile or scan/e-mail)	Review paper documentation	Authorized users appear in a decision authority list.	Automate verification of approval and invoice match

Remote procedures typically involved collecting business documentation, such as onboarding programs, organizational charts, policies and procedures, job descriptions or other reports. Partially remote procedures allow the auditors to select samples during their pre-audit and then inspect hard copies of the supporting documents or interview business process owners once they arrived on site. They could also potentially be completed entirely remotely if the business processes at a given division supported it. Generally the remote and partially remote procedures involved a great deal of electronic document filing or e-mailing requisite documents. The only procedure that was classified as onsite involved a rare instance where an external party (in this case an attorney) was involved and required in person follow up.

The analysis of their revenue audit procedures for the revenue and order-shipping-billing audit program resulted in 38 (58%) of the audit tests could be performed remotely, with an additional 27 (41%) that could be performed partially remotely, shown in Table 4.5. Additionally, 11 (16%) of the tests involved back office support, which bypassed the business process owners completely.

Table 4.5: Auditor classification of the revenue audit program

	Accounts Receivable		Order-Shipping-Billing		Total	
Classification	Count	Percent	Count	Percent	Count	Percent
Remote	27	68%	11	42%	38	58%
Partially remote	12	30%	15	58%	27	41%
Onsite	1	2%	0	0%	1	1%
Total	40	100%	26	100%	66	100%

As the auditors completed their analysis, they included other remarks based on their experiences in prior audits. These remarks expressed support of the given

classification and provided suggestions to other auditors for when they should request the data and anomalies to watch out for when completing their tasks. This last section is particularly because auditors working remotely may not be able to get the same sense of how the business operates as if they were physically there interacting with the business process owners and observing the business process.

As the auditors discussed their roles within the audit department, it was apparent that virtual teams had already been formed, although they weren't explicitly designated as such. The head of internal audit would coordinate the activities of the other auditors and communicate with them by e-mail and web conference as they complete their work in remote offices. When auditors in the field ran into questions or needed additional help, they contact headquarters for additional guidance.

Conclusion

Remote auditing allows internal auditors to leverage technology and adapt to a changing enterprise environment. When they are no longer constrained by physical location, auditors can reduced effort and long-term cost through automation and continuous deterrence. This also reflects the way global businesses have been operating for the past two decades through teleconferencing and telecommuting. As with audit automation and continuous monitoring, remote auditing requires a significant amount of reengineering of the audit and business processes, but most of that work is already underway as firms cope with more data and increased technology use.

Firms, such as the one discussed here, are looking for ways to improve their audit coverage and effectiveness while reducing the impact and cost of the internal audit

function. The level of existing technology use within a firm clearly corresponds with the amount of remote auditing that is possible. Auditors at highly digitized firms, such as Maritis, can “set and forget” a large portion of their audit procedures to run at scheduled intervals year-round, while auditors firms with more manual processes are limited to traditional audit cycles unless they adapt the business process first to enable new streams of data. Even where robust digitization and data analytics aren’t yet completed, auditors are already identifying areas where information and communication technology can facilitate evidence collection and communication between the audit staff members and business process owners.

This essay explores the role of information and communication technology as well as data analytics to provide a framework for future audit innovation. Future research can help explore this framework further by addressing some of the conceptual and behavioral issues that remain. Understanding how virtual audit teams work (in contrast with other virtual teams) will help determine the appropriate use of technology. Insight into how auditors structure their teams and utilize the technology can also help us understand the constraints to auditor behavior. Finally, auditors’ technology familiarity and competence could be tested in various settings to help researchers understand some of the obstacles to the use of this technology.

CHAPTER 5. THE ENHANCED AUDIT CLASSIFICATION MODEL

Introduction

Auditors face constant pressure to adopt contemporary audit procedures so that they can provide assurance on an expanding set of data and business processes while reducing the overall cost of the audit. Stakeholders demand that auditors address new and ever-changing areas of risk and provide enhanced assurance while minimizing the increasing audit costs and limiting their burden on the organization (PwC 2012). This demand for increased scope and decreased cost reflects a continual drive toward a more effective and efficient audit. The enhanced audit uses technology and data analytics to accomplish this goal.

Internal auditors appear to be leading the drive toward an enhanced audit (Kuenkaikaew et al, 2011). This is largely because internal auditors have a better grasp of the business processes and systems. Management can also coordinate monitoring efforts since they are pulling from the same data pools. Additionally, external auditors face greater litigation risk in cases where full population testing and reliance on technology viewed by outsiders as more comprehensive testing. In its annual survey of chief audit executives and other stakeholders, the public accounting firm PricewaterhouseCoopers notes that the organizations want internal auditors in particular to play a more substantial role in monitoring risks and providing objective assurance while efficiently leveraging technology. "Stakeholders value internal audit's ability to identify risks, evaluate threats, and recommend processes and controls to manage them" (PwC 2012, p. 10).

Despite the apparent demand for enhanced audit procedures, auditors struggle to embrace audit innovation. Whether due to resistance to change (Gonzalez et al, 2012), a lack of proper incentives (DeAngelo, 1981), or perceived complexity (Janvrin et al., 2008a), adoption of enhanced auditing procedures, including automated, remote, and continuous auditing, has been slow and inadequate (PricewaterhouseCoopers, 2012).

In the face of modern information systems, however, there is evidence that they have been slow to incorporate more sophisticated and advanced auditing procedures into their audit plans even as demand has increased (Chan & Vasarhelyi, 2011; Vasarhelyi & Kuenkaikaew, 2011). They understand that enhanced audit tools can improve their audit and communication efforts, but primarily rely on e-mail, some form of electronic document management (usually stored on local computers), and statistical sampling because many of the enhanced procedures require additional initial training and understanding (Janvrin et al, 2008). Management meanwhile has actively contracted data specialists to develop dashboards and real-time performance evaluation so they can monitor operations of the company in real time and mine for new opportunities that are found through data analysis.

A major source of frustration comes through what is ultimately an unclear definition. A PricewaterhouseCoopers survey in 2007 showed that the majority of internal auditors were using or planning to implement “continuous auditing”. Yet a separate survey of internal audit departments of leading firms found that the application of this enhanced audit technique is inconsistent and interpreted in different ways (Vasarhelyi & Kuenkaikaew, 2011). Some of the main issues arise from a perceived

lack of value of these enhanced procedures and an inadequate skill set on the part of the auditors (Gonzalez et al, 2012; Greenstein & McKee, 2004; Janvrin et al., 2008a).

Even the process alone of evaluating the audit and incorporating enhanced auditing techniques can be beneficial. The benefits of audit efficiency and effectiveness don't necessarily come directly from adopting new technology; rather, they are manifest as the audit is reevaluated and the number of redundant and ineffective tests is eliminated (Fischer, 1996).

The purpose of the EACM is to provide a systematic approach for auditors (both internal and external) to identify clear opportunities for enhanced audit procedures as they reengineer their audit plans. As auditors develop and share their approaches (as they have through Internet forums dedicated to audit scripting programs), more widespread use of these enhanced audit procedures is expected.

It is assumed that before applying this model, auditors have performed their risk assessment and identified their control objectives. This is crucial because the control objectives will pinpoint the types of evidence that will be evaluated to provide assurance. In turn, the evidence attributes will dictate the types of enhanced audit procedures that can be adopted.

The rest of this chapter is laid out as follows: section 2 defines enhanced audit procedures and types of audit evidence; section 3 details the EACM and provides examples of evidence; section 4 shows an application of the EACM to the audit plans of two multinational companies; section 5 contains a summary analysis and conclusions, with limitations and opportunities for future research.

The Enhanced Audit Approach

The term "enhanced audit" refers to advanced and emerging auditing techniques that are designed to increase audit efficiency and effectiveness. These include diverse types of data analytics, automated tools, remote information and communication technology, and the appropriate scheduling of audit procedures. In theory, greater use of these auditing techniques enables auditors to collect more reliable evidence and provide better insight for management and other stakeholders, although the benefits often come from the "reduction or elimination of audit procedures performed in the past" rather than by the technology itself (Fischer, 1996).

The academic literature has focused primarily on three major classes of enhanced audit procedures: audit automation (Coderre, 2008; Dowling & Leech, 2007; Janvrin et al., 2008a; Vasarhelyi, 1983), remote auditing (MacNee, 2010; Sayana & CISA, 2004; Teeter et al., 2010), and continuous auditing (Brown et al., 2007; Groomer & Murthy, 1989; Kogan et al., 1999; Rezaee et al., 2002; Warren & Smith, 2006). More classes likely exist or are emerging, but the discussion presented here will be limited to these three because of the prominence of these methodologies and to simplify the model.

Audit automation has gained traction as the format of audit evidence has shifted from an analog to digital format. The first automated audit procedures appeared shortly after computers entered the realm of business information in the 1960s (Cangemi & Singleton, 2003). With the popularization of spreadsheets in the 1980s and more advanced scripting languages of the 1990s and 2000s, computer assisted auditing tools and techniques (CAATTs) became the auditors' standby for collecting and analyzing

evidence (Coderre, 2008; Sayana & CISA, 2004). Automation reduces the number of steps that an auditor must perform manually to gather evidence and form an opinion about a particular process or control.

As more data are captured in relational databases and ERP systems, additional rich insight can be gathered from that data. Initially, auditors must use their analytical skills to manually discover relationships, patterns, and procedures that support an assertion or provide evidence of an internal control failure. Once a procedure is validated, it is then formalized and can be scripted to generate the same output with a defined set of parameters that can be adjusted as needed (Alles et al., 2006). Automated audit procedures make it trivial to analyze entire populations or filtered samples, decrease audit risk and increase effectiveness. Automation reduces the number of menial tasks that auditors perform, increasing efficiency and allowing them to allocate more time to interpret results and use their professional judgment rather than collect and manipulate data (Dowling & Leech, 2007).

Automation also brings a particular set of challenges to the audit. A common application of automation is through the use of decision aids, where data analysis generates a set of recommendations for the auditors (such as pass/fail, threshold values, and risk indicators). Audit firms have often shied away from automated decision aids because they feel auditors often over-rely on output generated by these automated procedures rather than exercising their professional judgment and skepticism (Dowling & Leech, 2007). This effect is particularly troublesome as employees learn how the automated tests work or the threshold limits for transactions and are able to pass

questionable transactions through the system undetected. For this reason, it is important that automated procedures are re-evaluated periodically and updated or deprecated as the business itself evolves.

Remote auditing adopts the notion of telecommuting as part of the audit process (MacNee, 2010). Primarily used as a cost-saving efficiency measure, auditors connect with evidence via information and communication technology. E-mail and web conferencing enable auditors to interact with clients and other audit team members. Centralized electronic working papers reduce redundancy and loss of audit evidence. Remote access to ERP systems allows auditors to collect and analyze data from any networked location. Coderre refers to these enabling technologies as beneficial electronic audit support tools (BEASTS) (2005).

Remote auditing is typically employed as part of the audit planning process and initial risk assessment. It can also be used to perform substantive testing during the audit and is a critical component of continuous monitoring. The most visible limitation to remote auditing procedures is that clients see the auditors less, though auditors can maintain contact with the audit committee through periodic conferences or e-mail and shift to a continuous monitoring role. This passive presence has been shown to have a negative effect on auditor performance and can be extended to controls compliance (Brazel, Agoglia, & Hatfield, 2004). While it is unlikely that an entirely remote audit will become common, where remote procedures are in place, fewer auditors are required to be onsite and can instead rely on virtual team members to provide support in the form of substantive testing or querying to those auditors.

Continuous auditing takes automated and remote auditing procedures and synchronizes them with the generation of key data. Instead of following the traditional cyclical approach of the traditional audit, continuous auditing procedures are be run at critical points throughout a business cycle to validate enterprise data and monitor the continual functioning of internal controls (Alles, Kogan, Vasarhelyi, & Wu, 2010b; Rezaee et al., 2002; Wu, Kogan, Alles, & Vasarhelyi, 2005). The goal of continuous auditing is to alert auditors of internal control failure as soon after the failure as possible, thereby limiting the exposure and resulting potential loss (Groomer & Murthy, 1989). One challenge with continuous auditing is controlling the volume of alerts generated by the system. Controls with a high volume of transactions are at a higher risk of false positives, so the continuous auditing procedures must be fine-tuned to reflect the risk associated with each of the controls (Alles et al., 2008).

Each of these three approaches provides clear benefits to the auditors and the organization being audited. The enhanced audit at IBM provides greater executive oversight, increased audit coverage, reduced audit and organizational costs, and reduced disruption of business operations (Langford, 2010). This is the result of the shift to an on-demand approach that requires fewer audit visits and a more comprehensive analysis provided by automation. Tables 5.1, 5.2, and 5.3 provide additional comparison with the traditional audit. Dowling and Leech (2007) also show that audit firms benefit from better compliance with auditing standards, improved risk management, and better consistency across firms when using enhanced auditing tools such as automated decision support. In the same study, audit managers caution that the increased

complexity is not always cost efficient and requires significant amount of training for the auditors. If the system appears to be too complex, auditors will cause auditors to ignore the system and revert to traditional methodologies instead.

Table 5.1: The value proposition of an enhanced audit approach at IBM[2]

	Traditional Audit Approach	Enhanced Audit Approach	Value Proposition
Data	Push When requested Single source (requires reconciliation) Risk Based Analysis	Pull Immediate when needed Multiple "trusted" sources Total Universe Analysis	Improved audit efficiency and effectiveness Improved executive oversight Reduced audit and line costs Reduced audit impact on respective line organizations
Coverage	Cyclical "Go" model Audit resources – 13-20 person-weeks/review Significant client impact	On demand Remote model Audit resource – 2-5 person weeks Minimal client impact	

Table 5.2: Perceived benefits and limitations of providing automated decision support [3]

Benefits	Limitations
Enhances audit quality through compliance with auditing standards and audit methodology Increases audit efficiency Consistent audit approach across clients Improves risk management Facilitates documentation Controls junior staff	Auditors can over rely on recommendations made by the system Mechanistic behavior — emphasis on ticking the box rather than judgment Significant amount of training required Stability of technology Not cost efficient on very small jobs Perceived complexity of the system can result in auditors not adopting the technology, or working around it by using word documents

The process of enhancing the audit requires an analysis of the audit plan to determine the tradeoffs that auditors and firms are willing to make to provide enhanced assurance, while minimizing the disruptive nature of the technology. Before that happens, an evaluation of the firm's information systems will provide valuable insight

[2] (Langford, 2010)

[3] (Dowling & Leech, 2007)

into the feasibility of the enhanced audit approach. The ability of an organization to adopt enhanced auditing techniques relies primarily on the format and availability of audit evidence. For example, automation makes little sense when the auditors are trying to analyze paper forms. But auditors who have online access to ERP tables can easily extract and analyze those tables over a network connection remotely rather than doing it on site.

Audit Evidence

Audit evidence is "all the information used by the auditor in arriving at the conclusions on which the audit opinion is based and includes the information contained in the accounting records underlying the financial statements and other information" (AICPA, 2006). This information is used to support or disprove management's assertions over financial and non-financial information, including the existence and operation of internal controls. Specific audit evidence is typically outlined in the audit plan and collected together in the audit working papers.

The audit objective (or assertion being tested) determines what evidence will be collected and the approach used to collect it. For example, an auditor who wanted to test the assertion of inventory existence would need to know where the inventory is located, and likely choose to observe the inventory in person. The evidence would be recorded on an inventory count reconciliation form. Likewise to test the assertion that IT controls function properly, the auditor might observe a transaction being processed through an online system or reperform a transaction with the intent to bypass controls.

The evidence would be found in the database table containing valid transactions, or a snapshot of the control configuration in an ERP system.

The PCAOB (2010) and AICPA (2006) outline general procedures for obtaining audit evidence in Auditing Standard 15 and SAS 106, respectively:

Inspection traditionally includes a spot check by the auditors of critical attributes of a piece of evidence, such as an authorized signature on a purchase order or a physical count of inventory items in a warehouse. If the signature is only available on a physical document, the auditor must physically locate that document and verify that the signature matches an authorized approver list. If the document is recorded in a well-controlled ERP system, the auditor could run an automated CAATT that would check the user ID of the person who created it and compare it to a table of authorized user IDs. This procedure would validate all of the records from the specified period and generate a list of unauthorized records for the auditors to validate, if any. If the auditor has network access to the ERP system, he could run the procedure remotely. Enabling continuous evaluation of those records would only require the additional step of scheduling the CAATT to run at a specified interval.

Observation allows auditors to follow a process from beginning to end. Typically an auditor would shadow en employee and watch them complete their workflow to ensure that all of the necessary steps are followed in the correct order. As more of these workflows are completed on the computer, log files record the date and time of each step as it's performed. Automated analysis of these logs provides auditors with a sequence of events that can be observed without disrupting the line employees and

identifies out-of-sequence events. Auditors can also observe manual business processes remotely through closed-circuit video recording.

Inquiry consists of collecting statements and observations from employees. This can be through in-person interviews; statements sent via e-mail, self-assessments collected through an online reporting system, or through web conferencing. Large quantities of text documents can be mined for key phrases through an automated process. Analysis of the formalized reporting can be automated and monitored at a scheduled interval for trends.

Confirmation requires an outside party to validate some data, such as an account balance or invoice amount. Confirmation is generally performed remotely via phone, letter, or e-mail. Electronic data processing (EDP) allows companies to validate balances with suppliers and providers automatically. Additional tools allow trusted remote electronic confirmation.

Recalculation ensures that a calculated value is correct by verifying the components built into the value as well as the arithmetic. Auditors typically perform this procedure is typically designed to be performed manually as a method for verifying calculations performed within computerized systems or spreadsheets, although replication of standard calculations can be automated to a certain degree.

Reperformance has auditors retracing the steps that created the output being tested. An auditor may follow an output back through a system to its source document or, alternatively, pull a source document that has been processed and go through the steps of recording and maintaining the data and matching it to an output. As with

recalculation, this is generally performed manually, although auditors could validate this process remotely if it is processed through an online system.

Analytical procedures identify plausible and expected relationships between financial and non-financial data. These include trend analyses through prior period comparisons, regression analyses involving complex relationships, ratios, and other substantive tests. In most cases analytical procedures are performed as part of the audit planning process to identify areas with high risk and exposure. Most analytical procedures are automated and performed remotely as part of the audit plan because they rely heavily on data. In continuous auditing, these are performed at specified intervals and can be used to trigger further procedures or auditor investigation.

Within each of these processes, there are multiple tools available to auditors to collect the evidence necessary, depending on the format and availability of the data being gathered. Table 5.3 presents examples of traditional and enhanced audit techniques that are available to aid the collection and analysis of the evidence. With any approach to evidence collection and analysis, there are limitations that guide the auditor's approach. The evidence must meet tests of appropriateness and sufficiency. Data that are unreliable require additional investigation into source documents, etc. Procedures that are untimely or dated may not give an accurate picture of today's operations. Data must also be valid for supporting audit conclusions. Also the number of observations required providing reasonable assurance will drive the selection of audit procedures.

Table 5.3: Evidence and examples of enhanced audit procedures

Types of Evidence	Traditional Audit Approach	Enhanced Audit Approach				
Sample Evidence	Audit Method	Limitations	Manual	Automated	Remote	Continuous
Documents Records	Inspection	Reliability	Vouching and physical tracing	OCR, automated source data evaluation	Evaluation of e-filed documents	Daily exception reporting
Process Procedure Control	Observation	Timeliness	Worker shadowing	Process log mining	Video recording	Evaluation of automated workflow controls
Written/oral statement	Inquiry	Reliability	In-person interview	Text mining	Web conferencing	Frequent control self-assessments
Account balance	Confirmation	Timeliness	Written oral response from third party	EDP for suppliers and providers	Electronic communication (e-mail/fax)	Real-time transaction validation
Calculated figure	Recalculation	Reliability	Manual recalculation	Macro with defined calculation values	Calculated values queried from ERP	Automatic calculation validation
Transaction	Reperformance	Reliability	Manual completion of workflow	Process log mining	Validate workflow in online system	Validate each transaction as processed
Relationships Exceptions Derivatives	Analytical procedures	Validity	Calculation of ratios	Macros, statistical software, scripting	Collection through online systems or e-filing	Scheduled validation of controls

A preliminary analysis of the audit plan provides the auditor with the entire set of evidence needed to substantiate the audit. More formalized procedures may even identify the specific table, field, and attribute in enterprise systems. This exercise produces a tailored data map that auditors can then use to request their data more easily (one large request rather than multiple small requests). As organizations have embraced modern computerized systems, however, gaining access to enterprise data needed to support the audit has proven to be particularly challenging to auditors. Beyond lack of clear communication of what data are "appropriate" and "sufficient" for the auditors to complete their work, the IT custodians and auditors are often at odds when it comes to sharing data. This may provide one explanation why audit procedures currently consist of multiple data requests and manual data manipulation as part of the cyclical audit.

Auditors need unrestricted access to certain data in order to provide evidence for their audit, and IT wants to control and restrict access, particularly if the data may implicate that their systems possess previously unknown weaknesses. Hermanson et al (2000) and Bierstaker et al (2001) observe this conflict, and anecdotal evidence from the research team's dealings with the internal audit departments of two firms suggests that some auditors continue to receive data that is often incomplete, delayed, or insufficient. As a result, auditors on strict engagement timelines must dedicate more time to clarify their data needs or limit the scope of their analyses.

Gaining access to data and evidence are one issue, understanding the data and how to apply specific enhanced audit procedures is another. This essay's main contribution is

to address the lack of clear guidance in this area by helping auditors focus on key evidence and identifying those opportunities for automated, remote, and continuous audit procedures.

The Enhanced Audit Classification Model (EACM)

The audit approach selected by auditors and incorporated into the audit plan is generally based on an analysis of the audit objectives or assertions and specifically based on the audit evidence the available to the auditors. In the traditional approach, auditors inspect, observe, inquire, confirm, recalculate, reperform, and analyze the evidence largely by hand, even when much of the data originates from computerized systems. Understanding the nature and format of the evidence can help auditors select more efficient and effective procedures. The EACM is designed to aid that understanding.

For the purposes of this model, evidence is defined as a specific set of data that is used in analysis. For example, authorization is validated by the existence of an authorized signature on a certain document type (such as a check or order). The remaining data contained in the document is considered irrelevant for the enhanced audit classification. Likewise, to inspect whether super user access is permitted in a system, the evidence is found in the specific binary field in the control settings matrix. The focus on specific data eliminates noise and can better identify the appropriate audit approach.

Each distinct piece of audit evidence possesses some attributes that describe its characteristics. The EACM focuses on three of these attributes: nature, extent, and

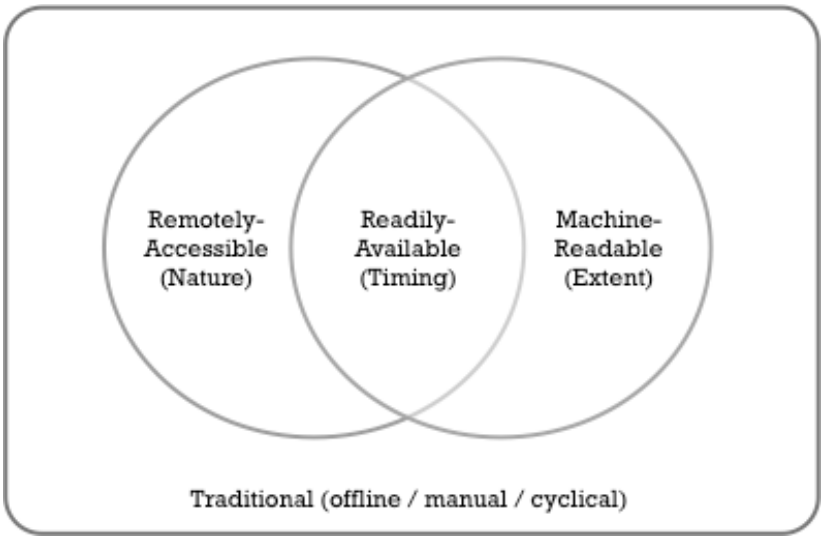
timing. These coincide with similar attributes of general audit procedures found in SAS 110 (AICPA, 2006).

Nature refers to the accessibility of the audit evidence. The nature of the evidence will guide the method (inspection, observation, etc.) and location chosen by the auditor for collection and analysis. The nature of the evidence more narrowly describes whether the evidence can be securely accessed remotely either through a direct network connection, in the case of online systems, filed electronically into an electronic document management system, or transferable to the auditor through e-mail or other reliable electronic means. If the evidence meets any one of these criteria, the auditors have an opportunity to implement remote auditing procedures where appropriate. Otherwise, the auditor must work onsite as in the traditional approach.

Extent describes the format of the audit evidence. This drives the useful quantity of evidence available to auditors for sample selection, exception reporting, or full population testing. Specifically, extent describes whether the evidence is available in a machine-readable, digital format (e.g. XML or SQL), and whether the data are sufficient on their own to support the auditor's conclusion. Automated procedures are dependent on structured, formalized data. Where the data are insufficient to produce an acceptable conclusion on their own, automation can be used to select targeted samples that focus on exceptions or other high-risk observations (as specified by the auditors) rather than relying on random sampling. Where data aren't available in a machine-readable format, traditional manual analyses are required. Timing describes when evidence is generated and relevant to an audit decision. This informs the auditors as to

the appropriate scheduling of auditing procedures, a key component of continuous auditing. Timing may fit in one of many intervals (daily, monthly, period end, etc.). While a continuous audit of varied evidence would theoretically match all auditing procedures to the availability of evidence (e.g. daily monitoring of sales transactions, monthly auditing of closing entries, etc.), the underlying assumption is that those procedures rely on automation and remote auditing to be efficient and effective for the auditors. Thus, only evidence that is both remotely-accessible and machine-readable would be evaluated on a staggered schedule. Otherwise, the evidence must be verified during the traditional cyclical schedule or adjustments to the manual audit schedule should occur.

Figure 5.1: Audit evidence classification Venn diagram



Using these three attributes, audit evidence can be classified into four categories, represented in the diagram shown in Figure 5.1. Some evidence is remotely accessible, other is machine-readable, and where these two classes overlap, the evidence is readily-available for continuous auditing, and the timing should be indicated. Everything else is considered traditional.

The visual representation of the model illustrated in Figure 5.1 is designed to illustrate the opportunities for enhanced audit techniques (inside the circles) for the auditors to consider when revising their audit work plan. Each class represents the proportion of evidence elements that meet the criteria indicated previously. This means that each organization's diagram will look a bit different depending on the amount of formalization that exists in their business processes.

Because of the nature of audit evidence and the requirements of the auditors and management, the classification process relies on manual evaluation and judgment by the auditors. Additional information may be necessary to determine whether a class is appropriate. For example, as an auditor determines whether evidence is remotely accessible, he must consider not only the inherent transferrable nature of digital data, but also privacy and security controls and regulations that may prevent the data from being accessed outside of the company's intranet or jurisdiction. If these policies can't be altered, the evidence is not remotely accessible and a traditional approach is appropriate.

The classification exercise also provides opportunities for auditors (internal auditors in particular) to make recommendations to management to modernize or improve business processes in a way that generates more easily accessible data. If the current process that generates audit evidence can be reengineered through automated systems or the implementation of other information technology, it should be noted. As auditors classify available audit evidence, it may be informative to collect additional supplemental attributes (such as whether the process can be reengineered, where the

data are located, critical or control values being evaluated, etc.) that would aid the selection and development of enhanced auditing procedures at a future date. See Table 5.4 for an example of classified audit evidence.

Enhancing the Audit Plan

This section outlines the process applying the EACM to an existing audit plan. The objective of this exercise is to identify opportunities for the enhanced audit and changes needed to generate an enhanced audit plan.

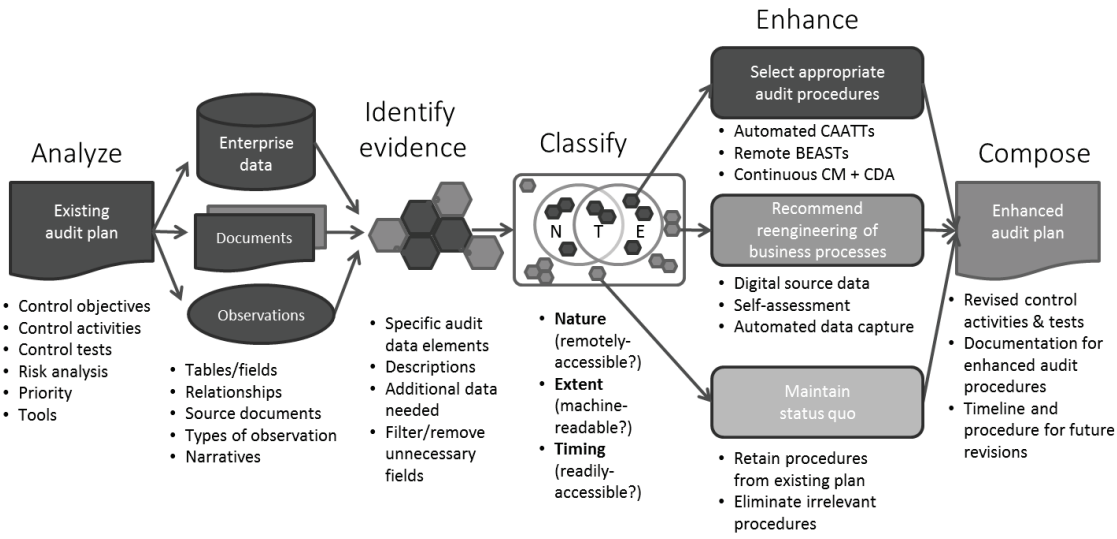
Auditors are more likely to begin with an existing audit plan rather than starting with a clean sheet of paper and developing one from scratch (Alles et al, 2008). Before beginning the process of identifying enhanced auditing techniques, auditors have carefully completed a risk assessment and chosen audit control objectives that will test the assertions made by management. Any additional continuous improvement or total quality management that may have occurred prior to this evaluation is ignored, although the output of this process will likely inform future audit plan revisions. Optimally, this process will be repeated as frequently as necessary to attain a specific goal (e.g. 60% automated, 45% remote, 20% continuous, and 15% traditional), demonstrate the evolution of the audit plan over time or as part of a continuous improvement effort. This is also meant to be scalable. An auditor could focus on a specific audit area, such as Accounts Receivable, or evaluate a comprehensive audit plan.

The process of enhancing the audit plan is illustrated in Figure 5.2.

Table 5.4: Sample audit classification with additional attributes

	Audit Evidence Classification			Additional Attributes			
	Remotely-accessible (Nature)	Machine-readable (Extent)	Readily-available (Timing)	Reengineerable	How	Location	Notes
Sales order amount (ERP)	YES	YES	DAILY	N/A		[Customer orders].[Amount]	Only values over $1000
Sales order amount (paper)	No	No	Daily	YES	(e-filing)	Bldg. A, Room 214, File Cabinet 23	Only values over $1000
Check authorization (e-file)	YES	No	Weekly	No		SharePoint > Bank Reconciliations > [Week#] > Checks	Match signature to authorized user
Inventory count	*No*	*No*	*Monthly*	*No*		Warehouse D	Physical count every 3 months
Superuser access control status (ERP)	YES	YES	DAILY	N/A		[ControlsSettings].[SUA]	High risk, should be 0
Adjusted cash balance (ERP)	YES	YES	MONTHLY	N/A		[FinancialStmt].[AjBal]	Calculated by hand, check [FinancialStmt].[Account]= 1001
Sales order authorization (paper)	YES	No	Weekly	YES	(Move to ERP)	Bldg. A, Room 214, File Cabinet 23	Match signature to authorized user
Sales process documentation	No	No	Yearly	YES	(Cloud)	Bldg. A, Room 219, File Cabinet 10	Review updates since last review

Figure 5.2: Enhancing the audit plan



Analyze the existing plan

The purpose of this step is to identify the specific audit evidence used in the existing audit plan. This involves identifying specific tables and fields within an ERP system, key attributes on source documents, sources of narratives, and/or specific items that require direct observation.

An audit plan typically contains the desired audit activities that are to be validated by the auditors to determine whether they meet management's assertions. While the exact terminology varies from company to company, the audit plan follows a basic hierarchy from general function to specific test (e.g. Operation > Process > Sub-process > Objective > Activity > Test). In the details of the audit test, most audit plans describe step-by-step the tasks an auditor must follow and identifies where the auditor can find the required evidence as well as key attributes that they are to evaluate. The analysis should produce a list of sources of audit evidence and identify the current audit

procedures, including those that involve macros, scripts or other CAATs. Table 5.5 illustrates a sample analysis of one control test.

Identify specific audit evidence used to test assertions

Next, auditors should compile a list of evidence elements that are found on documents, located in databases or other electronic files, or that need to be observed and recorded (e.g. interviews), as indicated in the prior step. This step requires the greatest amount of specific detail. From the attributes being tested, Identify the system, table, and field of data in databases, location of elements on paper documents, and what evidence is needed from observations or interviews (e.g. key words or phrases). Typically, spreadsheets containing this data and subsequent analyses end up in the auditor's working papers. Table 5.6 expands the control test form the previous example and identifies the specific evidence and attributes needed to complete the test.

Classify audit evidence using the EACM.

This step allows the auditor to now apply the EACM to the evidence identified in the previous step. The auditor should have a good indication at this point as to how much opportunity exists for enhancing the audit with automation or remote auditing procedures. For each piece of evidence the auditor will identify whether it is a) remotely-accessible (YES/NO), b) machine-readable (YES/NO), and c) readily-available (i.e. how frequently new observations are available). Some sample questions for determining the appropriate classification are presented in Table 5.7.

Table 5.5: Sample control test analysis

Objective	Activity	Test	Source	Attributes	Current procedure
Orders are only processed within approved customer credit limits.	Credit held orders are released by an independent authorized user.	Obtain a sample of 25 orders on credit limit hold or financial hold over the current fiscal year/period and verify the following key attributes: Released credit held orders were approved by authorized users. Reasons for releasing the order and supporting documentations exist and are filed (release sheets, proof of money in transit, etc.). The order has been released by a person who does not have access to either order entry or master data maintenance.	SAP Table VBAK	The person responsible to execute the credit hold release in the Order/Shipping/Billing system does not have access to order entry and master data transactions (or sufficient compensating controls are in place). The person executing the credit hold release is authorized and within the organization (AR, OM, authorized third party, etc.). List of authorized users for the release of credit held orders exist. All credit held orders are released as per the organization's local authorized user guidelines, prior to the order release in the system. Supporting documentation showing the reason for the release (e.g. proof of money in transit) exists and are filed (release sheets, proof of money in transit, etc.).	Generate the list of all orders that have been released from credit hold for a specific time frame. Obtain a sample of 25 orders on credit limit hold or financial hold over the current fiscal year/period and verify the key attributes

Table 5.6: Specific audit evidence and key attributes

System	Data	Table	Field	Lower Limit	Equals	Upper Limit	Notes	Remotely-accessible? (Nature)	Machine-readable? (Extent)	Readily-available? (Timing)	Reengineerable?	How?
SAP	Sales order Creation date from….to ….	VBAK	ERDAT	XX		XX	XX specified by auditor	YES	YES	DAILY	N/A	
	Company code	VBAK	BUKRS_VF		LE#		Local entity #	YES	YES	DAILY	N/A	
	Credit Control Area	VBAK	KKBER		CC#		Local credit control #	YES	YES	DAILY	N/A	
	Overall credit status	VBUK	CMGST		"D"		Released credit hold	YES	YES	DAILY	N/A	
	Released by	VBAK			T#			YES	YES	DAILY	N/A	
Document	Supporting documentation showing the approval for the credit hold releases selected in the sample				Auth user		Matches list of authorized users	No	No	No	YES	E-file, signature check

Table 5.7: Determining the audit evidence class

Remotely-accessible? (Nature)	Machine-readable? (Extent)	Readily-available? (Timing)
YES Data can be accessed over a network Documents can be transmitted electronically Interviews can be conducted by e-mail, phone, fax, video	YES Data is available in a computer-readable format (e.g. XML/XBRL, SQL, JSON) Data is generated automatically and has clear relationships No user involvement necessary beyond initial setup, exception resolution, and review	YES Both remotely-accessible and machine-readable High/medium risk of control failure High exposure, materiality, and magnitude per incident High volume of transactions
NO Privacy laws restrict data movement or disclosure (e.g. HIPAA, Safe Harbor) Auditors need to observe original documentation Auditors assess environment, interview managers, observe processes	NO An auditor must be involved in manually observing, collecting, extracting, manipulating source data Original source documents are required Interviews and observations of business processes	NO Low risk of control failure Non-material, self-correcting Appropriate risk tolerance

Evidence is classified as remotely-accessible if it can be accessed or transmitted over a network from a remote location and there are no legal restrictions or integrity concerns with its transfer. This typically includes data stored securely in ERP systems where even an auditor connecting from the business site would not typically be in the same physical room with the server. It would be inappropriate to classify evidence as remotely-accessible if there is the potential for material alteration of the source documents before submission or access, or if the control failure has sufficient exposure and the auditor would want a better understanding or feel for the process.

Evidence fits the machine-readable class when it is available to the auditor in a computer-readable format, such as XML. Data that are tagged or clearly identified with relationships to other data would fit this classification. Since this data lends itself greatly to automated procedures, it should require no user involvement beyond the initial

setup and review. Interviews and observations are not typically considered machine-readable unless the transcripts have been digitized and filed electronically, such as with a self-assessment.

Evidence that is both remotely-accessible and machine-readable is automatically classified as readily-available. The main difference with this class is in the determination of timing of evidence generation and availability. The auditor would determine the frequency of readily-available data to enable the scheduling of remote, automated procedures in the next step.

Auditors charged with identifying opportunities to reengineer the audit or improve the generation and collection of evidence will want to expand their analysis at this point. For example, they should identify additional or alternative attributes and parameters that may generate a richer conclusion. They might also suggest changes to the business process to enable greater use of information technology in capturing and storing operational data. Any additional notes will help as auditors move to the next stage of selecting and developing more appropriate tests than are in the current audit plan.

A measure of the raw percentage of audit evidence that fits within each of the four classes (Remotely-accessible, Machine-readable, Readily-available, and Traditional) provides a visualization of the opportunities for the enhanced audit, similar to Figure 5.1. Some examples of the classification percentages from different audit plans appear in Table 5.8.

Table 5.8: Sample distribution of classes for different companies

Class	Percentage	
	Highly-formal company	Highly-manual company
Remotely-accessible only	80	50
Machine-readable only	70	30
Readily-available (i.e. both remotely-accessible and machine-readable)	65	15
Traditional	20	45

Select or develop appropriate audit procedures.

In this step, the auditor will take the analysis of the audit plan and identify appropriate enhanced audit procedures that would enable the more effective and efficient audit. Tailoring the audit procedure to the available evidence enables greater coverage and the potential to minimize audit risk and exposure.

There are three primary outcomes of this process:

1. Select or build more appropriate audit procedures, such as automated CAATs, remote BEASTs, and continuous monitoring and data assurance;

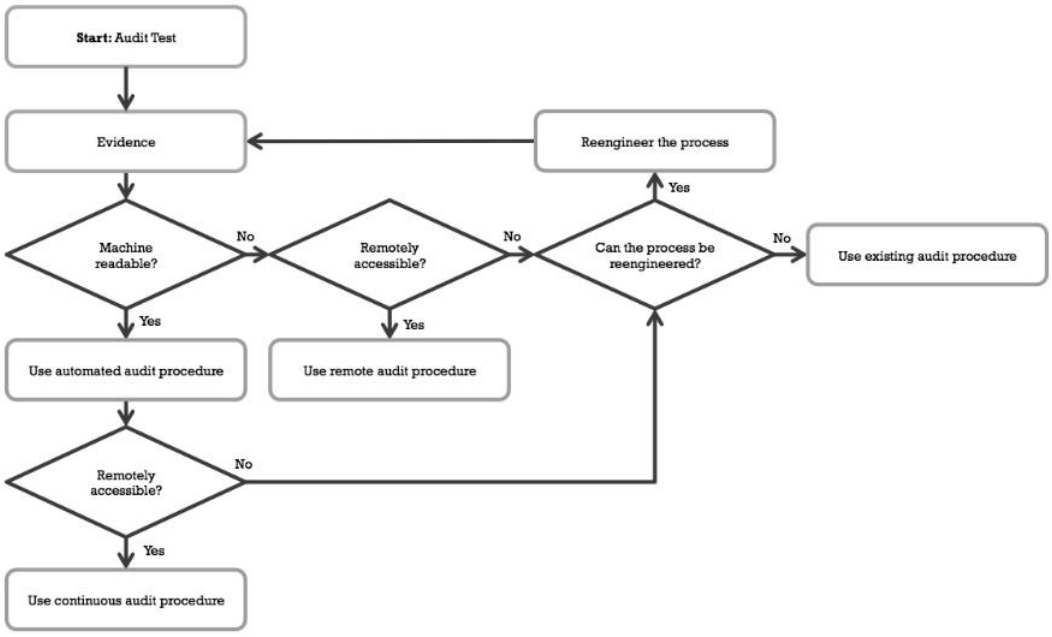
2. Recommend reengineering of business processes through increased use of digital source data, self-assessments, and automated data capture; and

3. Determine which tests are appropriate in their current state and eliminate irrelevant or redundant tests.

In selecting more appropriate audit procedures, the auditor should choose audit procedures that match the data class whenever possible and permitted within the audit framework, as described in Figure 5.3. Each procedure should match a sub-process of each audit test. Beginning with each test, the auditor first determines whether the corresponding evidence is machine-readable. If so, an automated audit procedure (such

as macros, scripts, or other analytical tools) can be used for a portion of the test. Next, the auditor determines whether the evidence is remotely accessible. If yes, then a remote audit procedure (such as passing work to virtual audit teams, linking databases, or combing through electronic document management systems) is appropriate. If the auditor answers yes to both questions, then the remote-automated procedure can be scheduled to run at the specified interval as a continuous audit procedure (including scheduled transaction analysis, continuous monitoring of business process controls, and data validation and assurance).

Figure 5.3: Classifying audit evidence and selecting appropriate audit procedures.



If the auditor finds the evidence to be neither machine-readable nor remotely accessible, a final determination must be made to see whether the process can be reengineered or not. The goal of the reengineering process is to ask better audit questions, and generate more appropriate audit data. The rationale given to management should include some additional benefit to tracking the business process

(through monitoring and enhanced evaluation) as well as the utility to auditors (lower cost, better results). If reengineering is permitted, the evidence will be reclassified one the reengineering has taken place. Reengineering efforts should result in evidence that is remotely accessible and/or machine-readable.

Finally, in many cases the existing (traditional) audit approach remains the most appropriate solution. Auditors should determine whether the existing approach continues to be effective and appropriate for the audit objective. If the test is no longer valid, the risk and exposure are low, and/or the usefulness no longer exceeds the cost, then the test should be eliminated.

For the example in Table 5.5, a script could be used to query a list of released orders on a daily basis, compare the release authorization to an authorized user table, and generate a list of orders that were released by an unauthorized user. In a well-controlled environment, exceptions would be very rare, but the auditors would not have to spend their time sampling and verifying documentation manually every time the audit came around. If the authorized user is not captured in the SAP system, then the sample and verify test remains the most appropriate test.

This phase includes testing the procedures, comparing them against traditional results, getting feedback from the business process owners and audit team, and identifying any changes that need to be made. In the future, a marketplace may exist that will simplify this process considerably. In the meantime, online auditor forums and communities provide the best resource for developing and selecting appropriate scripts

and procedures. The result of this exercise is an optimized set of audit procedures that are more appropriate for the evidence being generated and used in the organization.

Generate an enhanced audit plan

The end goal of the classification process is to establish an enhanced audit plan that reduces auditor effort by incorporating more appropriate procedures for analyzing audit data. This step involves compiling the procedures identified in the previous step, identifying the key attributes for testing, and completing the documentation necessary to describe the new and revised procedures and tests, and enhance the audit process. This will also divide the audit into the (potentially less frequent) cyclical manual audit, and a scheduled, exception-based continuous audit.

Validation of the Model

An analysis of the audit plans used in the field studies presented in earlier chapters of this dissertation was completed to provide examples of the extent that enhanced audit opportunities exist in formalized and manual environments. The validation process consisted of an analysis of the audit objectives and tests from the two plans, the identification of specific audit evidence (data and observations), and the classification of that evidence into one of the four categories. The selection of audit procedures and the reengineered plans for both are not covered in this paper.

Analysis of the Audit Plans

The breakdown of the classified evidence can be found in Table 5.9 below. For each audit plan, the control tests or activities were identified first and then broken down into individual sources of evidence.

The highly-formalized ERP certification audit plan contains 284 control tests covering all of the major business functions. These tests include authorization tests, baseline indicators, separation of duties constraints, automated controls, etc. Of those tests, 372 sources of evidence were identified. Through classification, it was determined that 306 sources of evidence were available remotely in their current form, 247 were machine-readable, with an overlap of 234 that were both. 56 data elements (including interviews and observations) were neither.

For the highly manual revenue audit, there were 40 control activities covering collection of accounts receivable, with 96 matching sources of evidence. The majority (79) of the evidence is transferrable and remotely accessible. However, given the nature of the current tests, most of the procedures require a comparison to some offline record, such as a piece of paper, so only 30 of the sources of evidence are in a machine-readable format and partially automatable.

Table 5.9: Evidence classification from two audit plans

Audit Plan	Tests	Evidence sources	Remotely-accessible	Machine-readable	Readily-available	Everything else
ERP Certification	284	372	306 (82%)	247 (66%)	234 (63%)	56 (15%)
Revenue	40	96	79 (82%)	30 (31%)	30 (31%)	17 (18%)

Generalizing the EACM

Because the EACM is used to classify the characteristics of audit evidence, it can be applied within the context of an organizations overall audit objectives and scalable to small subsets of an audit plan or expanded to larger sets of procedures. The absence of hard classification rules limits the direct comparability of one audit plan to another.

However, the purpose of the EACM is to help individual auditors easily identify opportunities for enhanced audit procedures and so such a direct comparison is not necessary. The auditor may wish to define the attributes used in the classification if he wants to compare the makeup of the audit plan over time.

Conclusion

This paper describes the EACM and provides analyses of the audit plans provided by two large multinational firms. These examples illustrate the fact that current audit procedures are not ideally matched with the underlying data produced by ERP systems. The paper also identifies opportunities for further research into an audit data standard and an additional push for audit reengineering.

The enhanced audit classification model (EACM) was developed to synthesize the audit automation, remote audit, and continuous auditing concepts and delineate the relationship between the three. The EACM provides auditors and researchers with a framework for identifying opportunities for audit innovation based on the properties of the underlying evidence used in the assurance process. This essay provides auditors with a method for identifying critical audit data and selecting appropriate enhanced auditing tools and techniques (EATT) based on the attributes of those data.

Additional research might explore whether there are additional or alternative classes beyond those mentioned in the EACM, how adoption of new systems would affect the different class distributions, and whether it would be appropriate to classify audit procedures in a similar manner. These questions will be addressed in extensions to this essay.

Finally, this chapter examined a process for identifying and selecting enhanced auditing procedures into an audit plan based on the underlying audit evidence. While a purely data-driven audit is not ideal, the nature, extent, and timing of audit evidence can inform the auditors of specific opportunities for enhanced auditing tools and help modernize the audit process.

CHAPTER 6. CONCLUSION

The objective of this dissertation is to provide a framework and methodology for enhancing the internal audit function within an organization. This is accomplished by 1) analyzing the existing audit plan, 2) classifying the audit evidence that is used to support management's assertions, 3) identifying opportunities that exist to develop and implement enhanced audit tools and techniques, and 4) measuring the outcome of the enhanced audit effort.

The enhanced audit combines contemporary information and communication technology with data analysis and auditor judgment with the goal of producing a more efficient (reduced auditor effort) and effective (increased audit coverage) method of providing assurance. The business environment and utilization of the enterprise system and the type and format of evidence (data) available to auditors within the enterprise are key drivers for determining where enhanced audit tools and techniques can be employed.

The benefits of automation in auditing are widespread and known (Coderre, 2008; Janvrin et al., 2008a; Keenoy, 1958; Manson, McCartney, & Sherer, 2001). Automated auditing procedures have been shown to increase the coverage of the audit while maintaining or reducing audit effort, including the amount of time spent by auditors on low-level tasks. However, automation requires auditors to better understand how these new auditing tools work and possess greater analytical and judgment skills.

Auditors are tasked with utilizing improved auditing procedures (PricewaterhouseCoopers, 2007). This involves creating automated tools and

procedures that can be used analyze evidence that is stored in or converted to a computer-readable format (such as XML). The algorithms used in these procedures can include straightforward queries of database elements, or incorporate more sophisticated rules and statistical analyses. Regardless of the methodology used, these tools enable auditors to offload tasks that are redundant and labor-intensive so they can spend greater effort on providing judgment. Additionally, the auditors can continually improve their audit function by exploring additional tools that will provide greater assurance. The more advanced of the processes borrow from the field of data mining and machine learning to identify patterns and trends that aren't apparent in casual observation (Janvrin et al., 2008a).

The increased frequency and availability of enterprise data enables more frequent auditing, which is one of the primary objectives of the continuous audit. Data portability enables the remote audit. The level of interactivity, frequency, and portability of data dictates what audit procedures are technically feasible within an internal audit organization, though there are certainly other organizational factors that provide constraints to these processes. The reengineering process then requires either selecting more appropriate data sources or formalizing business processes that will enable the generation of more readily available data.

Actual efforts to reengineer the audit appear to be more incremental than radical, as observed in the previous chapters. In practice, internal auditors who express interest in reengineer and enhance their audit to enable greater use of technology tend to begin with their existing audit plan and convert or reengineer the audit procedures one-by-

one. In the case of Maritis' IT certification audit, a large percentage of the procedures were converted to automated procedures directly while little reengineering of the underlying processes was necessary. Conversely, Nouant auditors found it difficult to enhance the audit plan without significant changes to how the business processes collect and store audit evidence. In that case, reengineering of the business processes precedes the use of enhanced audit technology that facilitates the collection and analysis of the data. In either case, the insight gathered in these studies support the observation that the automation/enhancing/reengineering process forces auditors to concurrently review and reduce or eliminate audit procedures that are no longer useful or relevant.

The field studies presented in the previous chapters highlight the complexity and considerations in automating existing audit procedures. While the current audit plan identifies the enterprise data to test and the details of the procedures to be performed, auditors and researchers continue to overestimate the formalizability of these procedures. In many cases the procedures are too limited or are located too far beyond the scope of electronic enterprise data to be automated. However, these studies validate the opportunities and need for enhanced audit tools and techniques.

Summary of Essays

The first essay (Chapter 2) describes the implementation of a continuous monitoring platform at Maritis. The study documents the process used to analyze the audit action sheets, develop formal, rules-based tests that could be automated, and implement and validate those rules against a concurrent manual audit. This study

provides a look at the comprehensive implementation of a continuous monitoring process for an IT certification audit. The uniformity of the implemented ERP system throughout Maritis worldwide allows scalability throughout the organization with significantly reduced effort. Of the population of audit tests, 63% were completely automated including 100% of authorization and access controls. The concurrent manual IT audit provided feedback and validation of the automation effort.

The second and third essays (Chapters 3 and 4) describe an attempt at implementing remote auditing procedures. The study documents the analysis of the revenue audit tests and recommendations made by the auditors to allow remote collection and analysis of audit data. Additionally, insight is gained into the methodology used in this analysis as well as the technical and political hurdles that exist as a part of the audit change. Nearly half of the audit procedures contain an element that can be remotely accessed and audited. However, significant changes to the business processes that generate the audit evidence are required if the auditors are to gain additional efficiency in the audit, a la data analytics and automation.

The final essay (Chapter 5) attempts to synthesize the overall process of selecting enhanced audit procedures as part of the audit reengineering process. By formalizing the characteristics of enterprise data, the enhanced audit classification model provides a simple tool for identifying opportunities for automated, remote and continuous auditing procedures within an organization. Analysis of the audit plans for Maritis' SAP certification and Nouant's order-to-cash audit provides insights into what is possible and what needs to change in the business processes themselves in order for auditors to

create more progressive audit plans. It also provides a metric for continuous improvement of the audit function.

Contributions

There are several practical and theoretical implications of these studies.

Audit efficiency: In highly formalized environments, automation provides significant gains in the scope of the audit and reductions in the frequency of traditional in-person audits. In highly manual environments, automation is difficult to achieve without significant changes to the underlying business processes that generate evidence. The observation and documentation of two real-world firms provides confirmation that this is the case and provide a normative process for firms interested in continuous assurance.

Technology adoption and use: This dissertation provides evidence that the political hurdles and technical limitations faced by auditors are significant, and greatly limit the speed of adoption of enhanced audit procedures. The Maritis study reveals that management buy-in was high initially but could only take the project to the initial implementation stage. The consumer goods firm studies show that the expectations of auditors and the capability of the technology are sometimes at odds. This corresponds to technology adoption and use literature that shows that auditors adopt technology when the expected effort and social buy-in are high (Gonzalez et al, 2012).

Opportunity for continual improvement in the audit: The enhanced audit classification model is the first to formally synthesize the research of audit automation, remote auditing, and continuous auditing into a unified frame for auditors and

researchers. It had been assumed previously that these fields were related; yet previous research has tended to treat these concepts as separate fragments or make assumptions about the underlying ideas. Sample validation of the model exposes the untapped opportunity that exists within current audit plans. The audit plan is continually and iteratively revised and updated within an organization and the EACM provides a tool for evaluating the current state of the audit plan and identifying areas for improvement. The output provides clear indicators for audit enhancement.

Limitations

The two field studies and conceptual model presented in this dissertation have several limitations that should be noted. First, the nature of field studies inherently limits the generalizability of the outcomes presented here. While there may be firms that are functionally identical to the two firms observed herein, those firms are unlikely to encounter identical results. There are a number of factors, including the type of enterprise system, brand of monitoring software, and technical expertise of the auditors that can alter the results greatly.

Second, while the general audit assertions covered in the audit plan are consistent across firms, the individual objectives, activities, and tests are proprietary to each organization. This means that researchers must rely on additional qualitative and anecdotal data in their analysis of the audit plan and are likely to classify data differently. This also introduces some limited observer bias, which may affect the objectivity of the study.

Third, the long-term effects and implications of automation, remote auditing, and continuous monitoring are not documented here. A future review of these cases may provide insight into the longevity of such attempts, or more likely the continuous evolution of the audit plans and tools.

Finally, the enhanced audit classification model presented in this dissertation was distilled from the process and results of the field studies instead of the other way around. Each of the studies provides a distinct dimension of the enhanced audit plan, but do not completely explain the model. Validation by implementation is only available for the respective halves. The ex-post analysis of the two audit plans in the context of the EACM reflects the current state of the audit at both firms at the time of implementation.

Directions for Future Research

The evolution of the audit toward more effective and efficient enhanced procedures provides a narrative into the decisions auditors make in the analysis, selection, and implementation of auditing tools and techniques. This dissertation provides a framework for that analysis. Future research should seek to document that continuous improvement through the lens of the availability of audit evidence. This would include a longitudinal study of firms' periodic evaluation of the audit plan and implementation of enhanced audit tools. The link to change management theory and technology adoption should also be explored in greater depth.

As market demand and institutional acceptance of a more robust assurance process increases, better understanding of the level of adequacy and quality of enhanced audit

tools is needed. A marketplace for these enhanced auditing tools is expected to emerge within the next few years. The execution and implications of that marketplace warrants additional research consideration.

In conclusion, auditors have much to gain from the increasing availability of information technology and sophisticated analytical procedures. Research into the effectiveness of these tools can guide auditors in their selection of appropriate procedures for their organizations. The field studies presented in this dissertation provide insight into that identification and selection process. The enhanced audit classification model advances theory and research by synthesizing complementary research and providing a clear framework and procedure for moving the internal audit forward.

REFERENCES

Aladwani, A. M. (2001). Change management strategies for successful ERP implementation. *Business Process Management Journal, 7*(3), 266–275.

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

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2004). Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems. *International Journal of Accounting Information Systems, 5*(2), 183-202.

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations. *Journal of Information Systems, 22*(2), 195–214.

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2010a). Principles and problems of audit automation as a precursor to continuous auditing. *Working paper, Rutgers Accounting Research Center,* Rutgers Business School.

Alles, M. G., Kogan, A., Vasarhelyi, M. A., & Wu, J. (2010b). Continuous data level auditing using continuity equations. *Working paper, Rutgers Accounting Research Center,* Rutgers Business School.

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation. *Organization Science, 18*(5), 763-780.

Beath, C. (1991). Supporting the information technology champion. *MIS Quarterly, 15*(3), 355–372.

Bierstaker, J. L., 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. *Managerial Auditing Journal, 16*(3), 159–164.

Bisbal, J., Lawless, D., Wu, B., & Grimson, J. (1999). Legacy information systems: Issues and directions. *IEEE software, 16*(5), 103-111.

Bonsón, E., Cortijo, V., & Escobar, T. (2009). Towards the global adoption of XBRL using International Financial Reporting Standards (IFRS). *International Journal of Accounting Information Systems, 10*(1), 46-60.

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

Brazel, J. F., Agoglia, C. P., & Hatfield, R. C. (2004). Electronic versus face-to-face review: The effects of alternative forms of review on auditors' performance. *The Accounting Review, 79*(4), 949-966.

Brewster, M., Gal, G., Rosen, S., & Zubenko, A. (2007). Monitoring Processes and Internal Control Adequacy: Continuous Monitoring Within. *Information systems control journal,* 1–6.

Brown, C. E., Wong, J. A., & Baldwin, A. A. (2007). Research Streams in Continuous Audit: A Review and Analysis of the Existing Literature. *Journal of Emerging Technologies in Accounting,* 4(1), 1–28.

Cangemi, M. P., & Singleton, T. W. (2003). *Managing the audit function: a corporate audit department procedures guide* (3rd ed.). Hoboken: John Wiley & Sons, Inc.

Cash, J., Jr, Bailey, A., Jr, & Whinston, A. (1977). A survey of techniques for auditing EDP-based accounting information systems. *Accounting Review, 52*(4), 813-832.

Chan, D. Y., & Vasarhelyi, M. A. (2011). An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. International *Journal of Accounting Information Systems, 12*(2), 152–160.

Coderre, D. (2005). *CAATTs & other BEASTs for Auditors* (3rd ed.). Ekaros Analytical Inc.

Coderre, D. (2008). *Internal Audit: Efficiency Through Automation* (Vol. 12). John Wiley & Sons.

Committee of Sponsoring Organizations of the Treadway Commission. (1992). *Internal Control--integrated Framework: Evaluation tools*.

Committee of Sponsoring Organizations of the Treadway Commission. (2009). *Guidance on monitoring internal control systems*.

Continuous Auditing in ERP System Environments: The Current State and Future Directions. (2010). Continuous Auditing in ERP System Environments: The Current State and Future Directions, 24(1), 91–112. doi:10.2308/jis.2010.24.1.91

Curtis, M. B., & Payne, E. A. (2008). An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. *International Journal of Accounting Information Systems, 9*(2), 104–121.

Cushing, B. E. (1974). A mathematical approach to the analysis and design of internal control systems. *Accounting Review*, 24-41.

DeAngelo, L. E. (1981). Auditor size and audit quality. *Journal of Accounting and Economics, 3*(3), 183–199.

Debreceny, R., & Gray, G. L. (2001). The production and use of semantically rich accounting reports on the Internet: XML and XBRL. *International Journal of Accounting Information Systems, 2*(1), 47-74.

Dowling, C., & Leech, S. (2007). Audit support systems and decision aids: Current practice and opportunities for future research. *International Journal of Accounting Information Systems, 8*(2), 92–116.

Downling, C., & Leech, S. (2007). Audit support systems and decision aids: Current practice and opportunities for future research. *International Journal of Accounting Information Systems, 8*(2), 92–116.

Elliott, R. K. (2002). Twenty-First Century Assurance. *Auditing, 21*(1), 139–147.

Elliott, R. K., & Jacobson, P. D. (2002). The Evolution of the Knowledge Professional. *Accounting Horizons, 16*(1), 69–80.

Elliott, R. K., & Rogers, J. R. (1972). Relating statistical sampling to audit objectives. *Journal of Accountancy, 134*.

Fischer, M. J. (1996). "Real-Izing" the benefits of new technologies as a source of audit evidence: An interpretive field study. *Accounting, Organizations and Society, 21*(2), 219–242.

Gonzalez, G. C., Sharma, P. N., & Galletta, D. F. (2012). The antecedents of the use of continuous auditing in the internal auditing context. *International Journal of Accounting Information Systems, 13*(3), 248-262.

Greenstein, M., & McKee, T. E. (2004). Assurance practitioners' and educators' self-perceived IT knowledge level: an empirical assessment. *International Journal of Accounting Information Systems, 5*(2), 213–243.

Groomer, M. S., & Murthy, U. S. (1989). Continuous Auditing of Database Applications: An Embedded Audit Module Approach. *Journal of Information Systems, 3*(2), 53–70.

Gupta, A. (2000). Enterprise resource planning: the emerging organizational value systems. *Industrial Management & Data Systems, 100*(3), 114–118.

Hall, J. A., & Singleton, T. (2005). *Information technology auditing and assurance* (2nd ed.). Mason, Ohio: Thomson/South-Western.

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

Hammer, M., & Champy, J. (1993). *Reengineering the Corporation.* New York: HarperCollins.

Hermanson, D. R., Hill, M. C., & Ivancevich, D. M. (2000). Information Technology-Related Activities of Internal Auditors. *Journal of Information Systems, 14*(1), 39–53.

Hoitash, R., Kogan, A., Vasarhelyi, M. A., & Srivastava, R. P. (2006). Measuring Information Latency. *The International Journal of Digital Accounting Research, 6*(May), 1–24.

Hong, K. K., & Kim, Y. G. (2002). The critical success factors for ERP implementation: an organizational fit perspective. *Information & Management, 40*(1), 25-40.

Hunton, J. E., Wright, A. M., & Wright, S. (2003). The Supply and Demand for Continuous Reporting. *Trust and Data Assurances in Capital Markets: The Role of Technology Solutions*, 7–16.

Janvrin, D., Bierstaker, J., & Lowe, D. J. (2008a). An examination of audit information technology use and perceived importance. *Accounting Horizons, 22*(1), 1–22.

Janvrin, D., Lowe, D. J., & Bierstaker, J. (2008b). Janvrin, Lowe, Bierstaker - 2008 - Auditor Acceptance of Computer-Assisted Audit Techniques (pp. 1–26). *Working Paper,* Iowa State University, Iowa, 2008.

Keenoy, C. L. (1958). The impact of automation on the field of accounting. *Accounting Review*, 230-236.

Kogan, A., Sudit, E. F., & Vasarhelyi, M. A. (1999). Continuous Online Auditing: A Program of Research. Journal of Information Systems, 13(2), 87–103. doi:10.2308/jis.1999.13.2.87

Langford, J. (2010). Enhanced Auditing or Auditing with Technology (p. 13). Presented at the 21st World Continuous Auditing and Reporting Symposium, Newark, NJ.

Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. MIS Quarterly, 461–491.

MacNee, C. (2010). What is Remote Auditing? *INform, 26*. The International Register of Certificated Auditors.

Manson, S., McCartney, S., & Sherer, M. (2001). Audit automation as control within audit firms. *Accounting, Auditing & Accountability Journal, 14*(1), 109–130.

Parente, S. L., & Prescott, E. C. (1994). Barriers to technology adoption and development. *Journal of Political Economy, 102*(2), 298.

Pitt, L. F., Watson, R. T., & Kavan, C. B. (1995). Service quality: a measure of information

systems effectiveness. *MIS Quarterly, 19*(2), 173–187.
PricewaterhouseCoopers. (2007). *Internal Audit 2012* (pp. 1–60). PriceWaterhouseCoopers.
PricewaterhouseCoopers. (2012). *2012 State of the internal audit profession study*. PriceWaterhouseCoopers.
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.
Public Company Accounting Oversight Board. (2010). *Auditing Standard No. 15.* PCAOB Release No. 2010-004.
Public Company Accounting Oversight Board. (2007, November 1). Auditing Standard No. 5. PCAOB Release No. 2010-004.
Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous Auditing: Building Automated Auditing Capability. *Auditing, 21*(1), 147–164.
Sayana, S. A., & CISA, C. (2004). Using CAATs to Support IS Audit. *Information systems control journal*, 1, 21–23.
Searcy, D., Woodroof, J., & Behn, B. (2003). Continuous audit: the motivations, benefits, problems, and challenges identified by partners of a big 4 accounting firm. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on* (pp. 10-pp). IEEE.
Shaikh, J. M. (2005). E-commerce impact: emerging technology – electronic auditing. *Managerial Auditing Journal, 20*(4), 408–421.
Soh, C., Kien, S. S., & Tay-Yap, J. (2000). Enterprise resource planning: cultural fits and misfits: is ERP a universal solution? *Communications of the ACM, 43*(4), 47–51.
Stark, P. B. (2009). CAST: Canvass Audits by Sampling and Testing. *IEEE Transactions on Information Forensics and Security, 4*(4), 708–717.
Teeter, R. A., Alles, M. G., & Vasarhelyi, M. A. (2010). The Remote Audit. *Journal of emerging technologies in accounting, 7*(1), 73–88.
Townsend, A. M., DeMarie, S. M., & Hendrickson, A. R. (1998). Virtual teams: Technology and the workplace of the future. *Academy of Management Perspectives, 12*(3), 17–29.
Turban, E., Sharda, R., & Delen, D. (2010). *Decision Support and Business Intelligence Systems* (9 ed.). Upper Saddle River, NJ: Prentice Hall Press.
Vasarhelyi, M. A. (1980). A Taxonomization of Internal Controls and Errors for Audit Research.
Vasarhelyi, M. A. (1983). A framework for audit automation: Online technology and the audit process. In *The Accounting Forum (March)* (pp. 30-44).
Vasarhelyi, M. A., & Alles, M. G. (2008). The “now” economy and the traditional accounting reporting model: Opportunities and challenges for AIS research. *International Journal of Accounting Information Systems, 9*(4), 227–239.
Vasarhelyi, M. A., & Halper, F. B. (1991). The Continuous Audit of Online Systems. *Auditing: A Journal of Practice & Theory, 10*(1), 110–125.
Vasarhelyi, M. A., & Kuenkaikaew, S. (2011). Continuous auditing and continuous control monitoring: case studies from leading organizations. *Working Paper, Rutgers*

Accounting Research Center, Rutgers Business School.

Vasarhelyi, M. A., Alles, M. G., & Williams, K. T. (2010, February). The Now Economy. *Working Paper, Rutgers Accounting Research Center, Rutgers Business School.*

Wang, R. Y., & Strong, D. M. (1996, Spring). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems, 12*(4), 5-33.

Warren, J. D., & Smith, M. (2006). Continuous Auditing: An Effective Tool for Internal Auditors. *Internal Auditing, 21*(2), 27–35.

Wu, J., Kogan, A., Alles, M. G., & Vasarhelyi, M. A. (2005). Continuity Equations in Continuous Auditing: Detecting Anomalies in Business Processes. *Working Paper, Chapman University*.

Zaheer, S., & Manrakhan, S. (2001). Concentration and Dispersion in Global Industries: Remote Electronic Access and the Location of Economic Activities. *Journal of International Business Studies, 32*(4), 667–686.

Zhao, N., & Yen, D. (2012). Zhao, Yen - 2004 - Auditing in the e-commerce era. *Information Management & Computer Security, 12*(5), 389–400.

CURRICULUM VITAE

Ryan Anthony Teeter

Born July 30, 1982 Keene, New Hampshire

EDUCATION

Timpview High School, Provo, Utah
Diploma – May 2000

Utah Valley University, Orem, Utah
Associate of Science – General Studies – May 2005
Bachelor of Science – Accounting, Minor in Spanish – May 2007

Rutgers, The State University of New Jersey, Newark, New Jersey
Doctor of Philosophy – Management, emphasis in Accounting Information Systems – May 2014

EMPLOYMENT

Google, Inc., Mountain View, California
External Training Specialist – Summer 2007

Siemens PLM, St. Louis, Missouri
Internal Audit Intern – Spring 2008

PUBLICATIONS

Teeter, R.A. and K.S. Whelan-Berry. 2008. **My Firm Vs. Our Firm: The Challenge of Change in Growing the Small Professional Services Firm.** Journal of Business inquiry.

Vasarhelyi, M.A., R.A. Teeter, J.P. Krahel. 2010. **Audit Education and the Real-time Economy**. Issues in Accounting Education. Vol 25, No. 3.

Teeter, R.A., M.A. Vasarhelyi, and M.A. Alles. 2010. **The Remote Audit.** Journal of Emerging Technology in Accounting. Vol. 7, No. 1.

Byrnes, P.A., A. Al-Awadhi, B. Gullvist, H. Brown-Liburd, R.A. Teeter, J.D. Warren Jr, M.A. Vasarhelyi. 2012. **Evolution of Auditing: From the Traditional Approach to the Future Audit.** American Institute of Certified Public Accountants White Paper.