CHAPTER 9
THE PERVASIVE IMPACT OF INFORMATION TECHNOLOGY ON INTERNAL AUDITING

Sridhar Ramamoorti[1]
Marcia L. Weidenmier

[1]The views expressed in this ROIA supplemental chapter are the personal views of Dr. Sridhar Ramamoorti and do not necessarily reflect the views of, nor endorsement by, Ernst & Young LLP.

Dedicated to the memory of William G. Bishop III, CIA
President, The Institute of Internal Auditors, 1992-2004

The Institute of Internal Auditors Research Foundation

Disclosure

The IIARF publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIA does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Professional Practices Framework for Internal Auditing (PPF) was designed by The IIA Board of Directors' Guidance Task Force to appropriately organize the full range of existing and developing practice guidance for the profession. Based on the definition of internal auditing, the PPF comprises Ethics and *Standards*, Practice Advisories, and Development and Practice Aids, and paves the way to world-class internal auditing.

This guidance fits into the Framework under the heading Development and Practice Aids.

The mission of The IIA Research Foundation (IIARF) is to be the global leader in sponsoring, disseminating, and promoting research and knowledge resources to enhance the development and effectiveness of the internal auditing profession.

ISBN 0-89413-498-1
04214 06/04
First Printing

I. Introduction

The impetus for this supplemental chapter titled *The Pervasive Impact of Information Technology on Internal Auditing* comes from The Institute of Internal Auditors Research Foundation (IIARF) monograph, *Research Opportunities in Internal Auditing* (2003), hereafter ROIA. ROIA combines theory and practice in conceptual frameworks to promote an understanding of the contemporary internal auditing environment.[1] The goals of ROIA include stimulating academic research on significant internal auditing topics and serving as a "communication bridge" between academics and practicing professionals. ROIA provided us with internal auditing related subject matter content, including the most promising areas of information technology[2] (IT) application in internal auditing.

One significant topic that is only briefly mentioned in ROIA is the impact of IT on the internal audit function.[3] IT is revolutionizing the nature and scope of worldwide communications, changing business processes, and erasing the traditional boundaries of the organization — internally between departments and externally with suppliers and customers. The resulting intra-enterprise coordination as well as inter-enterprise integration with external business partners through supply chain management and customer relationship management systems demonstrates the power of IT as both a driver and enabler of management processes and strategies. Indeed, internal auditors must recognize and leverage the powerful capabilities of computers and technology in collecting, generating, and evaluating information for managerial decision making related to strategy, risk management and controls, and, more broadly, for effective organizational governance. At the same time, internal auditors must recognize that IT, in itself, will not increase the function's effectiveness. Rather internal auditors must first understand the audit objectives and select appropriate IT to achieve those objectives (i.e., the task-technology fit is essential). It is also imperative that internal auditors understand their organization's appropriate leveraging of IT, and learn to harness additional IT to optimize internal audit performance.

Another recent monograph, *Researching Accounting as an Information Systems Discipline*, published by the Information Systems Section of the American Accounting Association and co-edited by Arnold and Sutton (2002), has also served as a key reference. *Researching Accounting as an Information Systems Discipline*, hereafter RAISD, provides a framework for and a synthesis of the extant and rapidly evolving accounting information systems (AIS) research.[4] RAISD was compiled for stimulating research in accounting and information systems among AIS researchers, as well as non-AIS researchers.

We draw upon ROIA to identify the nature, purpose, scope and contributions of the internal audit function in contemporary organizations. We also look to RAISD for providing us with

the overall philosophy and methodology of AIS research as well as promising avenues for exploring external and internal auditing applications. For ready reference, we have provided the topical content and sequence of chapters appearing in RAISD as well as ROIA in Table 1. In addition, to help identify current technology issues we have incorporated the top 10 technology issues as identified by The IIA's Advanced Technology Committee in December 2003 and The IIA's Strategic Directive regarding the top 30 IT issues identified in March 2003 (see Table 2).

We have written this supplemental chapter in a way that should help:

- Interested researchers better understand, evaluate, and enhance the context of internal auditing, including why IT is important to internal auditing and how internal auditors (may) generate and use IT in innovative ways that provide added value to their respective organizations; and
- Practicing internal auditors recognize, appreciate, and articulate the conceptual frameworks used in research to convey the strategic nature and relevance of their professional activities to those charged with governance within organizations.

Given this backdrop, whenever possible, we incorporate a discussion of pertinent topics included in ROIA and RAISD. To ensure that this chapter is tightly coupled with the original ROIA, we discuss the current and future impact of IT on the internal audit function relative to each ROIA chapter. In Section II (history, evolution, and prospects), we assess how IT has affected internal auditing in the past and, looking forward, how we expect it will likely continue to shape internal auditing in the future. Section III (organizational governance) describes how IT has helped create a demand for better corporate governance ("IT as driver" perspective) and provides the auditor with tools to meet that demand ("IT as enabler" perspective). Section IV (assurance and consulting) discusses the impact of IT on the different types of activities performed by the internal audit function. In section V (risk management) we discuss how IT changes the business environment and concomitantly business risks, as well as how the internal auditor helps management identify, assess, monitor, and manage these risks. Section VI (managing the internal audit function) examines how IT has influenced and, perhaps, altered the strategic positioning, scope, focus, and management of the internal audit function. In Section VII (independence and objectivity), we discuss the independence/ethical, as well as privacy, and security issues created by IT. Section VIII (systematic processes) explores how IT assists the systematic processes of internal auditors through the use of decision aids and knowledge management. Also, following the approach taken in other ROIA chapters, we identify numerous research questions at the end of each section to stimulate academic research related to IT and internal auditing. Readers may find it helpful to review the table of contents of the original ROIA and RAISD monographs (see Table 1).

A glossary of selected IT-related terms appears in the Appendix (these terms are identified by *italics and underscoring* the first time a technical term is used).

Two Important Caveats

During the process of writing this supplemental chapter, we noted that auditing research, including IT auditing research, has traditionally focused on the environment, scope, methodology, processes, and issues of ***external*** auditing. Researchers must exercise caution before attempting to generalize the results of external auditor/IT research to internal auditors and their settings. Future research can determine the specific circumstances under which external auditors and internal auditors perform/react similarly (or differently). To assist with this effort, research questions focusing on the differences between internal and external auditors are highlighted with a ✣ at the end of each section.

Secondly, it is important to recognize that internal audit functions may either be fully in-sourced, co-sourced, or fully outsourced. Each configuration affects the relationship between the internal audit function, the organization, and IT scope, budget, tools, and usage differently. In this supplemental chapter, we have primarily benchmarked on fully in-sourced internal audit functions that are substantially affected by the organization's use of IT. It is conceivable that the IT impact may be of a different kind or degree when contemplating a co-sourced or fully outsourced internal audit function (e.g., staffing and size of the internal audit function).

II. Historical Perspective on Information Technology and the Internal Audit Function[5]

To understand the impact of IT on the internal audit function, we first provide a historical perspective of how IT has developed over the last several decades from simple data input systems to complex management IS that support managerial decision making with relevant, reliable, and timely information. Chapter 1 of RAISD (Arnold and Sutton, RAISD, 2002) characterizes this evolution as a shift from automated systems performing only accounting functions (payroll, accounts payable, general ledger, etc.) to IS that perform enterprise-wide tasks that include accounting and auditing.

We begin our discussion in the 1950s that marked the dawn of the era of computers and technology in business. We describe how these IT developments caused the internal auditing function to (1) change the audit scope and approach, (2) use new auditing tools/techniques, and (3) execute operational audits of the entire organization. Specifically, we chronicle the

history and evolution of IT usage by internal auditors over the last four decades and outline emerging trends at the beginning of the 21st century.

1950s and 1960s

In the mid-1950s, the computer was first used to process business applications, with punched cards being used for data storage and batch processing. This "new" technology did not, initially, exert much of an impact on internal auditing. Rather, internal auditors generally followed an "auditing around the computer" approach because, relative to inputs and outputs, punched cards provided a visible and readable paper audit trail. Specifically, the auditor compared the machine's input with its output (parallel processing), just as he/she had compared the voucher files with the ledger books in the early 1900s.[6]

Over the next decade, as computers became increasingly faster and more versatile, tape drives replaced punched cards, and real-time online systems were introduced. These new systems threatened the existence of the paper audit trail, transforming it to a nonvisual, electronically stored format. At the same time, computer use within organizations proliferated. In fact, by the mid-1960s, over 50 percent of the top 500 industrial companies had extensive electronic data processing operations (Hafner, 1964). Specifically, in order to make information flow about manufacturing processes more efficient, several companies introduced Materials Requirements Planning (MRP) systems in the 1960s, and continued to refine them into the future (CICA, 2003b).

Beyond computer usage for payroll processing and other fairly pedestrian business applications, perhaps inspired by the impressive utility of the 10-key calculator, internal auditors also began to recognize that the computer could be used as an auditing tool. Consequently, they first began experimenting with sampling applications, which required complex calculations (Sandler, 1968; Will, 1975). The most popular and economical method for testing the system was a test deck (or test data). However, auditors also began developing a variety of new computer programs, called generalized audit software (GAS), to assist with audit tasks and verify the results of processing, e.g., testing mathematical accuracy, comparing files, and summarizing data.

Nevertheless, internal auditors only ***slowly*** realized that they needed to be technologically proficient and, perhaps, adopt new approaches (Hafner, 1964, p. 979, emphasis added). The notion of relinquishing the "black box" approach (i.e., looking at inputs and outputs but ignoring the processing) and instead, "auditing through the computer," required an intimate understanding of the logic behind computer operations, code review, as well as other sophisticated approaches for verifying general controls, application controls, and processing results.

Just as the extent of computer usage varied widely across organizations, the function, approach, and responsibility of the internal audit function also varied widely. More progressive organizations staffed audit functions with people trained in both auditing and IS to execute this new audit approach. For example, by 1968, Bell Laboratories had over 60 electronic data processing (EDP) auditors whose primary responsibilities were to: (1) develop new computerized audit techniques, (2) recommend and evaluate internal control procedures, and (3) evaluate controls over system testing and conversion (Wasserman, 1969). They also became involved in system design, disaster recovery plans, and other activities pertinent to systems installation and functioning. Some people, however, opposed internal auditors' participation in systems development (to provide controls expertise), claiming that it compromised the auditor's independence — a controversy that continues to be debated today.

In addition to changing the scope, approach, and techniques, IT also expanded the role of the internal auditor in the organization beyond just handling routine accounting transactions. While computers initially processed limited pockets of data, computers gradually processed data throughout the entire organization. This expansion of the computer's role created a demand for internal auditors to perform operational or management audits to ensure that management's policies were being carried out efficiently and effectively throughout the organization, making the internal audit function an integral part of management's controls over operational departments.

1970s and 1980s

By 1975, no less than 200,000 mainframe computers were in use in businesses (Peat, Marwick, Mitchell and Co., 1976), although they were concentrated in larger organizations. Moreover, Materials Requirement Planning (MRP) systems entered their second generation as MRP-II (Manufacturing Resource Planning), used to plan and control all of an enterprise's manufacturing processes and resources, during the 1980s (CICA, 2003b). Nevertheless, EDP audit functions were not universal and most internal audit functions did not perform EDP-related audits during the 1970s and early 1980s (Reilly and Lee, 1981). Internal audit functions were relatively slow in adopting the numerous "auditing through the computer" methods then in vogue: the *integrated test facility, tagging and tracing, mapping, parallel simulation, concurrent processing, controlled processing* or *reprocessing, program code checking*, and *flowchart verification* (Cash, Bailey, and Whinston, 1977). For example, a 1977 survey of internal audit managers revealed that, on average, test data was used less than 35 percent of the time and integrated test facilities less than 20 percent of the time (Rittenberg and Davis, 1977).

The slow adoption of EDP-related (internal) audit techniques from the 1960s through the 1980s may be potentially explained by the high level of technical skills required to implement audit procedures. Specifically, data and auditing tools existed only on mainframe and minicomputers (Coderre, 2001a, p. 134). To complicate matters further, a plethora of over 25 different proprietary GAS packages with different program languages, commands, functions, hardware, and input file formats were available for use by auditors (Adams and Mullarkey, 1972). Given these hurdles, organizations may also have decided that heavy investments in these audit techniques were not warranted.

Fortunately, with the passage of time, EDP-related audit techniques became more user-friendly and easier to implement. Organizations began moving from mainframe computers to personal computers (PC), making access to data easier. Proprietary GAS programs were eventually superseded by truly "generalized" audit software programs, like *ACL* (in the 1970s) and *IDEA* (in the 1980s), which work on multiple platforms and input file formats using audit specific language. During the 1970s, usage of GAS gained a powerful boost after the first major management fraud using a computer was perpetrated by the Equity Funding Corporation of America ("Billion Dollar Bubble"). This fraud was a catalyst for providing auditors with their own audit software, unrestricted access to data, and the responsibility to conduct data center and application system audits. During the 1980s, usage of GAS gained a second powerful boost when GAS could run on PCs, allowing analysis of data to take place virtually any time and place.

1990s and Beyond

In the 1990s, the global economy was at the cusp of entering the 21st century Information (Technology) Age. Technology was quickly recognized as an indispensable adjunct to information creation and collection, analysis, and dissemination. IT was also seen as the key enabler as well as driver of business strategy, particularly so because many "technological advances are almost immediately transferable across product markets and countries" (Bryan and Farrell, 1996). Organizations began implementing Enterprise Resource Planning (ERP) systems to manage all of an enterprise's internal processes (e.g., sales, procurement, human resources, finance and accounting, production, distribution, and quality control (CICA, 2003b). Sophisticated management information and executive decision support systems based on electronic document management systems, data warehouses, and intranets, allowing for internal sharing and analysis of information, also emerged. Organizational boundaries became blurred and the extended enterprise became a reality. Inter-enterprise integration necessitated alignment of technology platforms with trading partners (e.g., *electronic data interchange, electronic funds transfer at point of sale*) as exemplified by customer relationship management (CRM) and supply chain management (SCM) initiatives. As we have progressed

from using telegrams and telexes, to phone systems and fax transmissions, to e-mail, video conferencing, and interactive cable, and now to Internet webcasts and virtual presentations, it has become easier and easier to transfer "working knowledge," ideas, and techniques (Bryan and Farrell, 1996; Davenport and Prusak, 1998). The advent of global communications using the World Wide Web caused Larry Ellison of Oracle to make the sweeping, now-clichéd observation: "The Internet changes everything."

Recent surveys reveal that the impact of IT on the internal auditing profession is marked, and The IIA continues to lead the way in equipping the profession with technology-related publications and guidance. The IIA's influential reports on *Systems Auditability and Control (SAC),* 1977, were updated to reflect the increasingly "electronic" environment and released as eSAC. Almost 49 percent of internal auditors have integrated IT into all of their reviews, and 76 percent expect non-EDP auditors to have computer knowledge beyond basic competence in using the spreadsheet (IIA, 2002b). The percentage of EDP auditors to total internal auditors has increased to between 14 percent and 24 percent (Hermanson et al., 2000; IIA, 2000), and this percentage is far higher in technology intensive companies such as Intel, Microsoft, and AT&T. Regarding sophisticated IT tools, which could potentially increase their efficiency and effectiveness, a large proportion of internal auditors use GAS to extract and analyze data (83 percent) (McCollum and Salierno, 2003). Almost 38 and 29 percent of internal auditors utilize continuous monitoring and continuous auditing technology, respectively (IIA, 2002a, AICPA/CICA, 1999). At the same time the expansion of internal audit's function in organizations, including sophisticated IT usage, which began in the 1960s, continues.[7]

Table 3 presents a summary of the changes that occurred in IT and the (internal) audit function. For completeness, the table also includes the evolution of IT audit and topics that will be discussed in subsequent sections of this chapter.

Research Questions

- Given the historical reluctance to embrace IT, what are some ways to increase the rate of adoption of new IT audit techniques by internal auditors?

- Which of the IT audit applications described in this section deserved to be adopted? What are the differences, similarities, and objectives of each IT audit application?

- Which IT audit application is the best method to achieve efficiency, effectiveness, and/or a given objective? How do internal and external factors affect the choice of the appropriate IT audit application?

- What internal and external factors drive the adoption of IT by the internal audit function (e.g., organization's commitment to IT, IT's role in the organization's strategy, risk associated with the firm's IT)?

- What is the appropriate level of technological knowledge for EDP/IT auditors and non-EDP/IT auditors? How can internal auditor technology skills be enhanced?

- What internal and external factors drive the level of technological knowledge of EDP/IT auditors and non-EDP/IT auditors (e.g., size of the internal audit function, organization's commitment to IT, IT's role in the organization)?

- What is the most effective mix of EDP/IT and non-EDP/IT auditors in an internal audit department? What are the internal and external factors that should drive the mix of EDP/IT and non-EDP/IT auditors in an internal audit department?

- Does participation in systems development compromise the independence of internal auditors?

- ✜ How does the rate of adoption of new IT by internal auditors compare to that of external auditors? Have internal and external auditors adapted to the impact of IT at the same rate (and time frame)? If not, why not?

- ✜ Over the years, which internal auditor (and/or external auditor) technology applications have endured? Why — ease of use, inexpensive, scope of application, mission critical nature? What trends appear to be emerging about future IT applications? By internal auditors? By external auditors?

III. Corporate Governance

ROIA devotes two chapters to corporate governance and the role of the internal audit function. The chapters define corporate governance as the "structure through which objectives are set, and how these are achieved, and monitored" (Ruud, ROIA, p. 74). ROIA also identifies three key factors underlying the demand for better governance: organizational governance failures, increase in (institutional) investors with considerable clout in an era of investor capitalism, and the rising frequency of multimillion-dollar class action lawsuits (Hermanson and Rittenberg, ROIA, p. 38).

The IIA's *International Standards for the Professional Practice of Internal Auditing (2003)*, hereafter *Standards*, highlight the internal auditor's role in governance. Specifically, *Standard 2130* on governance states that:

> "The internal audit activity should contribute to the organization's governance process by evaluating and improving the process through which (1) values and goals are established and communicated, (2) the accomplishment of goals is monitored, (3) accountability is ensured, and (4) values are preserved."

The *Standards* also require the internal auditing function to report to the board and senior management on significant corporate governance issues (*Standard 2060*); evaluate risk exposures related to the organization's governance (*Standard 2110.A2*); and evaluate the adequacy and effectiveness of controls encompassing the organization's governance (*Standard 2120.A1*).

At the same time that the internal auditor's responsibility regarding corporate governance is increasing, IT's role in corporate governance is also increasing. IT is critical to organizational strategy development and execution because it can directly affect "what an organization does, how it operates, how it interacts with its customers, and its competitive position" (Davis and Hamilton, 1993). We now discuss how IT drives the demand for better governance and then helps organizations meet this demand; and how internal auditors can leverage IT to effectively discharge their professional responsibilities and fulfill rising expectations related to governance.

IT as a Driver

A key factor underlying the demand for better governance is IT because organizations are increasingly dependent on IT to enable business processes and activities to occur reliably (Vowler, 2003; Williams, 2003). As the backbone of e-commerce, the Internet has been described as the greatest opportunity and greatest threat facing organizations (Rosenoer, Armstrong, and Gates, 1999). Not only is IT changing the way business is conducted, but IT also increases risk and changes (needed) controls. The increased risk results from (1) the organization's inability to continue business if systems are not functioning properly, and (2) the use of IT to operate globally and interconnect with outside entities (Vowler, 2003). In this interconnected world, inter-enterprise integration of software and internal controls with business partners must be seamless (e.g., SCM, CRM). Internally, operational controls must integrate seamlessly with technical controls to assure that computer systems and networks are reliable and recoverable (Bishop, 1997).[8]

IT is an integral component of corporate governance because it is the primary method by which organizations achieve their objectives and at the same time changes the organization's risk level and needed controls. Surprisingly, IT is one of the least understood components of corporate governance — often overlooked by directors and CEOs until too late (Williams, 2002, 2003). Industry experts warn, however, that investors are becoming increasingly IT-literate, worrying about IT's risk to operations and beginning to scrutinize IT investments with the focus on the (timely) delivery of major IT projects and system efficiency (Huber, 2002). These new risks, controls, and investor scrutiny are driving the demand for improved governance to ensure that IT investments are appropriately and effectively implemented, ultimately increasing shareholder value.

Congress passed the U.S. Sarbanes-Oxley Act of 2002 to improve corporate governance and accountability with the expectation of preventing future corporate governance failures and for bolstering market confidence. Three sections of the Act are especially relevant to IT. Specifically, Section 302 requires CEO and CFO to annually certify the completeness and accuracy of financial statements; Section 404 requires external auditors to attest to management's assessment of the effectiveness of internal controls over financial reporting; and Section 409 requires companies to report material changes in their financial position on a "rapid and current basis." These sections of the Act require transparent systems and business processes, a clear understanding of internal processes and system controls, and (near) real-time reporting, respectively. A new publication by the IT Governance Institute (ITGI) furnishes timely guidance about disclosure controls as well as controls over financial reporting in response to the requirements of Sarbanes-Oxley (Fox and Zonneveld, 2003).[9]

IT as an Enabler

To meet the increased governance demands, organizations are implementing a variety of new IT measures. First, organizations are establishing IT governance committees to review IT strategy and execution with the chief information officer (CIO) playing a key role.[10] Second, organizations can use IT to meet the demands of corporate governance. For example, to detect risks and document controls, organizations are replacing narrative descriptions of controls with system flowcharts via flowcharting software. While flowcharts help visually in identifying functional aspects of a system, *state transition, activity, and interaction diagrams* provide a better means of identifying risks by allowing parallel activities and their synchronization, which help reveal the behavioral, dynamic, and interactive nature of the system.[11]

Sarbanes-Oxley places certain responsibilities on the audit committee with respect to data integrity, information security, and other contingencies. Attempting to create transparent

financial reporting systems, many organizations are completely overhauling their control, monitoring, and reporting processes, including those complying with the whistleblower provisions of Sarbanes-Oxley (Sarbanes-Oxley, Section 301.4). Organizations can select from several different internal control frameworks to comply with the Act, including *Committee of Sponsoring Organizations (COSO), ISO 17799*, and ISACA's *Control Objectives for Information Technology (COBIT)*.[12] Organizations can also streamline their ERP systems by implementing software preferably from a single vendor.[13] Software vendors are also helping this effort by developing Sarbanes-Oxley compliant applications (Schwartz, 2003) as well as applications to document and monitor controls and create user-defined alerts for noncompliance ("Market Dynamics," 2003). In addition, governance software is becoming available for monitoring IT projects with "IT dashboards" and user-defined alerts (e.g., timing, budget) (Krass, 2003).

IT can also help support near real-time reporting also referred to as the "virtual close." Fully integrated ERP systems, business intelligence (online analytical processing, data mining, digital dashboards or data visualization), data marts and warehouses, and enterprise analytics should allow organizations to identify material changes and help streamline their external reporting process in compliance with Sarbanes-Oxley (PricewaterhouseCoopers, 2003). In addition, *eXtensible Business Reporting Language* (XBRL) provides a standard way of sharing business information so that organizations can quickly aggregate external and internal information and share it with other external entities, including regulatory agencies, analysts, and investors.[14] The Internet can immediately distribute required information to shareholders and even allow them to vote electronically.

When information is placed on corporate Web sites, users visiting these sites are naturally entitled to rely on the information posted therein. However, in the presence of hyperlinks, users typically find it difficult, if not impossible, to locate the boundaries of financial information they read in electronic form (CICA, 1999). The issue of undefined borders opens up the question of responsibility, and hence, liability for linked information. Therefore, it has been recommended that the internal audit function should include the corporate Web site within its review scope to ensure that Web site activities and security issues are being monitored as part of the board of director's corporate governance mandate (CICA, 1999b).

Internal auditors can play a pivotal role in helping organizations leverage IT to meet the increased demand for improved governance by evaluating current risks and controls as well as define and assess the promise and utility of future, contemplated monitoring systems. Internal auditors can also help develop an information system to provide the board with mandated financial information, industry insights, risk and controls analysis, and the integrity of the financial reporting system (Bishop, Hermanson, Lapides, and Rittenberg, 2000, p.

50). Moreover, if internal auditors highlight the importance of using appropriate ontologies and semantic modeling (i.e., systems modeled using Resources Events and Agents, REA framework, McCarthy, 1982; David, Gerard, and McCarthy, 2002) to develop these systems, organizational transparency and performance should improve (see Chapters 2, 3, and 5 of RAISD for a more detailed discussion of these topics). Thus, internal auditors can leverage IT in setting and influencing the strategic direction of the organization in numerous ways.

Finally, internal auditors can coordinate with external auditors with respect to IT reviews and audits to improve the level of total audit coverage. Indeed, boards of directors and senior executive management prefer such cooperation to occur, primarily with a view to decreasing overall audit costs. Also, both internal and external auditors seem to agree that the benefits of coordination include greater achieved coverage simultaneously with a minimization of duplicate efforts (Felix, Gramling, and Maletta, 1998). A higher level of total audit coverage, when it has the outcome of reducing total audit costs while simultaneously enhancing audit effectiveness, should improve corporate governance by increasing the monitoring, accountability, and accuracy of the firm's transactions and financial reporting.

Research Questions

- Under what circumstances could IT automatically provide assurance on risk and controls to outside parties (e.g., SAS 70 reports)? Can IT automatically generate reports about the effectiveness of corporate governance processes tailored to meet stakeholders' specific needs?

- What are the impacts of XBRL on the organization and on external reporting? How can IT best streamline external reporting?

- What are the economic benefits of implementing "integrated" IT governance? What is the best way to keep stakeholders informed about the progress of IT projects?

- What are the key ways in which, by appropriately leveraging IT, internal audit can most effectively promote and support organizational governance?

- Under what circumstances would it be beneficial for internal auditors to work with external auditors to increase total audit coverage? Can a conceptual model be developed to indicate the appropriate level of total audit coverage?

- How can IT best enhance total audit coverage (between internal and external auditors)? Is there a trade-off between the desire to reduce combined audit costs against the goal of achieving enhanced overall audit effectiveness?

- Can internal auditors provide assurance about their organization's IS using criteria similar to AICPA's *Systrust*? Would stakeholders accept an internal auditor's assurance (e.g., for SAS 70 reports)? Is it possible to develop a conceptual model indicating the conditions under which different parties benefit from internal audit assurance?

IV. Assurance and Consulting Services

Chapter 4 of ROIA examines the range of assurance and consulting services provided by the internal audit function to "add value and improve an organization's operations" (Anderson, ROIA, p. 106). The chapter identifies six basic types of internal audit services using an Internal Auditing Activity Continuum (Anderson, ROIA, Exhibit 4-4, p. 107). The Continuum, moving from assurance to consulting, includes: financial auditing, performance auditing, quick response auditing, assessment services, facilitation services, and remediation services (see Figure 1). Professional standards require internal auditors to have the knowledge, skills, and competencies needed to perform all or part of any engagement in the Continuum (*Standard 1210*). In this section, we discuss the impact of IT on the activities in the Internal Audit Activity Continuum, describing how internal auditors can leverage IT to help them competently and effectively deliver a variety of audit services.

The internal auditor, however, must remember that use of IT in general is not the goal. Rather, the internal auditor must understand the audit objective(s) he/she is trying to accomplish and select the appropriate IT in terms of cost, efficiency, and effectiveness. The appropriate IT will be determined by a number of internal and external factors shaping the organization, including the perceived status, independence, and competence of the internal audit function. The internal audit function should report to the audit committee, make recommendations, and secure management's buy-in to implement key recommendations. While some organizations view the internal audit function as part of the control framework, other organizations view the internal audit function as being outside the control framework to provide assurance on IT and non-IT controls. Thus, the position/role of the internal audit function will greatly influence its ability to select and use IT for auditing purposes.

CAATTs[15]

IT fundamentally changes the way in which organizations operate internally and interconnect with external organizations — redefining the boundaries for cooperation (Elliott, 1994). For example, *electronic data interchange* (EDI), *electronic funds transfer* (EFT), and *financial electronic data interchange* (FEDI) allow organizations to share information and increase

operational efficiency.[16] These changes are increasing the "demands for assurances of computer systems, information security, controls over the privacy of data, and quality assurance practices" (Anderson, ROIA, 2003, p. 115). Concurrently, intense competition is increasing productivity, (cost) efficiency, and information requirements. In the challenging context of these increasing expectations and pressures, the internal audit function must cost-effectively provide a wider variety of organizational risk mitigation services (e.g., helping to anticipate problems proactively).

To meet these demands, internal auditors can use a variety of Computer Assisted Audit Tools and Techniques, or CAATTS (also known as CAATS), which are computerized tools or techniques that increase the efficiency and effectiveness of the audit. CAATTs originally supported a systems-based approach that tested controls using complicated, embedded techniques (integrated test facilities, *sample audit review file, system control audit review file***)** and parallel simulations. CAATTs include a wide variety of PC software tools that support a flexible, interactive, databased approach to verify data accuracy, completeness, integrity, reasonableness, and/or timeliness.[17] Internal auditors view CAATTs, especially word processing, spreadsheet, and data analysis/extraction (or GAS) software, critical to the day-to-day operations and success of the internal audit function (Prawitt and Romney, 1996).

CAATTs also include more advanced technologies such as digital agents, embedded audit modules, and neural networks that allow continuous auditing.[18] Static digital agents are programmed objects that help internal auditors by triggering alerts when values fall outside of pre-specified ranges, or activate randomly or at specified times. Mobile digital agents may also be used to search through networks and the Internet for specific (internal and external) information, conditions, or events.[19] For example, a digital agent performing analytical procedures on accounts receivable would e-mail the auditor an exception report when an alert occurs. The digital agent could even verify the sale with the customer and e-mail the confirmation to the auditor (Searcy and Woodroof, 2003). Similarly, embedded audit modules are subroutines in software defined by auditors to continuously perform audit procedures concurrently with application processing. When an exception occurs, the system can alert the auditor via e-mail for follow-up.

While some auditors view CAATTs as a way to automate manual tasks, to truly add value to the organization, (internal and external) auditors need to shift to a new paradigm that redefines CAATTs as "Computer Aided Audit Thought Support" (Will, 1995). This paradigm views CAATTs as freeing auditors from manual/routine tasks so they can focus on exercising judgment and thinking critically. For instance, neural networks can be used to evaluate soft business information and data generated by management's judgments (AICPA/CICA, 1999). The interactive, real-time nature of CAATTs, especially GAS, allows auditors to quickly

evaluate results, adjust initial audit plans, and test new hypotheses improving the effectiveness and efficiency of assurance and consulting services as described below.

Assurance Services

Assurance services collect evidence to provide an independent assessment of adequacy of controls, compliance with laws and regulations, and safeguarding of assets. These services are provided for management as well as an external third party with the goal of improving information quality. Assurance services include: (1) financial auditing, attestation/compliance audits that may be performed with the external auditor; (2) performance/operational auditing, traditional internal audits to assess risk and provide assurance on internal controls; and (3) quick response auditing, services done at the request of management, which are generally fraud investigations (Anderson, ROIA, 2003, p. 107).

Internal auditors can use CAATTs in financial and performance auditing to improve the efficiency, effectiveness, and quality of the audit because CAATTs automate existing manual audit procedures, allow new procedures, test the entire audit population, monitor operations, and permit consistent application of audit techniques across time, auditors, and engagements. CAATTs, especially GAS, improve the auditor's analytical abilities, widely accepted as the most effective audit technique for identifying financial statement errors (Hylas and Ashton, 1982).

All three phases (planning, execution/conduct, and reporting) of financial and performance auditing benefit from the use of CAATTs. In the planning phase, risk analysis and audit universe software can help select areas to audit, identify initial risks, and determine preliminary objectives. The execution/conduct phase of the audit offers many opportunities for utilization of CAATTS, particularly when testing IT controls (more on this below). In the reporting phase, auditors can utilize word processing, presentation, and graphics software to make audit reports easier to read and understand. Using CAATTs throughout the auditing process should also produce more complete and accurate reports because auditors can perform a more thorough analysis of the data.

In the execution/conduct phase, auditors can use GAS to perform tests on 100 percent of the audit population, which allows auditors to develop a better understanding of the data as well as precise error estimates (extrapolation is not required).[20] GAS allows auditors to easily perform a variety of financial auditing tasks, including recalculation of report totals and estimates, identification of unusual transactions and exceptions, generation of confirmations, and identification of items for testing. In performance audits, GAS can help examine the effectiveness of controls. For example, accuracy, completeness, and authorization controls

can be tested by identifying transactions that are incorrectly entered (keying errors), missing data, or not properly authorized, respectively. Flowcharting software can also assist the internal auditor in analyzing business processes and identifying needed controls. This is a critical need for auditors in directing their efforts on key business processes and associated controls.

GAS also provides a variety of functions to help internal auditors perform quick response audits to detect common fraud schemes perpetrated by employees.[21] Not only has IT increased the incidence of fraud, but it has also increased the average dollar amount of each fraud incident (Parker, 2001). The Association of Certified Fraud Examiners estimates that organizations lose as much as six percent of their annual revenue to occupational fraud (ACFE, 2002).

A 2003 survey of internal auditors found that 51 percent use GAS for detecting and preventing fraud (McCollum and Salierno, 2003). Coderre (2001b, p. viii) identifies eight categories of fraud detection tests that can be performed with GAS: completeness and integrity (data type), cross-tabulation (to organize and view data), duplicates, gaps, data profile (to determine if data falls outside the normal range), ratio analysis, and Benford's Law analysis (which compares patterns in the data to mathematically expected patterns).[22,23] In addition, GAS allows auditors to search for specific text strings and amounts (e.g., "C-A-S-H" and amounts ending in zeros). To make sure employees have not set themselves up as fictitious vendors, auditors can also compare employee names and addresses with vendor names and addresses.

Consulting Services

Consulting services are agreed-upon activities that the internal audit function performs for management with the goal of improving the organization's operations. While these advisory services are more commonly provided by the Big Four professional services firms to their non-audit clients, and also by smaller, boutique firms specializing in the supply of internal audit outsourcing services, in-house internal audit functions also perform these services for their organizations. Consulting services include: (1) assessment services, evaluations of operations to assist management decision making; (2) facilitation services, engagements to identify operational strengths and weaknesses to help change/improve operations; and (3) remediation services, designed to prevent/stop suspected organizational problems (Anderson, ROIA, 2003, p. 107).

CAATTs can assist internal auditors with providing consulting services, especially facilitation services, creating additional value for the organization. GAS can pinpoint underperforming areas of operations. For example, GAS helps optimize the purchasing function by identifying

duplicate payments, discounts not taken, and missed volume discounts. Internal auditors can use self-assessment and facilitation software to capture employees' opinions with real-time graphical feedback to determine which operational controls are important and how well the controls are functioning (Coderre, 2001a).

Data warehouses, which extract operational data from business systems, also represent opportunities for internal auditors to make recommendations to management.[24] Using data mining on a data warehouse allows internal auditors to create "what-if" scenarios and perform trend analyses, identify underlying relationships in the data, and conduct risk analysis to provide insightful, strategic analysis. Online analytical processing (OLAP) enables census sampling of transactions. Further, neural networks can be used for data mining and knowledge discovery to improve operations, in carrying out risk assessment, and prioritizing audit efforts to achieve optimal audit coverage (Ramamoorti and Traver, 1998). Using the IT techniques and tools described above should enhance the image and credibility of the internal audit function by highlighting their role and importance to the organization.

Research Questions

- How much more effective are audits using CAATTs? Does using CAATTs enhance the credibility of the audit function? How are/should constructs such as effectiveness and credibility (be) defined and measured in such studies?

- What is the return on investment for internal auditing from using CAATTs?

- What array of IT tools is available for specific tasks such as risk assessment, fraud detection, and compliance activities?

- Given the plethora of IT tools available, how should internal auditors match tools to tasks? Do variables, such as user sophistication, task complexity, speed, cost, familiarity, or software brand/reputation, matter in technology choice decisions?

- How does the role/position of the internal audit function affect IT (i.e., CAATTs) used for auditing purposes in the organization?

- How does internal auditor and external auditor use of CAATTs differ?

- Do auditors employ additional judgment and critical thinking when they use CAATTs? Do they gain a better understanding of the data and organization?

V. Risk Assessment and Risk Management

Chapter 5 of ROIA describes the role of the internal audit function in evaluating risk assessments and processes and reporting the results in the context of the *Enterprise Risk Management (ERM) Framework* recently exposed by the Committee of Sponsoring Organizations (COSO, 2003).[25] COSO's *ERM Framework* (2003) consists of the following elements: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. The *Framework* defines ERM as:

> "…a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (COSO, 2003, p. 6)

Corporate governance and risk management are intricately intertwined. Specifically, "corporate governance is the organization's strategic response to risk" (McNamee and Selim, 1998, p. 2). In response to the emergence of risk as a central component of corporate governance, internal auditing is moving from a control-based approach to a risk-based approach (McNamee and Selim, 1998). According to *Standard 2110.A1,* internal auditing should "monitor and evaluate the effectiveness of the organization's risk management system." This includes evaluating the risks regarding the reliability and integrity of information; effectiveness and efficiency of operations; safeguarding of assets; and compliance (*Standard 2110.A2*).[26] To support this paradigm shift, internal auditors must understand how one of the major sources of risks — IT — affects the organization. In the following section, we discuss how IT changes business risks and IT as one of the key components of the *ERM Framework*.

IT and Business Risks

Based on strategic objectives, the level of IT selected by an organization may, from a hardware perspective, range from a multi-terabit mainframe processing environment to a few PCs connected to a network. Its software might range from simple accounting to an integrated supply chain and electronic commerce solution.[27] While IT brings great opportunities to the organization, it also brings great risk. The interconnectivity of the e-commerce environment increases the scope and magnitude of risks faced by the organization (Parker, 2001). For example, e-commerce organizations are exposed to a variety of new risks, including viruses,

unauthorized access, hackers, worms, denial-of-service (DOS) attacks, technological obsolescence, system incompatibilities, repudiation, transaction failures, *spoofing*, hijacking, failure of partners, and availability.[28] E-commerce organizations also face the exigencies of operating on "Internet time" — shorter life cycles and faster paced transactions. RAISD (Boritz, RAISD, 2002) provides a comprehensive list of 31 features of IT that change the risks, control, and needed assurances of organizations (see Table 4).

While XBRL may make mergers, outsourcing, and continuous reporting easier, XBRL also exposes the organization to additional risks (Weber, 2003). Internal auditors must ensure that the correct and current XBRL taxonomy is used, financial statement elements are correctly mapped to that taxonomy, and XBRL financial documents are coded correctly. In addition, XBRL documents must be protected (e.g., encryption and digital signatures) to prevent easy spoofing, interception, or alteration (Boritz and No, 2003).

Unfortunately, despite the increase in risks as a result of IT, organizations are just beginning to develop ERM programs to address the risks. A 2001 survey of executives found that only 11 percent have full ERM systems in place, 38 percent have a partial model in place, and 42 percent are investigating or planning ERM (Tillinghast-Towers Perrin, 2001).[29] These executives report that the two primary reasons for implementing ERM are the need for a unifying framework for managing risk and corporate governance initiatives. While the largest impediment to implement ERM is organizational culture, the second largest impediment is a lack of appropriate technology, data, and tools (Tillinghast-Towers Perrin, 2001, p. 17). Therefore, internal auditors need to encourage (and help) their organizations to develop ERM programs.

Indeed, the lack of a sound risk management framework, formalized qualitative and quantitative risk metrics, and an accessible central repository of actuarial data has hampered the development of ERM by organizations (Ozier, 2003). To help organizations overcome these obstacles, as noted earlier, COSO is in the process of finalizing and releasing an *Enterprise Risk Management Framework* that encompasses and expands its 1992 *Internal Control - Integrated Framework*. The *Framework* stresses that ERM needs to be built into operations, requires a portfolio view of (stand-alone and interrelated) risks, and helps management establish a strategy consistent with its risk appetite. The goal of the *ERM Framework* is to develop a framework with integrated principles, common terminology, and practical implementation guidelines to ensure that the organization's objectives are achieved, reporting is reliable, and the organization is in compliance with all laws and regulations.

IT and the ERM Framework[30]

IT pervades the *ERM Framework* — it is not only a source of risk, it significantly provides managers with tools to implement the *Framework*. More precisely, IT is intertwined with all eight components of COSO's ERM framework (the components are identified below in **bold**). The **internal environment** reflects the risk attitude of the organization. The organization's risk attitude affects its choice of IT, level of e-commerce, and the use of emerging technologies — changing the risk of the organization. IT also affects the **objective setting** of the organization. IT is critical to the effective and efficient use of operational assets as well as to the reliability of the entity's reporting. Strong, effective controls in the system will help organizations comply with applicable laws and regulations, especially the sweeping requirements of Sarbanes-Oxley. On the other hand, the strategic objectives of the organization also affect the IT infrastructure of the organization.

IT plays a unique role in the **identification of events**, or incidents that may adversely affect the ability of the organization to achieve its objectives. IT can itself be viewed as an external event, an internal event, as well as an enabler to identify other events. When viewing IT as an external event, an organization must consider the impact of the changing e-commerce environment, increasing availability of data, and emerging technology. When viewing IT as an internal event, an organization must consider how the following items may affect its ability to operate (COSO, 2003, p. 44):

- The acquisition, maintenance, distribution, confidentiality, and integrity of data;
- The availability of data and systems;
- Capacity of its systems; and
- The selection, development, deployment, and reliability of its systems.

As an enabler, IT can be used to facilitate the identification of internal and external events. Managers can use software tools to help generate inventories/lists of relevant events and facilitate workshops to identify potential events from managers and other stakeholders (e.g., RealBiz, Visual Assurance software). In addition, process flow software can help develop process maps to identify and analyze potential events. Escalation/threshold triggers can be programmed to alert management to high-risk areas by comparing transactions/events to predefined criteria. Agents can collect data, identify trends or changes in the underlying population distribution, and communicate the results (Nehmer, 2003). Managers can also use data marts and data warehouses to collect data from past events.[31] This data can be analyzed using data mining software and other statistical packages to identify leading as well as lagging indicators, trends, and causes of events as well as interactions/combinations.

Audit data warehouses and data mining can also be used in **risk assessment** to estimate the likelihood of an event occurring, supplementing qualitative estimates by managers (Rezaee et al., 2002). One survey of executives found that while 89 percent of their internal auditors conduct risk-based audits, only one-third of their internal auditors conduct ERM risk assessments (Tillinghast-Towers Perrin, 2001). Fortunately, internal auditors can use a variety of different tools to estimate the various financial impacts of different time horizons and probabilistic models, including *Monte Carlo simulation, probabilistic or stochastic simulation, economic scenario generation, catastrophe modeling, optimization software, pro forma financial modeling, risk/frequency/severity mapping, scenario planning, algorithms,* and *risk matrices* (Tillinghast-Towers Perrin, 2001; Leithhead and McNamee, 2000).[32] Industry databases provide significant benchmarking opportunities.[33]

In addition, internal auditors may want to use artificial intelligence to help with risk assessment. Neural networks recognize patterns in data with a "learning" process similar to the human brain. Neural networks can generalize from noisy or incomplete data and output classifications or predictions for a situation. Ramamoorti and Traver (1998) found that neural networks can be used to help direct internal auditors' attention to high-risk audit areas. Specifically, such artificial intelligence tools could be a useful adjunct when engaging in "brainstorming" and "scenario building" activities that seek to track and monitor business risks as they develop (Kinney, ROIA, p. 149).[34]

Regarding **risk responses**, organizations selecting an avoidance response may choose to ignore/minimize e-commerce and emerging technologies. Alternatively, organizations may choose to reduce the risk of IT by establishing strong IT controls (discussed below). To share the risks of IT, an organization may choose to augment its standard insurance (which generally does not cover network-related incidents) by purchasing a variety of products specifically designed to cover IT risks. Currently, network risk and liability insurance is available to expand the traditional coverage for property, commercial general liability, and crime.[35] Software, for instance, the Bayesian Decision Support System, can help provide cost/benefit analysis of risk mitigation measures (Le Grand, 2001).[36]

IT plays a prominent role in establishing and maintaining **control activities** to ensure that risk responses are carried out. IT controls should support strategic, operations, reporting, and compliance objectives. Controls should also ensure that transactions are complete, accurate, authorized, and valid. E-commerce also changes the types of controls that are effective internally as well as externally with customers and suppliers (Parker, 2001). Moreover, e-commerce control activities must be automatic, dynamic, integrated, preventive, multi-compensating, real-time, and include sound authentication procedures and secured

audit trails (Parker, 2001). Potential automated controls include, but are not limited to, approvals, authorizations, reconciliations, segregation of duties, verifications, logic and reasonableness tests, check digits, as well as the automated generation of exception reports. Transaction (digital) agents could also implement internal controls such as imposing constraints on data entry (Nehmer, 2003).

IT also plays an important role in **information and communication**. Reliable, timely information is needed at all levels of the organization to identify, assess/analyze large amounts of data, and respond to risks. Information must also be communicated seamlessly across the organization. Enterprise resource planning systems (ERPs) in conjunction with integrated data warehouses can collect (and process) vast amounts of internal and external data for ERM. In addition, ERPs, which cut across functional silos, provide conduits for distributing information vertically and horizontally across organizations. The Internet also provides a method for distributing relevant information about the organization's risk to parties external to the organization.

Finally, in today's rapidly changing business environment, the organization's ERM plan must constantly change to ensure that the organization is controlling its risk effectively. This requires ongoing **monitoring** that is real-time, dynamic, and embedded in the organization (COSO, 2003, p. 79). This type of monitoring can only be achieved through the use of IT. Systems can include modules to identify exception conditions or, alternatively, data can be automatically extracted for analysis using CAATTs or audit data warehouses. Transaction agents can monitor software applications, other agents, and activities (Nehmer, 2003). Automated variance analysis, reconciliations, and comparisons may also be defined.

Given the pervasive impact of IT on the organization and ERM, internal auditors can add substantial value to the organization if they are familiar with IT that can assist their organization in developing a sound ERM program. Organizations need internal auditors to understand the system, infrastructure, programs, processes, and constituents; record and evaluate controls over critical/sensitive information; assess monitoring procedures; and obtain external assurances (Parker, 2001). In addition, Hunton (RAISD, 2002) suggests that internal auditors may be able to reduce the risk associated with the organization's IT by participating throughout the entire systems life cycle.

Research Questions

- How does IT affect risk, risk assessment, and risk management? (Kinney, ROIA, 2003, p. 147) How can IT best help organizations establish, monitor, and proactively change their ERM activities?

- How can the impact of IT on enterprise risk be accurately measured? How can emerging technologies be identified and their risk measured?

- What are the IT implications for each component of the ERM proposed framework?

- How can IT help communicate risk assessments and responses to stakeholders? Can the message be tailored to fit the needs of the stakeholder?

- What data is needed in an audit data warehouse to monitor and measure risk?

- What are some industry best practices in assessing (technology) risk?

- What is the risk of not converting from legacy technologies? How can the forfeited efficiency gains be measured?

- How does participation by the internal auditor in the entire systems life cycle affect the organization's risk associated with IT? (Hunton, RAISD, 2002, p. 97)

- What role should IT play in identifying (new) risks and assessing the effect of that risk? How does the use of IT in the organization affect the (internal) audit risk model?

- What is the impact of different internal and external factors on the organization's use of IT in risk assessment?

- How can the net effect of IT be assessed (risk vs. opportunity)?

✜ Do internal and external auditors evaluate IT-based controls using the same techniques? How can these controls be effectively audited?

✜ What is the best way to use IT to identify effective controls? Monitor controls and evaluate risks? Identify inefficient business processes?

- How do IT risk assessments differ between internal auditors and external auditors? Do the time horizons and number of risk scenarios used by internal auditors and external auditors differ?

VI. Managing the Internal Audit Function

Chapter 6 of ROIA discusses staffing and managing the internal audit function using the fundamental model of management that consists of planning, organizing, staffing, leading and controlling (Prawitt, ROIA, 2003, p. 172). In this section, we examine how IT has affected different components of this model — specifically the hiring and training of internal auditors, the managing of internal audits, and communicating internally and externally. We begin by highlighting The IIA's guidance regarding IT and audit management.

The IIA recently proposed a new *Standard* — 1210.A3 — which states "internal auditors should have general knowledge of key information technology risks and controls and available technology-based audit techniques." In addition, while all internal auditors are still not expected to have the level of knowledge required by IT auditors, all internal auditors must exercise due professional care by considering the use of CAATTs (proposed amendment to *Standard 1220.A1*). With respect to audit management, *Standard 2030* states that the chief audit executive must ensure that "internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan." With respect to communications, *Standard 2420* states that communications should be "accurate, objective, clear, concise, complete, and timely."

Strategic Positioning

It is critical that the chief audit executive (CAE), sometimes called the director of internal audit or the general auditor, project the image of the internal audit function as value-adding and one with a respected organizational status. The CAE should promote the view of heading up a competent, independent and unbiased function reporting to the audit committee. Given such strategic positioning within an organization, the function should clearly be technology-savvy and fully integrate IT into its methodology and activities. Indeed, IT audit expertise can go a long way in securing the credibility of the internal audit function in an increasingly "wired" or even "wireless" world of business. To achieve proper strategic positioning though, the internal audit function needs to hire personnel with the appropriate leadership-oriented skill sets and competencies; attention also needs to be paid to the IT/non-IT mix of professionals associated with the internal audit function. We turn to the topic of successfully recruiting and training IT audit professionals next.

Hiring

IT is changing the needed skill set of auditors. At the same time the above changes are being considered to the *Standards*, Sarbanes-Oxley is also increasing the level of IT knowledge required by auditors. As discussed in Section IV, Sections 404 and 409 of Sarbanes-Oxley require organizations to assess the effectiveness of their internal controls over financial reporting and report material changes in their financial position on a "rapid and current basis," respectively. In order to meet these requirements, organizations need internal auditors that understand controls, information systems, and IT usage to monitor the organization's operations. Internal auditors must be able to document controls using IT (flowcharting software) and recognize (and communicate) deficiencies.

AMR Research estimates that the Fortune 1000 organizations will spend $2.5 billion in initial compliance work and IT investments to be in compliance with Sarbanes-Oxley (Sodano and Hagerty, 2003). IT-savvy internal auditors will play a significant role in this effort. Therefore, large organizations, as well as internal audit outsourcing providers, will seek new and experienced hires with solid IT skills and/or provide internal auditors with IT training (as discussed below). In the current global business environment, as part of cost containment efforts and geographically concentrated availability of competent IT professionals, the IT needs of large organizations are also being met by "off-shoring" arrangements to countries such as India, Ireland, and China.

Training

IT is also beginning to play an important role in training new and experienced internal auditors. Organizations can use a variety of techniques to present new concepts to employees, including computer-based training (CBT), videoconferencing, and Web-based training (WBT). CBT provides interactive training on a CD-ROM and incorporates text, graphics, video, audio, and self-tests. WBT is a type of CBT in which materials are provided via the Internet, not a CD-ROM, and may provide interaction with others via chat rooms or discussion boards. Finally, the Internet can also be used for videoconferencing, allowing instantaneous and real-time interaction between geographically dispersed instructor(s) and students using cameras, microphones, speakers, and projection equipment.

All three methods can be used to train employees about new procedures, techniques, and software. Advantages include a reduction of training costs (versus travel and external training programs), consistency of delivery, easy access, organization-tailored materials, and use by internal auditors (almost) anywhere at any time. The methods also enhance learning because the materials are interactive, can easily be tailored to different learning styles and rates (i.e.,

material can be repeated as many times as necessary), and provide immediate feedback. In addition, W/CBT has been shown to reduce learning time by a third (Kulik and Kulik, 1991) and is well-suited for helping develop skills that require analysis, synthesis, and evaluation (Driscoll and Reid, 1999). Disadvantages include bandwidth limitations for both WBT and Internet video conferences. On the one hand, CBT can become obsolete quickly. On the other hand, WBT can be instantly (and universally) updated.

Some organizations have gone to extensive lengths to build effective training tools and ensure continuity over time. For example, Ameritech's internal auditing group developed an interactive, multimedia training tool called *Coach* to (1) quickly and efficiently train new auditors to perform operational audits, (2) capture and share knowledge, and (3) retain knowledge as turnover occurs. *Coach* uses virtual conversations and identifies past audits with similar characteristics to train auditors in workpaper preparation, risk assessment, and knowledge retention (D'Amico and Adamec, 1996; "How *Coach* Works," 1996).

To comply with laws, regulations, and policies, the organization can provide internal auditors with an electronic audit reference library. The library can be made available on the Internet, corporate LAN or WAN, or CD-ROM. This library should consist of audit standards, eSAC (The IIA's e-commerce Systems Assurance and Control guidance), industry standards, organizational policies and procedures, as well as forms and templates. A good search engine is essential so auditors can quickly shift through the multitude of professional literature and practice guidance available to them.

Managing the Audit

"Audit management is charged with providing an effective audit force, directing audit resources for maximum benefit to the organization, and complying with laws, regulations, and policies regarding auditing" (Le Grand, 2001).[37] To manage an adequate number of competent staff, the internal audit function needs to maintain a personnel database and skills inventory. This database helps ensure the professional development of auditors by tracking current skills, training attended, as well as needed future training. In addition, the software assists with audit planning and scheduling by highlighting weak/uncovered areas that require additional training or outsourcing.

Another way organizations help ensure an effective internal audit function is via benchmarking. Organizations benchmark themselves against the internal audit functions at other organizations to determine how they measure up and what they need to improve. Hendrey (1999) describes the IT audit benchmarking results of Dupont against Exxon Corporation, IBM, Ford Motor Company, J.P. Morgan & Co. Incorporated, General Electric,

and Prudential Insurance Company of America. Dupont identified 13 best practices that it used in developing a new IT Audit Integration Model.

To direct audit resources for maximum benefit, the internal audit function can utilize a variety of software tools to help manage the audit. This includes, but is not limited to, audit management and administration software that provides for inventory of the audit universe; planning and scheduling (including assigning auditors to projects based on their skills); project management and audit tracking; time, expense, and issue tracking; and measuring client satisfaction with the internal audit function.

Automated (or electronic) workpapers are replacing the cumbersome traditional paper workpapers in what is called an electronic hypertext systems (EHS) environment. The electronic version allows auditors to easily manage, organize, link and locate text, spreadsheets, graphs, and other sources of information that have been scanned in using scanning software (e.g., optimal character recognition (OCR)). All these hypertext links, combined with the ability to click and move out of sequence to selected workpapers and reference materials, allow the auditor to become more directed and efficient.

Despite these navigational efficiencies, recent research in an external audit setting has revealed that cognition in an EHS environment is more demanding than in the traditional paper environment (Bible, Graham, and Rosman, 2004). These researchers hypothesized that in EHS environments, audit workpaper reviewers must remember their initial location, the path taken from that point (especially because no explicit cross-referencing may exist), along with having to remember the workpaper information content, all of which may lead to "cognitive overhead" confirmed by the reported (reviewer) feelings of being "disoriented" or being "lost in space." Clearly, such an outcome can adversely affect audit review performance.

XBRL may also assist the internal auditor in managing the audit. The XBRL Steering Committee has identified new taxonomies — one for audit schedules and one for working papers. These tools would use XBRL to automate the retrieval of needed data allowing the internal auditor to focus on value-added portions of the audit (CICA, 2002).

Communicating

A variety of communication tools are making the internal audit function more efficient by allowing internal auditors to easily share information. E-mail and file transfer software allow internal auditors to easily and quickly share data and maintain contact. Video

conferencing allows internal auditors to conduct meetings face-to-face even if they are geographically dispersed. The Internet, LANs, WANs, intranets, and wireless networks also increase the connectivity and productivity of internal auditors. Communications software also it makes it possible for internal auditors to complete more work in their home office and reduce traveling time.

Chapter 7 of RAISD (Murthy, RAISD, 2002) discusses the benefits of group (decision) support system or groupware software (e.g., Lotus Notes), which supports groups of people working together on a project, often at different sites.[38] With respect to auditors, groupware has given them the capability of pulling the hiring, training, and audit management technologies described above together (Salamasick and Fraczkwski, 1995). Groupware allows internal auditors to share and collaborate on documents — even viewing the same (updated) document at the same time through database replication. This replication eliminates the conflict over who has control over the workpapers and reference library, because everyone has access to them (24 hours a day, 7 days a week). In addition, groupware can replicate server-based information to individual PCs, so that internal auditors can view/work on the information even when they are disconnected from the network. Internal auditors can hand off work to the next auditor via boxes/baskets. Time, date, and user ID stamps aid in tracking the quality and efficiency of internal auditors' work. Groupware also allows managers to monitor the progress of the engagement in real-time, which is becoming more important as organizations move toward (near) real-time reporting (Sarbanes-Oxley, Section 409).[39]

To be in compliance with *Standard 2420* (communications), IT should help internal auditors analyze and complete the engagement timely. Presentation software, which creates/embeds charts, graphs, pictures, sound, and video clips, can help internal auditors present clear, concise, and complete information. Internal auditors may also need to provide assurance over requested items (e.g., controls) for regulatory agencies, customers, and suppliers. Customized, dynamic, evergreen reports can be made available to various stakeholders via the organization's Web site.

Almost 52 percent of internal auditors report that IT groupware tools reduce the amount of time that they spend "on site" at distant locations from 10 percent to 80 percent (Glover and Romney, 1997). Despite these efficiency (and effectiveness) gains, internal auditors have been relatively slow in embracing these IT-oriented approaches in their work. Surveys of internal auditors find that only 50 percent to 76 percent of internal auditors use IT to assist in audit management and automated workpapers (Bierstaker, Burnaby, and Hass, 2003; McCollum and Salierno, 2003).

Research Questions

- What is the appropriate IT skill set for internal auditors? What must non-IT auditors who are subject matter specialists know about IT?

- What kind of additional cognitive demands (including possible "disorientation") do electronic hypertext systems (EHS) place on internal auditors when they navigate through electronic workpapers? If this feeling of being "lost in space" is validated, does it adversely affect internal audit (review) performance? What are some ways of mitigating or even eliminating such effects?

- How much does IT increase the efficiency and effectiveness of the internal audit function? What are the appropriate metrics to measure the improvement?

- What is the best combination of IT tools to improve the efficiency and effectiveness of the internal audit function?

- How do different internal auditing environments (e.g., size, dispersion, nationality, organizational structure, reporting structure, culture, number of IT auditors) influence the net benefits from IT deployment? Does IT provide more benefits under certain circumstances than others?

- What is the best way to equip internal auditors to use IT to improve the efficiency and effectiveness of the internal audit function?

- What is the best way to use IT to teach internal auditors new skills? Under what circumstances (task, learning preferences) is IT the best way to teach new skills?

- Under what circumstances should the internal audit function outsource IT audit? What are the costs and benefits of outsourcing IT audit? In similar vein, what are the costs and benefits of "off-shoring" IT audit work?

- How do the required IT skills of internal auditors and external auditors differ? How do internal and external factors affect the needed skills?

- How does the use of groupware differ between internal auditors and external auditors?

VII. Ethics, Privacy, and Security

Chapter 7 of ROIA discusses the concepts of independence and objectivity within the context of internal auditing, presenting a framework to identify and manage threats to objectivity of the internal audit function (Mutchler, ROIA, 2003). Independence and objectivity are components of The IIA's Code of Ethics, which states that internal auditors are expected to apply and uphold the principles of integrity, objectivity, confidentiality, and competency. We expand ROIA's discussion of independence and objectivity to encompass the ethical issues facing internal auditors in today's IT-driven world.[40]

Chapter 9 of RAISD (Dillard and Yuthas, RAISD, 2002) describes the current state of ethics research in AIS using traditional ethics perspectives. RAISD also discusses "ethical issues of the Information Age" identified by Mason (1986) as privacy, accuracy, property, and access. Similarly, Sutton et al. (1999) identify the ethical issues associated with auditing and IT as: epistemology, quality of work life, intellectual property, competitive advantage, and information privacy and security.

In today's litigious society and cyberspace environment, maintaining the security of confidential information has become an important professional and legal responsibility falling squarely within the compliance domain. Privacy, confidentiality, documentation and records retention, and identity and credit theft protection are significant concerns in a growing e-commerce marketplace. In this section, we focus on the recurring issues of information privacy and security and how they challenge the internal auditor's ability to uphold The IIA's Code of Ethics. Internal auditors must properly recognize and prepare for the impact of such vulnerabilities and exposure on the organization. Indeed, internal auditors can play a significant role in developing and maintaining an adequate internal control structure that incorporates prevention against system intrusion (Bou-Raad and Capitanio, 1999).

We also discuss how IT can help mitigate such threats as well. When reading this section, painting with a broad brush, the following quotes provide some perspective on the intersection of technology and ethics:

"Technology changes, compassion does not."
"What we have today are technological giants, but ethical infants."

Privacy

IT provides organizations with great capabilities and opportunities, allowing organizations to connect with customers across the globe. As technology increasingly pervades our lives, consumers are increasingly worried about informational privacy, or the individual's claim to control the terms under which identifiable personal information is acquired, disclosed, and used (Cuaresma, 2002). Hargraves, Lione, Shackelford, and Tilton (2003) outline four IT developments that have led to today's privacy issues. First, computer processing allows easy dissemination of information. Second, databases and data warehouses permit quick storage and retrieval of vast amounts of (personal) consumer information. Third, network communications make it easy to collect and disseminate information. Fourth, electronic document imaging and storage media allow users to retrieve data anywhere.

In addition to these four IT developments, consumers have additional reasons to worry about the privacy of their information because privacy over personal data is continually eroding (Spinello, 1998). IT allows organizations to collect more information about consumers than ever before on the Internet using cookies, Web bugs, and port scans (King, 2001) for commercial purposes. Moreover, IT increases the risk that proprietary information may be compromised accidentally or maliciously, through hacking or other forms of cyberterrorism.

To help ensure that consumer information is sufficiently protected, several laws have been passed recently to protect the privacy of consumers. Noncompliance with these laws increases the risk of legal action against the organization. Internal auditors need to understand the laws, how they affect their organization, and how to mitigate the risk through proper IT security measures.

The first comprehensive law passed in the U.S. was the 1996 Health Insurance Portability and Accountability Act (HIPAA), designed to protect the privacy of consumer's health records. The second privacy act passed was the 1998 Children's Online Privacy Protection Act (COPPA), regulating Web sites that collect information from children under the age of 13. The third law, Identity Theft and Assumption Deterrence Act of 1998, makes identity theft a true crime that can be investigated/combated by the Secret Service, FBI, and other law enforcement agencies. Finally, a fourth law, the 1999 Gramm-Leach-Bliley Act (GLBA), attempts to ensure that financial services companies preserve the confidentiality of customers' financial information.

Security

In general, security includes considerations such as **system confidentiality** (restricting access to authorized users) as well as **system availability** (ongoing systems resources being available for organizational use). Some of the ways in which computer online security is achieved are through encryption, Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA algorithm), digital/electronic signatures and biometrics (Friedlob, Plewa, Schleifer, and Schou, 1997). In this context, HIPAA, COPPA, Identity Theft and Assumption Deterrence Act, and GLBA demonstrate the increasing regulatory imperative for organizations to protect consumer data. At the same time, organizational Web sites and intranets are under attack from hackers and others. A survey by the Computer Security Institute (2003) and FBI reveals that 56 percent of respondents experienced attacks or unauthorized access and use with losses totaling $202 million during 2002. For those attacked, 38 percent report one to five incidents, 20 percent report six to 10 incidents, and 16 percent report 11 to 30 incidents. In addition, 25 percent experienced unauthorized access or misuse of their Web sites, including vandalism (36 percent), denial of service (35 percent), financial fraud (four percent), and theft of transaction information (six percent).

To comply with the privacy laws and combat these attacks, organizations are implementing a variety of security measures. Because physical storage, data access, and dissemination of personally identifiable information must be in accordance with each consumer/patient's wishes, an elaborate information gathering and reporting system, with suitable security measures, must be in place. Organizations also need to establish an enterprise-wide information security program that uses IT to enforce data protection rules (Hargraves et al., 2003). Potential IT tools include multilevel access controls, smart cards, firewalls and their continuous monitoring, intrusion detection software, encryption, tracking the frequency of confidential inquiries, filtering, virtual private networks, and biometrics.[41]

Organizations must also ensure that they do not capture information (about children) with passive tracking through cookies, Web bugs, or port scans. Because many organizations operate as extended enterprises today, they must ensure the security of systems belonging to business partners and suppliers that have access to their systems (Gilbert, 2001). Organizations must also ensure that systems are not affected by viruses or worms (via virus software) that may unintentionally distribute personal information — violating privacy laws (King, 2001).

In addition, organizations must protect themselves from abuse, fraud, and attacks from authorized users. For example, a Coca Cola employee stole salary and Social Security information on 450 co-workers (Husted, 2003). Organizations can implement Unified

Enterprise Application Security (UEAS) to protect against "abusive behavior by authorized users — whether employees, partners, or customers" (Cerebit, 2003). UEAS focuses on application security (versus network and operating security), which is important for organizations with applications using different protocols. The software provides for role-based/time-based/context-based authorization, public key infrastructure, audit logs, and non-repudiation services (through digital signatures).

In general, organizations are reinforcing security provisions. Almost 100 percent report using antivirus software and firewalls; 92 percent have access controls; 72 percent use intrusion detection software; 69 percent use encryption; and 11 percent use biometrics (Computer Security Institute, 2003). Unfortunately, 15 percent of respondents in the same survey did not know if their computer systems had unauthorized use in the last year, and 22 percent did not know if their Web site had experienced unauthorized access or abuse. Moreover, only 30 percent of attacked organizations report the incidents to law enforcement agencies because of negative publicity, fear that competitors could use the information to their advantage, lack of knowledge that the information could be reported, and civil remedy seemed best (Computer Security Institute, 2003).

The internal audit function is playing a critical role in insuring the privacy and security of an organization's data. Audit committees are turning to the internal audit function to assure compliance with all applicable laws because failure to comply and/or protect data exposes the organization to potential lawsuits, financial losses, and loss of reputation (cf. Cravens, Oliver, and Ramamoorti, 2003). The internal audit function needs to perform periodic qualitative and **quantitative** assessments of the organization's privacy and security provisions. As part of assessing the effectiveness of the provisions, the internal audit function needs to evaluate whether information privacy and security is fully integrated into organizational policies. The internal audit function also needs to determine that the organization has a viable (and periodically tested) disaster recovery plan in place to provide for continuity of operations in the face of unforeseen disturbances.

DOS Attacks

In addition to viruses and worms, organizations are subjected to denial-of-service (DOS) attacks, the second most expensive cyber crime in 2002 with an estimated cost of $65 million (Computer Security Institute, 2003). A DOS attack is an intentional attempt to prevent legitimate customers from accessing Web services. DOS exploit known bugs in operating systems and servers, while distributed DOS (or DDOS) use an army of *zombie computers* (taken over previously through downloaded agents) to flood and overwhelm the processing

resources of an organization's system.[42] The threat of DDOS is real, since there are over 4,000 DDOS attacks every week (Narayanaswamy, 2002). Moreover, new types of DOS are continuously being invented. For example, Distributed Reflection DOS (DRDOS) floods the server with forged, valid packets (Joyce, 2002).

To protect themselves from DOS attacks, organizations need to first ensure that intrusion detection systems are in place. Virus scanning software must also be up-to-date to detect rogue programs that turn computers into *zombies*. To stop *spoofing*, routers should not allow outgoing information with invalid source addresses. Organizations should also utilize host-based DDOS protection software that prevents a zombie takeover and damage-control device software to minimize the damage of a DDOS (Narayanaswamy, 2002).

Ethical Hacking

Despite increased security efforts by organizations, the intrusion into organizations' systems is increasing because (1) all IT components have security vulnerabilities and (2) powerful tools exist to exploit these vulnerabilities (CICA, 2003a). Unauthorized users, variously called hackers, red hat hackers, intruders, or crackers break into computers for fun, revenge, or profit (Palmer, 2001). Garg, Curtis, and Halper (2003) estimate the market impact of security incidents between 0.5 to 1.0 percent of annual sales for the average publicly listed organization.

To help identify these vulnerabilities before a hacker does, organizations are beginning to use ethical hacking (also known as penetration testing, or vulnerability testing) to evaluate the effectiveness of their information security measures (CICA, 2003a). The first public discussion of ethical hacking to assess the security of a system was by Farmer and Venema in December 1993. They secretly (and without authorization) tested the security of a variety of organizations, posted the results on an Internet discussion board (Usenet), described how they could exploit the weaknesses, and explained how the weaknesses could be prevented. Farmer and Venema even provided a software application, Security Analysis Tool for Auditing Networks (SATAN), which identified vulnerabilities of a system and gave advice on how to correct them (Palmer, 2001).

Today, organizations hire well-trained, certified ethical hackers (or tiger teams) to perform a series of activities to "identify and exploit security vulnerabilities" (CICA, 2003a) and then report the vulnerabilities and corrections to management. Several different penetration-testing strategies are possible: external, internal, blind, double blind, and targeted. In addition, the following types of penetration testing can be executed: application security testing,

denial of service (DOS testing), *war dialing*, local network, stolen laptop, wireless network penetration testing (or war driving), physical entry, and social engineering (see CICA, 2003a, and Palmer, 2001, for a detailed explanation of testing strategies and types of tests).

While penetration tests go beyond normal audits, they do have several drawbacks. First of all, penetration tests may not find all vulnerabilities. Second, tests are performed at a specific point in time and are not ongoing efforts. Third, they may crash the system. Finally, criminal hackers may be monitoring the transmissions of the ethical hacker and learn the same information (Palmer, 2001). The internal audit function can help the organization harness the power of ethical hacking, while minimizing its potential risk, in order to help protect the organization from seen and unseen vulnerabilities.

Computer Forensics

In addition to using ethical hacking to combat security breaches, organizations can also use computer forensics as a weapon in their arsenal. While ethical hacking attempts to prevent cyber crimes, computer forensics is used after a cyber crime has been committed. Computer forensics is broadly construed as having to do with the preservation, identification, extraction, and documentation of computer evidence (Marcella and Greenfield, 2002). Specifically, computer forensics includes "procedures applied to computers and peripherals for the purpose of producing evidence that may be used in a criminal or civil court of law" (Bigler, 2000, p. 54). In other words, computer forensics is an autopsy of a computer system to yield relevant and admissible evidence pursuant to a legal proceeding (Verton, 2002). Internal auditors can utilize computer forensics to investigate acts that are illegal, unethical, or against organizational policy and involve a computer. Examples include fraud, employee misuse, intellectual property theft, harassment, theft, pornography, or deception committed by employees, contractors, vendors, customers, or other third parties (Bigler, 2000).

Computer forensics requires a set of IT tools and IT knowledge to collect evidence from computers, networks, and the Internet. Software helps investigators create a mirror image copy of computer hard drives for further examination; recover erased files; perform keyword searches throughout the system — even in slack space where erased data resides; view files in any format; determine if the hard drive has been altered; review and analyze system and application logs; analyze e-mail for source and content; recover passwords; and rebuild directories. Bigler (2001) provides an extensive list of software packages that can be used in computer forensics to complete these tasks. Marcella and Greenfield (2002) have written a comprehensive and extremely helpful field manual for collecting, examining, and preserving evidence.

This section has presented a variety of privacy and security issues that threaten organizations' existence. Internal auditors should make sure that management is aware of these new threats as well as ways in which to mitigate those threats. The absence of effective privacy practices increases the inherent risk of the organization because financial and operations risk increases (Hargraves et al., 2003). Internal auditors can help their organization move from no privacy rules/policies to continuously monitoring and improving the effectiveness and quality of privacy policies, practices, and controls. (Hargraves et al., 2003 present a five level model to categorize the maturity of an organization's privacy efforts.) In the future, internal auditors certainly need to include evaluating compliance with privacy policies in their audit programs (Hargraves et al., 2003 also provide a privacy audit program).

Research Questions

- What metrics can the internal audit function use to assess the effectiveness of the organization's privacy and security provisions?

- How do internal and external factors change the metrics used by the internal audit function to quantify the effectiveness of the organization's privacy and security provisions?

- What are some appropriate metrics to measure the impact of a privacy or security breach? What is the best method to determine the financial impact of computerized system intrusion?

- How can the internal audit function help management understand the importance of monitoring unauthorized access to computer systems?

- What is the appropriate level of in-house knowledge of computer forensics techniques?

- What is the best way to monitor business partner's security policies and procedures? What metrics should be used to evaluate inter-organizational security?

- How effective is ethical hacking? Should the internal audit function permanently employ an ethical hacker?

- Should ethical hacking be done by EDP/IT internal auditors or by someone specializing in penetration/vulnerability testing?

- For a given set of internal and external factors, what is the best disaster recovery plan? How can the effectiveness of a disaster recovery plan be evaluated prior to a disaster?

- Do internal auditors' and external auditors' risk assessments of information privacy and security differ? If so, in what respects and why?

VIII. Internal Auditing's Systematic, Disciplined Process

Chapter 8 of ROIA discusses internal auditing's disciplined process and how internal auditors and external auditors are now using the business risk approach to audit organizations (see also Bell et al., 1997). This risk-based, controls-focused approach emphasizes high-level controls and monitoring controls over business processes. (External) auditors believe that this approach allows them to focus on understanding their client's business better. Moreover, "professional judgment plays a large role in answering the questions about how much and what kind of information should be gathered and analyzed during the engagement" (Lemon and Tatum, ROIA, 2003, pp. 283-284).

In this section, we look at the internal auditor's professional judgment in the context of decision aids. Specifically, we discuss human-computer interaction and how IT supports decision making by internal auditors in all phases of the audit — planning, execution/conduct, and reporting. We also discuss the growing importance of knowledge management. It is important not to forget that while decision aids can supplement an auditor's decision-making capabilities, they cannot supercede or supplant the professional judgment of the internal auditor. Our discussion of decision aids and knowledge management is guided by Chapters 4, 6, and 11 of RAISD, which provide in-depth discussions of expert systems, decision aids, and knowledge management, respectively.

Decision Aids

Internal auditors can make decisions in the following ways: (1) without computer support; (2) aided by computers; and (3) completely computerized. Given that IT is increasing the complexity, pace, and amount of information collected by organizations, auditors must work efficiently and effectively, assimilate large amounts of information, and not be overcome by information overload — which may not be possible for unaided humans in today's environment. Accordingly, auditors are using IT decision aids[43] to improve their efficiency and make better decisions by reducing cognitive limitations and biases.

Decision aids help users gather information, evaluate alternatives, and make a decision. Auditing, composed of planning, execution, and reporting, requires internal auditors to complete these three activities as well. Therefore, decision aids can help auditors perform the steps comprising the audit process. Internal auditors can use IT decision aids to help them make the decision or to fully automate monotonous tasks that can be accurately programmed.

While many decision aids are available, the appropriate decision aid depends on the structure of the task that the auditor is trying to perform. Messier (1995) and Rose (RAISD, 2002) describe three categories of decision aids: simple/deterministic aids, decision support systems, and expert systems.[44] Simple/deterministic aids are designed to correctly solve straightforward, highly structured problems. These (computerized and non-computerized) aids help the decision maker perform easy mechanical procedures or computations. Decision support systems are designed to help users make decisions about semi-structured problems requiring judgment. The decision support system helps by applying structure to the decision and "direct interaction with data and models" (Benbasat and Nault, 1990, pp. 203-204). The third type, expert system, is designed to help users make decisions requiring extensive judgment about unstructured, ill-defined problems characterized by high levels of uncertainty. Expert systems are computerized programs that capture the specialized knowledge of experts using symbolic reasoning so that novices can make judgments similar to experienced professionals. The goal of expert systems is to make expert decision processes and capabilities readily available throughout an organization. Ultimately, these systems are designed to allow novices to perform at the level of experts.[45]

All three types of decision aids can help internal auditors perform their task in each stage of the audit. Automated checklists (that adapt to responses by auditors) help ensure that internal auditors consider all relevant information. Intelligent bots can automate the gathering of information inside and outside the organization. IT can also be used to combine information and help compare alternatives through different format displays (numerical, table, graph), simulations, and automated calculations. GAS helps examine data in detail. Expert systems can be used to evaluate risk and make a decision at the level at which to set risk. Expert systems using case-based reasoning can identify similar past audits. Moreover, if expert systems incorporate neural network technology, the systems can learn and change dynamically with the audit environment.

Knowledge Management

IT is causing the value of most organizations to be generated by intangible rather than tangible assets. While IT is driving this change, IT is also enabling organizations to manage their knowledge through the use of knowledge management systems (KMS). O'Leary (RAISD, 2002, p. 275) defines knowledge management as consisting of capturing knowledge, converting personal knowledge to group-available knowledge, connecting people and knowledge, and measuring the current (and changing) levels of knowledge that is available to manage resources. KMS incorporate world/national/local/research news, who-knows-who contacts, industry intelligence, employee expertise information, frequently asked questions, lessons learned, proposal and engagement, best practice, and functional knowledge (O'Leary, RAISD, 2002).

KMS play an important role in the problem-solving ability of the organization. KMS should not only capture knowledge, but they should help organizations develop and distribute knowledge. To accomplish these goals, KMS integrate a variety of different IT, including data warehouses, data mining, OLAP, intelligent agents, groupware, neural networks, and networks (Internet, extranet, intranets). Knowledge mapping, which provides a visual display of the captured information and the relationships between the information components, plays an important role in communicating the knowledge within the database so users can understand and learn from the KMS, which is necessary for sustainable organizational learning (Chou and Lin, 2002).

To add value to the organization, internal auditors can help their organization develop a KMS that helps preserve institutional memory, organizational expertise, and ensure continuity/ consistency over time. An effective KMS requires knowledge to be constantly produced, captured at the source, transmitted to a data warehouse, analyzed within the data warehouse, and transmitted immediately to the appropriate users. Internal auditors should play an integral role in helping the organization design a seamless integrated KMS that generates and captures the ever-changing knowledge of the organization.

Research Questions

- What should be the internal auditors' role in designing, implementing, and monitoring KMS? How do different internal and external factors affect that role?

- Do internal auditors specializing in IT/EDP have different cognitive biases than other internal auditors?

- Do internal auditors specializing in IT/EDP use IT decision aids differently than other internal auditors? Are IT decision aids more effective for IT/EDP internal auditors?

- How can internal auditors select the best decision aid for a task? Which decision aids are best for a given task?

- Do internal auditors and external auditors have the same cognitive biases? Are internal auditors and external auditors exposed to the same amount of information overload? How does internal auditor and external auditor use of decision aids and KMS differ?

- How effective are decision aids in improving the efficiency and effectiveness of internal auditors and external auditors?

- What are the best decision aids to help internal auditors and external auditors? How do internal and external factors affect the selection?

- What are some threshold criteria and best practices for information that should be captured in KMS?

IX. Conclusion

The 21st century Information Age is characterized by the emergence of new, disruptive technologies with a global impact. Industry after industry is being rapidly revolutionized, whether traditional manufacturing or new service suppliers in areas such as banking, finance, insurance, or in wholesaling and retailing businesses. In 1985, McGowan (1985) prophetically stated:

> "…[these] information technologies are changing the structure of markets themselves, and altering the life cycles of products in these markets. They're reordering production and distribution patterns. And they're causing major changes in the structure of our organizations and in the way people work…preparing for the information age, and staying competitive in it, is the single most significant management challenge of our time."

Remarkably, almost 20 years later, McGowan's comments still apply and technology continues to redefine the business world. In fact, a recent *Wall Street Journal* front-page

article observes that "the powerful force of technology [is] reshaping one company after another…It is disrupting basic business models, plunging companies into new markets, creating new competitors and blurring the boundaries between industries" (Angwin, Peers, and Squeo, 2004).

In this supplemental chapter to the *Research Opportunities in Internal Auditing* monograph, we have sought to capture the key insights into how IT affects almost every important dimension of the internal audit function: its organizational status and charter, scope, methodology, and activities. Indeed, IT does seem to bear upon everything from strategy, to management IS, to managerial decision making, to business processes including reengineering efforts, and the overall stewardship and governance mandate. Consequently, the widespread influence of IT on almost all internal audit activities designed to promote and support effective organizational governance lead us to use the descriptive chapter title phrase: "pervasive impact." With respect to understanding IT's role and impact, we must recognize that IT serves as both a *driver* — in setting the strategic direction of the organization — as well as an *enabler* — in helping to execute effectively against the formulated and adopted organizational strategy.

Perhaps the most important consideration in using IT for competitive strategy formulation is to achieve a long-run, sustainable competitive advantage. Davis and Hamilton (1993) have convincingly argued that the interaction of business strategy, IT, and business processes is an iterative process. Thus, strategy considerations may suggest IT uses but IT uses in turn may suggest changes in strategy; in other words, strategy decisions lead to requirements for business processes, but innovative processes too may suggest changes in strategy (Davis and Hamilton, 1993). Such a bird's-eye view of the influence of IT on organizations today is critical for internal auditors who have a tremendous opportunity to contribute on dimensions such as organizational governance, risk management, and control processes and best practices. Not surprisingly, the embedded nature of the internal audit function within organizations naturally positions IT to exert a pervasive impact on the internal audit function.[46]

The chapter draws upon two monographs: *Research Opportunities in Internal Auditing* (ROIA) from The IIA Research Foundation, and *Researching Accounting as an Information Systems Discipline* (RAISD) from the American Accounting Association, to surface various researchable IT issues in the context of internal auditing. However, we caution researchers to first recognize and understand the differences between internal auditors and external auditors. This chapter has attempted to highlight some of these differences and how they affect the use of IT by the internal audit function as well as shape the internal audit function's contribution to the organization.

In closing, we must concede that the opportunities for carrying out research on IT and internal auditing are even richer than we contemplated initially. The Internet revolution, in conjunction with sweeping corporate governance reform legislation, will exert a tremendous impact on how internal auditing evolves as a profession. This is yet largely uncharted territory that promises to become a fertile ground furnishing an abundance of research possibilities for academics and reflective practitioners to make seminal contributions. We hope that the list of questions summarized in the Appendix will stimulate much theoretical and applied research that would be of interest to the academic and practicing arms of the internal auditing profession.

X. Tables and Figures

Table 1
ROIA and RAISD Table of Contents

Chapter	ROIA (2003)	RAISD (2002)
Editorial Preface	Monograph introduction by the co-editors, A.D. Bailey, A.A. Gramling, and S. Ramamoorti	Monograph introduction by the co-editors, V. Arnold and S.G. Sutton
1	Internal Auditing: History, Evolution, and Prospects (by S. Ramamoorti)	Foundations and Frameworks for AIS Research (by S.G. Sutton and V. Arnold)
2	Internal Audit and Organizational Governance (by D.R. Hermanson and L.E. Rittenberg)	Ontological Issues in Accounting Information Systems (by R.A. Weber)
3	The Internal Audit Function: An Integral Part of Organizational Governance (by T.F. Ruud)	Design Science: An REA Perspective on the Future of AIS (by J.S. David, G.J. Gerard, and W.E. McCarthy)
4	Assurance and Consulting Services (by U. Anderson)	Expert Systems in Accounting Research: A Design Science Perspective (by S.A. Leech and A. Sangster)
5	Auditing Risk Assessment and Risk Management Processes (by W.R. Kinney)	The Participation of Accountants in All Aspects of AIS (by J.E. Hunton)
6	Managing the Internal Audit Function (by D.F. Prawitt)	Behavioral Decision Aid Research: Decision Aid Use and Effects (by J.M. Rose)
7	Independence and Objectivity: A Framework for Research Opportunities in Internal Auditing (by J.F. Mutchler)	Group Support Systems Research in Accounting: A Theory-Based Framework and Directions for Future Research (by U.S. Murthy)
8	Internal Auditing's Systematic, Disciplined Process (by W.M. Lemon and K.W. Tatum)	Empirical Research in Semantically Modeled Accounting Systems (by C.L. Dunn and S.V. Grabski)
9	—	Ethics Research in AIS (by J.F. Dillard and K. Yuthas)
10	—	Research Opportunities in Electronic Commerce (by G.L. Gray and R. Debreceny)
11	—	Information Systems Assurance (by J.E. Boritz)
12	—	Concepts in Continuous Assurance (by M.A. Vasarhelyi)
13	—	Knowledge Management in Accounting and Professional Services (by D.E. O'Leary)

Table 2
Top Information Technology Issues in 2003

IIA Advanced Technology Committee's Top 10 Technology Issues in December 2003

1. Legislation and Regulatory Compliance
2. Threat and Vulnerability Management (application exploits, DDOS, IM, SPAM, Viruses, Trojans, Worms)
3. Privacy (including identity theft)
4. Continuous Monitoring/Auditing/Assurance
5. Wireless Security
6. Intrusion Protection (including firewalls, monitoring, analysis, reaction)
7. IT Outsourcing (including offshore)
8. Enterprise Security Metrics (dashboards, scorecards, analytics)
9. Identity Management
10. Acquisitions and Divestitures

IIA Strategic Directive #2 Top 30 IT Issues in March 2003

1. Intrusion protection
2. Physical and logical security
3. Web site management and security
4. Web-enabled systems
5. Computer networks
6. Privacy
7. Internal control assessments
8. Authentication
9. Contingency planning
10. E-commerce
11. Wireless communications
12. Continuous monitoring
13. Data encryption
14. File interrogation systems
15. Data theft
16. Automated internal control tools
17. Automated risk analysis tools
18. Document and electronic imaging
19. Distributed databases
20. Enterprise Resource Planning (ERP)
21. Automated audit planning tools
22. Human Resources Information System (HRIS)
23. E-mail and instant messaging
24. Executive decision support systems
25. Portable computing
26. Computer forensics
27. Architecture hardening
28. Customer Relationship Management (CRM)
29. Automated performance management systems
30. Groupware and collaborative computing

Table 3
Evolution of IT and the Internal Audit Function

Time Frame	IT Developments	Internal Audit Function Developments	Evolution of IT Audit
Mid-1950s	Computer begins processing business applications using punched cards.	(Internal) auditors "audit around the computer."	1st generation EDP Audit: Compliance
1960s	Tape drives replace punched cards. Generalized Audit Software emerges.	Sampling applications explored. Primitive "Auditing through the computer" approach emerges. Test decks used to test computerized systems. Internal audit functions begin to perform operational audits.	
1970s	25 proprietary GAS packages. ACL created. Multitude of tests created to test computerized systems.	IIA issues the influential *Systems Auditability and Control (SAC)* reports.	
1980s	Personal computer (PC) is born. IDEA software created for PC.	(Internal) auditors continue to slowly experiment with IT.	2nd generation IS Audit: Control frameworks
1990s	Enterprise Resource Planning (ERP) systems proliferate. Internet use soars. Inter-enterprise integration key to success (CRM, SCM). Ethical hacking commences.	Internal auditors continue to adapt GAS and expand role within organizations. Rate of IT adoption intensifies with the emergence of the Internet.	3rd generation IT Audit: Risk/Control

Table 3 (Cont.)
Evolution of IT and the Internal Audit Function

Time Frame	IT Developments	Internal Audit Function Developments	Evolution of IT Audit
1990s	Privacy laws enacted: HIPPA, COPPA, GLBA, Identity Theft and Assumption Deterrence Act.	Industry knowledge, regulatory compliance, and IT specialization become important.	COBIT framework released.
2000s	Internet and global communications technology revolutionize business; computer forensics surges ahead.	Internal audit focus on supporting Sarbanes-Oxley Sec. 302 (CEO/CFO certification), Sec. 404 (internal controls management assessment/ auditor/attestation), and Sec. 409 (real-time reporting by issuers).	4th generation IT Audit: Risk management process. IT Governance. Institute guidance. COSO ERM framework.

Table 4
Boritz's Features of IT that Change Risks, Control, and Needed Assurances of Organizations

Features of IT	Impact on Risk/Control/Assurance
Speed of processing enables processing of huge volumes of data.	Errors are magnified, potentially engulfing correction processes.
Real-time processing of transactions eliminates time buffer for error checking/ correction.	Errors affect business activities in progress. Systems no longer controllable by people; instead, require monitoring by systems themselves.
Consistency of performance promises steady operation of system processes.	Good news for well-tested processes; bad news for processes with flaws.
Relative inflexibility	Barrier to remedial action when problems are discovered. It is much easier and cheaper to design quality in rather than retrofitting later.
Shift from mainframes to small computers used alone, or increasingly, as part of networks devoted to information sharing and cooperative computing.	Corresponding changes in the nature, organization, and location of key information system activity, such as the shift to end-user computing. Risk and control points proliferate and require new assessment approaches.
Widespread availability of powerful yet inexpensive computer hardware and powerful, inexpensive, and relatively user-friendly software with graphical user interfaces.	Personnel with limited software training and IT skills have access to potentially powerful tools. This creates both control opportunities and risks.

Table 4 (Cont.)
Boritz's Features of IT that Change Risks, Control, and Needed Assurances of Organizations

Features of IT	Impact on Risk/Control/Assurance
Widespread incorporation, through miniaturization, of powerful computing capabilities in numerous devices designed for personal and professional use.	Significant processes can be embedded in small devices that may not give any visible clues about their system access, data storage, and processing capabilities.
Shift from custom-tailored systems to prepackaged software for both personal use and for enterprise-wide systems such as Enterprise Resource Planning Packages (ERP) and Customer Relationship Management (CRM) systems.	Entities rely on external suppliers for support and enhancement. Emphasis on controls over contracts and monitoring of supplier performance against contracts.
Continuing development of intelligent support systems incorporating expert systems, neural networks, intelligent agents, and other problem-solving aids.	Increases embedding of significant decision making within software. Emphasis on controls over software development, implementation, and maintenance.
New data capture and mass storage technologies.	Increases computerization of data/ information in text, graphic, audio, and video formats. Emphasizes managing, presenting and communicating information using multimedia approaches. Requires new techniques to access and analyze information.
Increasing availability of computerized data for access in real or delayed time both locally and through remote access facilities, including via the Internet.	More access points require logical as well as physical access controls.

Table 4 (Cont.)
Boritz's Features of IT that Change Risks, Control, and Needed Assurances of Organizations

Features of IT	Impact on Risk/Control/Assurance
Vulnerability of storage media.	Creates need for environmental and physical and logical access controls.
Convergence of information and communication technologies.	Affects how people work and shop. Breaks down familiar classifications of processes. Enables digitization of analog data, making it more available for processing and analysis.
Concentration of IS components such as infrastructure, software, data, and personnel functions and knowledge.	Reduces number of control points to be considered. Creates vulnerability to unauthorized access and abuse, as well as accidental destruction.
Distribution of IA components such as infrastructure, software, data, and personnel functions and knowledge.	Creates potential inconsistencies, version control problems, and multiple access control points to be considered. Creates coordination difficulties and vulnerability to loss of control or variation in level of controls.
Mass marketing and distribution of IT products and services such as computers, prepackaged software, online data retrieval services, electronic mail, and financial services.	Creates widely dispersed system users and developers with limited knowledge about controls.

Table 4 (Cont.)
Boritz's Features of IT that Change Risks, Control, and Needed Assurances of Organizations

Features of IT	Impact on Risk/Control/Assurance
Reduction of barriers to systems use, encouraging wider penetration of information systems into profit-oriented and not-for-profit organizations of all sizes for accounting and broader management and strategic purposes and increasing the role of end-user computing.	Creates risks of penetration by hackers and viruses and risks of significant system errors in a context of limited controls due to limited end-user knowledge about controls.
Increasing use of the Internet for conducting commerce between organizations and individuals and between organizations and other organizations through electronic commerce systems such as electronic data interchange (EDI) and electronic funds transfer systems (EFTS).	Magnifies business risks stemming from control weaknesses and other vulnerabilities.
Integration of subsystems through networks and data sharing; i.e., increasing use of networks to link individuals, intra-organizational units and inter-organizational units through systems such as electronic mail (e-mail) and the World Wide Web via the Internet.	Makes it possible for errors and malicious code such as viruses to propagate rapidly through connected systems. Creates control interdependencies among linked units.
Ease of access to data and software through remote access.	Creates vulnerability to intrusion by hackers and viruses.

Table 4 (Cont.)
Boritz's Features of IT that Change Risks, Control, and Needed Assurances of Organizations

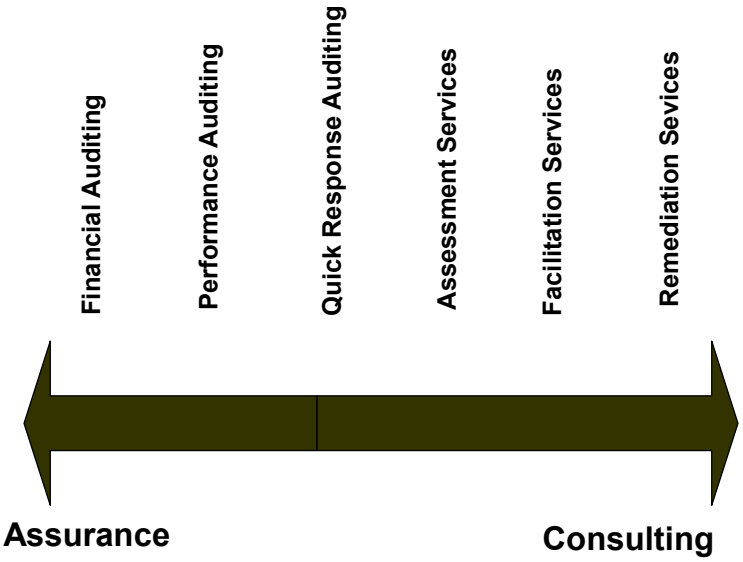
Features of IT	Impact on Risk/Control/Assurance
Indirect access to assets via access to data and software.	Creates need for access control over users' data access privileges and functional capabilities.
Reduction or absence of input documents.	Reduces or eliminates part of the audit trail that, ideally, should permit tracing of summary/aggregate amounts to individual source items.
Lack of visible output or visible audit trail.	Requires use of computer-assisted audit techniques and the proficiency to use them effectively.
Single transaction update of multiple databases.	Creates a difficult audit trail to trace errors to their sources and to correct all errors caused by a single transaction.
Automated accounting procedures and system-generated transactions based on programmed decisions.	Removes control and accountability from humans. Enables use of programmed controls designed to monitor system processes that are too fast, too complex, and too automated to be effectively monitored by humans, as noted earlier in connection with speed.
Interdependence of user controls and programmed procedures and controls.	The information used by users to control systems is itself produced by those systems.

Table 4 (Cont.)
Boritz's Features of IT that Change Risks, Control, and Needed Assurances of Organizations

Features of IT	Impact on Risk/Control/Assurance
Wider penetration of information technologies such as computer-assisted design and computer-assisted manufacturing (CAD/CAM), computer imaging systems, executive information systems (EIS), and electronic meeting systems (EMS).	Creates business dependence on IT and new risk and control implications, requiring continuous training.
Dependence on IT for competitive advantage.	Magnifies the potential consequences of unaddressed IS risks.
Interdependence of IT strategy and business strategy.	Requires joint decision making about business and IT issues and creates risk if IT and business strategies are not integrated.
Abdication of responsibility for IT control by senior management.	Magnifies the potential likelihood of unaddressed IS risks.
New system development techniques based around information technologies such as computer-assisted software engineering (CASE), object-oriented programming, and workflow technologies.	Requires continuous training to understand inherent risks.
New business reengineering approaches based on effective integration of information technologies and business processes.	Requires blending of IT and business skills more than ever before.

Reproduced from RAISD (2002) with permission from the American Accounting Association.

Figure 1
Assurance/Consulting Continuum



Reproduced from the ROIA monograph (Anderson, ROIA, Exhibit 4-4, p. 107) with permission from The IIA Research Foundation.

APPENDIX
SUMMARY OF RESEARCH QUESTIONS

Section II: Historical Perspective on Information Technology and the Internal Audit Function
Research Questions

- Given the historical reluctance to embrace IT, what are some ways to increase the rate of adoption of new IT audit techniques by internal auditors?

- Which of the IT audit applications described in this section deserved to be adopted? What are the differences, similarities, and objectives of each IT audit application?

- Which IT audit application is the best method to achieve efficiency, effectiveness, and/or a given objective? How do internal and external factors affect the choice of the appropriate IT audit application?

- What internal and external factors drive the adoption of IT by the internal audit function (e.g., organization's commitment to IT, IT's role in the organization's strategy, risk associated with the firm's IT)?

- What is the appropriate level of technological knowledge for EDP/IT auditors and non-EDP/IT auditors? How can internal auditor technology skills be enhanced?

- What internal and external factors drive the level of technological knowledge of EDP/IT auditors and non-EDP/IT auditors (e.g., size of the internal audit function, organization's commitment to IT, IT's role in the organization)?

- What is the most effective mix of EDP/IT and non-EDP/IT auditors in an internal audit department? What are the internal and external factors that should drive the mix of EDP/IT and non-EDP/IT auditors in an internal audit department?

- Does participation in systems development compromise the independence of internal auditors?

- ❖ How does the rate of adoption of new IT by internal auditors compare to that of external auditors? Have internal and external auditors adapted to the impact of IT at the same rate (and time frame)? If not, why not?

- ❖ Over the years, which internal auditor (and/or external auditor) technology applications have endured? Why — ease of use, inexpensive, scope of application, mission critical nature? What trends appear to be emerging about future IT applications? By internal auditors? By external auditors?

Section III: Corporate Governance
Research Questions

- Under what circumstances could IT automatically provide assurance on risk and controls to outside parties (e.g., SAS 70 reports)? Can IT automatically generate reports about the effectiveness of corporate governance processes tailored to meet stakeholders' specific needs?

- What are the impacts of XBRL on the organization and on external reporting? How can IT best streamline external reporting?

- What are the economic benefits of implementing "integrated" IT governance? What is the best way to keep stakeholders informed about the progress of IT projects?

- What are the key ways in which, by appropriately leveraging IT, internal audit can most effectively promote and support organizational governance?

- ❖ Under what circumstances would it be beneficial for internal auditors to work with external auditors to increase total audit coverage? Can a conceptual model be developed to indicate the appropriate level of total audit coverage?

- ❖ How can IT best enhance total audit coverage (between internal and external auditors)? Is there a trade-off between the desire to reduce combined audit costs against the goal of achieving enhanced overall audit effectiveness?

- ❖ Can internal auditors provide assurance about their organization's IS using criteria similar to AICPA's *Systrust*? Would stakeholders accept an internal auditor's assurance (e.g., for SAS 70 reports)? Is it possible to develop a conceptual model indicating the conditions under which different parties benefit from internal audit assurance?

Section IV: Assurance and Consulting Services
Research Questions

- How much more effective are audits using CAATTs? Does using CAATTs enhance the credibility of the audit function? How are/should constructs such as effectiveness and credibility (be) defined and measured in such studies?

- What is the return on investment for internal auditing from using CAATTs?

- What array of IT tools is available for specific tasks such as risk assessment, fraud detection, and compliance activities?

- Given the plethora of IT tools available, how should internal auditors match tools to tasks? Do variables, such as user sophistication, task complexity, speed, cost, familiarity, or software brand/reputation, matter in technology choice decisions?

- How does the role/position of the internal audit function affect IT (i.e., CAATTs) used for auditing purposes in the organization?

- How does internal auditor and external auditor use of CAATTs differ?

- Do auditors employ additional judgment and critical thinking when they use CAATTs? Do they gain a better understanding of the data and organization?

Section V: Risk Assessment and Management
Research Questions

- How does IT affect risk, risk assessment, and risk management? (Kinney, ROIA, 2003, p. 147) How can IT best help organizations establish, monitor, and proactively change their ERM activities?

- How can the impact of IT on enterprise risk be accurately measured? How can emerging technologies be identified and their risk measured?

- What are the IT implications for each component of the ERM proposed framework?

- How can IT help communicate risk assessments and responses to stakeholders? Can the message be tailored to fit the needs of the stakeholder?

- What data is needed in an audit data warehouse to monitor and measure risk?
- What are some industry best practices in assessing (technology) risk?
- What is the risk of not converting from legacy technologies? How can the forfeited efficiency gains be measured?
- How does participation by the internal auditor in the entire systems life cycle affect the organization's risk associated with IT? (Hunton, RAISD, 2002, p. 97)
- What role should IT play in identifying (new) risks and assessing the effect of that risk? How does the use of IT in the organization affect the (internal) audit risk model?
- What is the impact of different internal and external factors on the organization's use of IT in risk assessment?
- How can the net effect of IT be assessed (risk vs. opportunity)?

✜ Do internal and external auditors evaluate IT-based controls using the same techniques? How can these controls be effectively audited?

✜ What is the best way to use IT to identify effective controls? Monitor controls and evaluate risks? Identify inefficient business processes?

✜ How do IT risk assessments differ between internal auditors and external auditors? Do the time horizons and number of risk scenarios used by internal auditors and external auditors differ?

Section VI: Managing the Internal Audit Function
Research Questions

- What is the appropriate IT skill set for internal auditors? What must non-IT auditors who are subject matter specialists, know about IT?
- What kind of additional cognitive demands (including possible "disorientation") do electronic hypertext systems (EHS) place on internal auditors when they navigate

through electronic workpapers? If this feeling of being "lost in space" is validated, does it adversely affect internal audit (review) performance? What are some ways of mitigating or even eliminating such effects?

- How much does IT increase the efficiency and effectiveness of the internal audit function? What are the appropriate metrics to measure the improvement?

- What is the best combination of IT tools to improve the efficiency and effectiveness of the internal audit function?

- How do different internal auditing environments (e.g., size, dispersion, nationality, organizational structure, reporting structure, culture, number of IT auditors) influence the net benefits from IT deployment? Does IT provide more benefits under certain circumstances than others?

- What is the best way to equip internal auditors to use IT to improve the efficiency and effectiveness of the internal audit function?

- What is the best way to use IT to teach internal auditors new skills? Under what circumstances (task, learning preferences) is IT the best way to teach new skills?

- Under what circumstances should the internal audit function outsource IT audit? What are the costs and benefits of outsourcing IT audit? In similar vein, what are the costs and benefits of "off-shoring" IT audit work?

- How do the required IT skills of internal auditors and external auditors differ? How do internal and external factors affect the needed skills?

- How does the use of groupware differ between internal auditors and external auditors?

Section VII: Ethics, Privacy, and Security
Research Questions

- What metrics can the internal audit function use to assess the effectiveness of the organization's privacy and security provisions?

- How do internal and external factors change the metrics used by the internal audit function to quantify the effectiveness of the organization's privacy and security provisions?

- What are some appropriate metrics to measure the impact of a privacy or security breach? What is the best method to determine the financial impact of computerized system intrusion?

- How can the internal audit function help management understand the importance of monitoring unauthorized access to computer systems?

- What is the appropriate level of in-house knowledge of computer forensic techniques?

- What is the best way to monitor a business partner's security policies and procedures? What metrics should be used to evaluate inter-organizational security?

- How effective is ethical hacking? Should the internal audit function permanently employ an ethical hacker?

- Should ethical hacking be done by EDP/IT internal auditors or by someone specializing in penetration/vulnerability testing?

- For a given set of internal and external factors, what is the best disaster recovery plan? How can the effectiveness of a disaster recovery plan be evaluated prior to a disaster?

✜ Do internal auditors' and external auditors' risk assessments of information privacy and security differ? If so, in what respects and why?

Section VIII: Internal Auditing's Systematic, Disciplined Process Research Questions

- What should be the internal auditors' role in designing, implementing, and monitoring KMS? How do different internal and external factors affect that role?

- Do internal auditors specializing in IT/EDP have different cognitive biases than other internal auditors?

- Do internal auditors specializing in IT/EDP use IT decision aids differently than other internal auditors? Are IT decision aids more effective for IT/EDP internal auditors?

- How can internal auditors select the best decision aid for a specific task? Which decision aids are best for a given task?

- Do internal auditors and external auditors have the same cognitive biases? Are internal auditors and external auditors exposed to the same amount of information overload? How does internal auditor and external auditor use of decision aids and KMS differ?

- How effective are decision aids in improving the efficiency and effectiveness of internal auditors and external auditors?

- What are the best decision aids to help internal auditors and external auditors? How do internal and external factors affect the selection?

- What are some threshold criteria and best practices for information that should be captured in KMS?

Footnotes

[1]The ROIA monograph identifies and discusses research questions for a wide range of topics related to internal auditing, such as the profession's history and evolution, organizational governance, assurance and consulting services, risk assessment and management, independence and objectivity, and the systematic, disciplined process characterizing the methodology of internal auditing.

[2]Following Davis and Hamilton (1993, p. 1), we note that the terms information technology (IT) and information systems (IS) are often used somewhat interchangeably. IT encompasses the use of technology in products or services, but in the context of business systems. IS includes people, data, and procedures as well as technology. The integration of IS with advances in IT have allowed for the seamless flow of information we see in global organizations today (CICA, 2003).

[3]We are indebted to Professor Dan Stone of the University of Kentucky for pointing this out and for encouraging us to undertake the preparation of this ROIA supplemental chapter.

[4]The RAISD monograph covers a wide variety of information technology (IT) topics, including the Resources-Events-Agents (REA) paradigm, expert systems, artificial intelligence, decision aids, group support systems, ethics, e-commerce, information systems assurance, continuous assurance, and knowledge management — highlighting the enormous breadth of topics encompassed by accounting information systems (AIS) research.

[5]This section borrows heavily from Hafner (1964) and Wasserman (1968) in painting a historical perspective.

[6]"Auditing around the computer" was done without direct auditor involvement in the processing within the computer and included such techniques as observation of controls, system walk-through, documentation review, transaction tracing, and manual review and reconciliation of processing results (Yarnall, 1981).

[7]In this regard, the passage of the Sarbanes-Oxley Act of 2002 and the recent New York Stock Exchange Rule 303A requirement that every publicly listed company have an internal audit function will likely raise the profile of internal auditing and give it even greater prominence (see Ramamoorti, ROIA, 2003, pp. 14-15).

[8]Operational controls are implemented through and by people, while technical controls are implemented through and by IT and include hardware and software access control mechanisms, encryption, and monitoring for information, systems, programs, and operational configurations.

[9]Information Technology Governance Institute (ITGI) guidance document authors Fox and Zonneveld (2003) note that "organizations will need representation from IT on their Sarbanes-Oxley teams to ensure that IT general controls and application controls exist and support the objectives of the compliance effort…[including] mapping the IT systems that support internal control and the financial reporting process to the financial statements and ensuring that IT controls are updated and changed — as necessary — to correspond with changes in internal control or financial reporting processes." This will likely require close interaction between the chief audit executive (CAE) and the chief information officer (CIO).

[10]In specific circumstances, the organization's general counsel, as well as executives in charge of risk management, ethics, and compliance functions, may also need to be involved in such governance efforts.

[11]The use of state transition, activity, and interaction diagrams was mentioned on the AECM listserv by Dr. Jagdish S. Gangolly, an associate professor at State University of New York at Albany.

[12]However, it is conceivable at some point in the future that reconciliation among these partially overlapping frameworks will become necessary.

[13]Using software from a single vendor is referred to as instance consolidation. Multiple ERP systems make it more difficult for global organizations to scale up, build, and operate in different jurisdictions. Moreover, the divergence of multiple ERP systems over time could potentially present additional risks.

[14]The benefits and risks from deploying XBRL are also mentioned in subsequent sections of this chapter.

[15]This section borrows heavily from Coderre (2001a).

[16]Consider how electronic funds transfer point of sale (or EFTPOS, which draw money directly from a checking account) has revolutionized the operations of most large supermarket chains and other retail stores as seen daily at customer checkout counters.

[17]CAATTs include the following software: word processing, text search and retrieval, reference libraries, spreadsheets, presentation, utility, flowcharting, software licensing checkers, GAS, electronic questionnaires, control self assessment, data warehouse, expert systems, and data mining as well as a variety of audit management, administration, and security analysis software (Coderre, 2001a; CICA, 1999a).

[18]Vasarhelyi (RAISD, 2002) provides a discussion of continuous auditing from an external auditing perspective. However, many of the premises are applicable to internal auditing as well.

[19]For a good discussion of agents see Nehmer (2003) and Gray and Debreceny (RAISD, 2002).

[20]The two leading GAS packages used by internal auditors are ACL and IDEA (McCollum and Salierno, 2003). However, the majority of users (51 percent) are still relying on general-purpose Microsoft applications such as Excel for spreadsheets and Access for databases.

[21]Neural network technology can also assist with the detection of fraud (see Ramamoorti and Traver, 1998).

[22]Lanza (2003) provides an abbreviated list of tests for fraud and the appropriate CAATTS in his FEAR NOT TABLE (p. 33 and 42). In addition, the full document can be downloaded at www.theiia.org/ecm/iiarf.cfm?doc_id=4248.

[23]For an in-depth discussion of Benford's Law see Nigrini (2000).

[24]See David and Steinbart (2000) as well as Berry and Linoff (1997) for more in-depth discussions of data warehousing and data mining.

[25]The feedback period for comments on the July 2003 COSO ERM exposure draft ended on October 14, 2003. COSO expects to release the final ERM framework in summer 2004.

[26]In the external auditing domain, AICPA professional standards require external auditors to consider IT as part of overall internal control, to understand the design of controls, and to formally evaluate their effectiveness as an integral part of the financial statement audit (SAS 55, SAS 78, SAS 88, SAS 94). This has been further reinforced by Section 404 of the Sarbanes-Oxley Act of 2002, and the recently proposed PCAOB standard no. 2 (March 2004).

[27]RAISD (Gray and Debreceny, RAISD, 2002, p. 210) identify the four different stages of e-commerce as brochure ware, order entry, intranet, and extranet.

[28]Parker (2001, p. 86) provides a list of the 10 most common security holes on Web sites.

[29]A survey of corporate directors found similar results — 45 percent of participating organizations do not have formal methods for identifying risks and 19 percent did not know if their companies had risk identifying processes (Brune, 2003).

[30]Unless otherwise identified, the discussion in this section expands the ideas presented in the July 2003 exposure draft of the COSO *ERM Framework*.

[31]A multitiered data warehousing architecture has the following major components: (1) source systems, where the data comes from, (2) data transport and cleansing, which move the data between different data stores, (3) the central repository, the main store for the date warehouse, (4) the metadata, which describes what is available and where, (5) data marts, which provide fast, specialized access for end users and applications, (6) operational feedback, which integrates decision support back into the operational systems, and (7) end users, who are the reason for developing the warehouse in the first place (Berry and Linoff, 1997).

[32]See McNamee and Selim (1998) for a detailed description of scenarios analysis and risk matrices.

[33]XBRL should help proliferate the number of industry databases available.

[34]Internal auditors may also be able to use *data envelopment analysis (DEA)* to assess risk. Bradbury and Rouse (2002) describe DEA for external audit risk assessment, while Sherman (1984) described the use of DEA in operational audits.

[35]Salamasick and Le Grand (2003, p. 22-24) provide a detailed description of the gaps in traditional insurance coverage, while Parker (2001, p. 49) provides a list of needed insurance products for organizations engaging in e-commerce.

[36]Le Grand (2001, pp. 60-68) describes 16 software packages for risk management.

[37]Le Grand (2001) provides a complete list and in-depth discussion of tools and vendors that can be used in audit management and administration.

[38]See Fjermestad and Hiltz (2001) and Fjermestad (1998) for a review of extant group support system research.

[39]Huberty (2000) provides a description of how Cargill uses groupware (specifically Auditor Assistant and Lotus Notes) to improve the efficiency and effectiveness of the internal audit function.

[40]The ROIA chapter on independence and objectivity (ROIA, Mutchler, 2003, pp. 231-268) discusses several mitigating factors alleviating threats to objectivity and objectivity management tools for internal auditors using a comprehensive conceptual framework (see Section VII for a discussion).

[41]While HIPAA does not require these measures, health-care organizations may choose to implement them to ensure the security and privacy of their systems.

[42]Betts (2000) and Clark (2003) provide detail descriptions of different types of denial-of-service (DOS) attacks.

[43]Rohrmann (1986) broadly defines a decision aid as: "any explicit procedure for the generation, evaluation, and selection of alternative (courses of action) that is designed for practical application and multiple use. In other words, a [decision aid] is a ***technology*** not a theory" (emphasis added).

[44]This section presents a summary of the information presented in Table 1, p. 215, of Messier (1995).

[45]Expert systems do not include neural networks or other emerging and hybrid technologies such as neuro-fuzzy or genetic-neural applications. Artificial intelligence applications to the business domain are only now becoming popular (Ramamoorti and Traver, 1998).

[46]In cosourcing and outsourcing arrangements, it is extremely important that IT platforms, methodologies, tools, and techniques be compatible with those used in the organization itself.

Primary Sources

ROIA: *Research Opportunities in Internal Auditing*. The Institute of Internal Auditors Research Foundation monograph co-edited by Andrew D. Bailey, Audrey A. Gramling and Sridhar Ramamoorti. Individual chapters written by several authors.
Referenced as: [Author name(s), ROIA, 2003]

RAISD: *Researching Accounting as an Information Systems Discipline*. American Accounting Association monograph co-edited by Vicky Arnold and Steve G. Sutton, 2002. Individual chapters written by several authors.
Referenced as: [Author name(s), RAISD, 2002]

References

Adams, D.L., and J.F. Mullarkey, "A Survey of Audit Software," *Journal of Accountancy*, September 1972, pp. 39-67.

American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (AICPA/CICA), *Continuous Auditing* (Toronto, Ontario: The Canadian Institute of Chartered Accountants, 1999).

Anderson, U., "Assurance and Consulting Services," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Angwin, J., M. Peers, and A.M. Squeo, "Disney, Struggling to Regain Glory, Gets $48.7 Billion Bid from Comcast; Driving Force Behind Offer: Technology Tears Up Old Business Models; Rocky History of Mergers," *The Wall Street Journal*, February 12, 2004, p. A1.

Anonymous, "How Coach Works," *Internal Auditor*, June 1996, pp. 32-34.

Anonymous, "Market Dynamics: Sarbanes-Oxley – Financial Storm in an IT Teacup?," *Business Intelligence Market Watch*, June 19, 2003, pp. 2-10.

Arnold, V., and S.G. Sutton (eds.), *Researching Accounting as an Information Systems Discipline* (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Arnold, V., and S.G. Sutton, "Foundations and Frameworks for AIS Research," *Researching Accounting as an Information Systems Discipline* edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Association of Certified Fraud Examiners (ACFE), *Report to the Nation 2002* (Austin, TX). Retrieved online on December 1, 2003 from: http://www.cfenet.com/publications/RttN.asp.

Bailey, A.D., Jr., A.A. Gramling, and S. Ramamoorti (eds.), *Research Opportunities in Internal Auditing* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Bell, T., F. Marrs, I. Solomon, and H. Thomas, *Auditing Organizations Through a Strategic-Systems Lens: The KPMG Business Measurement Process* (KPMG Peat Marwick LLP, 1997).

Benbasat, I., and B.R. Nault, "An Evaluation of Empirical Research in Managerial Support Systems," *Decision Support Systems* (6), 1990, pp. 203-226.

Berry, M.J.A., and G. Linoff, *Data Mining Techniques for Marketing, Sales, and Customer Support* (New York: John Wiley & Sons, 1997).

Betts, W., "Defying Denial of Service Attacks," *Network Magazine*, December 2000, pp. 52-56.

Bible, L., L.E. Graham, and A. Rosman, "The Effect of Electronic Audit Environments on Performance," forthcoming in the *Journal of Accounting, Auditing and Finance*, 2004.

Bierstaker, J.L., P. Burnaby, and S. Hass, "Recent Changes in Internal Auditors' Use of Technology," *Internal Auditing*, July/August 2003, pp. 39-45.

Bigler, M., "Computer Forensics," *Internal Auditor*, February 2000, pp. 53-55.

Bigler, M., "Computer Forensics Gear," *Internal Auditor*, August 2001, pp. 27-31.

Bishop, W.G. III, "Technology: Changing the Rules for Business Controls and Internal Auditing," *Business Credit*, November/December 1997.

Bishop, W.G. III, D.R. Hermanson, P.D. Lapides, and L.E. Rittenberg, "The Year of the Audit Committee," *Internal Auditor*, April 2000, pp. 47-51.

Boritz, J.E., "Information Systems Assurance," *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Boritz, J.E., and W.G. No, "Assurance Reporting for XBRL: XARL (eXtensible Assurance Reporting Language)," *Trust and Data Assurances in Capital Markets: The Role of Technology Solutions* edited by S.J. Roohani (Smithfield, RI: PricewaterhouseCoopers: 2003).

Bou-Raad, G., and C. Capitanio, "The Implications of Computer Hacking on the Internal Audit Function: A Banking Industry Study," *Internal Auditing*, May/June 1999, pp. 36-41.

Bradbury, M.E., and P. Rouse, "An Application of Data Envelopment Analysis to the Evaluation of Audit Risk," *ABACUS*, June 2002, pp. 263-279.

Brune, C., "Internal Auditing Critical to Governance," *Internal Auditor*, June 2003, p. 19.

Bryan, L., and D. Farrell, *Market Unbound: Unleashing Global Capitalism* (New York: John Wiley & Sons, 1996).

Canadian Institute of Chartered Accountants (CICA), *The Impact of Technology on Financial and Business Reporting* (Toronto, Ontario: The Canadian Institute of Chartered Accountants, 1999).

Canadian Institute of Chartered Accountants (CICA), *Audit & Control Implications of XBRL* (Toronto, Ontario: The Canadian Institute of Chartered Accountants, 2002).

Canadian Institute of Chartered Accountants (CICA), *Using Ethical Hacking Technique to Assess Information Security Risk* (Toronto, Ontario: The Canadian Institute of Chartered Accountants, 2003a).

Canadian Institute of Chartered Accountants (CICA), *Electronic Audit Evidence* (Toronto, Ontario: The Canadian Institute of Chartered Accountants, 2003b).

Cash, J.I., A.D. Bailey, Jr., and A.B. Whinston, "A Survey of Techniques for Auditing EDP-Based Accounting Information Systems," *The Accounting Review*, October 1977, pp. 813-832.

Cerebit, "Enterprise Application Security," Technical White Paper 2003, Retrieved online on November 7, 2003, from http://www.cerebit.com/download/Cerebit-EnterpriseApplicationSecurity.pdf.

Chou, D.C., and B. Lin, "Development of Web-Based Knowledge Management Systems," *Human Systems Management* 12(3), 2002, pp. 153-159.

Clark, E., "Lesson 182: Distributed Denial of Service Attacks," *Network Magazine*, September 2003.

Coderre, D.G., *CAATTS and other BEASTS* (Vancouver, Canada: ACL Institute, 2001a).

Coderre, D.G., *Fraud Toolkit for ACL* (Vancouver, Canada: ACL Services, 2001b).

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management*: 2003. Retrieved online on October 24, 2003, from: www.coso.org

Computer Security Institute, *Eighth Annual CSI/FBI Computer Crime and Security Survey*. 2003. Retrieved online on November 7, 2003, from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

Cravens, K., E.G. Oliver, and S. Ramamoorti, "The Reputation Index: Measuring and Managing Corporate Reputation," *European Management Journal*, 21(2), 2003, pp. 201-212.

Cuaresma, J.C., "The Gramm-Leach-Bliley Act," *Berkeley Technology Law Journal* (17), 2002, pp. 497-517.

D'Amico, K.L., and B.A. Adamec, "Coach," *Internal Auditor*, June 1996, pp. 30-37.

David, J.S., G.J. Gerard, and W.E. McCarthy, "Design Science: An REA Perspective on the Future of AIS," *Researching Accounting as an Information Systems Discipline* edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

David, J.S., and P.J. Steinbart, *Data Warehousing and Data Mining: Opportunities for Internal Auditors* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2000).

Davenport, T.H., and L. Prusak, *Working Knowledge: How Organizations Manage What They Know* (Boston, MA: Harvard Business School Press, 1998).

Davis, G.B., and S. Hamilton, *Managing Information: How Information Systems Impact Organizational Strategy* (Homewood, IL: Business One Irwin, 1993).

Dillard, J.F., and K. Yuthas, "Ethics Research in AIS," *Researching Accounting as an Information Systems Discipline* edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Driscoll, M., and J.E. Reid, Jr., "Web-Based Training: An Overview of Training Tools for the Technical Writing Industry," *Technical Communication Quarterly*, Winter 1999, pp. 73-87.

Elliott, R.K., "Confronting the Future: Choices for the Attest Function," *Accounting Horizons*, September 1994, pp. 106-124.

Felix, W.L., A.A. Gramling, and M.J. Maletta, *Coordinating Total Audit Coverage: The Relationship Between Internal and External Auditors* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1998).

Fjermestad, J., "An Integrated Framework for Group Support Systems," *Journal of Organizational Computing and Electronic Commerce* 8(2), 1998, pp. 83-107.

Fjermestad, J., and S.R. Hiltz, "Group Support Systems: A Descriptive Evaluation of Case and Field Studies," *Journal of Management Information Systems*, Winter 2000-2001, pp. 115-159.

Fox, C., and P. Zonneveld, *IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation, and Sustainability of Internal Control Over Disclosure and Financial Reporting* (Guidance document: Information Technology Governance Institute, ITGI, 2003).

Friedlob, G.T., F.J. Plewa, L.L.F. Schleifer, and C.D. Schou, *An Auditor's Guide to Encryption* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1997).

Garg, A., J. Curtis, and H. Halper, "The Financial Impact of IT Security Breaches: What Do Investors Think?, *Information Systems Security*, March/April 2003, pp. 22-32.

Gilbert, A., "Security Beyond Your Borders," *Informationweek.com*, November 5, 2001, pp. 39-48.

Glover, S.M., and M. Romney, "20 Hot Trends," *Internal Auditor*, August 1997, pp. 28-36.

Gray, G. L., and R. Debreceny, "Research Opportunities in Electronic Commerce," *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Hafner, G.H., "Auditing E.D.P.," *The Accounting Review* 39(4), 1964, pp. 979-983.

Hargraves, K., S.B. Lione, K.L. Shackelford, and P.C. Tilton, *Privacy: Assessing the Risk* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Hendrey, D., "IT Audit Renewal," *Internal Auditor*, April 1999, pp. 36-40.

Hermanson, D.R., M.C. Hill, and D.M Ivancevich, "Information Technology-Related Activities of Internal Auditors," *Journal of Information Systems* (Supplement), 2000, pp. 39-53.

Hermanson, D.R., and L.E. Rittenberg, "Internal Audit and Organizational Governance," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Huber, N., "Business Scandals Put IT on the Spot," *Computer Weekly*, September 2002, p. 16.

Hunton, J.E., "The Participation of Accountants in All Aspects of AIS," *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Husted, B., "Hacker May Sit in Next Cubicle," *Atlanta Journal-Constitution*, May 14, 2003.

Hylas, R.E., and R.H. Ashton, "Audit Detection of Financial Statement Errors," *The Accounting Review*, October 1982, pp. 751-766.

Institute of Internal Auditors (IIA), *Percent Audit Staff IT/IS Auditors – All Insurance Companies* (2000, http://www.gain2.org/itis.html).

Institute of Internal Auditors (IIA), *Continuous Monitoring* (2002a, http://www.gain2.org/cmsum.htm).

Institute of Internal Auditors (IIA), *eSAC Technology Survey* (2002b, http://www.gain2.org/esacsum.htm).

Joyce, J., "Distributed Denial of Service Attacks," *Scientific Computing & Instrumentation*, June 2002, pp. 12, 47.

King, C.G., "Protecting Online Privacy," *The CPA Journal*, November 2001, pp. 66-67.

Kinney, W.R., "Auditing Risk Assessment and Risk Management Processes," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Krass, P., "A More Perfect Union?," *CFO*, July 2003, p. 25-26.

Kulik, C.C., and J.A. Kulik, "Effectiveness of Computer-based Instruction: An Updated Analysis," *Computers in Human Behavior* (7), 1991, pp. 75-94.

Lanza, R.B., "Fear Not the Software: Proactively Detecting Occupational Fraud Using Computer Audit Reports," *The White Paper*, September/October 2003, pp. 31-33, 41-42.

Le Grand, C., *Information Technology in Auditing* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2001).

Leithhead, B.S., and D. McNamee, "Assessing Organizational Risk," *Internal Auditor*, June 2000, pp. 68-69.

Lemon, W.M., and K.W. Tatum, "Internal Auditing's Systematic, Disciplined Process," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Marcella, A.J., and R.S. Greenfield (eds.) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crime* (Boca Raton, FL: Auerbach Publications, CRC Press LLC, 2002).

Mason, R., "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), 1986, pp. 5-12.

McCarthy, W.E., "The REA Accounting Model: A Generalized Framework for Accounting Systems in a Shared Data Environment," *The Accounting Review* 57 (3), 1982, pp. 554-578.

McCollum, T., and D. Salierno, "Choosing the Right Tools," *Internal Auditor*, August 2003, pp. 32-43.

McGowan, W.G., "Information Age Technology—The Competitive Advantage," *Views from the Top: Establishing the Foundation for the Future of Business*," edited by J. M. Rosow (New York, NY: Facts on File Publications, 1985).

McNamee, D., and G.M. Selim, *Risk Management: Changing the Internal Auditor's Paradigm* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1998).

Messier, W.F., "Research in and Development of Audit Decision Aids," *Judgment and Decision-Making Research in Accounting and Auditing*, edited by R.H. Ashton and A.H. Ashton (New York, NY: Cambridge University Press, 1995).

Murthy, U.S., "Group Support Systems Research in Accounting: A Theory-Based Framework and Directions for Future Research," *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Mutchler, J.F., "Independence and Objectivity: A Framework for Research Opportunities in Internal Auditing," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Narayanaswamy, K., "ISPs and Denial of Service Attacks," *Information Systems Security*, May/June 2002, pp. 38-46.

Nehmer, R., "Transaction Agents in eCommerce, A Generalized Framework," *Trust and Data Assurances in Capital Markets: The Role of Technology Solutions*, edited by S. J. Roohani (Smithfield, RI: PricewaterhouseCoopers, 2003).

Nigrini, M.J., *Digital Analysis Using Benford's Law* (Vancouver, BC: Global Audit Publications, 2000).

O'Leary, D.E., "Knowledge Management in Accounting and Professional Services," *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Ozier, W., "Risk Metrics Needed for IT Security," *ITAudit*, April 1, 2003.

Palmer, C.C., "Ethical Hacking," *IBM Systems Journal* (40:3), 2001, pp. 769-780.

Parker, X.L., *An e-Risk Primer* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2001).

Peat, Marwick, Mitchell & Co., *Research Opportunities in Auditing*, 1st ed. (New York, NY: Peat, Marwick, and Mitchell & Co., 1976).

Prawitt, D.F., "Managing the Internal Audit Function," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Prawitt, D.F., and M.B. Romney, "Super Software," *Internal Auditor*, August 1996, pp. 16-25.

PricewaterhouseCoopers, *Technology Forecast: 2003-2005* (Menlo Park, CA: PricewaterhouseCoopers, 2003).

Ramamoorti, S., "Internal Auditing: History, Evolution and Prospects," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Ramamoorti, S., and Traver, R.O., *Using Neural Networks for Risk Assessment in Internal Auditing: A Feasibility Study* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1998).

Reilly, R.F., and J.A. Lee, "Developing In-House EDP Auditing Capabilities," *Management Review*, April 1981, pp. 57-63.

Rezaee, Z., A. Sharbatoghlie, R. Elam, and P.L. McMickle, "Continuous Auditing: Building Automated Auditing Capability," *Auditing: A Journal of Practice & Theory*, March 2002, pp. 147-163.

Rittenberg, L.E., and G.B. Davis, "The Roles of Internal and External Auditors in Auditing EDP Systems," *The Journal of Accountancy*, December 1977, pp. 51-58.

Rohrmann, B., "Evaluating the Usefulness of Decision Aids: A Methodological Perspective," *New Directions in Research and Decision Making*, edited by B. Brehmer, H. Jungermann, P. Lourens, and G. Sevon (Amsterdam, The Netherlands: North Holland Publishing Company, 1986).

Rose, J.M., "Behavioral Decision Aid Research: Decision Aid Use and Effects," *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Rosenoer, J., D. Armstrong, and J.R. Gates, *The Clickable Corporation: Successful Strategies for Capturing the Internet Advantage* (New York, NY: Arthur Andersen LLP, 1999).

Ruud, T.F., "The Internal Audit Function: An Integral Part of Organizational Governance," *Research Opportunities in Internal Auditing*, edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

Salmasick, M., and W. Fraczkwski, "Using Groupware for Audit Automation," *Internal Auditor*, April 1995, pp. 18-22.

Salamasick, M., and C. Le Grand, *PC Management Best Practices: A Survey of the Total Cost of Operations, Risk, Security, and Audit* (Altamonte Springs, FL: The Institute of Internal Auditors, 2003).

Sandler, I.J., "Plain Talk about Auditing in an ADPS Environment," *Journal of Accountancy*, April 1968, pp. 43-48.

Schwartz, E., "Think Outside the SarbOx," WWW.INFOWORLD.COM, April 2003, p. 16.

Searcy, D.L., and J.B. Woodroof, "Continuous Auditing: Leveraging Technology," *The CPA Journal*, May 2003, pp. 46-48.

Sherman, H.D., "Data Envelopment Analysis as a New Managerial Audit Methodology-Test and Evaluation," *Auditing: A Journal of Practice and Theory*, Fall 1984, pp. 35-53.

Sodano, L., and J. Hagerty, *Prioritizing IT Investments for Sarbanes-Oxley Compliance* (AMR Research: 2003).

Spinello, R., "Privacy Rights in the Information Economy," *Business Ethics Quarterly*, October 4, 1998, pp. 723-763.

Sutton, S.G., T.D. Arnold, and V. Arnold, "An Integrative Framework for Analysis of the Ethical Issues Surrounding Information Technology Integration by the Audit Profession," *Research on Accounting Ethics* (5), 1999, pp. 21-36.

Tillinghast-Towers Perrin, *Enterprise Risk Management: Trends and Emerging Practices* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2001).

Vasarhelyi, M.A., "Concepts in Continuous Assurance," *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Verton, D., "Let the Pros Investigate," *Computerworld* (36:29), 2002, pp. 34-36.

Vowler, J., "Make Sure IT's Risk Factor is Built into Governance," *Computer Weekly*, February 13, 2003, p. 28.

Wasserman, J.J., "New Approached to EDP Problems: Auditing the Computer," *Management Review*, July/August 1968, pp. 40-44.

Wasserman, J.J., "Bridging the Computer-Auditor Gap," *Banking*, December 1969, pp. 83-85.

Weber, R., "XML, XBRL, and the Future of Business and Business Reporting," *Trust and Data Assurances in Capital Markets: The Role of Technology Solutions*, edited by S. J. Roohani (Smithfield, RI: PricewaterhouseCoopers LLP: 2003).

Will, H.J., "ACL: Audit Command Language," *NFOR* 13(1), 1975, pp. 99-111.

Will, H.J., "The New CAATS: Shifting the Paradigm," *EDPACS*, May 1995, pp. 1-14.

Williams, P., "Directors Can't Hide Behind IGNORANCE," *Computer Weekly*, November 28, 2002, p. 36.

Williams, P., "Directors Must Take IT Responsibilities on Board," *Computer Weekly*, February 13, 2003, p. 30.

Yarnall, K.F., "Auditing in an EDP Environment," *Handbook of Accounting and Auditing* edited by J. C. Burton, R.E. Palmer, and R.S. Kay (Boston, MA: Warren Gorham & Lamont, 1981).

Glossary of Selected Information Technology Terms (initial usage within chapter indicated using *italics and underscoring*)

ACL (Audit Command Language) – Generalized audit software used by internal and external auditors to extract and analyze data.

Algorithm – Step-by-step procedure (using logic or mathematics) to correctly solve a problem.

Catastrophe modeling – Computer models that estimate losses from potential disasters.

Committee of Sponsoring Organizations (COSO) of the Treadway Commission (cf. Report of National Commission on Fraudulent Financial Reporting, 1987) – COSO consists of five member organizations, viz., American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), The Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA), and Financial Executives International (FEI). COSO's *Internal Control - Integrated Framework*, first released in 1992, is a control and governance framework for processes and management supervisory activities to ensure efficiency and effectiveness of operations, the reliability of financial reporting, and compliance with laws and regulations. The COSO framework includes five components, viz., control environment, risk assessment, control activities, information and communication, and monitoring. COSO's efforts to formulate an Enterprise Risk Management (ERM) framework, is sometimes referred to as COSO II. The final COSO II ERM document is expected to be released in Summer 2004. For more information, see **www.coso.org**

Concurrent processing – Computer code designed to detect exception or unusual conditions as data are processed.

Control Objectives for Information Technology (CobiT) – The Information Systems Audit and Control Association's (ISACA) internal control framework that defines standards for good IT practices for control over information, IT, and related risks. The framework focuses on the perimeter network, internal network, systems, and application and databases.

Controlled processing (reprocessing) – Auditor reprocesses the data, using a system that the auditor has already verified and tested, to verify and validate the accuracy of the financial statements.

Data envelopment analysis (DEA) – Linear programming-based technique that combines multiple input and output measures into a single measure of productive efficiency.

Economic scenario generation – Models that generate some economic value or capital market value predictions into the future by factoring in assumptions that reflect real world behavior.

Electronic data interchange (EDI) – The exchange of transactional information between organizations using computers.

Electronic funds transfer (EFT) – The transfer of funds between organizations using computers; EFTPOS refers to EFT occurring at the point-of-sale.

eXtensible Business Reporting Language (XBRL) – Implementation of Extensible Markup Language (XML) designed specifically for financial and business reporting.

eXtensible Markup Language (XML) – Language defining tags (or codes) that can be attached to text to identify the meaning of the text.

Financial data interchange (FEDI) – Combines EDI and EFT, simultaneously exchanging funds and transactional data.

Flowchart verification – Analyzing the program logic with flowcharts.

IDEA (Interactive Data Extraction and Analysis) – Generalized audit software used by internal and external auditors to extract and analyze data.

Integrated test facility – System testing by creating a dummy division or company and entering test data into the live system.

ISO 17799 – A control framework that focuses on the internal network and provides technical standards to help establish security controls on the IT processing environment and infrastructure.

Mapping – Techniques to identify logical paths in a process and determine whether all paths are used.

Monte Carlo simulation – Computer simulation with a built-in random process, allowing one to see the probabilities of different possible outcomes.

Optimization software – Software that uses simulation to design a system (or make a decision) that yields optimal expected performance by examining various combinations of input factors.

Parallel simulation – An independent program written to simulate a live program, run on the same source data, and with the resulting output compared to output of live system.

Pro forma financial modeling – Software to help generate forecast and budget financial statements.

Probabilistic or stochastic simulation – Using probability distributions to generate sample distributions that are used to study stochastic behavior observed in a system.

Program code checking – A line-by-line analysis of computer code.

Risk matrix – A matrix with risk on the horizontal axis and system components or audit steps on the left axis; the matrix is sorted to produce high, medium, and low quadrants (see McNamee, 1998, for more information).

Risk/frequency/severity mapping – Graph summarizing the risks facing the organization (frequency vs. severity), to help management with strategic decision making.

Sample audit review file (SARF) – Randomly selects transactions for audit review.

Scenario planning – Identifying trends and projecting them into the future (see McNamee and Selim, 1998, for more information).

Spoofing – Creating an exact replica of a Web page to trick a person into giving personal information.

State transition, activity, and interaction diagrams – State diagrams describe the behavior of a single object; activity diagrams describe processes capturing parallel activities and their synchronization; interaction diagrams describe behavior involving several objects.

System control audit review file (SCARF) – Uses reasonableness tests to identify exception transactions.

Systrust – The AICPA's assurance framework: an assurance service provided by external auditors that an organization's system meets defined standards of availability, security, integrity, and maintainability.

Tagging and tracing – Selected records are tagged in an extra field so that they can be easily identified during the audit.

War dialing – A computer hacking technique that uses a software program to automatically call thousands of telephone numbers to find modems.

Zombie(s) computer – A hidden software program that allows the computer to be controlled remotely

Acknowledgments: We gratefully acknowledge the financial support, reference materials, and chapter review arrangements made available by The IIA Research Foundation. We wish to thank Andy Bailey, Russ Gates, Audrey Gramling, Bonnie Klamm, Charles Le Grand, Sara Peterson, Larry Rittenberg, Mark Salamasick, Dan Stone, and Dick Traver for their suggestions and comments on earlier versions of this supplemental ROIA chapter.