JOURNAL OF INFORMAITON SYSTEMS
Vol. 20, No. 1
Spring 2006
pp. 205–219

Research Opportunities in Information Technology and Internal Auditing

Marcia L. Weidenmier
Mississippi State University

Sridhar Ramamoorti
Grant Thornton LLP

ABSTRACT: This paper presents research opportunities in the area of information technology (IT) within the context of the internal audit function. Given the pervasive use of IT in organizations and the new requirements of the Sarbanes-Oxley Act of 2002, internal audit functions must use appropriate technology to increase their efficiency and effectiveness. We develop IT and internal audit research questions for three governance-related activities performed by the internal audit function-risk assessment, control assurance, and compliance assessment of security and privacy.

Keywords: IT/IS auditing; internal auditing; information technology; research opportunities; Sarbanes-Oxley; corporate governance; risk management; security; privacy.

Data Availability: Please direct all comments and suggestions to Dr. Marcia Weidenmier.

I. INTRODUCTION

This paper develops information technology-related research questions within the context of the internal audit function. The internal audit function (IAF) is one of the cornerstones of corporate governance along with the external auditor, executive management, and the audit committee of the Board of Directors (Gramling et al. 2004). The Board of Directors determines the overall governance process, which senior management implements and internal and external auditors evaluate, under the watchful eye of the audit committee (Blue Ribbon Committee 1999; Treadway Commission 1987).

The IAF occupies a unique and pivotal role in corporate governance. First, the IAF is an information gathering and reporting resource for the three other governance parties (Gramling et al. 2004). Second, the IAF is an integral part of the organization's internal control structure. In fact, Rule 303A of the New York Stock Exchange requires listed companies to have an IAF. Third, the IAF executes important governance-related activities including risk assessment, control assurance, and compliance assessment, which are critical

We thank JIS editor Dan Stone for suggesting and encouraging us to write the supplemental technology chapter to the *Research Opportunities in Internal Auditing* (2003) monograph. We remain grateful to the IIA Research Foundation for granting us permission to reproduce, paraphrase, and/or use copyrighted materials in preparing this paper for the *Journal of Information Systems.* (Copyright 2004, *The Pervasive Impact of Information Technology on Internal Auditing,* by the Institute of Internal Auditors Research Foundation, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201 U.S.A. Reprinted with permission.) The views expressed in this paper are the personal views of Dr. Sridhar Ramamoorti and do not reflect the views of, nor endorsement by, Grant Thornton LLP.

in complying with the new requirements of the Sarbanes-Oxley Act of 2002 (SOX). Internal auditors are central figures and function as a key support in providing assurance for meeting the requirements of SOX Section 302 (annual certifications of the completeness and accuracy of the financials by the CEO and the CFO) and Section 404 (external auditor attestation of the effectiveness of internal controls over financial reporting). As an integral part of corporate governance, internal auditors must now consider the "probability of significant errors, irregularities, or noncompliance" (Implementation Standard 1220.A1 [IIA 2004]) as they execute their governance-related activities.

As IT and business models become virtually inseparable and inextricably intertwined, IT is playing a pivotal role in corporate governance and SOX compliance. IT both enables and drives effective governance structures, risk management, and control processes because it (1) shapes an organization by influencing the governance structure selection and the organization's level of risk (Boritz 2002; Parker 2001), (2) helps establish, maintain, and enforce new governance processes throughout the organization (Hamaker 2004; Fox and Zonneveld 2004), and (3) helps integrate the risk management and compliance processes—improving reputation, employee retention, and revenue (by as much as 8 percent), and lowering costs of capital and insurance premiums (PricewaterhouseCoopers 2004).

IT's rapid change is dramatically altering the IAF (Gorman and Hargadon 2005). Accordingly, the Institute of Internal Auditors (IIA) requires internal auditors to understand how IT is used and should be used in an organization, as well as key IT risks, controls, and IT-based audit techniques (Implementation Standard 1210.A3 [IIA 2004]). Thus, given the new requirements of SOX and the IIA, both the IAF and IT have risen in prominence and impact within organizations.

In this new era of governance reform, "IT-internal auditing research" has become a critical imperative. Surprisingly, however, "while the role of assurance practitioners, from an external perspective, has often been publicly discussed and debated, the role of the internal auditor and the resulting changes have not been quite so publicized" (Boritz 2002, 232). Significant prospects exist for academic research in the areas of internal auditing and technology from theoretical and practical perspectives. To help encourage research on IT and the IAF, we develop research questions for three governance-related activities performed by the IAF: risk assessment, control assurance, and compliance work (Hermanson and Rittenberg 2003).

Our research builds on the following studies, which provide comprehensive syntheses of extant literature. Almost 30 years ago, Cash et al. (1977) reviewed existing studies and techniques on auditing and electronic data processing (EDP) (primarily from an external audit perspective) to encourage future EDP research. More recently, O'Leary (2000) discusses the enterprise resource planning systems (ERPs) literature. The Information Systems Section of the American Accounting Association published *Researching Accounting as an Information Systems Discipline* (Arnold and Sutton 2002), which presents research opportunities in a variety of areas including expert and group support systems, decision aids, electronic commerce, continuous and information systems assurance, and knowledge management. Finally, Ramamoorti and Weidenmier (2004) develop IT-related research opportunities in internal auditing for eight different areas, as part of the *Research Opportunities in Internal Auditing* (Bailey et al. 2003) monograph published by the IIA Research Foundation. We use the chapter by Ramamoorti and Weidenmier (2004) as our starting point.

The remainder of the paper develops IT-related research questions for each governance activity performed by the IAF. Section II focuses on risk assessment. Section III explores control assurance, while Section IV discusses two primary areas of compliance assessment—security and privacy. Section V concludes.

II. RISK ASSESSMENT

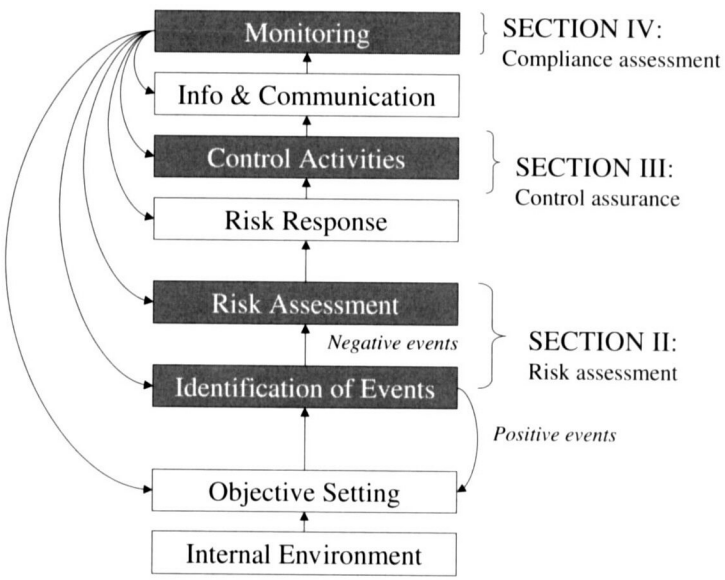
Traditionally, internal auditing used a control-based approach for planning its activities. More recently, corporate governance focuses on risk management, providing the impetus for the IAF to move to a risk-based approach (McNamee and Selim 1998). In fact, the IAF, in the context of organizational risk assessment (Ramamoorti and Traver 1998), must identify and assess risks to define the audit universe and to plan its engagements (IIA Performance Standard 2010.A1). Unfortunately, organizations struggle with enterprise-wide risk management and "conflicting evidence exists regarding what [enterprise risk management] means and how common[ly] it actually is" implemented (Kleffner 2003, 66). Moreover, a lack of risk management frameworks, qualitative and quantitative risk metrics, and accessible central repository of actuarial data has hampered risk management efforts (Ozier 2003). To help overcome some of these obstacles, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released the 2004 *Enterprise Risk Management (ERM) Framework* that encompasses and expands its 1992 *Internal Control-Integrated Framework*. The *ERM Framework* presents an integrated framework with practical implementation guidelines to ensure achievement of organizational objectives, reliable reporting, and regulatory compliance.

IT and the IAF are both integral components of ERM. The Board's corporate governance process directs senior management's development and implementation of the risk management process, which the IAF must evaluate for "adequacy and effectiveness" as well as for "significant risks that might affect objectives, operations, or resources" (Sobel and Reding 2004; Implementation Standards 1220.A1 and 1220.A3 [IIA 2004]). IT also permeates the risk management process as a source of risk and as a tool to implement the following eight components of the *ERM Framework*: internal environment, objective setting, identification of events, risk assessment, risk response, control activities, information and communication, and monitoring (Ramamoorti and Weidenmier 2004). While research opportunities exist for each *Framework* component, we focus only on the third and fourth components, identification of events and risk assessment, which we consider to be the pinnacle of the *ERM Framework*. To help the reader understand the context of our research questions, Figure 1 presents an overview of the *Framework* and its relationship to this paper. In addition, we now briefly describe how the other *ERM Framework* components relate to risk assessment and IT.

The first two *ERM Framework* components, the internal environment and objective setting, shape the organization's risk assessment process. The internal environment reflects the organization's risk appetite, or how much risk that management and the Board are willing to accept when conducting business, and is the basis for all other *Framework* components. Objective setting ensures that the organization has a process to define high-level strategic objectives as well as detailed operational, reporting, and compliance objectives that are consistent with its mission and risk appetite. Based on their strategic objectives, organizations must identify and assess the risk of events, which are internal or external incidents that may negatively affect strategy and the achievement of objectives.

The last four *ERM Framework* components—risk response, control activities, information and communication, and monitoring—delineate the organization's response to the assessed risk. Organizations can avoid, minimize, share, reduce, or accept the assessed risk via their response to identified risks. Control activities ensure that risk responses are implemented via controls that support strategic, operational, reporting, and compliance objectives. An information and communication system must identify, analyze, and respond to new and existing risks as well as communicate needed information across the organization.

FIGURE 1
The Enterprise Risk Management Framework and its Relationship to this Paper



The Enterprise Risk Management Components are from COSO (2004a).

Moreover, in today's rapidly changing business environment, the ERM plan requires continuous monitoring that is real-time, dynamic, and embedded in the organization (COSO 2004a, 75) to ensure that the ERM plan evolves to effectively manage the organization's risk.

IT is intricately intertwined with the components of the *ERM Framework* affecting how the organization manages risk. For example, the organization's risk appetite affects its choice of IT, level of e-commerce, integration with business partners, and the use of emerging technologies—all changing the risk of the organization. While strategic objectives influence the IT infrastructure, IT can simultaneously help (1) shape strategy, (2) use operational assets efficiently and effectively, (3) increase reporting reliability and regulatory compliance, (4) communicate information globally, and (5) ensure that the organization is operating within established risk tolerances, the acceptable level of variation around objectives (PricewaterhouseCoopers 2003; Tillinghast-Towers Perrin 2001; Leithhead and McNamee 2000).

Keeping this framework in mind, we turn to the third and fourth components of the *ERM Framework*—the identification of events and risk assessment. Negative events are risks that must be assessed. Positive events are opportunities that may redirect the organization's objective setting process. The *Framework* identifies IT as an external event and an internal event. In fact, IT is the only item classified as both types of events. For external events, organizations must consider the impact of the changing e-commerce environment, the increasing availability of external data, potential technological interruptions, and emerging technology (COSO 2004a, 47). For internal events, organizations must consider how data integrity, data and system availability, and system selection, development, deployment,

and maintenance may affect their ability to operate (COSO 2004a, 46). IT also enables the organization to identify other events. As an enabler, IT can help internal auditors facilitate interactive group workshops, pinpoint areas of concern via escalation or threshold triggers, and identify trends and causes of risks by statistically analyzing historical data via data mining and data warehouses (Nehmer 2003; Searcy and Woodroof 2003; Rezaee et al. 2002).

Once the negative events (i.e., risks) have been identified, organizations must estimate the likelihood and timing of the events occurring and their impact on the organization. To estimate the financial impact of different time horizons and probable outcomes, internal auditors can use a variety of simulation, mapping, benchmarking, and modeling tools. Data warehouses and data mining can estimate the likelihood an event will occur, thereby supplementing managers' qualitative estimates (Rezaee et al. 2002). Neural networks and data envelopment analysis (DEA) can also be used to assess risk, direct internal auditors' attention to high risk audit areas, and engage in "brainstorming" and "scenario building" activities that seek to track and monitor business risks as they develop (Kinney 2003, 149; Bradbury and Rouse 2002; Ramamoorti and Traver 1998). According to PricewaterhouseCoopers Internal Audit Services Practices, the IAF needs a level of IT sophistication that matches the level of risk that it is trying to manage (Heffes 2002); i.e., the concept of requisite variety applies to the IAF and the system it regulates (Weick 1969, 1979). While prior studies examine what tools the IAF uses (e.g., Hermanson et al. [2000]; annual IAF surveys by the *Internal Auditor*), we lack evidence regarding how well the risk identification and assessment tools used by the IAF match the organization's current and planned level of risk and IT usage.

Understanding the impact of IT on risk assessment is especially important for organizations with ERPs. O'Leary (2000) and Addison (2001) state that ERPs expose organizations to significantly different risks including business interruption, change management, process interdependency, privacy and confidentiality, data content quality, and system security. Moreover, newly implemented ERP processes potentially alter and even weaken traditional segregation of duties, because traditional controls are often eliminated and not replaced during implementation (Bae and Ashcroft 2004). Wright and Wright (2002) delineate additional risks associated with ERP implementations from customization, process reengineering, bolt-on software (i.e., software from a different vendor that adds functionality to an ERP), and incompatibilities with organizational requirements. Thus, ERPs may not reduce control risk if organizations modify key process linkages and integrated controls are not fully implemented.

In light of these concerns, internal auditors must examine ERP risk carefully. Given the large variety of ERPs available, how is risk affected if organizations implement primary (manufacturing) versus support (financial and human resource) software components? Does risk vary with the specific ERP software (vendor) selected or with internal audit involvement? How much risk exists if organizations do not convert from existing legacy systems to ERPs?

As a starting point in answering these questions, Wright and Wright (2002) report that then-Big 5 information systems auditors identify supply-chain and payroll ERP subsystems as having the highest control and security risks. Other areas of concern include interfaces with legacy systems and non-ERP bolt-ons. Interviewees also state that the major vendor ERPs differ in terms of access and encryption controls as well as input devices and controls. External information systems auditors also appear not to be concerned with the security and control risks of business intelligence systems (Wright and Wright 2002). To better understand how organizations manage and control ERP risks, future research can determine

how the IAF's perspectives compare to those of external auditors and whether internal auditors consider the risks of business intelligence systems and other areas that are apparently overlooked by external auditors (Wright and Wright 2002). Given that internal auditors work in the same organizational environment with the same system(s) all year, their depth-oriented viewpoints are likely to be different than the breadth-oriented viewpoints of external auditors who work on multiple clients (and systems). In addition, future research could examine the underlying software (O'Leary 2002) to understand how the actual risks match those perceived by internal and external auditors.

Kinney (2003, 147) asks, "How does IT affect risk, risk assessment, and risk management?" Answering this question requires a better understanding of the differential impact of internal and external factors on the organization's use of IT in risk assessment. For example, organizational structure and its use of IT may affect the ERM process. Kleffner (2003) identifies silo (or functional) organizational structure, resistance to change, lack of qualified personnel, and need for internal controls and review systems as deterrents to ERM. Similarly, Wah (2000) identifies traditional silo structure as among the top barriers to successful ERP implementations. Thus, organizational structure appears to affect the success of ERM and ERP implementations. It would be interesting to investigate whether firms that have successfully implemented ERP are more likely to successfully implement an ERM process.

Hunton (2002) suggests that internal auditors may be able to reduce the risk associated with the organization's IT by participating throughout the entire system's life cycle. Extant research also finds that the involvement of information system (IS) auditors in the systems development stage reduces future software maintenance costs (Wu 1992), indicating that risks (from software and control errors) should be reduced as well. Unfortunately, despite the potential to reduce future costs, internal auditors spend the least amount of their time on the development, acquisition, and implementation of new systems (Hermanson et al. 2000).

Why are internal auditors not more actively involved in the development, acquisition, and implementation of new systems? Prior research suggests that this is because of independence and objectivity concerns (Boritz 2002). However, extant literature (generally) finds that IAF quality depends more on work performance than independence, objectivity, and competence (Gramling et al. 2004). Moreover, Krishnamoorthy's (2001, 2002) analytical models suggest that the relative importance of objectivity, work performance, and competence varies with audit conditions. On the other hand, extant literature reports conflicting evidence regarding whether internal auditors' judgments and decisions are affected by prior design involvement (Grabski 1986; Gramling et al. 2004). Therefore, more research is needed to determine the net benefits of IAF participation in each stage of the system's life cycle.

Internal auditors, outsourced internal audit service providers, and external auditors make risk assessments. Inconsistent evidence exists regarding whether the risk assessments made by these various parties are the same. For example, Hunton et al. (2004) find that external then-Big 5, IT auditors assess higher risks in ERP than non-ERP systems when compared to external Big 5, non-IT auditors. However, Grabski et al. (1987) report no differences in the internal control evaluations of EDP and non-EDP internal auditors. Church and Schneider (1995) find that internal auditors are more likely to generate cutoff errors than external auditors, but Blocher (1993) finds that internal auditors are less likely to use analytical procedures compared with external auditors. Moreover, Caplan and Embry (2003) find that internal auditors, outsource providers, and external auditors make similar judgments about the severity of internal control weaknesses; where there are differences, the

evaluations of outsourced internal auditors tend to fall between internal and external auditors. On the other hand, in a study of the relative importance of risk factors for fraud, Apostolou et al. (2001) report that the mean decision models of Big 5, regional, and internal auditors are not significantly different.

In light of these mixed results, how do the overall risk assessments of internal, external, and outsourced (IT and non-IT) auditors compare? Extant research does not fully support the correlation between external auditor's risk assessments and audit plans (Zimbelman 1997; Mock and Wright 1999). Do internal auditors incorporate IT considerations into risk assessments *and* their subsequent audit plans (see Church et al. 2001)? The audit committee now expects the IAF to monitor, evaluate, and report recommendations for the organization's risk management process (COSO 2004b, 104). Given the growing importance of risk management, outsourcing opportunities, and the expanding role of the IAF, audit committees need answers to these questions.

III. CONTROL ASSURANCE

Control assurance is another important governance activity performed by internal auditors. To ensure that risk responses are implemented, audit committees rely on the IAF to determine if internal controls effectively support strategic, operational, reporting, and compliance objectives (Gendron et al. 2004). This task is critical because "a strong system of internal control is essential to effective ERM" (COSO 2004c, slide 22).

Traditionally, corporate governance was synonymous with organizational oversight by various committees, internal auditors, and external auditors. This was a costly, misleading, and disempowering approach because businesses did not make IT governance (risk and compliance) investments a high priority (Meyer 2004). An alternative, and better, approach makes compliance *integral*, not incremental, by embedding IT controls throughout the organization's business processes (PricewaterhouseCoopers 2004). Embedded controls ensure compliance at the time of the business process entry, making employees systematically follow governance directives, ultimately changing the organizational culture (Heffes 2004; Meyer 2004).

While corporate governance and ERM are rising into prominence, investors are increasingly IT-literate and sophisticated, now worrying about IT's risk to operations, and scrutinizing IT investments and system efficiency (Huber 2002). Together these forces drive the demand for a new type of governance, "IT governance," which coordinates IT with business objectives to establish effective IT controls efficiently (ITGI 2004). The relationship between IT and governance exhibits "reciprocal causation." In other words, they feed into, shape, and fuel the demand for each other (Hamaker 2004).

Organizations can also use IT—as an enabler—to help comply with SOX Sec. 404 requirements that external auditors attest to management's assessment of the effectiveness of internal controls relevant to financial reporting. In fact, PCAOB Auditing Standard No. 2 encourages the implementation of entirely IT automated application controls by allowing the external auditor to utilize a benchmarking (and audit efficiency-increasing) strategy when there are effective IT general controls. The PCAOB's rationale seems to be that entirely IT automated application controls are not subject to breakdowns resulting from human failure (e.g., error, complacency, distraction) and, once properly defined, should continue to perform effectively (PCAOB 2005). This new environment requires controls that are automatic, dynamic, integrated, preventive, multi-compensating, real-time, and include sound authentication procedures and secured audit trails (Parker 2001), which can only be accomplished through automated IT controls.

But, do controls implemented in organizations achieve these high standards? Despite the increased demand for IT controls, even the largest organizations still use manual controls for compliance processes—increasing the likelihood of compliance failures considerably (PricewaterhouseCoopers 2004) and leading to the question: Why do most companies still continue to use manual compliance controls? Is it because IT usage has generated significant operational problems (see ITGI 2004)? Or is IT implementation too costly? Perhaps senior management is still wary of utilizing IT for governance-related activities because they are unfamiliar with its deployment or unsure of its impact.

IT can automatically monitor control effectiveness and changes and automatically identify control weaknesses in ERPs. Organizations can also use IT for "corrective control" purposes to identify these gaps, e.g., control mapping with alarms and alerts (Alles et al. 2004) and segregation of duties analysis software (Lightle and Vallario 2003). How effective are these monitoring and corrective controls? Are there systematic differences (e.g., IT placement in organization, existence of integrated IT governance process, IAF characteristics) in the companies that use these IT controls versus those that do not?

SOX Sec. 404 requires that a control framework be used but does not specify which framework. Perhaps the most popular choice is the 1992 *Internal Control-Integrated Framework* by COSO. Despite its formal publication and release over a decade ago, many users are unfamiliar with the COSO framework, particularly as it interacts with IT applications. Few firms showed interest in COSO until SOX's passage (Alles et al. 2004; Hermanson 2000). Other potential control frameworks include CobiT (Information Systems Audit and Control Foundation, ISACA), e-SAC (IIA), CoCo (Canadian COSO) and SAS Nos. 55, 78, and 94 (AICPA Professional Standards). (See Hermanson et al. [2000]; Curtis and Wu [2000]; Colbert and Bowen [2005] for a comparison of the frameworks.)[1]

Because of the new SOX 404 disclosure requirements, researchers can more easily identify which control framework organizations use to evaluate their controls for initial (and subsequent) annual report filings. Promising research questions include: Are there systematic differences in the framework selection (i.e., industry, size, IAF characteristics, IT characteristics, external auditor, supply partner integration, or international presence)? Are there systematic control weaknesses in certain industries? How does an organization's Sec. 404 internal control opinion affect the overall audit opinion? Carcello et al. (2002) examine audit committee disclosures and state that future research can determine (1) whether companies with more complete disclosures have fewer internal control failures and (2) whether enhanced disclosures improve internal control effectiveness. The new SOX 404 internal control attestation report should help answer these two questions as well as other governance questions about the interactions among the audit committee, the external auditor, the IAF, management's assessment of the effectiveness of controls over financial reporting, and financial-reporting quality.

Obtaining better internal control effectiveness requires answers to the following questions: Which (COSO) control components are the strongest and weakest in organizations? How does the selected framework affect the (IT) audit? Are internal controls more effective when the organization has a well-developed ERM process? Moreover, PCAOB Auditing Standard No. 2 does not prescribe the scope or the required amount of testing of internal

[1] CobiT stands for Control Objectives for Information and Technology. eSAC is the electronic version of the IIA's Systems Auditability and Control guidance. CoCo stands for Criteria of Control developed by the Canadian Criteria of Control Board. SAS 55 is the AICPA's Statement of Auditing Standard No. 55 (SAS No. 55) titled *The Consideration of the Internal Control Structure in a Financial Statement Audit*. SAS No. 78 amends SAS No. 55. SAS No. 94 is titled *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*.

controls (Brady and Postal 2005). How much testing is needed to be effective? Research is needed to determine which method(s) might be best for evaluating controls, how much testing is needed to be effective, and whether SOX has changed the IAF's priorities and use of resources as well as how it views, evaluates, and monitors controls? Furthermore, a survey by ACL Services Ltd. and the Center for Continuous Auditing finds that 67 percent of organizations do not have a budget for continued compliance with SOX after the initial filing deadline, indicating a short-term compliance response (Anonymous 2004). Research is needed to determine the long-term effects and effectiveness of SOX and compliance by organizations.

Finally, large organizations (with over $5 billion in revenues) are spending approximately $4.36 million to comply with SOX Sec. 404, which requires management to assess the organization's internal controls *only over* financial reporting (Levinsohn 2005). Given the increased focus on sound corporate governance by SOX, internal auditors could reduce organizational risk by expanding the audit scope to include the entire underlying database.[2] In other words, "substance attestation" may shift to "process attestation" through continuous control monitoring techniques that focus on the process rather than the financial statement numbers generated (Pacini and Sinason 1999). Are internal auditors adjusting their audit procedures (appropriately) for increased IT usage and the audit of the entire operational database? What barriers, if any, exist?

IV. SECURITY AND PRIVACY COMPLIANCE ASSESSMENT

Internal controls also help ensure compliance with applicable laws and regulations (COSO 2004a, 109), an activity that becomes even more important in heavily regulated industries such as healthcare and financial services. Accordingly, yet another significant governance activity performed by internal auditors is compliance assessment. We develop research questions focusing on two increasingly important areas of compliance—privacy and security. Privacy and security have been identified as two of the "Ethical Issues of the Information Age" (Mason 1986; Sutton et al. 1999). They help ensure data integrity to support the governance and risk processes and must be part of the ERM process. IT acts as both a driver and enabler for compliance. As a driver, IT poses additional security and privacy risks of its own (e.g., cyber-security breaches, or unauthorized disclosure of confidential consumer information). As an enabler, IT can help mitigate these risks.

Personal privacy is eroding as IT enables organizations to collect, store, and ubiquitously retrieve more consumer information than ever before, e.g., using cookies, web bugs, and port scans (Spinello 1998; King 2001). IT increases the risk that information may be accidentally or maliciously compromised, through hacking or other forms of "cyber-terrorism." Given this environment, several laws have been passed to protect the privacy of consumers such as the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), the Identity Theft and Assumption Deterrence Act, and the Gramm-Leach-Bliley Act (GLBA). Noncompliance with these laws, as well as failure to protect other data, exposes the organization to potential lawsuits, financial losses, and loss of reputation (cf. Cravens et al. 2003).

International organizations that operate or trade in Europe must also contend with the 1995 European Union (E.U.) Data Protection Directive (Directive 95/46/EC) for the strict privacy of consumer information or personally identifiable information (PII). The E.U. will prevent noncomplying organizations from transferring paper and electronic customer data

[2] This discussion of database audits was inspired by Dr. Brad M. Tuttle's remarks on January 7, 2005, at the AAA Information Systems Section Midyear Meeting 2005.

from European to U.S. operations. To do business in Europe now, the U.S. Department of Commerce must certify that an organization complies with the U.S. Safe Harbor Privacy Principles (notice, choice, onward transfer, security, data integrity, access, and enforcement).[3]

Internal auditors can assess their organization's privacy measures via a privacy impact assessment (PIA). PIA is a generic framework for mapping data sources and uses to data privacy regulations (Kenny 2004). With this framework, internal auditors can assess the current state of privacy provisions and monitor future configuration changes. Internal auditors need to understand the laws, how they affect their organization, and how to mitigate the risk through proper IT security measures. Given the growing need for sound privacy measures, research is needed to better understand the privacy environment. Jamal et al. (2003, 2005) examine the privacy policies of high-traffic websites in the United States and heavily regulated United Kingdom and find that most organizations in both countries follow stated policies. They also state that compliance with U.K. disclosure requirements is poor, but regulations appear to reduce the use of cookies. Unfortunately, they do not have data on the substantive tests to verify compliance. This leaves unanswered the issue of how organizations assure compliance. Do internal auditors actively assess compliance with applicable privacy laws? Do websites with lower levels of traffic ensure compliance? Do different stakeholders in non-E.U. jurisdictions reward organizations that conform to the higher privacy standards of the E.U. Directive?

To help ensure privacy, organizations are implementing a variety of security measures to protect themselves from external *and* internal threats. In fact, information security has been the number one technology concern in the United States for the last three years (AICPA 2005). The importance of security is unsurprising given that more than ten new vulnerabilities are created each day (Cohen 2005). Furthermore, the importance of security is highlighted by the *ERM Framework* that states "[given the] growing reliance on information systems at the strategic and operational level" new security risks "such as information security breaches or cyber-crimes ... must be integrated into the entity's ERM" (COSO 2004a, 69).

Security includes considerations such as system confidentiality (restricting access to authorized users), and system integrity as well as ongoing system availability. Organizations must establish an enterprise-wide information security program that uses IT to enforce data protection rules (Hargraves et al. 2003). Organizations must also ensure that systems are not affected by viruses or worms that may unintentionally distribute personal information in violation of privacy laws (King 2001). Potential privacy and security IT tools include biometrics (Chandra and Calderon 2003), encryption (Friedlob et al. 1997), and attack simulation (Cohen 2005).

To prevent becoming victims of cyber-crimes, 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 2003). After a cyber-crime, computer forensics can preserve, identify, extract, and document computer evidence for use in a criminal or civil court of law (Marcella and Greenfield 2002). Properly trained internal auditors can utilize IT tools and knowledge to collect evidence from computers, networks, and the Internet to investigate acts that are illegal, unethical, or against organizational policy and involve a computer. The use of ethical hacking and computer forensics are in their infancy; therefore research should determine the appropriate level of in-house (and IAF)

[3] A list of companies that are Safe Harbor certified can be found at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

knowledge of computer forensic techniques. In addition, how effective and pervasive is ethical hacking? What is the most effective way for organizations to obtain forensics expertise—outsourcing, co-sourcing, or in-house?

The IAF must periodically assess security provisions. Particularly in the wake of Hurricane Katrina, a viable and tested disaster recovery plan must be in place to provide for operational continuity in the face of unforeseen disturbances. Internal auditors must understand how to mitigate security risk through proper IT security controls. Surprisingly, Ivancevich et al. (1998) find that the existence and size of the IAF is not associated with (perceived) disaster recovery plan strength. Additional research can help identify appropriate metrics for internal auditors to measure the impact of a privacy or security breach and improve disaster recovery plans. What is the best method to determine the financial impact of computerized system intrusion (cf. Garg et al. 2003)?

V. CONCLUSION

IT changes and the SOX corporate governance reform legislation continue to exert a tremendous impact on how internal auditing evolves as a profession. Despite these developments, research in IT and IAF is largely uncharted territory that promises to become fertile ground with an abundance of research possibilities. Our goal in this paper is not to be exhaustive but rather to stimulate IT-related research in internal auditing in the areas of risk assessment, control assurance, and security and privacy compliance. The IAF and IT are both integral components of these three areas.

IT plays the dual role as a driver and an enabler in all three areas. For example, regarding risk assessment, IT increases organizational risk. At the same time, IT can be a tool to implement the eight ERM components to mitigate risk. Regarding control assurance, IT's risk to operations drives the demand for IT governance, which coordinates IT with business objectives to establish effective IT controls by embedding controls into business processes. IT makes compliance integral, helping organizations comply with increasing regulatory requirements like SOX Sec. 404. Regarding security and privacy compliance, IT increases security and privacy risks because organizations store more information than ever before, which can be compromised in violation of privacy laws. Fortunately, IT can help mitigate these risks as well.

The IAF must not only understand the IT used by the organization, but it must also understand applicable regulatory and privacy laws—how the laws affect its organization, and how to use IT to ensure compliance. In addition, the IAF should use the appropriate level of IT sophistication to evaluate and monitor organizational risk, controls, and compliance (i.e., requisite variety). Moreover, understanding how the IAF should and does relate to IT will help improve the corporate governance process and the quality of financial reporting.

REFERENCES

Addison, S. 2001. Risk and governance issues for ERP enterprise applications. *IS Control Journal* (4): 53–54.

Alles, M., A. Kogan, and M. Vasarhelyi. 2004. The law of unintended consequences? Assessing the costs, benefits, and outcomes of the Sarbanes-Oxley Act. *IS Control Journal* (1): 17–21.

American Institute of Certified Public Accountants (AICPA). 2005. Information security tops technical issues for 2005. *AccountingWeb* (January 4). Available at: http://www.accountingweb.com/cgi-bin/item.cgi?id=100297.

Anonymous. 2004. Continuous monitoring, auditing needed for Sarbanes-Oxley. *Financial Executive* (September): 19.

Apostolou, B. A., J. M. Hassell, S. A. Webber, and G. E. Summers. 2001. The relative importance of management fraud risk factors. *Behavioral Research in Accounting* (May): 1–24.

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

Bae, B., and P. Ashcroft. 2004. Implementation of ERP systems: Accounting and auditing implications. *The Information Systems Control Journal* (4): 43–48.

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

Blocher, E. 1993. *The Role of Analytical Procedures in Detecting Management Fraud*. Montevale, NJ: Institute of Management Accountants.

Blue Ribbon Committee (BRC). 1999. *Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees*. Stamford, CT: BRC.

Boritz, J. E. 2002. Information systems assurance. In *Research Accounting as an Information Systems Discipline*, edited by V. Arnold, and S. G. Sutton. Sarasota, FL: American Accounting Association Information Systems Section.

Bradbury, M. E., and P. Rouse. 2002. An application of data envelopment analysis to the evaluation of audit risk. *ABACUS* (June): 263–279.

Brady, M., and A. D. Postal. 2005. Tweaking SOX: Regulators ease up on compliance cost. *National Underwriter Property & Casualty Risk & Benefits Management Edition* (May 23): 31–32.

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

Caplan, D., and C. Emby. 2003. An investigation of whether outsourcing the internal audit function affects internal controls. Working paper, Iowa State University and Simon Fraser University.

Carcello, J. V., D. R. Hermanson, and T. L Neal. 2002. Disclosures in audit committee charters and reports. *Accounting Horizons* (December): 291–304.

Cash, J. I., Jr., A. D. Bailey Jr., and A. B. Whinston. 1977. A survey of techniques for auditing EDP-based accounting information systems. *The Accounting Review* (October): 812–831.

Chandra, A., and T. G. Calderon. 2003. Toward a biometric security layer in accounting systems. *Journal of Information Systems* (Fall): 51–70.

Church, B. K., and A. Schneider. 1995. Internal auditors' memory for financial statement errors. *Behavioral Research in Accounting* 7: 17–36.

———, J. J. McMillan, and A. Schneider. 2001. Factors affecting internal auditors' consideration of fraudulent financial reporting during analytical procedures. *Auditing: A Journal of Practice & Theory* (March): 65–80.

Cohen, G. 2005. The role of attack simulation in auditing security risk management. *The Information Systems Control Journal* (1): 51–54.

Colbert, J. L., and P. L. Bowen. 2005. A comparison of internal controls. Available at: http://www.isaca.org/PrinterTemplate.cfm?Section=Home&CONTENTID=8174&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Committee of Sponsoring Organizations (COSO). 2004a. *Enterprise Risk Management-Integrated Framework: Executive Summary Framework*. Jersey City, NJ: AICPA.

———. 2004b. *Enterprise Risk Management-Integrated Framework: Application Techniques*. Jersey City, NJ: AICPA.

———. 2004c. Applying COSO's enterprise risk management-integrated framework. (September 29). Slideshow. Available at: http://www.coso.org/publications.htm.

Cravens, K., E. Oliver, and S. Ramamoorti. 2003. The reputation index: Measuring and managing corporate reputation. *European Management Journal* 21 (2): 201–212.

Curtis, M. B., and F. H. Wu. 2000. The components of a comprehensive framework of internal control. *The CPA Journal* (March): 64–66.

Fox, C., and P. Zonneveld. 2004. *IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation, and Sustainability of Internal Control over Disclosure and Financial Reporting*. Rolling Meadows, IL: Guidance document: Information Technology Governance Institute.

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

Garg, A., J. Curtis, and H. Halper. 2003. The financial impact of IT security breaches: What do investors think? *Information Systems Security* (March/April): 22–32.

Gendron, Y., J. Bedard, and M. Gosselin. 2004. Getting inside the black box: A field study of practices in "effective" audit committees. *Auditing: A Journal of Practice & Theory* (Spring): 153–171.

Gorman, J. F., and J. M. Hargadon. 2005. Accounting futures: Healthy markets for a time-honored profession. *Journal of Financial Service Professionals* (January): 74–79.

Grabski, S. V. 1986. Auditor participation in accounting systems design: Past involvement and future challenges. *Journal of Information Systems* (Fall): 3–23.

———, J. H. Reneau, and S. G. West. 1987. A comparison of judgment, skills, and prompting effects between auditors and system analysts. *MIS Quarterly* (June): 151–161.

Gramling, A. A., M. J. Maletta, A. Schneider, and B. K. Church. 2004. The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature* 23: 194–244.

Hamaker, S. 2004. Principles of IT governance. *The Information Systems Control Journal* 2: 47–50.

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

Heffes, E. M. 2002. PWC's 10 imperatives for internal audit transformation. *Financial Executive* (June): 61.

———. 2004. Is software the solution for Sarbanes-Oxley? *Financial Executive* (June): 19–20.

Hermanson, D., M. C. Hill, and D. M. Ivancevich. 2000. Information technology-related activities of internal auditors. *Journal of Information Systems* (Supplement): 39–53.

Hermanson, D. R., and L. E. Rittenberg. 2003. Internal audit and organizational governance. In *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.

Hermanson, H. M. 2000. An analysis of the demand for reporting on internal control. *Accounting Horizons* (September): 325–341.

Huber, N. 2002. Business scandals put IT on the spot. *Computer Weekly* (September): 16.

Hunton, J. E. 2002. The participation of accountants in all aspects of AIS. In *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S. G. Sutton. Sarasota, FL: American Accounting Association Information Systems Section.

———, A. M. Wright, and S. Wright. 2004. Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems* (Fall): 7–28.

Institute of Internal Auditors (IIA). 2004. *The Professional Practices Framework*. Altamonte Springs, FL: The Institute of Internal Auditors.

IT Governance Institute (ITGI). 2004. *IT Governance Global Status Report*. Rolling Meadows, IL: The IT Governance Institute.

Ivancevich, D. M., D. R. Hermanson, and L. M. Smith. 1998. The association of perceived disaster recovery plan strength with organizational characteristics. *Journal of information Systems* (Spring): 31–40.

Jamal, K., M. Maier, and S. Sunder. 2003. Privacy in e-commerce: Development of reporting standards, disclosure, and assurance services in an unregulated market. *Journal of Accounting Research* (May): 285–310.

———, ———, and S. Sunder. 2005. Enforced standards versus evolution by general acceptance: A comparative study of e-commerce privacy disclosure and practice in the United States and the United Kingdom. *Journal of Accounting Research* (March): 73–96.

Kenny, S. 2004. Assuring data privacy compliance. *The Information Systems Control Journal* 4: 31–33.

King, C. G. 2001. Protecting online privacy. *The CPA Journal* (November): 66–67.

Kinney, W. R. 2003. Auditing risk assessment and risk management processes. In *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.

Kleffner, A. E. 2003. The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management & Insurance Review* (Spring): 53–74.

Krishnamoorthy, G. 2001. A cascaded inference model for evaluation of the internal audit report. *Decision Sciences* (Summer): 499–520.

———. 2002. A multistage approach to external auditors' evaluation of the internal audit function. *Auditing: A Journal of Practice & Theory* (March): 95–121.

Leithhead, B. S., and D. McNamee. 2000. Assessing organizational risk. *Internal Auditor* (June): 68–69.

Levinsohn, A. 2005. First-year verdict of SOX 404: Burdensome, costly, and confusing. *Strategic Finance* (June): 67–68.

Lightle, S. S., and C. W. Vallario. 2003. Segregation of duties in ERP. *Internal Auditor* (October): 27–31.

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

Mason, R. 1986. Four ethical issues of the Information Age. *MIS Quarterly* 10 (1): 5–12.

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

Meyer, N. D. 2004. Systematic IS governance: An introduction. *Information Systems Management* (Fall): 23–34.

Mock, T. J., and A. M. Wright. 1999. Are audit programs risk-adjusted? *Auditing: A Journal of Practice & Theory* (Spring): 55–74.

National Commission on Fraudulent Financial Reporting (the Treadway Commission). 1987. *Report of the National Commission on Fraudulent Financial Reporting*. Washington, D.C.: Government Printing Office.

Nehmer, R. 2003. Transaction agents in eCommerce, A generalized framework. In *Trust and Data Assurances in Capital Markets: The role of technology solution*, edited by S. J. Roohani. Smithfield, RI: PricewaterhouseCoopers.

O'Leary, D. E. 2000. *Enterprise Resource Planning Systems: Systems, Life Cycle, Electronic Commerce, and Risk*. Cambridge, U.K.: Cambridge University Press.

———. 2002. Discussion of information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems* (Supplement): 115–126.

Ozier, W. 2003. Risk metrics needed for IT security. *ITAudit* (April 1). Available at: http://www.theiia.org/itaudit/index.cfm?fuseaction=print&fid=5396.

Pacini, C., and D. Sinason. 1999. The law and CPA Webtrust. *Journal of Accountancy* (February): 20–25.

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

PricewaterhouseCoopers. 2003. *Technology Forecast: 2003–2005*. Menlo Park, CA: PricewaterhouseCoopers.

———. 2004. Integrity driven performance. Available at: http://www.pwcglobal.com/images/gx/eng/about/svcs/grms/PwC_GRC_WP.pdf.

Public Company Accounting Oversight Board (PCAOB). 2005. Staff questions and answers on Auditing Standard No. 2—Internal Control. Available at: http://www.pcaob.org/Standards/Staff_Questions_and_Answers/Auditing_Internal_Control_over_Financial_Reporting_2005-05-16.pdf.

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

———, and M. L. Weidenmier. 2004. *The Pervasive Impact of Information Technology on Internal Auditors*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.

Rezaee, Z., A. Sharbatoghlie, R. Elam, and P. L. McMickle. 2002. Continuous auditing: Building automated auditing capability. *Auditing: A Journal of Practice & Theory* (March): 147–163.

Searcy, D. L., and J. B. Woodroof. 2003. Continuous auditing: Leveraging technology. *The CPA Journal* (May): 46–48.

Sobel, P. J., and K. F. Reding. 2004. Aligning corporate governance with enterprise risk management. *Management Accounting Quarterly* (Winter): 29–37.

Spinello, R. 1998. Privacy rights in the information economy. *Business Ethics Quarterly* (October 4): 723–763.

Sutton, S. G., T. D. Arnold, and V. Arnold. 1999. An integrative framework for analysis of the ethical issues surrounding information technology integration by the audit profession. *Research on Accounting Ethics* 5: 21–36.

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

Wah, L. 2000. Give ERP a chance. *Management Review* (March): 20–23.

Weick, K. E. 1969. *The Social Psychology of Organizing*. Reading, MA: Addison-Wesley.

———. 1979. *Social Psychology of Organizing*. Reading, MA: Addison-Wesley.

Wright, S., and A. M. Wright. 2002. Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems* (Supplement): 99–114.

Wu, R. 1992. The information systems auditor's review of the systems development process and its impact on software maintenance costs. *Journal of Information Systems* (Spring): 1–13.

Zimbelman, M. F. 1997. The effects of SAS No. 82 on auditors' attention to fraud risk factors and audit planning decisions. *Journal of Accounting Research* (Supplement): 75–97.