Communications of the Association for Information Systems

Volume 23 Article 26

11-2008

# Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit

Jeffrey W. Merhout
*Miami University*, jmerhout@muohio.edu

Douglas Havelka
*Miami University*



Recommended Citation
Merhout, Jeffrey W. and Havelka, Douglas (2008) "Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit," *Communications of the Association for Information Systems*: Vol. 23 , Article 26.
DOI: 10.17705/1CAIS.02326
Available at: https://aisel.aisnet.org/cais/vol23/iss1/26

Communications of the Association for Information Systems

CAIS

# Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit

Jeffrey W. Merhout

Douglas Havelka

*Decision Sciences & MIS*

*Miami University (Ohio)*

*jmerhout@muohio.edu*

Abstract:

Information systems provide both the means for organizations to transact business and the ability to report the financial results of their operations. Information technology auditing is an integral part of corporate governance. However, information technology auditing is often looked upon as a "necessary evil" or is overlooked entirely by IT management We argue that IT audit activities can provide additional value beyond the primary objective of assurance, assuming the organization embraces IT governance partnerships between IT management and the audit function. We also analyze factors developed from field study research that suggest IT audits are special projects requiring a quality audit process and sound project management principles. These success factors, if managed properly, can lead to high-quality IT audit products (i.e., engagements) that could conceivably free audit resources for more value-added projects and enterprise oversight. We close with a discussion of future research directions.

**Keywords**: Sarbanes-Oxley, COBIT, IT Governance Institute, risk management, internal controls

Volume 23. Article 26. pp. 463-482. November 2008

The manuscript was received 3/21/2008 and was with the authors 4 months for 2 revisions.

## I. INTRODUCTION

Compliance with laws and regulations is a major requirement of corporate governance. For example, the Sarbanes-Oxley Act of 2002 (SOX) requires CEOs and CFOs of large, publicly traded organizations in the United States to personally certify their organizations' financial statements. Per the Act [see Hall and Liedtka 2007, and Mishra and Weistroffer 2007 for more details], these officers are responsible for designing, establishing, and evaluating the internal controls necessary to produce accurate financial statements. These financials are, in turn, significantly dependent on the information systems used in the organization. Because of this dependence senior managers in many large organizations have recently become aware of the strategic significance and cost of their organizations' IT (information technology) architecture; i.e., the applications, operating systems, hardware, and networks used by the organization, as well as the significant cost of IT personnel. Moreover, achieving compliance with SOX requires organizations and their external auditors to perform more frequent, highly detailed IT audits, and CEOs comment publicly that the financial costs associated with these requirements are onerous and unreasonable.

We, however, believe these statements demonstrate a marked underestimation of the benefits of IT audit activities being performed to comply with SOX and other regulations. In this article, we summarize the explicit benefits of an internal IT audit function. We also suggest several "value-added" benefits from IT audit activities that are commonly overlooked by managers. The evidence for our thesis comes from multiple sources, including trade and academic literature, discussions with IT audit practitioners, and qualitative data from field study research with audit professionals. We believe our discussion is of interest to a broad audience including corporate board(s) of directors, C-suite executives (such as the CIO, CEO, and CFO), IT managers, and IT audit management. For example, IT audit managers could apply the suggestions we developed from our research by embracing the possibility of value-added partnerships. Such partnerships would require educating IT directors and managers regarding the importance of governance and controls and on the subject of how a formal information technology audit program can provide significant value-added benefits (beyond compliance with SOX).

To clarify our arguments, we will illustrate research into the primary factors that affect the quality of an IT audit from the perspective of project management. The factors uncovered thus far indicate that both sides of the audit equation —the auditee and the auditor—can control (or at least influence) many of the key variables that lead to audit project success. Thus, we will illustrate a comprehensive framework of IT audit quality/success. Moreover, we present evidence that a quality IT audit process (or methodology) combined with sound project management principles can ultimately lead to a value-added quality audit product. For example, auditee (i.e., IT personnel) assignments for engagements should be carefully selected to facilitate the auditors' requests. A quality audit process and product can hence lead to a more efficient use of the resources of an annual risk-based internal IT audit program which should conceivably free some audit resources to be used for more value-added projects and enterprise oversight. Our paper thus addresses recent calls for more research that incrementally develops a "greater understanding of the problems presented by information security and assurance activities and more acutely, solutions to those problems" [Choobineh, Dhillon, Grimaila, and Rees 2007, p. 13].

The remainder of this paper proceeds as follows. Section II summarizes what an IT audit involves, and in Section III, we discuss the explicit, direct benefits an organization would expect to receive from the usual annual IT audit program. In Section IV, we review a new framework we developed for Information Technology Audit Quality that supports our main thesis. In Section V, we argue that an organization where IT governance partnerships exist can receive additional value-added benefits from its IT auditors and discuss several of these possible benefits. In Section VI, we then present a caselet that illustrates our framework, and in Section VII, we follow with a suggested agenda for IT audit research. We finalize the paper with a call for organizations to form value-added IT governance partnerships.

## II. INFORMATION TECHNOLOGY AUDITING

An *audit* is an independent examination of an organization's management assertions that must follow a set of guidelines and standards promulgated by an external sanctioning body. An audit can be either an external engagement conducted by certified public accounting (CPA) firms or an internal engagement performed by an organization's internal audit function. To technically be classified as an IT audit, the examination must involve information technology, either as the specific focus of the examination (even indirectly, such as IT governance), or as the means to complete an engagement. And, in most cases, it involves both. An IT audit can be executed by

external auditors as part of the annual audit of financial statements with the primary purpose of testing the structure of internal controls surrounding key information systems; it can also be performed by the internal audit function for a similar purpose, but with the intent of satisfying management's responsibility surrounding governance. Additionally, IT audits may be performed in the context of a business process review or as part of a larger "integrated" audit where financial and technology auditors work together (e.g., a financial statement audit) or perhaps when internal operational and IS auditors team up to critique business processes along with their supporting systems.

Most audits, including IT audits, are conducted using a "risk-based" approach: potential risks are identified and prioritized, control mechanisms are assessed (or perhaps created by management as a result of the audit's findings), and the controls are tested. Activities and procedures performed during an IT audit include: reviewing documentation for business processes; evaluating controls embedded in applications such as enterprise systems (e.g., enterprise resource planning, customer relationship management, or supply chain management systems); testing the interfaces between these systems; reviewing audit logs of transaction processing; testing the accuracy and validity of data in databases; reviewing and testing access controls to applications, databases, and networks; and evaluating the status of systems development projects. These activities can range from very detailed tasks to high-level analyses requiring experience and expertise with specific technologies.

Other researchers have noted that IT governance is situated at multiple layers in the organization [DeHaes and Van Grembergen 2008; Van Gremberger 2003]. At the strategic level the organization's board of directors is involved, at the management level the "C"-level officers are involved, and at the operational level IT and business management are involved. This implies that IT audit could be used at each level to evaluate the processes, structures, or mechanisms used to implement IT governance [DeHaes and Van Grembergen]. At the strategic level, IT governance is the process for controlling an organization's IT resources and developing the IT strategy. IT auditing is an integral part of the IT governance and is recognized as a critical IT process in the COBIT and ITIL governance frameworks (discussed in Section V). At this highest level, IT audit can be used to ensure that the IT strategy is aligned with the overall organization strategy and that specific IT policies are in place and being followed. Organizations can use the IT audit process to reduce the risk associated with IT investment and deployment. At the management level, IT audit can be used to ensure that IT budgets and plans are being prepared and executed according to the appropriate business rules, as well as ensuring that development and implementation projects are controlled properly. At the operational level, IT audits ensure the proper processing of day-to-day business transactions and events as well as ensuring the adequacy and proper operation of the IT function within the organization. This includes identifying risks and controls related to specific applications and business processes and testing whether these controls are working properly.

## III. DIRECT BENEFITS OF IT AUDITS

One primary purpose of IT auditing is to assess whether or not an information system is meeting stated organizational objectives and to ensure that the system is not creating an unacceptable level of risk for the business. The terms "assurance," "attestation," "audit," and "control" generally refer to this same general purpose, while each has a very specific meaning in context. The primary benefit of an IT audit is to ascertain with a certain level of confidence that an information system is working properly, e.g., that it processes inputs into outputs correctly, that only authorized individuals can access specific data and execute specific programs, and that data are stored correctly and securely. Moreover, to comply with SOX, any system that significantly impacts the financial statements must be evaluated. Although systems audits are potentially resource intensive, the ultimate benefit from IT audits is a greater confidence in the financial statements of the organization and in the investment environment in general (e.g., the capital markets).

While this overarching benefit to stockholders and the investment community is crucial (and the stated intent of SOX), other explicit benefits accrue to organizations conducting IT audits. These benefits include (or should include): compliance with other various government regulations (e.g., the Health Insurance Portability and Accountability Act [HIPAA], and laws aimed at combating identity theft); the identification of effective control mechanisms and those in need of improvement; improved documentation of information systems and business processes; and improved systems security. One aspect of conducting IT audits is the discovery of irregular acts, i.e. intentional violations of policies or regulations, or unintentional breaches of the law. The IT auditor must work with corporate legal counsel whenever an irregular or illegal act is suspected. ISACA guidelines indicate that IT auditors are not qualified to determine whether such behavior has occurred. Management and legal counsel are responsible for making these determinations.

Despite these benefits, SOX is a significant compliance burden for many organizations, and it is not the only legislation that has implications for the use and operation of information systems. IT audits, both internal and external, should, however, allow managers to more efficiently utilize resources by providing evidence or documentation for compliance with other regulations. In other words, complying with SOX may provide compliance

coverage for significant requirements of other regulations, such as HIPAA. In addition, one of the most prevalent reasons for an internal IT audit, separate and distinct from the external audit and external compliance requirements, is to test system compliance with specific organizational policies and procedures for maximum operational efficiency or effectiveness.

Perhaps the most direct benefit that should be attained by a comprehensive IT audit program is the identification and documentation of effective control mechanisms for information systems, or raising awareness of the lack of adequate and appropriate controls. Adequate command and control over business processes and the information systems that support these processes is sound, fundamental management practice. The documentation of these controls should allow management to evaluate the tradeoffs between control requirements and operational efficiency, where they exist, and to make better decisions for establishing appropriate control mechanisms. For example, controls such as network and database access might be either redundant or, conversely, synergistic; or they might cost differing amounts to implement (through specific overall control structures) even though they would deliver about the same level of control. In cases of redundant or cost-ineffective controls, control rationalization (elimination) can lead to a more efficient mix of control structures.

In addition to documenting the adequacy of controls structures, an IT audit usually requires the generation of documentation of business processes, applications, and the IT architecture. The production of this documentation should lead to a greater understanding of these business processes and technology enablers by management, which should enhance an organization's ability to effectively manage these valuable resources. The existence of this documentation should also help in training new employees, performing evaluations of operations and systems, and measuring the return on investments in IT, especially when evaluating the costs and benefits of new systems.

Although not all IT audits have fraud detection and prevention or systems security as stated goals, conducting the IT audit should enable fraud detection and prevention and overall systems security improvement. Given the ubiquity of malicious code, e.g., spam, phishing, spyware, etc., the use of computer-based systems to commit fraud or corporate espionage is a significant threat. In this environment, organizational policies and procedures must include "enterprise wide" access controls (specifically detective/preventive controls) to information systems and digital and electronic assets. Without regular reviews and continuous vigilance for adherence to these policies, these security controls may become ineffective. The IT audit could also possibly serve as a deterrent to malicious acts. When individuals know that their electronic actions might be reviewed during the audit (thereby raising the real possibility of having their illegal actions discovered), they are less likely to act maliciously or irresponsibly.

## IV. COMPREHENSIVE FRAMEWORK OF IT AUDIT QUALITY/SUCCESS

IT audit functions in the U.S. are required to adhere to quality control standards, such as those promulgated by the Public Company Accounting Oversight Board (PCAOB) and the American Institute of Certified Public Accountants (AICPA) for public accounting firms and the Institute for Internal Auditors (IIA) for internal IT audit operations. As every information systems audit is unique, the factors that affect IT audit success (i.e., quality) will vary based on the circumstances of the project (e.g., the industry, size of the organization, and complexity of the systems involved). We argue, however, that it is possible to identify a comprehensive set of critical success factors that are considered important across IT audits by auditors and business managers, regardless of the unique aspects of an IT audit. Further, the identification of a comprehensive set of factors that may influence the IT audit process could pinpoint specific areas that are problematic or opportunistic. Overall, these factors can act as important antecedents to the IT audit process and influence the successful outcome of a specific IT audit and of an IS audit department's overall assurance program. Consequently, if an overall audit program is successful in efficiently utilizing resources, then it might be possible for IT audit's management to use excess capacity (or obtain more resources) to provide truly value-added assistance to the company, as outlined in this paper.

To establish an understanding of the research domain of IT audit, we undertook a field study to develop a model of IT audit quality. The field study was composed of two stages: the first to develop an initial framework and the second to provide validation and refinement of the framework. Both stages consisted of a series of focus groups using a nominal group process including IT auditors, financial and operational auditors, and IT audit managers. The first stage was conducted at a large (Fortune 20) health care products and services organization with three distinct groups of participants: Group 1 consisted of IT audit managers with an average of 6.9 years of audit experience; Group 2 consisted of financial and operational audit managers and staff auditors an average of 5.1 years of audit experience; and Group 3 consisted of IT audit seniors and staff auditors with an average of 2.8 years of audit experience. More details related to this work can be found in prior research (Havelka and Merhout 2007). The second stage of the field study was conducted at a large, regional bank with two groups of participants: Group 4 consisted of IT audit managers with an average of 5 years of audit experience; and Group 5 consisted of IT audit seniors and staff auditors with an average of 1.7 years of audit experience. The results from the second stage were used to refine and confirm the initial framework.

Nominal group techniques have been used for group problem solving, particularly where fact gathering is a primary concern. Nominal group techniques have been found to be superior to personal interviews and surveys when the desired goal is the generation of a maximum number of ideas or alternatives [Delbecq, Van De Ven, and Gustafson 1982; Van de Ven and Delbecq 1971; Van de Ven and Delbecq 1974]. By using individuals who have had experience in a problem area, the critical factors influencing the problem can be identified. In our study, five different groups of subjects that have had experience with the IT audit process were used to identify factors that affect IT audit process quality. The nominal group technique is composed of a group session where structured brainstorming and consensus techniques are used to elicit the desired data. The nominal group techniques are applied to distinct groups of subjects to obtain representative and comprehensive results. The output of these focus groups include a set of factors that can be used by managers to improve the IT audit process or by researchers to further investigate the relationships among the various factors. To this end, the factors identified by the first set of groups were classified into categories for an initial analysis, and then this framework was verified by using the factors identified by the second set of groups. Based on the outcomes of these group sessions, further study of the factors and their impact on IT audit quality can be conducted.

## Field Study Results

The nominal group process yields two types of qualitative data: 1) a comprehensive set of factors that the participants identify as influencing the quality of the IT audit process; and 2) a more refined set of factors that the participants indicate as being "critical" to IT audit quality. A summary of the outcomes of the group processes is given in Table 1 (G1 is Group 1, etc.).

**Table 1. Overall Results of Field Study**

| | Stage I | | | Stage II | |
|---|---|---|---|---|---|
| | **G1** | **G2** | **G3** | **G4** | **G5** |
| Number of participants in the group | 4 | 7 | 5 | 5 | 6 |
| Total number of factors identified (including duplicates) | 22 | 44 | 48 | 33 | 41 |
| Total number of factors selected as critical | 16 | 40 | 42 | 30 | 34 |
| Total number of factors not considered critical | 6 | 4 | 6 | 3 | 7 |
| Percentage of factors selected as critical | 73% | 91% | 88% | 91% | 83% |

Stage I resulted in a total of 80 unique factors identified as having some influence on the quality of the IT audit process. Of these 80 factors, 69 were considered to be "critical" to IT audit quality by at least one participant. Stage II resulted in a total of 59 unique factors being identified as influential and 52 of these were considered to be "critical" by at least one of the participants. The breakdown of factors identified and rated as critical by the five groups from both Stage I and Stage II are given in Table 2.

A total of 108 unique factors were identified by all the groups. Of the 108 unique factors identified overall, only 31 of these were identified in both Stage I and Stage II (Stage I identified 49 factors that were not identified in Stage II, and Stage II identified 28 additional factors that were not identified in Stage I).

**Table 2. Detailed Outcomes of Field Study**

| | |
|---|---|
| **Factors Identified by Groups** | |
| Factors identified by all 5 groups. | 6 |
| Factors identified by 4 of the 5 groups. | 6 |
| Factors identified by 3 of the 5 groups. | 10 |
| Factors identified by 2 of the 5 groups. | 18 |
| Factors identified by only 1 of the five groups. | 68 |
| Total number of factors identified. | 108 |
| **Factors Rated Critical by Groups** | |
| Factors were rated as critical by all 5 groups. | 6 |
| Factors were rated as critical by 4 of 5 groups. | 5 |
| Factors were rated as critical by 3 of 5 groups. | 8 |
| Factors were rated as critical by 2 of 5 groups. | 14 |
| Factors were rated as critical by 1 of 5 groups. | 60 |
| Factors were rated as critical by none of the 5 groups. | 15 |
| Total number of factors identified. | 108 |

Overall, of the 108 unique factors identified by the five groups, 93 of these were considered critical by at least one participant of the field study. 28 of the factors were considered critical in both Stage I and Stage II and 15 were not considered critical in either stage (there were 41 factors rated as critical in Stage I only and 24 rated as critical in Stage II only).

As noted in Table 2, there are six factors that were identified and rated as critical by all five groups. Assuming that this is an indication of the relative importance of these factors, they deserve further discussion. The six factors that were considered critical by all five groups were: 1) Audit method; 2) Sufficient time allowed for the audit; 3) Support from the client/auditee and management; 4) Client relations; 5) Organizational change; and 6) Clear scope and objectives for the IT audit.

The first factor rated as critical by all five groups is that an audit methodology is used. In general, using an audit method helps to ensure that audits are performed similarly from one audit to the next and that standards and best practices are followed. Participants also indicated that using a method versus not using one increased the quality of the audit work.

The second factor rated as critical by all five groups is sufficient time allowed for the audit, especially fieldwork. Sufficient time is necessary to gather relevant documents, evaluate processes, learn technology, run tests, and to evaluate the results of fieldwork. Participants indicated that this was an issue due to the pressure to perform audits quickly and due to the large number of audits being performed by their organizations.

The third factor rated as critical by all five groups is support, cooperation, and buy-in from the client, auditee, and top-level management. Having adequate support from these critical stakeholders impacts the auditor's work in several ways. Adequate support will allow easier access to documents and records, access to the correct people and their time. Adequate support will impact the availability of other resources such as computer time and additional audit personnel.

The fourth factor rated as critical by all five groups is client relationships. This refers to the quality and responsiveness of the client to inquiries and the audit in general as well as the level of honest and open communication between the audit and client personnel. This should lead to increased understanding, by the auditor, of the system or process being audited. This factor as well as the preceding one may be based on the higher level construct of trust or level of trust that exists between the auditor and the client. This emphasizes the prior experience between the auditor and the client and the importance of maintaining on-going cordial association between the two groups.

The fifth factor rated as critical by all five groups is organizational change. In general, group participants observed that mergers and acquisitions, re-structuring of business processes, and systems implementations all require significant change to business processes and that these changes can lead to challenges for management to implement the changes in operations and in implementing adequate controls. It was noted that organizational change can lower the level of understanding of the business process by operational and management personnel and can lead to outdated or incorrect process documentation and procedures. Organizational changes may also mean that the auditors will have little or no experience with the new, changed processes. These changes usually mean new roles for old personnel and new personnel also. These changes would lead to higher audit risk and require more time for the audit to be performed.

The sixth, and final, factor rated as critical by all five groups is the clear definition of the project objectives and scope. The participants emphasized that knowing the boundaries of the process or system being audited was critical to help identify inputs, outputs, and controls for the process. The objectives will drive the type and level of testing that is performed. Scoping as part of the audit method, mentioned earlier, is critical due to its impact on the allocation of resources and risk assessment performed during the planning of the audit. Particularly, the objectives and scope will determine the skills and experience that are required by the audit team. The scope can also help the auditor identify specific tasks that must be performed and controls that should be implemented in a given system or process.

To partially validate that there exists some consensus regarding the factors identified we tested whether the results from Stage I and Stage II are consistent with one another. A Chi-square test for independence (based on whether the groups rated the factors as critical or not), i.e. Critical in Both Stages, Critical in Neither Stage, Critical in Stage I only, and Critical in Stage II only) was performed. This test results in the rejection of the null hypothesis that the outcomes from the groups in Stage I are independent from the groups in Stage 2 at a .05 level of significance (Chi-Sq = 4.384, DF = 1, P-Value = 0.036). This result provides evidence that there is some consensus or agreement

regarding the evaluation of the factors and supports the idea that there are factors critical to IT audit quality across industries and businesses.

These results support the notion that there are common factors that are critical to IT audit quality across businesses and industries; however, these results also suggest that in addition to the common factors there appear to be many factors that may be organization or industry specific. Identifying and weighing these factors appropriately when planning a given IT audit would be critical to the success of the audit. Based on these results, we further analyzed the factors identified and describe the development of a framework for studying the IT audit domain in the next section.

## Framework Development

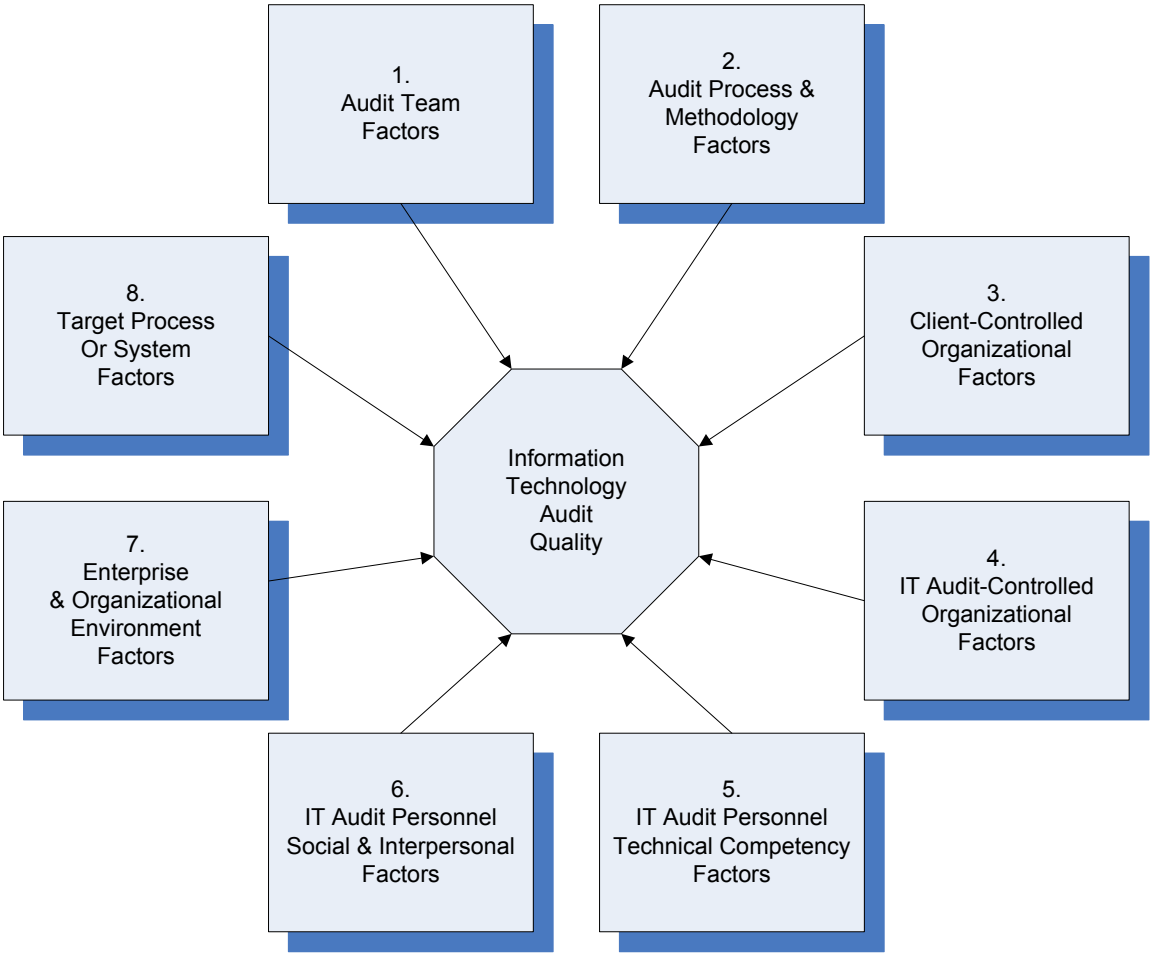


**Figure 1. The Information Technology Audit Quality Framework**

Using the results of the first stage, the factors were classified into logical categories providing the foundation for a model of IT audit process quality. We have thus far found no concrete categorization frameworks for this topic in the literature nor did we find a precise explanation of how to create categories from factors in the nominal group technique literature. Accordingly, we independently grouped the factors identified into logical categories based on our professional experiences. Discrepancies between the results were discussed and resolved. The resulting initial model consisted of five categories of factors: Client-related; Target Process or System; IT Audit Personnel; IT Audit Organization; and Audit Process/Methodology. Based on the results of the second stage, we refined and expanded the framework to eight logical categories based on who or what entity might control, influence, or determine the factor. The framework is presented in Figure 1 and the descriptions of each category are presented in Table 3. The specific factors identified and classified into each category can be found in APPENDIX A.

After analyzing and categorizing the factors to develop the framework, several observations were made. The framework consists of eight categories, but it appears that these categories are not equally important. Based simply on the number of factors identified, the audit process and methodology factors category is most important with a

| Table 3. Descriptions of IT Audit Quality Framework Categories | |
|---|---|
| **Category** | **Description** |
| 1. Audit Team Factors | The *audit team* category refers to audit team characteristics, such as team communications, experience working together, and cohesiveness. |
| 2. Audit Process & Methodology Factors | The *audit process or methodology* category refers to the specific procedures and practices followed by the IT audit team. Some of these factors are: the existence of an audit methodology for the team to follow, scope definition, the use of automated tools, and timely oversight/review of audit work. |
| 3. Client-Controlled Organizational Factors | The *organizational factors, client-controlled* category includes any factors that were characteristics of or dependent on the client (or auditee), including management's support and adequacy of documentation. This category is where partnerships are critical for the ability of IT audit to influence how the client (i.e., auditee) cooperates during the course of an audit. |
| 4. IT Audit-Controlled Organizational Factors | The *organizational factors, IT audit-controlled* category includes those factors that are characteristics of the IT audit function within the organization. Examples of these factors include: relationships with clients, adequate time allocated for the entire audit, leadership, and understanding of business unit and IT organizational initiatives and changes. |
| 5. IT Audit Personnel Technical Competency Factors | The *IT audit personnel, technical competency* category includes factors that are dependent upon the individuals performing the IT audit tasks. Some of the factors in this category are: understanding of risks and control weaknesses, project management, and staff experience. |
| 6. IT Audit Personnel Social & Interpersonal Factors | The *IT audit personnel, social and interpersonal skills* category includes factors that are dependent upon the individuals performing the IT audit tasks. Some of the factors in this category are: independence, communication skills, willingness and ability to change, and motivation/enthusiasm. |
| 7. Enterprise & Organizational Environment Factors | The *enterprise and organizational environment* category refers to overall characteristics of the corporation and/or the unit being audited. Factors in this category include financial resources, corporate culture, the reporting structure of Internal Audit, perception of value-added from audits, and the number of recent audits (from all sources) of a particular area being audited by an IT Audit team. Here again is a key opportunity for the benefits of IT governance partnerships to positively influence the overall success of an annual IT audit plan. |
| 8. Target Process or System Factors | The *process or system* category included any factors based on the process or system being audited, i.e., the target of the audit, and specific considerations for the specific audit "project" being performed. Some examples of process or system factors are: clearly defined project scope, system complexity and type, amount of manual versus automation in process, and the level of documentation for the process or system. |

total of 27 factors identified. This would suggest that management focus on developing a sound audit methodology with best practices, hiring competent audit personnel that understand the methods, and provide adequate resources for the audit function. However, this conclusion should be viewed critically, given that all of our group participants had an audit background. Perhaps more interesting is the "number 2" category: Client-controlled organization factors (19 factors identified, three of them rated critical by all five groups). This seems more interesting because these factors are beyond the control of the audit team, but were considered important to the quality of the IT audit. This

suggests that regardless of the "quality" of the IT audit function, the client has a significant influence over the quality of any given IT audit. These factors could be considered constraints or moderating variables on the quality of IT audit from the auditors' perspective.

From the perspective of the management hierarchy, most of the factors identified and the categories suggested in the model focus on the operational level. With the notable exception of the enterprise and organizational environment factors, nearly all of the factors are related to either IT audit management, audit management, or management of the functional areas (e.g., customer order process). The factors identified and categorized in the enterprise and organizational environment could be considered to be "higher" level responsibility, i.e. either strategic or management level. Most of these could be considered "structural" or "relational mechanisms" using the IT governance framework proposed by DeHaes and Van Grembergen [2008].

This model can be used by managers to analyze and plan for IT audits by identifying risks and opportunities associated with the eight categories of factors. In addition, IT audit managers and clients could use the detailed factors identified to develop and establish metrics to evaluate IT audit quality after the fact. Finally, researchers could use this model to further study the relationships among the various factors and their affects on IT audit quality. For example, we note that Lampe and Sutton [1994] include an "audit quality factor" they refer to as "audit team experience and training," which was a factor they identified at all six companies researched for their study on internal audit quality. This factor appears to map into our "IT audit team factors" category. This mapping leads to additional research questions, such as whether there is additional overlap with factors identified in other studies of IT audit quality, perhaps in both public accounting and internal audit, or whether there are factors unique to IT audit versus general audits.

Based on our work, it appears IT management needs a better understanding of the role the auditee plays in the outcome of a successful IT audit. To address this, IT management needs to communicate this message and educate the various levels of staff throughout the entire scope of IT operations. Our field study research with the internal audit departments of two major corporations shows support for several factors, some of which may be under the control of the client/auditee (e.g., IT management), some that are controlled by the auditors themselves, and some that are characteristics of the environment or system under study and therefore act as constraints to the IT audit process.

## V. VALUE-ADDED BENEFITS OF IT AUDITS

Given the inevitability of being audited for purposes of compliance and governance assurance, IT management should adopt an attitude that embraces the opportunity for a value-added audit experience. Developing such a culture would require senior corporate management leadership and possibly the utilization of incrementally more resources to accomplish the overall requirements of the IT audit program. Eventually, despite the requisite cultural changes and allocation of resources, these partnerships could also significantly facilitate the possibility that the auditors (internal or external) could provide a quality product that truly adds value commensurate to the resources required for an audit to occur. Many audit practitioners [e.g., Bassett 2007; Champlain 2003; Kumar 2006] argue that the "old school" of auditing where auditors function as "police" is the inappropriate approach and call for IT auditors to adopt the roles of consultant, counselor and liaison instead. Indeed, we have discovered such a promising philosophy in the internal audit groups we have studied.

In addition to the direct, explicit benefits outlined above, we believe opportunities exist for organizations to further leverage the work performed during IT audits to provide additional, value-added benefits. Some of these benefits include:

**Table 4. Value-added IT Audit Services**

| | |
|---|---|
| 1. | Improved return on investment in information technology through improved IT governance. |
| 2. | Using audit documentation to improve operational efficiency through business (and IT) process reengineering or improved business process management. |
| 3. | Using audit observations to improve risk mitigation through enhanced enterprise risk management (ERM) awareness. |
| 4. | Improved business continuity planning and associated systems disaster recovery planning. |
| 5. | Improved systems development quality. |
| 6. | Increased organizational communication and trust development through facilitation among various stakeholders. |

## Improved Return on Investment in Information Technology through Improved IT Governance

The primary duties of Chief Information Officers (CIOs) and other senior IT directors and managers have evolved over the years from a predominantly technical perspective to a more strategic viewpoint. One of the key strategic roles upon which these senior IT staff are beginning to focus, or arguably, should be focusing, is enterprise risk management and more specifically, IT governance [Sutton and Arnold 2005]. The IT Governance Institute (ITGI) defines IT governance as "leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the enterprise's strategies and objectives" [ITGI 2008]. However, research compiled for practitioners shows an interesting contradiction. Society for Information Management (SIM) Executive surveys [e.g., Luftman, Kempaiah and Nash 2006] consistently find that IT management is concerned with the alignment of IT and business strategy. Nonetheless, other research (e.g., ITGI 2006; Kerstetter and Porrello 2007] finds that a large percentage of directors (on corporate boards) and corporate executives (e.g., CIOs and CEOs) are not giving adequate consideration to IT governance even if they recognize that IT governance leads to improved profitability [Blecher 2007].

This apparent gap between senior corporate management and IT management is puzzling. Theoretically, IT governance should facilitate more alignment between IT and business strategy (as recognized by 57 percent of CIOs in an ITGI survey [ITGI 2006]). Moreover, this governance can be facilitated through existing controls frameworks, such as COBIT® [ITGI 2007a] and/or the IT Infrastructure Library (ITIL). COBIT (Control Objectives for Information and related Technology) is an IT governance framework with a supporting set of tools; i.e. references, worksheets, and templates, whose goal is to allow managers the ability to bridge gaps between control requirements, technical issues, and business risks [ITGI 2007a]. ITIL (the IT Infrastructure Library) is also a framework focusing on best practices for delivering IT services. Either, or both, of these frameworks can be used to manage and evaluate the IT function and processes within an organization. IT audit could then be used to test and evaluate specific controls implemented within these processes or to evaluate the operational effectiveness of specific IT services being delivered. The frameworks can provide standards, benchmarks, and metrics that can be used by the IT audit function. Senior IT directors and managers can benefit from understanding the importance of governance and its relationship to strategy. The self-assessment of risks and controls related to information technology is a key requirement of IT governance that often does not receive much attention from IT practitioners, and IT auditors can provide valuable knowledge for this task.

In addition to being a necessary assurance requirement for IT operations for publicly traded companies in the United States, IT auditing is also required by the internal audit functions of all types of organizations that strategically deploy IT to meet their missions. Because IT audits are going to occur frequently and require significant resources, we argue that audits should not be viewed as a "necessary evil," but rather as an opportunity for value-added partnerships between IT management and their auditors (whether external or internal). Corporate boards of directors, C-suite executives, and IT management, as well as internal IT audit management, should embrace and encourage the possibility of such value-added partnerships. Thus, IT audit management should make efforts to educate IT directors and managers and their staff about the importance of governance and controls and about how a formal information technology audit can provide significant value-added benefits. Such education can suggest the value of IT audits on several dimensions: strategic (e.g., ERM, SOX compliance, IT governance, alignment of IT and strategy, utilization of assets, etc.), operational (e.g., security, fraud prevention, disaster recovery preparedness, and best practices), financial (e.g., return on investment [ROI]), and IT/IS quality (e.g., the systems development process). At the same time, IT management should demand real value-added services from their auditors and seek their counsel for identifying opportunities for improvement.

One way an organization's IT function can better ensure an acceptable financial ROI of its investments in new technology and systems is to use a governance framework, such as VAL IT™ from the ITGI [ITGI 2007b]. The Val IT initiative by the IT Governance Institute was conducted to address C-level managers' concerns regarding the return on investments in information technology; this initiative resulted in the Val IT Framework. Val IT is a model consisting of a set of principles, processes and management practices that guide an organization in managing its IT-enabled business investments from inception of the project through the assessment of the realized benefits from that project. VAL IT complements COBIT, which is used by numerous organizations as a high-level IT governance and control framework. VAL IT and COBIT together can allow an organization to focus on the value-added business component of IT investments, such as establishing clear accountability for ensuring the realization of expected benefits, including difficult-to-quantify "soft" benefits, and comprehensively appraising the risk associated with specific projects. Schaafsma, Spangenberg, and Williams [2007] completed preliminary empirical work on a large sample of IT projects and found evidence suggesting COBIT-like IT project management principles and practices lead to lower instances of projects exceeding cost and time budgets. Accordingly, we see this focus on governance frameworks as another opportunity for IT audit management to provide guidance for executive management about this key component of overall enterprise governance.

As an illustration of applying a controls framework to improve IT governance using a risk-based approach and the utilization of appropriate IT control frameworks, we use the COBIT model to provide details for a hypothetical banking environment. Banking is a relevant example because the industry is both highly automated and heavily regulated, thus requiring strong IT governance. The Federal Reserve outlines several enterprise risk categories for financial institutions, including market risk, credit risk, liquidity risk and operational risk [Federal Reserve System, 1995]. Shabudin [2007] details operational risks that banks typically address in their ERM initiatives: strategic risk, including business units, IT and people; reputation risk, including business continuity and internal fraud; transaction risk, including IT processing and identity theft; and compliance risk, including regulatory compliance. While each of these risk categories includes significant possible exposure for a bank's IT and systems, we focus only on strategic risks for this brief example. Table 5 illustrates IT strategic risks and controls objectives for the two of the 34 COBIT High Level Objectives (Process Descriptions): Plan and Organize (PO)1 — Define a Strategic IT Plan; and PO6 — Communicate Management Aims and Direction [ITGI 2007a]. See Mishra and Weistroffer [2007] for more details on COBIT.

**Table 5. Banking Strategic Risks Related to IT Mapped to COBIT**

| Strategic Risks | COBIT Process Description | COBIT Objective | Details of Objective |
|---|---|---|---|
| Enterprise Mission Not Supported by IT | PO1 – Define a Strategic IT Plan | PO1.2 – Business-IT Alignment | Education and involvement by business units and IT to mutually agree on priorities to ensure IT alignment and integration |
| No Common Understanding and Agreement about Business Unit and IT Priorities | PO1 – Define a Strategic IT Plan | PO1.2 – Business-IT Alignment | |
| IT Management Not Understanding Business Unit Requirements | PO1 – Define a Strategic IT Plan | PO1.4 – IT Strategic Plan | Relevant stakeholders create a sufficiently detailed IT strategic plan. The plan should define how IT goals align with the enterprise's strategic objectives, how the IT objectives will be achieved, and how these objectives will be measured. |
| IT Plans Not Aligned with Business Unit Requirements | PO1 – Define a Strategic IT Plan | PO1.4 – IT Strategic Plan | |
| IT Management Not Focusing on Correct Priorities | PO1 – Define a Strategic IT Plan | PO1.4 – IT Strategic Plan | |
| Lack of Awareness of Management Goals and Objectives Related to IT | PO6 – Communicate Management Aims & Direction | PO6.5 – Communication of IT Objectives and Direction | Appropriate management processes are in place to clearly communicate awareness of senior management's philosophy, mission, objectives and expectations. |
| IT Goals and Objectives Not Realized | PO6 – Communicate Management Aims & Direction | PO6.5 – Communication of IT Objectives and Direction | |

## Using Audit Documentation to Improve Operational Efficiency through Business (and IT) Process Reengineering or Improved Business Process Management.

The value that an independent evaluator can provide in the review and analysis of business processes and practices is potentially significant [Champlain 2003]. When the internal audit function reports directly and independently to the audit committee of the board of directors [e.g., see Hall and Singleton 2005, p. 5], they have an ideal platform to assess IT and business processes from a fresh perspective. Such independent vision can facilitate the identification of new opportunities (e.g., for implementation of best practices) in governance and control. Auditors are trained to map processes and to dissect, analyze and critique existing processes, which allows for opportunities for improvements in operational efficiencies or effectiveness in addition to facilitating strategic objectives. For example, IT auditors can identify redundant processes as well as controls gaps and optimize the controls structure mix to mitigate the most risk for the least cost.

The IT auditor may have other advantages in identifying potential opportunities. The IT auditor is independent of the politics of the day-to-day operations and should be able to provide honest feedback regarding operational

performance. The IT auditor should have a "big picture" perspective of the organization that allows the auditor to see how processes interact with one another, i.e. to see the larger business process and any bottlenecks that may exist. Finally, the IT auditor should be able to provide information regarding competitive best practices. For example, an IT audit manager in the internal audit department of a large, midwestern financial services institution (wishing to remain anonymous) explained to us that the company's audit methodology requires the development of risk and controls matrices and process/system/data flow diagrams in almost every technology and process audit performed. This information serves a very useful purpose to corporate management looking to re-align or better control business processes. These documents are not only part of the audit work papers, they are available to the management of the area being audited to use as they deem appropriate.

Furthermore, a partner at one of the large, international accounting firms observed that the IT audit of one of its clients revealed several areas where processes could be streamlined or standardized. The audit identified six different methods to process cash receipts, and the client was able to create one standard process for use at all of the cash collection centers. The audit also found several different processes for granting access to applications, which the client was able to replace with one process with centralized control. The client was also able to reduce multiple, separate data centers to one center with appropriate backup and recovery procedures, thereby mitigating the risk of not being able to recover quickly from a disaster.

### Using Audit Observations to Improve Risk Mitigation through Enterprise Risk Management (ERM) Awareness

Risk management is a significant component of corporate IT governance [ITGI 2005]. Overall enterprise risk management consists of a "structured, consistent and continuous process across the whole organization for identifying, assessing, and deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives" [IIA 2004, p. 3]. Although ERM is clearly the responsibility of the board of directors and senior business management, which is a key point with respect to audit's need for independence, IT audit observations can increase the visibility of overall risk management and specific high-risk information assets and systems. Roles thus appropriate for IT audit in the context of ERM include: championing the establishment of ERM by senior management, critiquing risk management practices, and providing assurance on risk management processes, including the accuracy of risk evaluations [IIA 2004].

Sutton and Arnold [2005, p. 125] argue that, because of SOX, the "CIO has little choice other than to become a key participant in the governance and risk management process — and seemingly a leader in both areas." One key reason for this IT management requirement is that many significant threats to an organization's operations can arise from external technology linkages (with customers and business partners) and from electronic data repositories. For example, Champlain [2003] points out an IT audit identifying a control weakness in a wire transfer system's security parameters that exposed the entire amount of all wire transfer transactions, valued at over one billion dollars, to potential losses.

### Improved Business Continuity Planning and Associated Systems Disaster Recovery Planning

Ensuring that an organization is capable of continuing to provide value to its stakeholders in the event of some substantial business disruption is a vital component of corporate governance [Cascarino 2007], and thus a key responsibility of executive management. In order for an organization to recover from a disaster and be able to function as a business and process transactions, the organization needs a clearly detailed business continuity plan (BCP) and a complementary systems disaster recovery plan (DRP). Executive management has the key role in the prioritization of business processes, making associated risk assessments, and in the planning and development of continuity plans for the organization. While the IT function should play a significant role in the development and design of IT recovery strategies to meet business needs, delegating the entire task to IT could result in significant gaps in the continuity plans and lead to failure during an actual disaster [Kothari 2007]. IT auditors play an important role in providing audit oversight over BCP and DRP by independently evaluating the processes for developing, testing, and deploying these plans [Muthukrishnan 2005]. The IT Audit function should thus work closely with both the business side of the organization and with IT to identify significant continuity risks and to align the BCP strategy "to attain an acceptable level of readiness that matches the risk appetite of the organization" [Kothari 2007, p.25].

### Improved Systems Development Quality

IT auditors are concerned with the quality of controls within and over the system development life cycle and have an important role in assuring systems development quality, such as reviewing policies, processes, and plans around feasibility studies, software development, and system conversions [Cascarino 2007]. Being integrally involved in these phases on the systems development life cycle may even include placing an auditor in a consultant role on an IT project development team, where the auditor is a "non-voting" member of the team. Accordingly, the audit function can provide comfort to business managers that the ultimate systems will be delivered as required to meet

business objectives and will fall within capital budgeting investment guidelines. Moreover, auditors can ensure that adequate controls are built into the system from the very beginning, not as an afterthought when they would be very expensive to incorporate. As an example of improving quality, the IT audit department of the large, midwestern financial services firm cited previously made a successful case, based on root cause analyses of project failures, that the enterprise should change to a Project Management Office (PMO) approach for developing systems. This approach places a focus on providing professional project management on all significant systems development initiatives in the company.

Cardinal Health Corporation is a major global manufacturer and distributor of medical supplies and technologies, and they illustrate another example of value-added IT audit practices. Cardinal's internal IT audit function is integrally involved in large project implementation reviews, such as providing consultative advice and recommendations on control frameworks. Their projects have included a critique of their PMO, a project expense and capitalization review, an interface and conversion review, a critical reports review, and process control framework reviews. Cardinal's IT audit organization also assists in evaluating potential relationships with third parties, such as assisting the corporate due diligence team in touring and reviewing the physical and environmental controls over enterprise resource planning (ERP) servers in overseas data centers as part of a human resources outsourcing agreement.

Lawton [2007] argues that the IT function can overcome the burden of compliance by seeking value-added steps to meet requirements in an efficient manner by adopting (and adapting) control frameworks, such as ITIL and COBIT, to meet the control requirements for legislative regulations. He discusses an explicit systems development change management example at Employers Insurance Company of Nevada which "added value" to the IT function by implementing the ITIL framework for managing change and mapping it to COBIT. This model allows the company to focus on five key change management control objectives and create a disciplined, manageable, repeatable, and sustainable process that meets its compliance requirements (such as SOX and HIPAA) and automatically generates appropriate evidence for audit purposes, thereby enabling better IT governance.

### Increased Organizational Communication and Trust Development through Facilitation among Various Stakeholders

Auditors are also in a unique position to act as a catalyst for change and for providing a communications channel to facilitate organizational change management [Bassett 2007; Champlain 2003]. Because auditors are independent, they can serve as an effective liaison (e.g., without fear of reprisal) between IT management and the board, between IT management and IT staff, and between IT management and the business functions (including system users). For example, if IT auditors can illustrate how poor data quality can lead to reduced customer service and/or lost revenues (such as when data are inconsistent across data repositories), then organizational resources may be made available from top management to automate input processes. This automation would lead to increased data quality that would result in better information from the systems that rely on the data stores and ultimately to enhanced decision making by management. The resulting perception, by the business unit, of better information because of the cleaner data may not necessarily lead to significant accolades for IT management, but could conceivably result in increased trust in making IT investments for supporting the business, in addition to fewer data management complications for IT operations.

## VI. CASELET EXAMPLE OF ADDITIONAL RESEARCH: APPLICATION OF OUR MODEL TO A LARGE CORPORATION'S IT AUDIT FUNCTION

In this section we provide a brief case, or caselet, that illustrates value-added IT audit activities performed by a global banking and financial services firm with over a trillion dollars in assets. We henceforth refer to this firm as "XYZ Corporation" to preserve anonymity. In focus group sessions with XYZ internal auditors (using the same process described in Section IV), the internal auditors of XYZ identified numerous factors that map to the categories in Figure 1. These include a consistent audit methodology (audit process category), experienced staff with appropriate technical skills (technical competency category), and the allocation of adequate time for engagements and the utilization of automated auditing tools (IT audit-controlled organizational factors category). Given that these factors tend to be controlled by IT audit management, we argue that this organization exhibits key characteristics of having a quality IT audit process.

XYZ's IT audit manager estimates that 25 percent of their annual audit coverage is focused on value-added activities. This is not surprising, given the evidence that the firm is operating in a manner that should produce a quality IT audit product (in the form of an annual risk-based audit program), thus freeing up resources for value-added projects. Moreover, this manager emphasizes that the real value-added benefit that comes from their function is mostly due to the key requirement of being independent (both in form and in appearance) from the areas that they

examine. This focus on the importance of independence is one of the major benefits he sees that resulted from the visibility that the internal audit function gained because of SOX.

The value-added areas within their annual audit coverage include three main categories: "all-hands" projects, oversight/governance, and system change activities. All-hands projects are infrequent, but major initiatives that require an integrated audit and business unit approach to meet some important IT requirement for the enterprise, including compliance and strategic business opportunities. One example is a regulatory data reporting requirement from a banking industry governmental oversight agency that required the close examination of eighty thousand loan files for compliance. Governance and audit oversight is particularly focused on escalating emerging trends that are of concern, such as identified technology risks within a line-of-business or the entire firm, up to the audit committee of the corporation's board of directors. One way they identify such trends is by having the business owners complete control self assessments at various sub-divisions within the enterprise, such as at the business unit level, at the business processes level, or for individual applications.

System change activity audits provide early identification of process risks, control design weaknesses, and testing deficiencies. For example, when XYZ was converting to check processing of images rather than the actual paper checks, IT audit gained a non-voting (i.e., independent) seat on this major project's governance board. Furthermore, when the firm was investigating a new mortgage servicing platform, IT auditors voiced performance concerns over the business unit's preferred vendor, and the firm heeded this advice and eventually chose another vendor.

## VII. INFORMATION TECHNOLOGY AUDIT RESEARCH AGENDA

In addition to the specific research opportunities we mention in the discussion of the model of IT audit quality, we note several other research possibilities that would help to build a cumulative body of knowledge about IT audit. First, we call for additional research into the factors that are antecedents to IT audit quality, both for effectiveness and for efficiency. Our model of success factors gleaned from IT auditors from internal audit departments in corporations could be tested by other researchers, perhaps via a survey or qualitatively via a case study (similarly to our caselet in Section VI). Another similar model developed from research with IT auditors in public accounting might be informative, if only to see if the factors are comparable. It would also be interesting to test our contention that a quality audit process (facilitated by the critical success factors we identified) leads to a quality product. More work into identifying value-added IT audit services could prove invaluable for practitioners looking for more justification for the resources consumed by the IT audit function. Perhaps these last two areas could be the focus of a combined study, presumably of an organization that manages the quality factors related to IT audit in a manner that allows them to provide more value-added services.

## VIII. CONCLUSION

Efforts directed at conforming to the rules and regulations of SOX should be regarded as much more than a compliance requirement. Meeting these requirements also affords an opportunity to establish governance frameworks and to form value-added partnerships between IT management and IT auditors. Partnership initiatives can also enhance senior management's understanding of IT's role in corporate governance and ultimately lead to better business decision making by providing timely and higher-quality information. Moreover, the high quality IT audit process we outline should free up resources to devote to developing such partnerships. This contention is the essence of the contribution from our research. By following a sound IS audit methodology focusing on success factors (e.g., consistent communications with IT management), an organization can deliver high quality IT audits that meet the requirements of a risk-based assurance program while simultaneously delivering value-added governance services to the organization. These value-added services can contribute to a quality IT audit process because of the partnership nature of the IT auditor-IT management (i.e., the auditee) relationship that will develop over time. In short, an IT governance partnership can be a win-win scenario for the entire enterprise.

### Notes:

Earlier versions of portions of this paper were presented at Americas Conference on Information Systems (AMCIS) in August, 2007, and at the Workshop on Information Security and Privacy (WISP) in December, 2007.

We recognize the assistance of Samantha Ducheny, Tracy Heckmann, and Steven Peach, three students in Miami University's Masters of Accountancy program, on the application of COBIT to the key risks in the banking industry.

## REFERENCES:

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers, who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The authors of the Web pages, not CAIS, are responsible for the accuracy of their content.
4. The author of this article, not CAIS, is responsible for the accuracy of the URL and version information.


Bassett, J. (2007). "Closing the IT Audit Communication Gap," *ITAudit*, vol. 10, May 10, 2007, www.theiia.org/ITAudit/index.cfm?act=ITAudit.home&aid=2654.

Blecher, M. (2007). "Outsourcing IT Governance to Deliver Business Value," *Information Systems Control Journal*, v4, 2007, pp. 13-14.

Cascarino, R. E. (2007). *Auditor's Guide to Information Systems Auditing*, John Wiley & Sons, Inc., Hoboken, NJ, pp. 249-250, 289, 339-348.

Champlain, J. J. (2003). *Auditing Information Systems*, 2nd ed., John Wiley & Sons, Inc., Hoboken, NJ.

Choobineh, J., G. Dhillon, M. R. Grimaila and J. Rees. (2007). "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems*, 20(57), pp. 1-28.

DeHaes, S., and W. Van Grembergen. (2008). "An Exploratory Study into the Design of an IT Governance Minimum Baseline through Delphi Research," *Communications of the Association for Information Systems*, 22(24), pp. 443-458.

Delbecq, A. L., A. H. Van De Ven, and D. H. Gustafson. (1982). "Guidelines for Conducting NGT Meetings," in D.R. Hampton, C.E. Summer and R.A. Webber (eds.), *Organizational Behavior and the Practice of Management,* Glenview, IL: Scott, Foresman, and Company, pp. 279-298.

Federal Reserve System (1995). "SR 95-51 (SUP): Federal Reserve Guidelines for Rating Risk Management at State Member Banks and Bank Holding Companies," Board of Governors of the Federal Reserve System, Washington, D.C., http://www.federalreserve.gov/boardDocs/srletters/1995/sr9551.htm

Hall, J. A. and S. L. Liedtka. (2007). "The Sarbanes-Oxley Act: Implications for Large-Scale IT Outsourcing," *Communications of the ACM*, Mar 2007, Vol. 20, No. 3, pp. 95-100.

Hall, J. A., and T. Singleton. (2005). *Information Technology Auditing & Assurance*, 2nd ed., Thomson, South-Western Publishing, p. 5.

Havelka, D. J. and J. W. Merhout (2007). "Development of an Information Technology Audit Process Quality Framework," Proceedings of the Thirteenth Americas Conference on Information Systems (AMCIS 2007), Keystone, CO, August 8-12, 2007.

IIA (The Institute of Internal Auditors). (2004). "The Role of Internal Auditing in Enterprise-wide Risk Management," September 29, 2004 Position Paper, www.theiia.org/guidance/standards-and-practices/position-papers/current-position-papers/

ITGI (IT Governance Institute). (2005). *Information Risks: Whose Business Are They?*,www.itgi.org.

ITGI (IT Governance Institute). (2006). *IT Governance Global Status Report—2006*, www.itgi.org.

ITGI (IT Governance Institute). (2007a). *Control Objectives for Information and Related Technology* (COBIT 4.1), www.isaca.org.

ITGI (IT Governance Institute). (2007b). *IT Governance Implementation Guide: Using COBIT ® and Val IT™,* 2nd Edition, www.itgi.org.

ITGI (IT Governance Institute). (2008). "About IT Governance." http://www.itgi.org/template_ITGI.cfm?Section=About_IT_Governance1&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19657

Kerstetter, T. K. and K. J. Porrello. (2007). "2007 Board and Information Technology Strategies Report: Maximizing Performance Through IT Strategy," *Corporate Board Member*, 2007 Special Supplement, www.boardmember.com.

Kothari, P. (2007). "Is Your Business Continuity Plan a Paper Tiger?" *Information Systems Control Journal*, v3, 2007, pp. 25-26.

Kumar, P. (2006). "The Technological Auditor: How Automation Is Changing Auditors' Roles," *Information Systems Control Journa*, v5, 2006, pp. 41-42.

Lampe, J. C. and S. G. Sutton. (1994). "Evaluating the Work of Internal Audit: A Comparison of Standards and Empirical Evidence," *Accounting and Business Research* 24(96), pp. 335-348.

Lawton, R. (2007). "Transitioning IT from a Compliance to a Value-driven Enterprise Using COBIT," *Information Systems Control Journal* v6, 2007, pp. 43-44.

Luftman, J., R. Kempaiah, and E. Nash. (2006). "Key Issues for IT Executives 2005," *MIS Quarterly Executive* 5(2), June 2006, pp. 81-99.

Mishra, S. and H. R. Weistroffer. (2007). "A Framework for Integrating Sarbanes-Oxley Compliance into the Systems Development Process," *Communications of the Association for Information Systems* 20, pp. 712-727.

Merhout, J. W. and D. J. Havelka (2007). "Maximizing the IT Audit Bang for the Buck: Increasing the Benefit/Cost Ratio of Complying with Sarbanes-Oxley," Second Pre-ICIS Workshop on Information Security and Privacy (WISP 2007), Montreal, Canada, December 8, 2007.

Muthukrishnan, R. (2005). "The Auditor's Role in Reviewing Business Continuity Planning," *Information Systems Control Journal* v4, 2005, pp.52-56

Schaafsma, S., J. Spangenberg and P. Williams. (2007). "Empirical Research into Val IT Supports the Use of COBIT," *Information Systems Control Journal* v5, 2007, pp. 31-32.

Shabudin, E. (2007). "An Operational Risk Framework." *The RMA Journal* 89(9), pp. 44-47.

Sutton, S. G. and V. Arnold. (2005). "The Sarbanes-Oxley Act and the Changing Role of the CIO and IT Function," *International Journal of Business Information Systems* 1(1/2), pp. 118-128.

Van de Ven, A. H., and A. L. Delbecq. (1971). "Nominal Versus Interacting Group Processes for Committee Decision Making Effectiveness," *Academy of Management Journal* 14(2), pp. 203-212.

Van de Ven, A. H., and A. L. Delbecq. (1974). "The Effectiveness of Nominal, Delphi, and Interacting Group Decision Making Processes," *Academy of Management Journal* 17(4), pp. 605-621.

Van Grembergen, W. (ed.) (2003). *Strategies for Information Technology Governance*, Idea Group Publishing.

## APPENDIX A: IT AUDIT QUALITY FRAMEWORK WITH FACTORS IDENTIFIED

| Table A1. Audit Team Factors | | |
|---|---|---|
| **Factors** | **# Groups Identifying** | **# Groups Rated As Critical** |
| Audit team characteristics: Team work ethic; character and integrity; willingness to learn; Team cohesiveness, ability to "get along," Team dynamics/synergy (individuals' personality) | 4 | 4 |
| Motivation of team, "sense of urgency" | 2 | 2 |
| Diversity of team (e.g., thoughts; ways of doing multiple measures; background; experiences) | 1 | 0 |
| Auditor-in-charge (e.g., manager) needs balance (should not feel overwhelmed) | 1 | 1 |

| Table A2: Audit Process & Methodology Factors | | |
|---|---|---|
| **Factors** | **# Groups Identifying** | **# Groups Rated As Critical** |
| Audit methodology is used. | 5 | 5 |
| Sufficient time is allocated to execute the audit (especially field work). | 5 | 5 |
| Effective reporting mechanisms, distribution to client organization, audit committee, and finance, communicate project results to appropriate level. | 4 | 3 |
| Follow-up on issues (close out observations, persistence), Observation/follow-up methodology (did they respond) | 2 | 2 |
| Risk assessment process - use of continuous process | 2 | 2 |
| Documentation (work product) standards. Document results to appropriate level of detail (as evidence to support findings, to be able to re-perform work, for efficiency, over-doc). | 2 | 1 |
| Review of prior audit work | 2 | 2 |
| Risk-based audit approach, understandable risk assessment model to auditee and audit team. | 2 | 2 |
| Representative sampling | 2 | 2 |
| Timely oversight, feedback, review; adequate supervision | 2 | 1 |
| Project management | 2 | 2 |
| Design of quality test steps | 1 | 1 |
| Identify control gaps & assigning ownership to remediate | 1 | 1 |
| Metrics to measure quality (metrics vs standards) | 1 | 1 |
| Control identification (Preventative, Detective, Corrective categorization). | 1 | 1 |
| Being able to see impact of work (of audit) | 1 | 1 |
| Review of fieldwork and reporting by a higher level person (ensure consistent reporting). | 1 | 1 |
| Long-term audit plan (goals) | 1 | 1 |
| Adequate testing. Testing performed meets objectives, tests assertions, and supports conclusions. | 1 | 1 |
| Timing of audit | 1 | 1 |
| facilitation/collaboration techniques | 1 | 1 |
| Flexibility (time) - able to change schedule | 1 | 1 |
| Coordination w/ external auditors | 1 | 1 |
| Quality assurance process (internal) - audit the auditors. | 1 | 0 |
| Conflict management. | 1 | 1 |
| Documentation templates / forms | 1 | 0 |
| Planning. Timing and duration of planning are adequate and comprehensive. | 1 | 0 |

| Table A3. Client-Controlled Organizational Factors | | |
|---|---|---|
| **Factors** | **# Groups Identifying** | **# Groups Rated As Critical** |
| Support, cooperation, and buy-in exist from the client, auditee, and top-level (executive) management | 5 | 5 |
| Client relationships, quality and responsiveness, honesty and openness | 5 | 5 |
| The amount of organizational change, e.g. M&A, divisional restructuring, internal process change, and the organization's ability to manage the changes | 5 | 5 |
| Client understanding of audit process (and purpose of the audit) | 3 | 3 |
| Complete, timely, and accurate data/info from client (e.g., via database or inquiry), documentation | 3 | 3 |
| Separation of management from operations - level employees of audited group, Segregation of duties (SOD) / analyst not the code | 2 | 1 |
| One system platform (e.g., SAP) or "spaghetti" systems. | 1 | 1 |
| Feedback mechanism from auditee/post-audit | 1 | 1 |
| IT organization/client morale | 1 | 1 |
| Client's mgt participation in definition of audit scope | 1 | 1 |
| Client understanding of business process (i.e. their own area) | 1 | 1 |
| Realistic expectation of audit | 1 | 1 |
| Impact of audit rating/findings on auditee management's annual review or consequences to the business | 1 | 1 |
| Number of different recent audits (external and internal) in a particular area. | 1 | 1 |
| Does business follow/embrace SDLC methodology? | 1 | 1 |
| Auditee's perception of auditor | 1 | 1 |
| Environment of audit-physical location | 1 | 1 |
| SOX controls contained in the control framework | 1 | 1 |
| Business interruption (auditee not available/system down) | 1 | 0 |

| Table A4. IT Audit-Controlled Organizational Factors | | |
|---|---|---|
| **Factors** | **# Groups Identifying** | **# Groups Rated As Critical** |
| Computer-assisted auditing tools (CATs, e.g. ACL) are available and used for testing and analysis. | 4 | 4 |
| Internal policies and procedures, external regulations, standards, and best practices are followed. | 4 | 4 |
| The level of experience of the IT audit staff | 4 | 4 |
| Resource availability, time, and budget constraints | 3 | 3 |
| Resources available for the audit; staffing, tools, etc. | 3 | 2 |
| Management, support, and direction of the internal audit team including vision, mission, leadership of IT audit | 3 | 3 |
| The audit organizational structure and reporting relationships to audit committee and auditees (independence) | 3 | 3 |
| IT audit staff management. Ability to attract & retain IT audit staff (recruitment, turnover of IT auditors) | 2 | 2 |
| Defined roles and responsibilities on the audit team and within the audit organization | 2 | 2 |
| Audit division feedback | 1 | 1 |
| Level of distractions (e.g., special projects, such as investigations that interfere) | 1 | 1 |
| Maturity of IT audit organization | 1 | 1 |
| Audit team reward structure must match enterprise (and client) objectives (e.g. # of findings vs. impact on openness of client) | 1 | 1 |
| Resources to create and document audit plan: databases, online forums (e.g., auditnet.org), tools, Web sites, services | 1 | 0 |

| | | |
|---|---|---|
| Governance level issues (communication among IT audit staff) | 1 | 0 |
| "Desktop" auditing - analytics | 1 | 0 |

**Table A5. IT Audit Personnel Technical Competency Factors**

| Factors | # Groups Identifying | # Groups Rated As Critical |
|---|---|---|
| Competence of the IT auditor and client personnel | 3 | 3 |
| Training & Development | 3 | 2 |
| Understand why technology is being used and the associated risks | 2 | 1 |
| Understand business rules (does code match), subject matter | 1 | 1 |
| System code understanding | 1 | 1 |
| Level of technical expertise | 1 | 1 |
| Understand output of testing results | 1 | 1 |
| Auditor understanding of supported business processes | 1 | 1 |
| Auditor judgment (e.g., assessment of risk rating) | 1 | 1 |
| Ability to identify control weaknesses | 1 | 1 |
| Report writing/documentation skills | 1 | 1 |
| Knowledge and ability to use audit tools | 1 | 0 |
| Knowledge of technology infrastructure within the organization, knowledge of systems integration | 1 | 0 |

**Table A6. IT Audit Personnel Social & Interpersonal Factors**

| Factors | # Groups Identifying | # Groups Rated As Critical |
|---|---|---|
| Interpersonal skills of auditors, including written and oral communications skills | 4 | 4 |
| Knowledge of business of auditee (industry, organization, and business unit) | 2 | 2 |
| Effective work/life balance & job satisfaction | 1 | 1 |
| Auditor decision making skills | 1 | 1 |
| Willingness to change, ability to change (individual level) | 1 | 1 |
| Ability to build consensus or solutions | 1 | 1 |

**Table A7. Enterprise & Organizational Environment Factors**

| Factors | # Groups Identifying | # Groups Rated As Critical |
|---|---|---|
| Communication between auditor & auditees before and during fieldwork, diplomacy (tradeoff b/w forceful and good rapport) | 3 | 3 |
| Negative stigma of word "audit" →"review" would be nicer | 2 | 1 |
| Integration of IT audit into the F&O (financial and operations) audit plan, coordination between F&O & IT auditor | 2 | 2 |
| Organizational communication | 2 | 1 |
| Control environment (degree of control) | 1 | 1 |
| Legal and regulatory guidelines and requirements | 1 | 1 |
| Size of IT audit org in relation to size of company | 1 | 1 |
| Healthy corporate culture | 1 | 1 |
| Media attention | 1 | 0 |
| Organization/dept. politics | 1 | 0 |

| Table A8. Target Process or System Factors | | |
|---|---|---|
| **Factors** | **# Groups Identifying** | **# Groups Rated As Critical** |
| Project objectives and scope are clearly defined and planned. | 5 | 5 |
| The complexity, type (in-house v COTS), and size (volume) of the application, system, transactions, or unit being audited and the IT environment | 3 | 2 |
| Well-defined organizational standards & processes (of auditee)/adequate documentation) | 2 | 0 |
| Accuracy/reliability of data in system | 1 | 1 |
| System flow charts | 1 | 1 |
| Overall risk rating of area being audited | 1 | 1 |
| Routine audit vs. non-routine special project | 1 | 1 |
| Auditability of system being audited | 1 | 1 |
| Manual w. automated process under audit | 1 | 1 |
| Existence and effectiveness of key controls and their effect on testing. | 1 | 1 |
| Primary intention/use of system by auditees/ everyday | 1 | 1 |
| Availability of documentation | 1 | 0 |
| Intent of audit (any hidden agendas/objectives) | 1 | 0 |

## ABOUT THE AUTHORS

**Jeffrey W. (Jeff) Merhout** is an Assistant Professor of MIS at Miami University in Oxford, Ohio. He holds a Ph.D. and MBA from Virginia Commonwealth University, and is a Certified Public Accountant (Inactive). He has two years auditing experience in public accounting and another year as an operational internal auditor. His current research interests focus on: qualitative methodological issues, particularly in positivist case studies; pedagogical issues, such as adult training and development; and information risk management, IT security and information systems auditing. He has presented and published his research at numerous MIS conferences and in journals, including the *Communications of the ACM, Journal of Information Systems Education,* and *Information Systems Control Journal*.

**Douglas Havelka** is an Associate Professor of Management Information Systems in the Farmer School of Business at Miami University. He received a Ph.D. in MIS from Texas Tech University and is a C.P.A. in Ohio. Prior to joining Miami, Dr. Havelka worked for AT&T as an industry negotiator for Electronic Communication Standards.

Communications of the Association for Information Systems

ISSN: 1529-3181