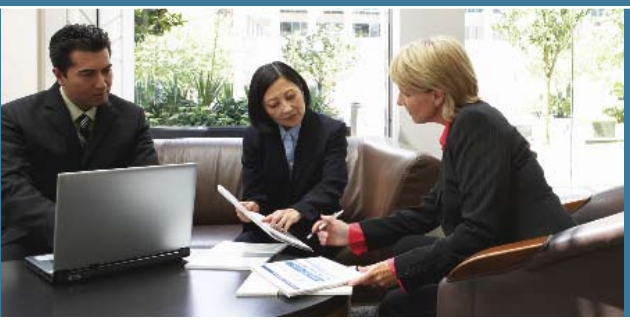


High Value Audits: An Update on Information Technology Auditing

Edward Hill, Managing Director
Robert B. Hirth Jr., Managing Director

protiviti®
Independent Risk Consulting

The technology landscape and its impact on internal audit

Technology is playing an ever-growing role in how organizations achieve their business objectives. In this environment, it is increasingly important to assess appropriately technology vulnerabilities and risks as they relate to critical business processes. As an organization develops a suitable internal audit plan, risks related to the use of technology left unaddressed or partially addressed result in an incomplete plan, at best. At worst, they expose an organization to huge risk and potential, or even likely, failure.

An organization's top executives, board of directors and audit committee members look to information technology (IT) management for effective oversight of IT risks. The controls in place to manage these risks are an essential part of the internal control environment and structure. These same executives look to internal audit to evaluate whether IT risks are appropriately understood, managed and controlled. This important check and balance, or creative tension, forms an integral part of today's corporate governance process.

In order to adequately address technology risk, organizations must have the appropriate technology skill sets. Recently, Protiviti conducted a survey in which it asked chief audit executives, as well as their internal audit directors, managers and other professionals, to determine how they perceive their departments' capabilities concerning internal auditing, where they currently see a need for improvement, and how they prioritize those needs.[1] Survey respondents rated auditing skill sets around IT change management, security, computer operations, program development and business continuity as having the lowest average competency of all the internal audit process skills listed in the questionnaire.

Evolving technology and technology trends contribute to the skill and capability gap (see Table 1), and drive new IT risks that create further challenges for internal audit departments. For example, an organization may have a customer-facing Internet application with multiple technology layers. These layers most likely include a middleware component that is overlooked by many audit organizations based on the fact that middleware expertise does not exist within the audit department. As a result, the audit scope may not even include a middleware component that may be responsible for interface controls, data mapping, currency conversion and presentation of data.

The demand for qualified and experienced IT audit professionals continues to be high and is not likely to diminish. Competition for talent with the vast array of skills needed to address technology risks makes it challenging to achieve the staffing levels needed for an effective IT audit function. In addition, because systems and applications are often numerous and complex, it is difficult to hire and retain individuals with the precise skills necessary to fulfill a complete annual audit plan. As a result, organizations continue to look for outside assistance with IT auditing. For example, financial systems, customer relationship management solutions, network operations, data warehouse management and information security all require different technical skills for effective auditing.

Table 1: Overall Results,* Audit Process Knowledge

"Need to Improve" Rank	Audit Process Knowledge	Competency (5-pt. scale)
1	Computer-Assisted Audit Techniques (CAATs)	3.0
2	Continuous Auditing	3.1
3	Data Analysis Tools: Data Manipulation	3.0
4	Data Analysis Tools: Statistical Analysis	3.0
5	Auditing IT: Program Development	2.9

*Results are discussed in Protiviti's *2008 Internal Audit Capabilities and Needs Survey.*

[1] For more information, see Protiviti's *2008 Internal Audit Capabilities and Needs Survey*, available at **www.protiviti.com**.

Over the past year or so, many companies have begun to pay more attention to the link between IT risks and business risks as they relate to Sarbanes-Oxley Act compliance. In the first few years of the compliance requirement, most companies and their external auditors erred on the side of caution and put everything they could think of into scope. If there was any question about whether a certain process was in scope, auditors typically included it. It is generally agreed that too much work was initially performed on IT controls related to the Sarbanes-Oxley assessment of internal control over financial reporting. This had two results that no organization wants: unnecessary work and unnecessary cost. The focus on Sarbanes-Oxley compliance also had two other negative consequences for many IT audit departments. First, the audit effort focused on "IT General Controls" for financial systems, which lessened the focus on other technology risks. Second, it may have caused "erosion" of the skills of the IT auditors due to the narrow focus of the IT Sarbanes-Oxley work.

Effective view of technology risk

Once an organization has achieved initial Sarbanes-Oxley compliance, efforts begin to shift toward maintaining compliance while working to drive down compliance costs and improve the balance of audit coverage for other areas of risk. According to Protiviti's 2007 Internal Audit Rebalancing survey,[2] after having been consumed with Sarbanes-Oxley compliance projects for the past four years, 24 percent of companies report their internal audit departments have achieved "rebalancing" – a renewed focus on their traditional responsibilities that is balanced with compliance activities. This number is more than double the response (10 percent) from a similar survey conducted by Protiviti in 2005.

Thus, internal audit's focus once again should include a wider view of risk, often considering IT risk management, as well as the efficiency and effectiveness of IT operations. Achieving balance with the right focus involves approaching audit planning and execution as a two-step process. First, the organization must look at its risk profile and determine the right things to audit. As an organization develops its IT audit plans, key areas to consider include:

- The organization's business applications
- The IT infrastructure components (e.g., databases, operating systems, networks and data centers)
- The IT organization and processes
- The current year's IT-related projects and capital spending
- The organization's enterprise risk management (ERM) profile

The second step in developing the organization's audit plan – including the IT audit plan – is the performance of an enterprisewide risk assessment. As an organization considers the technology impact on the risk assessment, there are a number of risks that should be considered based on the organization's specific and often unique use of technology.

These risks include:	
• Reputation risk	• Sourcing and cycle time risk
• Compliance risk	• Product and service failure risk
• Business continuity (business interruption) risk	• Trademark and brand erosion risk
• Customer confidence and satisfaction risk	• Fraud risk

[2] See Protiviti's *Moving Internal Audit Back into Balance: A Post-Sarbanes-Oxley Survey*, available at **www.protiviti.com**.

As these risks are considered, a related question arises as to how an organization's use of technology impacts these risks. Consider, for example, reputation risk for a retailer that processes a majority of its sales using customer credit cards. In today's retail industry, if there is a breach of security resulting in the theft of customer names, credit card numbers and other information, public disclosure of the breach and notification of the customers may be required by law (depending on the state in which the breach occurred). This obviously creates a risk to the organization's reputation that should be addressed in the risk assessment and most likely in the annual audit plan. This entity would in all likelihood have a Payment Card Industry (PCI) risk assessment and audit included in its annual audit plan.

The development of an appropriate IT audit plan takes into account the organization's overall risk assessment from its use of technology, as well as which technology components (from those that make up the technology audit universe) should be addressed to mitigate the areas of highest risk. An organization must consider carefully the risks, and through discussion with senior executives, the audit committee and the board of directors, agree upon an annual plan suitable for the organization given its risk tolerance, resource allocation and that year's operations, projects and activities.

Adopting a competency approach to IT auditing

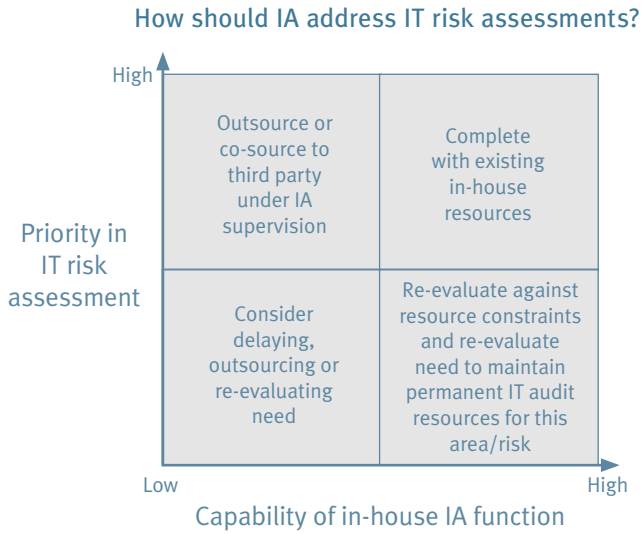
Once the audit plan has been finalized, the organization must determine the skills necessary to complete the plan, including various IT audits that have been identified. To formulate a comprehensive view of a company's IT audit skills and knowledge, management and the audit committee should see that the chief audit executive implements a well-defined competency model and approach to IT auditing. Part of this competency-based approach is to link the audit areas to the skills needed to audit each area. Some assume that IT audit involves a single set of skills and that broad IT knowledge is sufficient for executing all IT audits. However, in today's complex business and technical world, a much wider array of skills and technical knowledge is typically required for effective IT auditing. The internal audit function – whether it is in-house, co-sourced or outsourced – should have specialties in a number of IT audit competency areas, such as those listed below:

- IT governance and management
- IT risk assessment and audit planning
- IT processes and operations (including system development life cycle and change management)
- Information strategy and data management
- Application controls and configuration
- Security and privacy
- IT infrastructure, technology components and configurations
- Data analysis and tools usage
- Disaster recovery

As an organization develops IT auditing capabilities, it should ensure that its IT audit group has an appropriate mix of skills. This mix should be based on the skills most needed (i.e., those skills used most often) by the organization. For example, it is common for an internal audit staff to have basic knowledge of application controls and configuration, IT general controls testing (a broad level of understanding specific to the IT environment), and IT risk assessment and audit planning. Thus, it is likely that an internal audit function can maintain the skills necessary to address the risks in these areas. However, more advanced skills are likely to be needed to address adequately all of the business's technology risks, processes, components and infrastructure.

Hiring a large staff to cover all of the necessary competencies requires a substantial budget, as well as fortitude in recruiting to locate the precise skills necessary in a tight labor market. Further, there may be

a number of IT audit areas where the audit skills are not needed full time. Organizations should determine what skills are desired in-house, and consider co-sourcing the audits where the required skills do not fit in the organization's standard competency profile.



Outside experts and resources can provide value in a number of ways that can help an organization improve business results, including:

- Providing audit coverage for previously neglected components of the IT risk universe
- Applying audit software and tools that may otherwise be cost-prohibitive to acquire
- Utilizing individuals who have extensive expertise in a given area
- Performing audits where a third party may be considered more credible
- Transferring knowledge to the in-house team
- Bringing new insights and suggestions for improvement based upon experiences gained at other organizations

High value IT audits

We at Protiviti have found that there are a number of IT audits frequently selected by audit committees, chief audit executives and others in the organization for their annual plans. A number of these audits have been determined to be "high value IT audits" because they fall into one or both of the following categories:

- Audits having a high value proposition as determined by the audit committee and internal audit leadership (who know and recognize the risks)
- Audits where the auditee is likely to challenge the capabilities of in-house audit resources in identifying useful observations, findings and improvement opportunities – where there is no resident "subject matter expert"

High value audits are designed to provide the audit committee and process owner with cutting-edge insights into the technology risks and related recommendations in the area under audit. The high value audit delivers actionable findings that drive the improvement of the organization's financial and business systems and business operations. For each audit, we have developed standardized work plans, sample deliverables and resource recommendations (e.g., requisite skills). In many cases, automated tools are used for more effective and efficient auditing.

The 10 most common high value IT audits are:

- Data privacy audits
- PCI reviews
- IT Infrastructure Library (ITIL) assessment audits
- Software licensing compliance reviews
- ERP (e.g., SAP and Oracle) configuration assessments
- ERP segregation of duties and sensitive access audits
- IT governance assessments
- IT performance management and metrics assessments
- Technology architecture evaluations and assessments
- Business continuity and disaster recovery assessments

A successful high value IT audit appropriately assesses technology risks and the control environment as they relate to critical business processes in a particular area. Having deep expertise in IT audits can help ensure the integrity, reliability and performance of these processes. Using the right methodologies, businesses realize more effective and efficient technology controls that better align the internal audit function with their business and IT strategies.

Protiviti's IT internal audit services

IT internal auditing helps a company understand the key technology risks and how well the company is mitigating and controlling those risks. IT internal audit also provides insight into the threats inherent in today's highly complex technologies.

At Protiviti, we believe that an IT audit plan should be based on a company's specific technology risk profile. We assist our clients in managing the technology risks and efficiently integrating technology with business processes. Protiviti provides a wide range of services for IT internal audit outsourcing and co-sourcing. The Protiviti methodology, which is both COSO- and COBIT-based, facilitates an overall IT internal audit management team (either Protiviti-led, client-led or in combination) with execution of individual projects by subject matter experts in each IT audit area.

For more information about the topics covered in this white paper or our IT internal audit services, please contact:

Edward Hill
Managing Director
713.314.5010
edward.hill@protiviti.com

Robert B. Hirth Jr.
Managing Director
415.402.3621
robert.hirth@protiviti.com

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting and internal audit firm composed of experts specializing in risk and advisory services. We help our clients solve problems in finance, operations, technology, litigation and GRC. Our highly trained, results-oriented professionals serve clients in the Americas, Asia-Pacific, Europe and the Middle East and provide a unique perspective on a wide range of critical business issues.

Protiviti is proud to be a Principal Partner of The IIA. More than 1,000 Protiviti professionals are active members of The IIA, and these members are involved with local, national and international leadership to provide thought leadership, speakers, best practices, training and other resources that develop and promote the internal audit profession.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Other relevant publications and resources from Protiviti:

- *Guide to Internal Audit: Frequently Asked Questions About the NYSE Requirements and Developing an Effective Internal Audit Function*
- *2007 U.S. Risk Barometer: Survey of C-Level Executives with the Nation's Largest Companies*
- *2008 Internal Audit Capabilities and Needs Survey*
- *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements*
- *Internal Auditing Around the World, Volumes I, II and III*
- *Moving Internal Audit Back into Balance: A Post-Sarbanes-Oxley Survey*
- *Top Priorities for Internal Audit in a Changing Environment*
- *Partnering with the Rest of the Board*
- *Guide to Enterprise Risk Management: Frequently Asked Questions*
- *Enterprise Risk Management in Practice: Profiles of Companies Building Effective ERM Programs*

In addition, Protiviti publishes *The Bulletin*, a periodic newsletter covering key corporate governance and risk management topics of interest to internal auditors, board members and C-level executives.

To request a complimentary copy of any of our publications, please visit **www.protiviti.com** or call **1.888.556.7420**.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti.com

1.888.556.7420