IT Audit Topics Research Symposium

Houston, Texas • Sunday, June 18, 2006

Symposium Facilitator: Steve Mar

On Sunday, June 18, more than 30 information technology (IT) and audit professionals gathered to attend the *IT Audit Topics Research Symposium*, organized by The IIA Research Foundation (The Foundation) and The IIA's Advanced Technology Committee (ATC). The aim of the symposium was to:

1. Evaluate IT audit research.
2. Create a pipeline and portfolio of IT audit topics.
3. Provide a source of IT topics for The IIA Research Foundation.
4. Provide a means to research and distribute IT audit topics to IIA members.

In addition to these objectives, topics discussed during the symposium will help The IIA promote emerging IT audit research projects that will serve as a springboard for future IIA technology initiatives and to increase interest in IT audit topics among researchers.

Microsoft Senior Director of IT Audit Steve Mar served as facilitator for the day-long event, which featured four research paper presentations on a variety of IT control management issues.

How the Symposium Came About

The Foundation and ATC recognized the importance of providing IIA members with IT audit research. As a result, the ATC formed a research task force. To generate IT audit topics, the task force surveyed IIA members, chapters, and ATC participants on potential topics. The ATC voted on the most promising topics and proposed the symposium idea to The Foundation's Board of Research and Education Advisors (BREA), which approved the symposium.

Symposium Planners and Other Contributors

- Carolyn Newman, President of Audimation Services; ATC member
- Don Sparks, Vice President of Audimation Services; ATC member
- Steve Mar, Senior Director IT Audit, Microsoft Corp.; ATC member
- Gene Kim, Chief Technology Officer, Tripwire; ATC member
- Cindy Heagy, Professor of Accounting, University of Houston, Clear Lake; symposium scribe
- Mark Salamasick, Director of Endorsed Internal Audit Program, University of Texas, Dallas; BREA member
- Douglas E. Ziegenfuss, Department of Accounting Chair, Old Dominion University; BREA member
- Charity Prentice, Vice President, The IIA Research Foundation
- Nicki Creatore, Operations Manager, The IIA Research Foundation
- Lily Bi, Manager Technology Practices, The IIA
- Raquel Filipek, Editor, *ITAudit*, The IIA

Presenters

- Bernice Lemaire, Director of Internal Audit, CA (Computer Associates)
- Kurt Milne, Managing Director, IT Process Institute
- Andrew Moore, Senior IT Staff Member, CERT Coordination Center, Carnegie Mellon University
- Hubert Glover, Professor, Howard University

Paper 1

Enterprise Risk Management — Linkages to Corporate Strategy Increases the Effectiveness and Efficiency of IT Risk Management

Presenter: Bernice Lemaire, Director of Internal Audit, CA

Synopsis

The first paper discussed how implementing the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) enterprise risk management (ERM) framework can enhance the efficiency of IT risk management and risk reporting efforts. The paper provided a quick overview of the COSO ERM framework, ways to identify business risk, as well as efficient and effective IT risk management practices IT auditors need to consider.

The paper's main hypothesis is that the earlier detection of excessive risk taking during an organization's business planning cycle will reduce rather than eliminate duplicate risk management activities and expensive last-minute mitigation efforts. To avoid last minute efforts, IT needs to be an integral part of the company's strategic planning process. In addition, IT risks need to be considered because they can change the company's control environment. IT also is critical to ensure operational assets are used effectively and maintain the integrity and reliability of the organization's financial reporting process.

According to Lemaire, implementing the COSO ERM framework should enhance the efficiency and effectiveness of IT risk management, business operations, and risk reporting. The ERM framework highlights the unique role that IT plays when identifying events or incidents that may affect the organization's ability to achieve its objectives. In addition, auditors can be an agent for change, and with the establishment of proper controls, they can help to facilitate and coordinate ERM initiatives.

COSO's ERM framework can help organizations improve their IT risk management efforts by:

- Aligning the company's risk appetite and risk strategy.
- Enhancing risk response decisions.
- Reducing operational surprises and losses.
- Identifying and managing multiple and cross-enterprise risks.

To identify risks using the ERM framework, auditors can help companies conduct an enterprisewide risk assessment. This also will help to identify any risks that are inconsistent with or in excess of the organization's risk appetite.

In terms of IT systems, IT controls, and risks, the ERM framework allows organizations to look at risks holistically as it implements an enterprise resource planning system. In addition, the framework enables IT auditors to understand where the company is headed and the business' planning process. One of the best ways for IT auditors to understand this planning process is by studying the company's strategic and operations plan. Studying the strategic and operations plan also will help auditors identify IT audit risks, IT controls issues, software development, and lifecycle management issues. Other plans auditors can examine to help the company align business strategies with IT risk considerations include the company's marketing plan and mergers and acquisitions plan.

Furthermore, auditors should consider auditing the organization's risk management processes around its strategic and operations plan, as well as identify the tradeoffs among investment, risks, and opportunities by objective. Questions auditors can ask include: Do the plans explain the interdependencies of risks among business units? And, are the plans developed in a silo, or are they the result of multiple business units discussing mutual opportunities and interdependencies of risk?

When reviewing the business objectives in the operations plan, auditors need to look for areas of business change. This enables auditors to obtain a predictive value on how the internal control environment might be changing, as well as identify how business objectives challenge IT processes and resources, the IT infrastructure, and the development, deployment, and management of IT systems. In addition, auditors can learn the opportunities each of the business objectives brings to the IT organization.

Paper 2

Understanding the Audit, Operations, and Security Performance Impact of IT Control Objectives

Presenter: Kurt Milne, Managing Director, IT Process Institute

Synopsis

The second paper consisted of a pilot study created in collaboration with Dr. Daniel Phelps of Florida State University, which explored the question, "Is there a business case for IT control?" To answer this question, the study asked 100 mandatory and 100 exploratory questions that examined the benefits of IT controls and whether these controls help to improve IT operations, security, and audit performance.

Determining whether IT controls help improve IT operations, security, and audit performance can help organizations make a case for their use, as well as show how specific IT controls can enhance the efficiency and effectiveness of business processes. According to Milne and Phelps, 80 percent of IT spending is used to run what's already in place. The use of efficient and effective IT controls can free IT resources for other kinds of activities.

Milne and Phelps looked at six categories of IT controls, as well as operations and security measures. They then analyzed the correlation and impact of those controls on performance measures (i.e., operational measures and security measures) by asking questions pertaining to specific aspects of IT controls. Questions asked include:

- Does the use of IT controls correlate with the performance measures collected?
- What activities have the biggest impact on each of the performance measures?
- Do foundational controls have a higher performance?
- Do companies using foundational controls have higher performance?
- What's the performance improvement potential for companies that don't have foundational controls in place versus those that do?

Results found that companies that had more controls in place had higher performance levels. In addition, a well-controlled process can help companies improve IT operations, security, and audit performance more effectively.

The pilot study also identified which subset of foundational controls are most important from a performance improvement perspective by conducting a cluster analysis of study participants, which identified the specific controls that are frequently used by top performers, medium, and low performers. These controls include, but are not limited to, operations and change management, as well as controls that measure the percentage of unplanned work, incidents, and service to administrative ratios.

Furthermore, controls that differentiate medium and low performers are activities that organizations use to build their control systems, while controls that differentiate top from medium performers center around change and configuration-related controls, including activities that sustain and continually improve their control systems. In addition, top performers have an environment in place that systemically maintains and sustains controls.

In terms of the performance improvement potential, the study found that top performers had significantly better improvement and performance in areas that have a big cost impact. Costly areas in which high performers succeeded included unplanned work, change success rate, and higher fix rates. For instance, fixing an incident after a call is first made is cheaper than escalating the call to an expert in the organizations or having to circle the call back.

The survey featured responses from 100 surveys collected from a mixture of operations, audit, and security professional representing different industries in North America. In the future, Milne and Phelps would like to repeat the study with a sample of 1,300 people to obtain higher confidence levels.

Paper 3

The Case for an IT Ops Learning Laboratory: Improved Understanding and Communication of IT Control Integration Through Business Management Simulation

Presenter: Andrew Moore, Senior IT Staff Member, Carnegie Mellon University's Computer Emergency Response Team Coordination Center

Synopsis

Building on the previous discussion, the third article — co-written by Rohit S. Antao a former student at Carnegie Mellon University's Information Networking Institute — provided information on a simulation and modeling study that analyzed the causal relationships between change controls and IT performance. As shown by field work of the IT Process Institute, change controls are critical to organizational success. Many high-performing organizations believe that change controls facilitate high performance and ease regulatory compliance, while low performers believe that change controls hinder recovery from performance problems and diminish productivity.

The model used in the study assumes organizations have enough staff to maintain a certain level of service availability given a fixed set of operational problems. Once this norm was established, the researchers examined what would happen if the organization was faced with additional operational problems. Two conditions were evaluated: One where the organization maintained a rigorous level of change control and another where the organization bypassed its change control to respond to the operational problem quicker.

Based on this these two scenarios, the simulation study found that strict change controls worsen business IT service availability in the short term. However, performance leveled off or improved in the long term. Hence, organizations displayed a "worse-before-better" behavior when strict change controls were used. In organizations with lax controls, good performance was sustained for a period of time at the beginning after which performance decreased.

The study also found evidence of a tipping point regarding change control. Increasingly rigorous change controls show added performance benefits involving service availability, but only up to a point. After that point change controls become bureaucratic — excessive change controls cost more than they are worth. One also can see evidence of diminishing returns from increased levels of change control. The authors have yet to determine the optimal level of change control based on return on investment.

The above observations indicate why organizations have such a difficult time adopting and maintaining rigorous change controls. To ensure effective change controls are implemented, Moore recommends that organizations evolve from a reactive change culture that focuses on fixes to artifacts to repair failed services, to a proactive change culture that focuses on handling fragile artifacts to improve change success. The improvement goal in the reactive approach is to minimize maintenance costs locally and make repairs more efficiently, whereas in a proactive culture, the goal is to optimize maintenance activities systematically and reduce the need for repairs.

In terms of the "worse-before-better" behavior, reactive change cultures focus on repairing problems as fast as possible to increase their availability in the short term, which reinforces the use of shortcuts. Therefore, things improve in the short them, but they get worse over time. This makes it difficult to determine a cause and effect relationship, especially when the effect is farther in time. A reactive change culture also makes it difficult to reinstate rigorous controls after a crisis.

In the future, Moore and Antao would like to develop a learning laboratory where professionals can learn the lessons associated with high-performing IT operations and understand how time delays affect managerial decision making exhibited in reactive organizations.

Special permission to use "The Case for an IT Ops Learning Laboratory" (c) 2006 by Carnegie Mellon University in proceedings of the IT Audit Topics Research Symposium is granted by the Software Engineering Institute.

Paper 4

Impact of Emerging IT Practices for Internal Controls

Presenter: Dr. Hubert Glover, Howard University

Synopsis

The final proposal was created in collaboration with Dr. Rajni Goel from Howard University and consisted of a research proposal. When conducted, the study will examine the impact of emerging IT practices on internal controls. More specifically, the study will identify whether IT has been developed and applied effectively as a tool to help support business processes and operations.

The study also will analyze whether there are risks associated with the use of a specific technology. For instance, at the beginning of the presentation, participants were asked to list the top technologies used by organizations today. Responses included radio frequency identification, mobile phones, wireless technology, digital rights management, e-commerce, nanotechnology, open source, the Internet, digital signatures, and data interchange.

Suggested hypothesis/research questions from participants included:

1. Have the inherent risks of new hardware technologies been identified, assessed, and mitigated by the organization?
2. Do internal auditors understand and review the company's risk assessment?
3. Is deployment of tools in the audit process effective?

In addition, part of the study will consist of a literature review on the subject and an examination of how organizations identify their use of controls on emerging technologies. Auditors, for example, could help organizations clarify what they are doing in terms of IT and internal controls, and how these controls address the use of new technology.

The next step of this proposal is to outline the specific technologies Glover and Goel will examine their study, develop the research questionnaire, and fine-tune the specific areas the research will explore.

Research Requests and Open Discussion

Synopsis

After the four presentations, symposium participants and observers provided their opinion on the four papers presented and suggested ways to improve the research proposals discussed. The purpose of this session was to help each of the presenters get feedback from experts in the fields of technology and IT auditing that would enable them to fine-tune their research papers prior to submitting their proposals to The IIA Research Foundation for funding.

Areas for improvement on each of the four presentations included:

- Further refining each of the hypotheses or research questions.
- Expand the testing approach and methodology.
- Define the research deliverables.
- Commit to a research timeline.

The day ended with an interactive discussion of which IT controls are most important to increase enterprisewide effectiveness and efficiency and the benefits of conducting research in the area of IT controls. IT controls identified included change, access, and automation controls.

Symposium attendees also discussed:

- The need to reach a consensus on the value of IT in an audit environment.
- The problems faced by internal auditors when monitoring IT controls.
- The use of metrics to measure audit performance.
- The related standards, frameworks, legislation, and best practices for improving IT controls, namely ISACA's Control Objectives for Information and related Technology framework and the IT Infrastructure Library.
- The benefits of conducting research in the area of IT controls, such as the use of better metrics, the collection of needed empirical evidence, more guidance and knowledge on best practices, and tools to help inexperienced auditors perform their work.
- The expected results and deliverables from such research, including better guidance.

Moving Forward

Future IT audit research symposiums are in the works. The next symposium will be held in July 2007 in Amsterdam.

In the coming months, The IIA will send a "Call for Proposals" to invite internal audit scholars, researchers, educators, and practitioners around the world to share ideas, thoughts, and working and teaching experiences on internal auditing.

For more information about this and future IT audit research symposiums and ways to participate as a presenter, contact IIA Technology Practices Manager Lily Bi at lily.bi@theiia.org or +1-407-937-1360.