

# Why Enterprise Risk Management is Vital

Learning from Company Experiences  
With Sarbanes-Oxley  
Section 404 Compliance

*Principal Investigator  
and Project Manager*  
Steve G. Sutton

*Co-Principal Investigators*  
Vicky Arnold  
Tanya Benford  
Joseph Canada

February 2009

## **Disclosure**

Copyright © 2009 by The Institute of Internal Auditors Research Foundation (IIARF), 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means — electronic, mechanical, photocopying, recording, or otherwise — without prior written permission of the publisher.

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

The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The mission of The IIARF is to expand knowledge and understanding of internal auditing by providing relevant research and educational products to advance the profession globally.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN 978-0-89413-671-9

03/09 First Printing

## TABLE OF CONTENTS

Acknowledgments.....	iv
About the Authors.....	v
Executive Summary .....	vi
Introduction.....	1
<b>Part I: Case Studies: Early Adopter Small- and Medium-sized Enterprises .....</b>	<b>2</b>
I(a): Description of Participating Organizations .....	2
I(b): Company Sarbanes-Oxley Compliance Strategies .....	3
I(c): Summary Research Findings .....	5
<b>Part II: IIA Survey: Chief Audit Executives' Experience With Sarbanes-Oxley Compliance .....</b>	<b>8</b>
II(a): Methodology and Demographics.....	8
II(b): Enterprise Risk Management and Sarbanes-Oxley Implementation Difficulty .....	11
II(c): Enterprise Risk Management and Supply Chain Performance.....	13
II(d): Summary .....	15
<b>Part III: What About Tomorrow? .....</b>	<b>16</b>
III(a): Ownership and Control Changes.....	16
III(b): Still Out of Control?.....	17
III(c): Maintaining Compliance During Acquisitions and Mergers.....	18
<b>Implications and Conclusion.....</b>	<b>20</b>

## **ACKNOWLEDGMENTS**

This report documents the findings from a study funded by The Institute of Internal Auditors Research Foundation (IIARF). The authors wish to thank The IIARF for its generous funding and support of our research, IIARF members who participated in the survey portion of the study, and the organizations that participated in the case studies and exhibited a great willingness to share their experiences. Finally, we also thank Randy Kuhn for his research assistance during the early stages of this project.

## ABOUT THE AUTHORS

**Steve G. Sutton** is KPMG Professor of Accounting in the Kenneth G. Dixon School of Accounting at the University of Central Florida and Professorial Fellow in the Department of Accounting and Business Information Systems at the University of Melbourne (Australia). He serves as editor of the *International Journal of Accounting Information Systems*. Professor Sutton has authored and co-authored five books, four research monographs, and more than 90 articles in a broad range of accounting (e.g., *Auditing: A Journal of Practice & Theory*, *Behavioral Research in Accounting*, *Journal of the American Taxation Association*), information systems (e.g., *MIS Quarterly*, *Journal of the Association for Information Systems*, *Decision Sciences*), and accounting information systems journals (e.g., *Journal of Information Systems*, *Journal of Emerging Technologies in Accounting*). His research has been funded by grants from The IIA, the KPMG Foundation, Australian Research Council, and the Financial Industry Regulatory Authority (FINRA) Investor Education Foundation. Prior IIA grants have resulted in one monograph widely used by internal audit departments to develop quality management programs, and a second monograph currently available to internal audit departments and others through The Institute of Internal Auditors (IIA) as a part of its enterprise risk management series.

**Vicky Arnold** is Ernst & Young Professor of Accounting in the Kenneth G. Dixon School of Accounting and professorial fellow in the Department of Accounting and Business Information Systems at the University of Melbourne. She is editor of *Advances in Accounting Behavioral Research*. Professor Arnold has authored and co-authored more than 50 articles in a broad range of accounting (e.g., *Auditing: A Journal of Practice & Theory*, *Behavioral Research in Accounting*, *Journal of the American Taxation Association*), information systems (e.g., *MIS Quarterly*, *Journal of the Association for Information Systems*, *Database*), and accounting information systems journals (e.g., *International Journal of Accounting Information Systems*, *Journal of Information Systems*, *Journal of Emerging Technologies in Accounting*). Her research has been funded by grants from The IIA, the Australian Research Council, and the FINRA Investor Education Foundation. A prior IIA grant resulted in a monograph currently available to internal audit departments and others through The IIA as a part of its enterprise risk management series.

**Tanya Benford** is assistant professor of accounting in the Kenneth G. Dixon School of Accounting and recently came to the University of Central Florida from Texas A&M University. Her research has been published in leading journals such as *Auditing: A Journal of Practice & Theory*, *International Journal of Accounting Information Systems*, and *Journal of Emerging Technologies in Accounting*. Her research and teaching interests are in the areas of business process control and corporate governance. She is a former KPMG Ph.D. Project fellow.

**Joseph Canada** is a Ph.D. candidate in the Kenneth G. Dixon School of Accounting at the University of Central Florida. His research appears in the *Journal of Emerging Technologies in Accounting*, *Critical Perspectives on Accounting*, and *Corporate Ownership & Control*. His research focuses on managerial control systems including risk management and Sarbanes-Oxley Section 404 compliance processes. His doctoral studies are being supported in part by the KPMG Ph.D. Project.

## EXECUTIVE SUMMARY

The purpose of this study was to investigate the impact of the U.S. Sarbanes-Oxley Act of 2002 Section 404 internal control reporting and assurance requirements on the performance of small- and medium-sized enterprises (SMEs) conducting business in tightly coupled supply chain environments with publicly traded organizations. There have been numerous claims in the business press that the increased emphasis of Sarbanes-Oxley on internal controls may affect organizational flexibility and production cycle times as well as absorb funds that might otherwise be used to improve processes and maintain compatibility. To understand the challenges faced by SMEs and how organizations have overcome these challenges, this study systematically examined the impact of Sarbanes-Oxley compliance on accelerated filers to better understand: 1) the successes and challenges experienced, 2) the factors impacting compliance difficulty, 3) the methods employed to minimize the impact on supply chain performance, and 4) the ongoing challenges of continued compliance. The study was executed in three distinct parts:

**Part I. Case Studies of SMEs:** Four in-depth case studies were conducted with the individuals responsible for leading the Sarbanes-Oxley Section 404 compliance effort in their respective organizations. A diverse set of companies was selected to include both a successful and a challenged company representing both small and medium company sizes. Key findings indicated that:

1. The a priori development level of enterprise risk management (ERM) processes had a major impact on the organizations' ability to cope successfully with compliance requirements. The better the ERM focus, the less difficult the compliance process seemed to be across the four companies.
2. The behavior and attitude of senior management was key to dictating that of the employees involved in the compliance effort. When senior management exhibited a positive attitude and a strong emphasis on compliance, employees generally fell in line and the compliance implementation process was much smoother. This was even truer when the organizations were smaller and more flexible.
3. The accessibility of information necessary to maintain effective risk management and control of operations was key to understanding the pain experienced in meeting compliance. The more control processes that could be automated, the easier the compliance, while the more manual controls that needed to be implemented, the greater the apparent impact on supply chain flexibility and performance.

**Part II. Survey of Chief Audit Executives:** Using a Web-based survey, responses were collected from 251 chief audit executives (CAEs) via the Global Audit Information Network (GAIN), the premier benchmarking program of The Institute of Internal Auditors (IIA). Data were collected on pre- and post-Sarbanes-Oxley organizational characteristics and processes, along with Sarbanes-Oxley implementation experiences for the 139 CAE responses from organizations that had issued at least one compliance report. In addition, supply chain performance data were collected from the 155 respondent organizations for which it was applicable with approximately 60 percent of these organizations having completed Sarbanes-Oxley compliance. The survey was designed to expand upon findings from the initial case studies to improve the generalizability to a broader range of organizations. Key findings indicated that:

1. ERM was the key underlying driver facilitating organizations' strategic flexibility, which in tandem with ERM dictated the effectiveness of the implementation processes utilized, and in turn helped minimize the difficulty of the compliance process.
2. ERM, along with strategic flexibility, was fundamental to maintaining effective supply chain performance. The more effective ERM processes, the better strategic flexibility was maintained and the more effective supply chain performance.
3. The availability and accessibility of enterprisewide information through information technology (IT) systems formed a critical link in understanding the relationship between ERM and strategic flexibility, and the relationship between ERM and supply chain performance. Essentially, the availability of well-integrated enterprise systems was critical to effective ERM and overall organizational performance.
4. The control environment of the organization was a critical catalyst to the relationship between strategic flexibility and effective Sarbanes-Oxley compliance implementation processes. The proper "tone at the top" was critical and the creation of an organizational culture of control paramount. Further, ERM had a major impact on the strength of the control environment, but this impact was even further strengthened through the indirect impact of ERM through effective enterprise systems and strong organizational strategic flexibility.

**Part III. Follow-up Case Studies on Subsequent Sarbanes-Oxley Challenges:** During the course of the study, it became clear that the issues surrounding Sarbanes-Oxley Section 404 compliance led to another set of issues as organizations went through various evolutions. For instance, it is well known that a large number of organizations have attempted to delist on U.S. exchanges or go private. Additionally, the normal process of mergers and acquisitions can lead to new challenges of maintaining business processes and information systems that are Sarbanes-Oxley compliant during and after the integration process. Finally, there is great emphasis on firms easing the difficulty of the process by embracing Sarbanes-Oxley, but what happens to those organizations that continue to fight the regulatory mandates and fail to embrace them? Three additional case studies were conducted to look at company experiences under these various scenarios. Key findings indicated:

1. The decision to privatize can be fairly unpredictable. In our case, the original owner of the company made an offer to buy the company back and take it private because the owner believed Sarbanes-Oxley was impacting supply chain performance and hurting the company. The board of directors demonstrated due diligence by soliciting other bids, and a private equity firm topped the offer and eventually gained control. The company was merged with a U.K. company also owned by the private equity firm. The compliance knowledge gained through the experience of the acquired firm was used to help prepare the U.K. company to achieve compliance prior to a planned public offering.
2. The second company fought the Sarbanes-Oxley compliance mandates and had strong disagreements with its auditors. Eventually, the auditor dropped the company as a client. Weaknesses were clearly present as billing systems were unreliable and billing statements could not be supported. As the company continued to deteriorate, it began outsourcing operational functions on top of previously outsourced support functions, ultimately merging with an international competitor.

3. The Sarbanes-Oxley compliance process is one more process that must be coordinated during the merger of two public companies. In this case, a small utility company that had met Sarbanes-Oxley compliance requirements decided to sell off parts of its company due to other regulatory complexities and disadvantages in scalability. The company has been considered a model firm for how to address compliance in a proactive manner. Merger discussions led to the formation of a coordination team to handle the transfer of operations specifically for Sarbanes-Oxley. The selling company, as a part of the agreement, agreed to maintain support and operations for the underlying information systems supporting the sold utility for several months post sale until the sold utility could be integrated into the other company's operations. Similarly, all nonautomated control structures were to be maintained by the selling company until final transfer of operations was feasible.

Overall, the findings indicate that effective ERM and an embracing of a risk management and control culture generally relieves the difficulty of compliance. Additionally, such a culture actually promotes organizational strategic flexibility (i.e., the ability to respond to changes in the marketplace) and facilitates enhanced supply chain performance. Simply meeting compliance requirements is insufficient and may just prolong problems. Rather, embracing a culture of risk management and control helps organizations meet regulatory mandates in a more efficient and effective manner while supporting organizational viability and competitiveness on an ongoing basis. Given the vital role that internal auditors play in the implementation and support of ERM processes, the findings also provide evidence of the strategic importance of a strong internal audit function to an organization's strategic goals.

## INTRODUCTION

The study documented in this report has been designed to address many of the questions that have arisen during the course of the implementation of the U.S. Sarbanes-Oxley Act of 2002 provisions on effective systems of internal control and the mandates under Section 404. A broad view has been taken during the research in an effort to highlight why some organizations have had an easier time with implementation than others.

There also have been widespread concerns over how control systems are impacting organizations' competitiveness and their ability to meet business partners' expectations for supply chain performance. These issues have been argued to be of even greater concern to small- and SMEs.

The study approached these questions with a fairly open slate. While it was expected that the issues would revolve around organizational structure, top management response to the mandates, and the nature of control structures put in place to meet the new mandates, every effort was made to allow organizations' experiences to drive the evolution of the study. These efforts were initiated by originally seeking out two small and two medium-sized companies with each pair representing an organization that had a difficult time meeting compliance requirements and one that did not. These organizations' experiences highlight the critical roles of top management's attitudes, the integrated nature of enterprisewide information systems, and the strategic flexibility of the organization.

The lessons learned from these four companies were used to design a questionnaire that could be broadly disseminated to CAEs representing many different organizations to get a broad-based view on the relationships of the key factors identified in the case studies. The results provide substantial insight into the issues and concerns that have been raised in the business press. In short, we find that the strength of and support for ERM processes had a major influence on the organizations' difficulty in meeting compliance requirements and on the insulation of supply chain processes from negative effects.

While many SMEs are only now receiving their first audit opinions over management's assessment of their internal controls systems, many others have several years behind them. We look to these organizations to garner a better understanding of the other question that has received little attention to date: "What about tomorrow?" In asking this question, we turn not to organizations that are simply going through their third or fourth (or more) compliance year, but rather to those that provide a specific perspective. One organization successfully made it through the compliance process, but the reliance on manual controls was perceived to hinder its ability to compete in a supply chain environment where timing is critical. Making the decision to delist and go private, the original owner attempted to privatize the organization; however, a private equity firm outbid the original owner and took the organization private under its (i.e., the private equity firm's) control. Another organization struggled terribly during the compliance process, lost its auditor, and eventually merged with an international competitor that is benefitting from the hard lessons as the organizations are integrated. A third organization had a very successful compliance effort and was regarded as a model for compliance in earlier IIA reports, but unfortunately its financial growth was hindered by size and structure. We examine this organization's sharing of compliance models to facilitate the sale of business units to another organization.

There are many lessons to be learned from all of these organizations' experiences. In the remainder of this report, we elaborate on their experiences to allow other organizations to learn from them — particularly those SMEs that are just concluding their first years requiring an external auditor's report on their entitywide systems of internal controls.

## PART I: CASE STUDIES

### EARLY ADOPTER SMALL- AND MEDIUM-SIZED ENTERPRISES

Few corporate regulatory acts passed by the U.S. Congress have spurred as heated a debate in the public press and in speeches around the country (and the world) as has the U.S. Sarbanes-Oxley Act of 2002. Many have questioned whether the benefits outweigh the costs<sup>1</sup> while others have viewed Sarbanes-Oxley as one of the most important pieces of legislation related to financial reporting and corporate governance in terms of protecting the public interest.<sup>2</sup>

The debate has been most heated in weighing the impact on SMEs. This debate has revolved around the unanticipated consequences that compliance is projected to have on the operations of these smaller enterprises and their ability to remain competitive. These concerns arise mostly from the perceived restrictiveness of extensive internal control systems that may hinder SMEs that succeed based on fast-changing and flexible structures.<sup>3</sup> The restrictiveness of these control systems has been viewed as potentially impacting innovation, job creation, and global competitiveness.<sup>4</sup> However, despite all the outcry, these concerns have not been substantiated by prior research. Indeed, research focusing specifically on management control and its role in the strategic orientation of organizations has found that the more strategically oriented the organization, the stronger the managerial control processes required for such organizations to maintain their ability to strategically respond to marketplace changes.<sup>5</sup>

The purpose of Phase I of this study was to investigate the impact of Section 404 internal control reporting and assurance requirements on SMEs' ability to maintain competitiveness and to attain or maintain strong supply chain performance. Of particular interest were the processes implemented by various organizations to respond to compliance requirements and how these various processes impacted the flexibility of operations, the ability to strategically respond to market shifts, and overall supply chain performance.

#### **I(a): Description of Participating Organizations**

Given the focus of the research on understanding the Sarbanes-Oxley Section 404 internal control reporting and compliance experiences of organizations and putting together the pieces of the picture that help explain the interactive effect of organizational structures and compliance requirements on competitiveness and supply chain performance, we conducted a series of case studies. In each instance, we conducted interviews with the individuals representing the primary leaders in the Sarbanes-Oxley 404 compliance effort. Four targeted case studies were conducted with the goal of achieving diversity in the participating organizations across size, compliance experience, industry, processes, structure, and experience.

---

<sup>1</sup>Holstein, W.J. 2006. "Rethinking SOX." *Directorship*, (June): <http://www.directorship.com/publications/oxley.aspx>.

<sup>2</sup>Canada, J., J.R. Kuhn, and S.G. Sutton. 2008. "Accidentally in the Public Interest: The Perfect Storm That Yielded the Sarbanes-Oxley Act." *Critical Perspectives on Accounting*, 19(7): 987–1003.

<sup>3</sup>Katz, D.M. 2006. "Panels on 404 Skirt Small-company Woes." *CFO.com* (May 2).

<sup>4</sup>Reason, T. 2006. "Cry of Pain From Small Companies." *CFO.com* (May 10).

<sup>5</sup>Ditillo, A. 2004. "Dealing With Uncertainty in Knowledge-intensive Firms: The Role of Management Control Systems as Knowledge Integration Mechanisms." *Accounting Organizations and Society*, 29: 401–421.

Chenhall, R. H. and K.J. Euske. 2007. "The Role of Management Control Systems in Planned Organizational Change: An Analysis of Two Organizations." *Accounting Organizations and Society*, 32: 601–637.

Company A was an air and ocean freight company providing value-added logistics services to its customers. The company was relatively young, having been in business for only 40 years. Company A's logistics network includes 400 facilities located in 100 countries and employing more than 10,000 workers. In the year preceding our interviews, the company had US \$3.1 billion in revenue, US \$1.09 billion in assets, and a total market capitalization of US \$1.5 billion. Its annual audit was conducted by a Big Four public accounting firm.

Company B was a defense and space systems manufacturer selling primarily to defense contractors and the U.S. military. The entirely U.S.-based company employs more than 3,000 workers. While this was our oldest company (nearing 100 years since its formation), its experience dealing with government regulatory compliance over the years left it well prepared to address Sarbanes-Oxley compliance mandates. Company B reported US \$624 million in revenue and US \$1.06 billion in assets for the year preceding our interviews. They had a market capitalization of US \$1 billion and were audited by a Big Four public accounting firm.

Company Y was a manufacturer of corporate apparel, identification, and accessories for use in the healthcare, hotel, restaurant, public safety, industrial, transportation, and commercial markets. This company was also quite mature with more than 85 years of experience and a well-developed global network consisting of a broad array of offshore suppliers that produce more than 70 percent of the company's output. The managing arm and remaining 30 percent of production are all U.S. based with a total of 700 domestic employees. In the prior year the company reported US \$144 million in revenue, US \$106 million in assets, a market capitalization of US \$104 million, and a 30-percent controlling interest by the founding family. Company Y employed a non-Big Four international public accounting firm to complete its audit.

Company Z was a supplier of durable medical equipment for homebound patients. The company has operations spread across 490 locations in 48 states and employs approximately 4,600 workers. This relatively young company had been in business for about 25 years and appeared to be operating solidly with prior year revenue of US \$533 million and US \$1.02 billion in assets. Company Z's market capitalization was US \$426 million and they used a Big Four public accounting firm for their audit needs.

### **I(b): Company Sarbanes-Oxley Compliance Strategies**

In evaluating the spectrum of experiences among our four organizations, it is clear that no single strategy was found to be preferable for all. Rather, in their compliance efforts we see a mix of strategies between external consultants, outsourced internal audit expertise, development of new internal audit capabilities, and an expanded role for internal audit. In general, the organizations that carefully built their own internal audit capabilities over time seemed to handle the transition to compliance most successfully.

Company A invested a substantial amount of funding into the compliance effort, having a Big Four firm as an auditor and two other Big Four audit firms as Sarbanes-Oxley compliance consultants to assist in planning, documenting, and testing internal controls. To facilitate the effort, Company A also invested in new workflow and document repository software requiring assistance from another external consultant. Additionally, two new employees were added to the IT staff to deal specifically with compliance issues. The company adopted a balanced scorecard approach to assessing risks that led to a myriad of new control procedures that at times appeared to hamper supply chain performance. The multifaceted strategy was viewed as providing the greatest opportunity for successful compliance as the company felt the lack of overall guidance by the U.S. Securities and Exchange Commission (SEC) and The Public Company Accounting Oversight Board (PCAOB) necessitated over-compliance. The expensive strategy adopted

was further exacerbated by rises in audit fees from pre-Sarbanes-Oxley levels of US \$1.3 million to US \$4.7 and US \$4.9 million in the first two years of the compliance effort. Management's view was that the incorporation of very structured internal controls into the business processes hurt the company competitively in the global market as process time and costs increased. These changes made it difficult to compete for many jobs due to hampered speed of delivery and increased costs they felt they needed to pass on to their customers.

The stringent control guidelines placed on government contractors put Company B in a strong starting position for undertaking the compliance effort. Nonetheless, facing similar concerns to those of Company A in regards to the perceived ambiguity of the required control processes for achieving compliance, Company B decided to hire a Big Four accounting firm to provide consulting services to assure success. After two years of weighing and implementing a multitude of specific control processes, a new position, director of Sarbanes-Oxley 404, was hired in the third year of the compliance effort to streamline the effort and improve its overall effectiveness. Amidst the compliance effort, audit costs also rose significantly from pre- Sarbanes-Oxley levels of US \$2.8 million to US \$5.3 and US \$4.9 million respectively in the first two years of the compliance effort. When asked whether the internal control compliance effort was a good investment of resources, the response was a clear no. Management viewed Sarbanes-Oxley 404 compliance as little more than a regulatory activity and the controller estimated that only about 20 percent of the total compliance cost had been productive. As a government contractor, Company B felt their internal control system was already in excellent condition and that the costs of compliance had simply been an additional regulatory cost.

Company Y was very proactive in its compliance efforts and appeared to take control of the situation very quickly. Top management was quick to jump on board the compliance effort and began documenting procedures very early on, hiring a boutique specialty consulting firm — which was later replaced — to facilitate the effort and assign related responsibilities to existing staff. However, most of this early documentation effort had to be scrapped and Company Y was set back in its effort. A new consulting firm was brought in and the process essentially restarted from scratch. The process was further hindered by early protest and noncooperation by the vice president of IT who was much more focused on a SAP software upgrade. Once the vice president got behind the effort, the IT staff also became engaged in the compliance effort and the process went very smoothly from that point forward. However, the early hiccup was costly because the auditors had to re-audit the new documentation, so this baseline cost was incurred twice. Audit fees rose from a pre-Sarbanes-Oxley level of US \$154,000 to US \$369,000 and US \$409,000 in the first two years of the compliance effort.

Company Z also was proactive in its efforts to achieve compliance, but rather than try to achieve compliance through additional responsibilities being placed on existing personnel, an internal audit function was created. The company created the internal audit function to specifically handle financial-related processes and hired an outside specialty consulting firm to complement the internal audit function with IT specialists. The consulting firm also supported the implementation of content repository software to facilitate the documentation effort. The compliance process progressed well early on despite the chief financial officer's (CFO's) staunch opposition as the new director of internal audit understood the importance and pushed the effort forward. As a result, compliance costs were viewed as being well contained. The CFO's fierce opposition did prove costly, however, as a rift developed with the external auditor who was pushing for quick compliance. The audit cost also was costly because the auditor was forced to complete substantial additional testing late in the process to assure compliance. Thus, audit fees only rose the first year from US \$332,000 to US \$433,000 before quadrupling to US \$1.2 million in the second year of compliance. Eventually, the CFO was replaced by the director of internal audit and the manager with the external consultant was hired as the new director of internal audit, bringing a cadre of

IT audit specialists with him to enhance the internal audit department's capability and self-sufficiency. Even after this change, the consulting firm continued to provide some controls testing support.

Our companies' experiences appear to be typical of the broad range of SMEs' experiences that have been briefly reported in the business press. The process has often been difficult as organizations stagger through new processes and mindsets. On the other hand, some organizations have complied much easier than others. In the following section, we integrate the various experiences of our case study companies to identify general patterns and critical factors that appear to impact compliance difficulty and the impact on business processes' efficiency and effectiveness.

### **I(c): Summary Research Findings**

In evaluating the spectrum of experiences among our four companies, three fundamental areas stood out most prevalently: 1) ERM strategies, 2) the role of structural inertia and the corollary ability to adapt to change, and 3) organizational flexibility. We consider these three areas across the four companies participating in our case studies.

Improved ERM represents the biggest benefit of Sarbanes-Oxley 404 when considering our companies' experiences. Clearly, an objective of Sarbanes-Oxley was to push organizations toward better governance and stronger financial controls — key components of ERM. However, many organizations viewed the mandates as extending to robust ERM processes that are more strategic than operational, and each of our companies made significant strides in this direction. Likewise, the stronger the ERM processes in place pre-Sarbanes-Oxley, the easier time our case study companies had with the compliance process. This effect was perhaps best summarized by the chief information officer (CIO) at Company A who, despite the highly challenging experience in achieving compliance, still noted that “Sarbanes-Oxley does not ask for companies to do anything that they should not have been doing already.”

Sarbanes-Oxley required organizations to stop and assess what were often long-neglected ERM processes that no longer were sufficient for their organizations. Company A, despite its bitterness about the Sarbanes-Oxley mandates, noted that new risk assessment processes were implemented and formalized to allow the company to match assessed risks with business priorities using a balanced scorecard-based approach. They further noted that Sarbanes-Oxley “. . . forces us to apply our practical pragmatic business approach to these types of issues and stop ‘reacting’ to perceived issues. We have improved in recognizing the importance to the company, as well as having a balanced approach.” Company B instituted a training program to educate employees on risk-related issues with the intent to get employees to embrace control procedures, take ownership over control effectiveness, and recognize when risks threaten business process success. Company Y adopted a risk matrix that uses cross-functional teams to conduct annual risk analyses where potential risks are rated high or low in terms of consequence and probability with two high ratings requiring a written analysis report. Company Y further acknowledged that the formalization of policies and procedures provided a long-term impact on infrequent risks that might otherwise have been ignored. Company Z noted that one big benefit of Sarbanes-Oxley compliance was that it served to greatly improve the relationships between internal auditing and other departments. As internal auditing helped resolve complex compliance issues for the departments, department leaders gained a healthier appreciation for risk assessment and related internal control system processes. There was also little doubt that all of the companies' ERM processes were far more effective post-compliance.

Structural inertia<sup>6</sup> and companies' ability to cope with change provided another significant, contributing explanation to the companies' experiences. Structural inertia comes into play when assessing how organizations would react to Sarbanes-Oxley mandates. Theory suggests that older, more mature organizations will struggle far more to make the changes in their processes. On the other hand, organizations that have substantial experience in dealing with change as an ongoing part of their business model are able to use that experience to adapt much more quickly to new mandates. This held true with our companies. Company A, a medium-sized established enterprise, was most affected by Sarbanes-Oxley and struggled the most to comply. Its size and established structure, coupled with its far-reaching global operations, confounded the process. Company B, also a medium-sized enterprise but one that had dealt with government regulations in government contracting for an extended period, was quick to adapt and had a fairly smooth transition during the compliance process. Company Y, a smaller company, was able to react quickly; once the vice president of IT got behind the effort, size was an advantage and the "tone at the top" was a very effective driver of the compliance effort. Company Z benefitted perhaps the most of any of the organizations because of its size and the change experience it hired (i.e., while the organization itself was not highly experienced in change, they hired people from the outside — such as the IT audit director from the consulting firm — who had extensive experience with multiple organizations).

Organizational flexibility was the other prevalent factor impacting the companies' experiences. The loss of flexibility was frequently raised as a concern to all of the organizations. As noted earlier, Company A felt there were serious impacts on competitiveness due to loss of flexibility. More specifically, they noted that "time to process normal business transactions has increased an estimated 5 percent. In the transportation industry, any additional time the customer experiences can — and probably has — lost us business . . . . The time impact is greater as transactions increase in complexity." Company B's CFO noted that Sarbanes-Oxley "negatively impacted flexibility due to a fear that doing anything not in the documented procedures would result in a material weakness." The CFO also noted that while the strategic plan for the company was not altered, Sarbanes-Oxley compliance costs were now required to be included in every new project budget, thus making many strategic processes appear no longer cost beneficial. Company Y noted that Sarbanes-Oxley concerns influenced the decision to drop the SAP HR (human resources) module over concerns of the impact on overall compliance assessments. Company Z's head of internal audit acknowledged "there are specific areas where having to comply with Sarbanes-Oxley has made processes more involved, resulting in more time and effort required to perform a process for controls in that specific area to operate effectively." Company Z also noted that new information systems interfacing with the financial reporting system were delayed indefinitely until the associated Sarbanes-Oxley documentation was completed, which would clearly articulate the completeness of controls. Thus, Sarbanes-Oxley appeared to affect the companies' flexibility in many ways, but not necessarily all for bad reasons.

Also of note is the reverse influence of organizational flexibility. While often viewed as an attribute perceived to be hampered as an outcome of the Sarbanes-Oxley compliance process, organizational flexibility also proved to be a major input into its effectiveness. Overlapping to some degree with the

---

<sup>6</sup>Structural inertia is an organization's ability or inability to change under conditions of environmental turbulence. Age and size are considered to be the two largest impediments to changeability, while change experience can help overcome.

See: Hannan, M.T. and J. Freeman. 1984. "Structural Inertia and Organizational Change." *American Sociological Review*, (49) 2: 149–164; Amburgey, T.L and A.S. Miner. 1992. "Strategic Momentum: The Effects of Repetitive, Positional, and Contextual Momentum on Merger Activity." *Strategic Management Journal*, (13): 335–348; and Amburgey, T.L., D. Kelly, and W.P. Barnett. 1993. "Resetting the Clock: The Dynamics of Organizational Change and Failure." *Administrative Science Quarterly*, (38): 51–73.

structural inertia foundation for addressing change, the companies' flexibility was important in coping with change and adapting to the new mandates. Interestingly, it was the ready flow of information across the company that often dictated how well flexibility was able to help. Those companies with strong, integrated information technologies maintained higher flexibility and were better able to gather and assess the information needed for effective ERM. We see this in Company B with its size and maturity still able to react due to tight information integration and strong preexisting control structures that enabled it to react to changes. Companies Y and Z also were able to adapt more quickly once they embraced change and gained management's consistent support for the efforts, while automation of control processes influenced the ease of compliance. Company A's lack of integration across a dispersed global network coupled with surprising inflexibility for an organization that viewed itself as flexible in its business processes led to increased compliance difficulties.

Our team walked away from these four companies with a vision of the basic structures that impacted organizations' ability to address compliance mandates, maintain organizational flexibility, and maintain effective supply chain performance. Phase II of the study used this information in the design of a survey issued to a much broader set of organizations to test whether these observed phenomena held across a larger cross-section.

## **PART II: IIARF SURVEY**

### **CHIEF AUDIT EXECUTIVES' EXPERIENCE**

### **WITH SARBANES-OXLEY COMPLIANCE**

Based on the case studies completed in the first portion of the study, several factors appeared to capture the major issues surrounding Sarbanes-Oxley compliance. The outcome issues of most concern generally focused on the difficulty in complying with Sarbanes-Oxley 404 mandates, supply chain performance, and the organization's ability to maintain flexibility and agility in its strategic operations. The enablers of these outcomes revolved around the effectiveness of ERM processes, strength of the control environment, and the compatibility and flexibility of IT systems in terms of bringing together the information necessary to support ERM, compliance documentation, well-controlled supply chain activities, and strategic flexibility.

The focus in Part II of the research study shifted to attaining a better understanding of whether the key issues identified in our sample of case study companies were representative of the experiences endured by a broader range of organizations. In conjunction with The IIARF, we launched a survey on The IIA's GAIN system and e-mailed solicitations for participation to members who are CAEs. The survey collected both pre- and post-Sarbanes-Oxley data on ERM process effectiveness, supply chain performance, IT flexibility from connectivity and compatibility perspectives, organizational strategic flexibility, and control environment. In addition, we collected data on Sarbanes-Oxley implementation processes and experiences, whether Sarbanes-Oxley 404 compliance was required, and a variety of demographic information related to the CAEs and their organizations. The remainder of the discussion in this part focuses on the execution of that portion of the study and our findings.

#### **II(a): Methodology and Demographics**

The IIARF's solicitation of CAE participation resulted in 251 members completing the survey (a response rate of 18.1 percent). The response rate is indicative of organizations' strong interest in Sarbanes-Oxley 404 compliance processes and challenges. Out of the 251 respondents to the survey, 139 (55.6 percent) were from organizations that had already completed the Sarbanes-Oxley 404 compliance process at least once and had issued both management and auditor's reports on internal controls. A different cross-section of the sample was analyzed for purposes of evaluating the impact of strategic ERM processes on supply chain performance. Of the 251 respondents to the survey, 155 (61.8 percent) of the CAEs provided information consistent with active involvement in a supply chain with 90 (58.1 percent) of those organizations having completed at least one Sarbanes-Oxley 404 compliance cycle. These two subsamples form the basis for our analyses in Phase II of the research study.

In the first subsample consisting of organizations having completed at least one Sarbanes-Oxley 404 compliance effort, 93.8 percent were publicly traded companies. A broad range of industries were represented in the sample with the largest groups coming from manufacturing (23 percent), financial services and real estate (16.8 percent), technology (10.6 percent), insurance (9.7 percent), and utilities (8.9 percent). (See Table 1 for details.)

**Table 1**  
**Demographics for Companies with**  
**Completed Sarbanes-Oxley Section 404 Compliance**

Category	Percentage
<i>Gender</i>	
Male	69.03%
Female	29.20%
Not answered	1.77%
<i>Age</i>	
25 to 40 years	24.78%
40+ years	74.34%
Not answered	0.88%
<i>Experience</i>	
3 to 10 years	18.58%
10+ years	81.42%
<i>Industry</i>	
Manufacturing	23.01%
Financial services and real estate	16.81%
Technology	10.62%
Insurance carriers and agents	9.73%
Utilities	8.85%
Wholesale and retail	5.31%
Transportation	5.31%
Communication	3.54%
Health	2.64%
All other	14.16%
<i>Organizational Structure</i>	
Publicly traded	93.81%
Not publicly traded	5.31%
Not answered	0.88%

In the second subsample consisting of organizations substantially involved in supply chain interactions, 58.1 percent were publicly traded companies. A broad range of industries also were represented in this sample with the largest groups coming from manufacturing (18.7 percent), insurance (16.8 percent), financial services and real estate (14.2 percent), wholesale and retail (8.4 percent), technology (7.7 percent), and utilities (7.1 percent). (See Table 2 for details.)

**Table 2**  
**Participant Demographics**

Category	Percentage
<i>Gender</i>	
Male	70.3%
Female	29.0%
Not answered	0.7%
<i>Age</i>	
25 to 40 years	20.65%
40+ years	76.77%
Not answered	2.58%
<i>Experience</i>	
3 to 10 years	15.48%
10+ years	84.52%
<i>Industry</i>	
Manufacturing	18.71%
Insurance	16.77%
Financial and real estate	14.19%
Wholesale and retail	8.39%
Technology	7.74%
Utilities	7.10%
Health	4.52%
Communication	2.58%
Aerospace and defense	2.58%
Transportation	2.58%
All other	14.84%
<i>Organizational Structure</i>	
Publicly traded	58.06%
Not publicly traded	40.65%
Not answered	1.29%

A field survey method was used in the research to rapidly gather data on a broad range of organizations to examine the expected relationships among the various issues identified in the case studies. A field survey focuses on a key respondent who is in a position to observe the actual phenomena of interest in the study. In this case, we focus on CAEs based on their integral role in the Sarbanes-Oxley implementation process and their dual role in monitoring organizational efficiency and effectiveness. We adopted structural modeling techniques for the analysis of the data to both validate the overall measurement constructs (each

issue of concern was measured with multiple questions) and assess the overall fit of a conceptual model representing the expected relationships among the organizational attributes and the resulting outcomes.

## **II(b): Enterprise Risk Management and Sarbanes-Oxley Implementation Difficulty**

The goal of our analyses on Sarbanes-Oxley implementation difficulty was to examine the drivers of our case study companies' experiences in an effort to better understand how they influenced the resulting compliance difficulty. Based on our earlier case studies, we viewed the critical relationships as focusing around the pre-Sarbanes-Oxley compliance state of an organization's ERM processes, control environment, IT flexibility in terms of compatibility, and strategic flexibility. As such, our research model examines these four factors as being predictive of an organization's difficulty in implementing effective Sarbanes-Oxley compliance procedures. However, we do not see these four factors as operating independently. Accordingly, our models consider the impact of factors on each other. Most notably, effective ERM necessitates the development of strong information flow across the organization (e.g., IT compatibility) and a strong control environment. Without the latter, it is unlikely that an organization will be able to easily implement effective Sarbanes-Oxley compliance procedures.

To develop measures of each of the factors within our responding organizations, we used a combination of questionnaire measures used in prior academic studies and measures developed by our team to address more contemporary factors where previously validated measures were not available. For ERM, we developed a five-question instrument based on the ERM framework prescribed by COSO.<sup>7</sup> Similarly, for the control environment, we developed a multi-question instrument based on COSO's<sup>8</sup> original framework description. For strategic flexibility we used a common measure from strategic management research first put forth by Cannon and St. John.<sup>9</sup> IT compatibility was a subcomponent of an overall IT flexibility instrument developed and validated by Byrd and Turner.<sup>10</sup> We focused on the compatibility component given its ability to capture the degree to which an organization's information systems are capable of sharing data from across the entire organization. As noted previously, the focus of these factors is on the difficulty an organization encountered in complying with Sarbanes-Oxley 404 mandates. We assess the efficiency of the Sarbanes-Oxley compliance implementation process through a set of questions we developed that focus on best practices for organizational and business process change. These questions were derived based on an amalgamation of related studies along with our original case studies.<sup>11</sup> The resulting model shown in Figure 1 supports our prediction of the influences of the various factors on the efficiency of the Sarbanes-Oxley compliance implementation process. Analyzed in its entirety, the model shows strong simultaneous fit among all of the various factors and relationships specified in the

---

<sup>7</sup>Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management – Integrated Framework*. (Committee of Sponsoring Organizations of the Treadway Commission, American Institute of Certified Public Accountants: New York).

<sup>8</sup>Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control – Integrated Framework*. American Institute of Certified Public Accountants.

<sup>9</sup>Cannon, A. R. and C. H. St. John. (2004). "Competitive Strategy and Plant Level Flexibility." *International Journal of Production Research*, 42(10): 1987–2007.

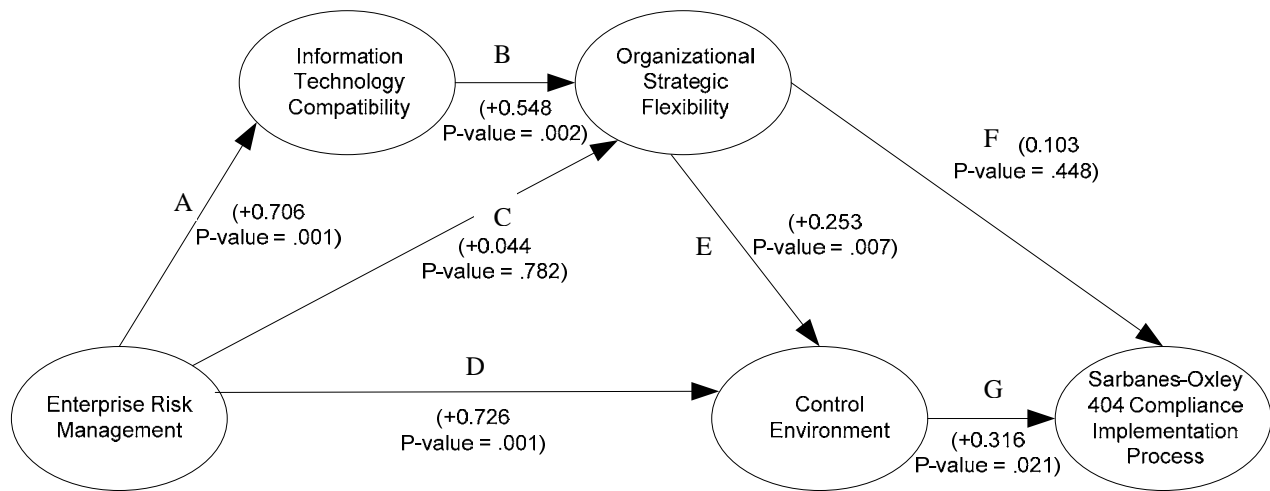
<sup>10</sup>Byrd, T. A. and D. E. Turner. 2000. "Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct." *Journal of Management Information Systems*, Summer Vol. 17, No. 1: 167–208.

<sup>11</sup>Kettinger, W. K. and V. Grover. 1995. "Toward a Theory of Business Change Management." *Journal of Management Information Systems*, Vol. 12, No. 1: 9–30.

Ungan, M. 2005. "Management Support for the Adoption of Manufacturing Best Practices: Key Factors." *International Journal of Production Research*, Vol. 43, No. 18: 3803–3820.

model.<sup>12</sup> To overview the model, we will quickly review the various relationships captured. The “A” path indicates that stronger ERM processes lead to higher levels of IT compatibility, a relationship that is highly significant in the model. The “B” path indicates that higher levels of IT compatibility support higher levels of strategic flexibility, a relationship that is also highly significant. On the surface, the “C” path appears to reflect the absence of a direct relationship between ERM and strategic flexibility. However, “C” is reflective of a *mediating* relationship indicating that the relationship between ERM and strategic flexibility is *fully mediated* by IT compatibility. In essence, the positive relationship between ERM and strategic flexibility is dependent upon strong IT compatibility.<sup>13</sup>

**Figure 1**  
**Predictive Model for Efficiency of Sarbanes-Oxley Section 404 Compliance Implementation Process**



Chi-square = 141.726 df=111 p-value = .026  
CFI = .972 RMSEA = 0.050

The “D” path indicates that strong ERM leads to a strong control environment, a basic COSO premise that not surprisingly is highly significant in the model. What may be less evident at first glance is that the inclusion of IT compatibility and strategic flexibility in the model results in an additional 15 percent of the relationship between ERM and the control environment. In other words, per the path weight on “D” of 0.726, ERM explains directly 72.6 percent of the control environment’s strength. However, when IT compatibility and strategic flexibility are added into the model, a total of 83.5 percent of the control environment’s strength is explained via direct and indirect effects of ERM.

<sup>12</sup>The model was tested using AMOS 7.0 (2006) software for structural equation modeling. The Comparative Fit Index (CFI) of 0.972 and the Root Mean Square Error of Approximation (RMSEA) of 0.050 provide solid support for concluding there is good overall model fit.

<sup>13</sup>If we extract ERM and strategic flexibility to only look at this relationship in isolation, there is a direct and significant relationship (p-value = 0.001). Similarly, when we add IT compatibility and look at the three factors in isolation together, the relationship between ERM and strategic flexibility lacks significance (p-value = 0.577), verifying that IT compatibility fully mediates the relationship.

The “E” path indicates that increased strategic flexibility leads to a stronger control environment, a relationship that is highly significant in the model. This is consistent with findings noted earlier that suggest organizations must build strong managerial control systems to sustain strategically flexible organizational structures over time. The “F” path indicates that a stronger control environment facilitates a more efficient Sarbanes-Oxley 404 compliance implementation process. The “G” path is reflective of a situation similar to that found with the “C” path. The “G” path is reflective of a *mediating* relationship which indicates that the relationship between increased strategic flexibility and a more efficient Sarbanes-Oxley 404 compliance implementation process is *fully mediated* by a strong control environment. In essence, the positive relationship between strategic flexibility and efficient Sarbanes-Oxley 404 compliance implementation processes is dependent upon a strong control environment.<sup>14</sup> This relationship highlights one possible explanation for many organizations’ complaints that their flexibility was hampered by Sarbanes-Oxley 404 compliance processes — without strong ERM and a strong control environment, organizations have difficulty sustaining flexibility and reacting to new regulatory mandates such as those mandated by Sarbanes-Oxley.

### **II(c): Enterprise Risk Management and Supply Chain Performance**

The goal of our analyses on supply chain performance was to better understand how ERM impacts performance. However, similar to our study of Sarbanes-Oxley 404 implementation difficulty, we recognize the intermediary effects of IT compatibility and strategic flexibility in facilitating ERM impacts on organizational performance. Based on our earlier case studies, we viewed the critical relationships as focusing on the current state of an organization’s ERM processes, IT flexibility in terms of both compatibility and connectivity, and strategic flexibility. As such, our research model examines these three factors as being predictive of an organization’s supply chain performance. As in the prior analyses, we do not see these three factors as operating independently, but rather we view them as highly interrelated. Accordingly, our model again considers the impact of the factors on each other. In particular, we view effective ERM as necessitating the development of strong information flow across the organization (e.g., IT compatibility and connectivity) to promote strategic flexibility and, in turn, supply chain performance.

To develop measures of each of the factors within our responding organizations, we used a combination of questionnaire measures, as noted earlier, used in prior academic studies and measures developed by our team. In this study, we used the same ERM measurement instrument based on the COSO ERM framework,<sup>15</sup> but this time we focused on current ERM processes as opposed to pre-Sarbanes-Oxley ERM as used in the earlier study. IT compatibility and connectivity are both subcomponents of the IT flexibility instrument developed and validated by Byrd and Turner.<sup>16</sup> In this part of the study we focus on the current state of both connectivity and compatibility to capture the intra-organizational information sharing capability necessary to support both strategic flexibility and supply chain activities. Our interest in this study is in understanding the intermediary effects on strategic flexibility and the overall effects on supply

---

<sup>14</sup>If we extract strategic flexibility and Sarbanes-Oxley Section 404 compliance implementation processes to only look at this relationship in isolation, there is a direct and significant relationship (p-value = 0.011). Similarly, when we add strength of control environment and look at the three factors in isolation together, the relationship between strategic flexibility and Sarbanes-Oxley 404 compliance implementation processes lacks significance (p-value = 0.678), verifying that strength of the control environment fully mediates the relationship.

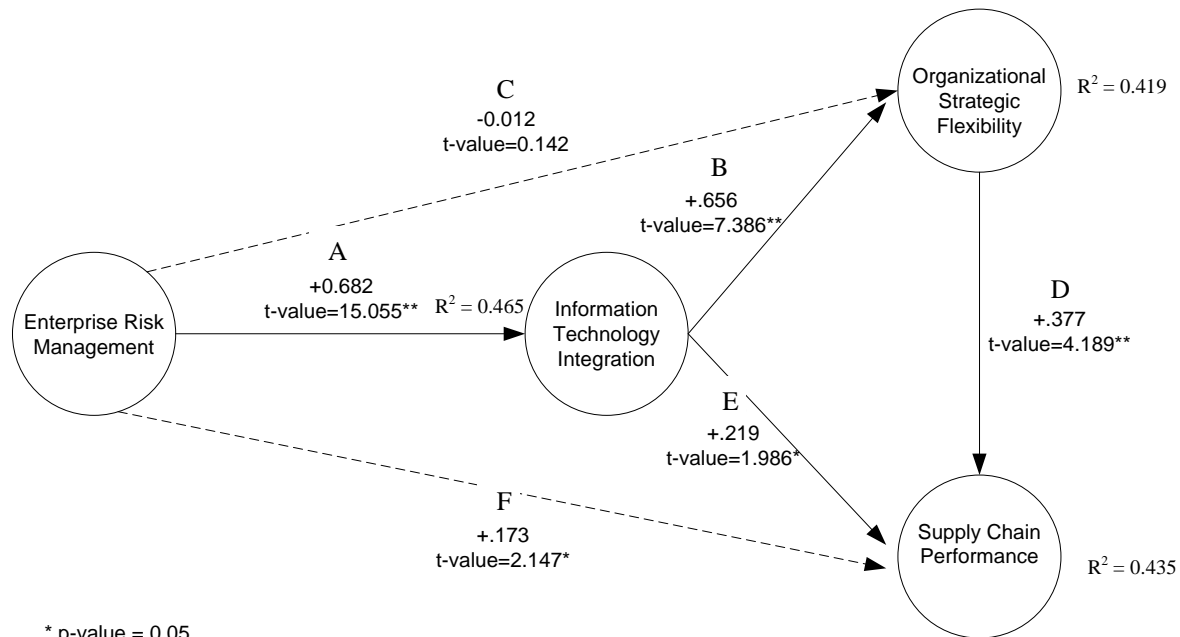
<sup>15</sup>Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management – Integrated Framework*. (Committee of Sponsoring Organizations of the Treadway Commission, American Institute of Certified Public Accountants: New York).

<sup>16</sup>Byrd, T. A. and D. E. Turner. 2000. “Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct.” *Journal of Management Information Systems*, Summer Vol. 17, No. 1: 167–208.

chain performance that result from strong ERM processes in a post-Sarbanes-Oxley world. For strategic flexibility we again used the Cannon and St. John<sup>17</sup> measure, but similarly with a focus on the current state. For supply chain performance, our interests are on customer service goals and objectives and as such we adopt measures from Beamon<sup>18</sup> that are reflective of this interest.

The resulting model shown in Figure 2 supports our prediction of the influences of the various factors on both strategic flexibility and supply chain performance. Analyzed in its entirety, the model shows strong simultaneous fit among the various factors and relationships specified in the model. To overview the model, we will briefly review the various relationships captured. It should be noted that relationships in this model are quite complex recognizing the interrelationships of the particular factors of interest.

**Figure 2**  
**Predictive Model for ERM Effects on**  
**Strategic Flexibility and Supply Chain Performance**



The “A” path indicates that stronger ERM processes will lead to higher levels of IT integration (i.e., compatibility and connectivity), a relationship that is highly significant in the model. The “B” path indicates that higher levels of IT integration support higher levels of strategic flexibility, a relationship that is also highly significant. On the surface, the “C” path appears to reflect the absence of a direct relationship between ERM and strategic flexibility. However, “C” is reflective of a *mediating* relationship, indicating that the relationship between ERM and strategic flexibility is *fully mediated* by IT integration. In essence, the positive relationship between ERM and strategic flexibility is dependent upon

<sup>17</sup>Cannon, A. R. and C. H. St. John. (2004). “Competitive Strategy and Plant Level Flexibility.” *International Journal of Production Research*, 42(10): 1987–2007.

<sup>18</sup>Beamon, B. (1999). “Measuring Supply Chain Performance.” *International Journal of Operations and Production Management*, 9(3): 275–292.

strong IT integration.<sup>19</sup> This finding is consistent with the relationships found in examining a similar set of factors in a pre-Sarbanes-Oxley environment in the previous analyses when testing the other subset of data.

The “D” path indicates that higher levels of strategic flexibility lead to better supply chain performance, a relationship that is highly significant in the model. On the surface, the “E” path is significant, but appears to not be as strong as some other relationships in the model. However, “E” is reflective of a *mediating* relationship, indicating that the relationship between IT integration and supply chain performance is *partially mediated* by strategic flexibility. In essence, the positive relationship between IT integration and supply chain performance is *partly* dependent upon higher levels of strategic flexibility that allow an organization to leverage information into performance.<sup>20</sup>

The “F” path represents a third *mediating* relationship where IT integration is viewed as *mediating* the relationship between ERM and supply chain performance. Similar to the “E” path, the “F” path represents a *partially mediating* relationship. This indicates that strong ERM processes have a positive impact on supply chain performance, but a portion of this relationship is dependent on the availability of strong IT integration that facilitates the necessary information flows to both efficiently control supply chain processes and facilitate monitoring of supply chain performance.<sup>21</sup>

## II(d): Summary

On an overall basis, the results of the two models indicate that a strong ERM focus actually improves strategic flexibility and supply chain performance, contrary to many of the concerns voiced over the last few years in regards to potential negative effects of Sarbanes-Oxley 404. Further, the results suggest that organizations that had implemented strong ERM processes prior to Sarbanes-Oxley Section 404 and those organizations that similarly established strong control environments experienced significantly less difficulty in meeting compliance requirements. At the same time, the results highlight the critical role of strong IT integrated systems — a perspective that is consistent with COSO’s long emphasis on information flow as being critical to strong control systems and is also consistent with the recent focus on automating Sarbanes-Oxley Section 404 compliance efforts to improve both efficiency and effectiveness of ERM processes. While not directly measured, the results also infer that a strong internal audit function can greatly benefit both an organization’s flexibility and performance.

---

<sup>19</sup>If we extract ERM and strategic flexibility to only look at this relationship in isolation, there is a direct and significant relationship (p-value < 0.01). Similarly, when we add IT integration and look at the three factors in isolation together, the relationship between ERM and strategic flexibility lacks significance (t-value = 0.294), verifying that IT integration fully mediates the relationship.

<sup>20</sup>If we extract IT integration and supply chain performance to only look at this relationship in isolation, there is a direct and significant relationship (p-value < .01). Similarly, when we add strategic flexibility and look at the three factors in isolation together, the relationship between IT integration and supply chain performance decreases in significance (change in t-value from 11.545 to 3.211), verifying that strategic flexibility partially mediates the relationship.

<sup>21</sup>If we extract ERM and supply chain performance to only look at this relationship in isolation, there is a direct and significant relationship (p-value < .01). Similarly, when we add strength of IT integration and look at the three factors in isolation together, the relationship between ERM and supply chain performance decreases in significance (change in t-value from 7.810 to 1.576), verifying that strength of the control environment partially mediates the relationship.

## PART III: WHAT ABOUT TOMORROW?

While the first set of case studies and the follow-up survey provided a strong basis for understanding key issues surrounding initial compliance with Sarbanes-Oxley Section 404 internal control compliance mandates, the question that is left unanswered is how Section 404 affects organizations' business decisions in the future (i.e., What about tomorrow?). Our research team conducted three additional case studies designed to look at three specific situations with organizations facing ownership and control changes: 1) what are some of the risks and pitfalls that can occur when attempting to take a company private (i.e., delisting), perhaps to avoid Sarbanes-Oxley Section 404 mandates? 2) for companies that keep fighting the mandates but attempt to stay public, what are some of the business concerns? and, 3) what are the challenges that Sarbanes-Oxley Section 404 introduces to the mergers and acquisitions process? The first two situations relate to companies who fought the Sarbanes-Oxley compliance effort to various degrees. The latter is an almost reverse situation where a company that was a model for compliance encounters financial and business challenges that lead to divestiture of business units. We explore these three organizations to get some view of the challenges faced in each situation that go beyond the typical compliance efforts we had studied to date.

### III(a): Ownership and Control Changes

The passage of Sarbanes-Oxley marked a significant change in corporate governance policies under the auspices of the public interest and altered the relationship between shareholders and management. As a result, regulations have altered organizations' business models, and concerns have been raised regarding the impact on global competitiveness.<sup>22</sup> Companies feeling that Sarbanes-Oxley Section 404 mandates hamper their business activities fall into three groups: 1) acceptance, 2) denial, or 3) avoidance. Here we look at avoidance through an organization that chose a delisting option as a means of getting out of the requirements. Many firms have explored this option of not being traded on exchanges, instead choosing to avoid the corporate governance requirements prescribed by Sarbanes-Oxley. Consistent with this approach, there has been a significant increase in delisting activity on U.S. exchanges.<sup>23</sup> Publicly traded U.S. companies can delist by either *going dark* or *going private*. Firms that go dark can continue to trade on over-the-counter markets if they have less than 300 shareholders or if they have both less than 500 shareholders and less than US \$10 million in assets. Going private requires the shareholders to sell all ownership interests to a private individual owner or group of owners. We were allowed to interview one such company as it endeavored to go private — albeit not in the manner originally intended.

Subsequent to our original study, one of our case study companies (reported about in Part I of this research report) decided to privatize to avoid the perceived negative effects of Sarbanes-Oxley Section 404 compliance structures on the firm's global competitiveness. Before the decision to privatize, the founder of the company held the positions of CEO and chairman of the board of directors, as well as being the single largest shareholder with an approximately 20 percent ownership interest. The founder and CEO put forth a proposal to make a leveraged buyout of the company with an explicitly stated concern that Sarbanes-Oxley Section 404 compliance was too costly. The board showed due diligence as it formed a special committee to review the offer, hire an investment banking firm to review the offer, and

---

<sup>22</sup>Katz, D.M. 2006. "Panels on 404 Skirt Small-company Woes." *CFO.com* (May 2).

Reason, T. 2006. "Cry of Pain From Small Companies." *CFO.com* (May 10).

<sup>23</sup>Leuz, C., A. Triantis, and T. Y. Wang. 2008. "Why Do Firms Go Dark? Causes and Economic Consequences of Voluntary SEC Deregistrations." *Journal of Accounting and Economics* (forthcoming).

had the investment banker solicit additional offers. Another suitor arose and outbid the CEO, placing the company under the ownership and control of a private equity firm. The CEO was subsequently dismissed. The private equity firm's successful pursuit of the company was inconsistent with prior research on acquisitions, as most of the normal motivators for acquisition were not present. First, the amount of free cash that was available to disperse to shareholders as dividends was very small, so excess cash reserves were not present. Second, there were no large blocks of stock held by institutional investors who might be more willing to facilitate an outside sale. Third, there was no unhappiness with the founder serving as CEO and chairman of the board; rather, the board actually chose the CEO's buyout offer over the private equity firm even though the CEO's price was lower. Fourth, other than the CEO, the remainder of the board consisted of independent directors.

However, there were alternative aspects of the organization that made it an attractive takeover target. First, it had performed very well and had high growth up until the last two quarters. The slowdown was blamed on the effects of Sarbanes-Oxley Section 404 compliance on the company's global competitiveness. Second, the slowdown over the last two quarters had led the company to be undervalued by approximately 25 percent based on its stock price. The CEO's failed offer was 20 percent over the current stock price at the time. Finally, when the board accepted the CEO's lower offer, a shareholder sued and required the deal to be nullified so as to maximize the value to shareholders.

The active involvement of a private equity firm in the bidding for the company and its ultimate success was only predictable if the impact of Sarbanes-Oxley Section 404 compliance was considered. First, a private equity firm had no requirement to obtain Sarbanes-Oxley compliance, so this perceived impediment to competitiveness was nullified. Second, the private equity firm held another similar company that was U.K.-based and viewed the acquisition of the company's industry expertise as valuable. Third, the private equity firm wished to take the U.K. company public on the U.S. exchanges, but needed to prepare for Sarbanes-Oxley Section 404 compliance before going public. The private equity firm, it turned out, was intentionally acquiring in part the company's expertise in Sarbanes-Oxley compliance, but at the same time backed off some processes in the acquired U.S. company to focus on a more risk-based approach for both companies. The risk-based focus that was encouraged under revised SEC interpretations of Sarbanes-Oxley Section 404 mandates allowed the firm to leverage what worked well in the acquired U.S. company to improve controls in both companies while eliminating a number of unnecessary manual processes that hampered competitiveness. The intent is to eventually go public with both companies.

### **III(b): Still Out of Control?**

Sarbanes-Oxley Section 404 requires extensive strengthening of governance structures and reporting systems. The intense scrutiny of internal control systems has led many organizations to invest in IT to improve the reliability of such systems. However, maintaining the same corporate culture may inhibit an organization's ability to achieve operational and internal control synergies despite heavy investments in IT.

The organization examined in this case study specializes in developing cutting-edge Internet marketing solutions. The organization grew exponentially during 2000 to 2004, but that changed in 2005. Internal control issues surrounding their billing processes and the accuracy of billings contributed to customer attrition and accordingly the organization's performance suffered. The interview, as well as the Sarbanes-Oxley Section 404 management and auditor's reports, revealed that the organization lacked adequate controls, documentation, and automation. Attempting to satisfy Sarbanes-Oxley Section 404, the organization created an internal audit function and a Sarbanes-Oxley Section 404 compliance team, and

invested heavily in IT. Further complicating their Sarbanes-Oxley compliance, the organization merged with a European competitor and changed auditors from a Big Four firm to a local firm.

The major difference between this organization and the others that were examined lies in the failure of top management to embrace the goal of better corporate governance and enhanced risk management. The organization's founder and CEO had an entrepreneurial spirit that pushed the envelope as he developed and provided cutting-edge marketing solutions to the organization's customers. While this maverick attitude served the organization well in its early years as it navigated through its less travelled niche in the marketing sector, the same attitude and entrepreneurial spirit became a hindrance in the more control-oriented post-Sarbanes-Oxley regulatory environment. The interview revealed that the organization's top management viewed Sarbanes-Oxley compliance as a nuisance task that interfered with their market flexibility and business operations. In short, the organization did not embrace ERM as a facilitator of strategic flexibility and, not surprisingly, the focus on strategic responsibility caused the organization to unravel in the absence of managerial control processes.

Although the organization competed in a technology-driven market, it focused its investments in IT on external reporting processes, which were neither intended nor designed to be integrated into the organization's business processes. Many of the controls that were designed to meet Sarbanes-Oxley Section 404 compliance mandates were superficial and intentionally designed to minimize any impact on operations. Top management was adamant about continuing business in its unfettered reactionary form despite Sarbanes-Oxley compliance and had no desire to create synergy between the system of internal controls and the business operations. The goals for the new IT systems were so narrowly defined that, in many cases, due diligence simply was not performed. For example, a popular system integration software (Hyperion) was purchased, but would not work because one of the major systems (SAP 1) was customized. Top management's attitude toward Sarbanes-Oxley compliance can be summed up as "Hire some people, buy some software, and make this thing go away."

Notwithstanding the investments in technology, the organization still manually extracted financial data from different systems and compiled them to produce organizationwide financials. With heavy investments in IT and very little Sarbanes-Oxley Section 404 compliance progress, the organization subsequently outsourced the majority of its accounting functions. Only the compilation of financial data was performed by the organization's in-house accountants. Eventually, their problems with IT led the firm to outsource their operating systems as well. Unfortunately, outsourcing operating systems in a technology-driven market can lead to a shedding of tacit knowledge that provides the organization's competitive advantage. The organization eventually downsized 20 percent of its employees in 2007 and another 15 percent in 2008. The CEO and founder has since been relieved of his position and the organization began to sell off certain core operating units while acquiring other small organizations. Not surprising, today the organization is very different than it was when it started the Sarbanes-Oxley Section 404 compliance process in 2004. It has spun out of control by trying to achieve performance while employing pre-Sarbanes-Oxley designed business processes without post-Sarbanes-Oxley ERM processes that would monitor and enable strategic flexibility.

### **III(c): Maintaining Compliance During Acquisitions and Mergers**

For many organizations, the Sarbanes-Oxley Section 404 compliance process was a very inward focused approach that was tailored to their specific organization. But what happens when an organization that has achieved compliance wants to add to their business through an acquisition or a merger? How does the organization handle the transition without risking an exception or qualification on their management and audit reports on controls? To look at answers to these questions, our team turned to a utility company that had been previously documented in a prior IARF study on ERM as a model organization. The key was

that the organization we studied was now selling off operations to other organizations who were acquiring the business.

The U.S. Midwestern utility was relatively small and attempting to compete in an environment dominated by large players. It became increasingly clear that the logical business decision was to sell off some smaller business units that fell under specific state regulatory frameworks and required different tracking and control from other business units. However, the acquiring organizations were concerned with the specific issue addressed in this section — how to assure that the acquiring organization's overall Sarbanes-Oxley Section 404 compliance was not jeopardized by the merger. Our case study company used their expertise in Sarbanes-Oxley Section 404 compliance and ERM as a selling point during the process. A little history might help.

The utility was an accelerated adopter of Sarbanes-Oxley Section 404 internal control mandates and accordingly, like most organizations in that era, they focused on a bottom-up approach to controls, identifying key controls in all major processes. The result was an extensive documentation and testing of close to 600 control procedures. With the release of AS 5, the Q&A released by the PCAOB, and the clear message that a top-down approach is what was really desired, the organization took on a retooling of the control processes. At the same time, the CAE undertook an extensive ERM implementation plan. The ERM strategy worked in synergy with the top-down risk-based focus on controls that was desired after the first year of Sarbanes-Oxley compliance. Additionally, the utility purchased software to help automate the documentation and monitoring of control processes. As a result, the utility became a model of how the Sarbanes-Oxley Section 404 compliance process should be handled and how ERM can help make the process more efficient through a risk-based orientation.

The effectiveness with which the utility handled the compliance process was an asset during the business sell-off process. The utility agreed during the sale and acquisition process to provide transition services to maintain the controls over the processes. As transition teams were set up with the acquiring organization to handle the transition across a broad range of business issues, a transition team also was set up to specifically handle Sarbanes-Oxley Section 404 compliance processes. The utility agreed to maintain control processes and procedures, and monitor them for the first three months after the sale. As noted by the CAE, this transition process was not viewed as a Sarbanes-Oxley issue, but rather as a business issue and a part of effective ERM.

One other aspect of interest was the use of SAS 70s for relationships with trading partners. The utility used SAS 70s extensively in the first year of compliance to make sure the bases were covered. With the transition to a risk-based approach, the trading partners were re-scoped and many of the SAS 70s were dropped in the third and fourth years of compliance. This experience and knowledge attained in risk-based compliance was also applied during the transition. When the acquiring organization insisted on a SAS 70 from the utility to cover the three-month transition period, the utility countered that under a risk-based approach, there was no way that the relationship should be considered material and it was therefore an unnecessary control procedure and expense. The acquiring organization reviewed the counterarguments and relented on the requirement of a SAS 70 from the utility.

Review of the sale and acquisition process demonstrates an effective strategy for the transition period that alleviates concerns from a compliance perspective. The process provides a good best practices example for use by other organizations both in terms of considering the process from a risk-based orientation and determining how to handle transition processes smoothly. Just as organizations would do for other aspects of the business, a transition team to facilitate both maintenance of control processes and the integration of ERM strategies should be an integral part of the overall transition process.

## IMPLICATIONS AND CONCLUSION

The results from the research conducted provide an array of insights into the Sarbanes-Oxley compliance process. The Phase I case studies provided insights into the key role that ERM, IT systems and data availability, organizational adaptiveness to change, and the control environment established by the “tone at the top” all played in the difficulty of the Sarbanes-Oxley implementation process and the perceived impediments to supply chain performance. The Phase II survey of a broad range of organizations added clarity to the overall picture as the results confirm the importance of the factors identified in the initial case studies, but also demonstrate that strength across the factors on a whole both eased the difficulty of implementation and actually led to improved supply chain performance. Effective ERM in particular appears critical to making compliance processes work efficiently while at the same time enhancing performance. The Phase III case studies focused on issues surrounding ongoing compliance and provided perspectives on a variety of dimensions — most notably challenges to delisting organizations to avoid regulatory oversight, approaches to protecting compliance during mergers and acquisitions, and negative impacts from failing to both address control deficiencies and embrace control processes as an integral part of critical business processes.

In Phase I, we conducted four case studies with a range in size among SMEs and with both difficult and non-difficult experiences in meeting compliance. All of our organizations adopted a perspective that Sarbanes-Oxley Section 404 compliance was really a focus on improving overall ERM. As such, all four organizations substantially improved their ERM procedures and felt that they benefited from the compliance process. However, the organizations that relied more on manual controls and did not have strong information systems in place to facilitate information sharing struggled through the process. The organizations with stronger information systems had an easier time complying and more effective ERM processes at the end of their first-year experiences. A focus on further automating control processes was a prevalent theme during the subsequent year’s compliance focus. It was also notable that firms that developed stronger ERM processes maintained a better culture in terms of adapting to change — a key component of strategic flexibility. Thus, while the organizations broadly felt their supply chain performance was hampered by lost flexibility (only Company A provided evidence of such an effect), in the team’s discussions with the organizations the lost flexibility was not apparent for the other companies.

Based on these findings, Phase II of the study focused on a broad-based survey of organizations to better understand the relationships among these various factors. We collected survey responses from more than 250 CAEs to learn more about their experiences. The initial analyses focused on organizations’ structures and processes prior to Sarbanes-Oxley Section 404 compliance and the relationship with the difficulty of meeting compliance mandates. The data supports the view that ERM was fundamental to easing the process and also shows that effective ERM drives better integration of information systems with enterprisewide data sharing, enhances strategic flexibility, and leads to a stronger control environment. It is worth noting, however, that the integrated information systems were a critical bridge for effective ERM to drive enhanced strategic flexibility. The analyses also showed that strategic flexibility coupled with a strong control environment were critical to efficient Sarbanes-Oxley compliance efforts.

The survey data also covered organizations’ post-Sarbanes-Oxley organizational structures and processes along with performance. Analysis of this data shows that organizations with stronger ERM post-Sarbanes-Oxley exhibit higher levels of strategic flexibility and better supply chain performance. However, in this post-Sarbanes-Oxley environment, it was clear from the study results that strong, integrated information systems were critical to this positive effect of ERM on strategic flexibility and supply chain performance.

The Phase III case studies focused on specific concerns of interest in a post-Sarbanes-Oxley compliance world. We looked at a company that struggled but made it through the Sarbanes-Oxley process, an organization that failed to achieve control at a level appropriate for a positive Sarbanes-Oxley, and a company who very successfully handled the Sarbanes-Oxley Section 404 compliance process, but due to business and industry issues needed to sell off certain business units while helping the acquiring companies avoid any risk of control weaknesses developing during the transition.

The first company that struggled through the process attempted to delist by going private. The CEO and founder of the company attempted to buy the company back. The board was favorable, but the CEO and founder was blindsided by a private equity firm that came in and outbid the founder to essentially acquire the company's expertise from both a business and a compliance perspective. The events suggested that compliance processes can be an important factor that should be considered when weighing business acquisitions.

The second company basically disdained the compliance process and tried to keep it separate from the actual business processes. This failure to view controls as an integral part of business operations and business processes predictably led to more problems. The company had to report material weaknesses in controls and subsequently the uncontrolled business processes began to unravel and the company's market share dipped substantially. The company eventually merged with a competitor and the joint company continues to struggle to bring processes under control and to reverse the business spiral downward. The business issues can be directly tied to control weaknesses and failures to integrate business processing with effective control procedures.

The third company strongly reinforced a view of compliance process value. This utility sold off several of its units to competitors in the same region. An integral part of the transition process as units transferred to the acquiring companies was the existence of a transition team specifically focused on Sarbanes-Oxley Section 404 compliance issues and the maintenance of controls over processes. The company agreed during the sale to continue managing business processes for the sold-off units for three months post-sale while the units were integrated into the new company's systems and processes.

On an overall basis, our results indicate that effective ERM processes should be an integral part of an organization's strategic vision and operations. Well-controlled companies that manage their risks are shown to have better strategic flexibility, better performance, and enhanced value. Ultimately, the results of this study suggest that the Sarbanes-Oxley Section 404 compliance process helped most organizations and that better controls lead to more successful businesses. As one of our case participants noted, "Sarbanes-Oxley does not ask for companies to do anything that they should not have been doing already."

## **UNDERSTAND, SHAPE, ADVANCE**

*The IIA Research Foundation is a 501(c)(3) corporation formed to expand knowledge and understanding of internal auditing by providing relevant research and educational products to advance the profession globally.*

*Through its research reports, Bookstore products, and GAIN Knowledge Services, The Foundation provides resources that help understand, shape, and advance the global profession of internal auditing by initiating and sponsoring intelligence gathering, innovative research, and knowledge-sharing in a timely manner.*

*To learn more, visit [www.theiia.org/research](http://www.theiia.org/research)*

**ISBN 978-0-89413-671-9**

**Item #2019.dl**

**Free to IIA Members**

**Non-members: US\$40**

