

Executive Snapshot

Reframing IT Audit and Control Resource Decisions

Study shows top performers gain performance
improvement through use of IT controls

Based on findings of the IT Controls Performance Study



Advancing the Science
of IT Management

IT Process Institute
www.itpi.org

©2006 IT Process Institute

Summary

Many IT executives view spending on IT audit and control activities as a necessary burden required to comply with industry regulations such as Sarbanes-Oxley. The increasing costs related to implementing and maintaining IT controls have prompted many IT executives to frame IT control investment decisions in terms of minimizing ongoing cost. A more productive perspective for making IT control investment decisions is to view IT controls as an effective way to better manage and improve IT operations, security, and audit processes.

To show that IT controls improve performance, the IT Process Institute conducted a study of how IT controls affect operations, security, and audit measures. Our approach was to study top-performing IT organizations so that we could identify the specific IT controls that have the greatest impact and quantify the potential performance improvement for organizations that have ongoing investment in control activities.

Our conclusion is that when IT organizations focus ongoing audit- and control-related resources on those foundational control activities that have been proven to improve performance measures, then they will generate a significant return on investment realized through improvements in a wide range of key performance measures.

Many IT executives view IT controls as a necessary burden. They must comply with a variety of new regulations in addition to managing the already difficult trade-off between running existing infrastructure and supporting new strategic business initiatives. Many believe that Sarbanes-Oxley Section 404, industry regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Basel II, and other country-specific regulations such as privacy laws have received a forced level of priority in their organizations.

Although some IT executives reluctantly agree that financial disasters such as Enron and WorldCom would not have happened if Sarbanes-Oxley had been in place, they see the business at large—not the IT organization—as the primary beneficiary of these laws. They observe an increase in spending on IT control activities, putting an undo resource and financial burden on the IT organization.

Framing IT Control Resource Decisions

The increasing costs related to implementing the IT controls necessary to comply with various regulations have prompted many IT executives to frame IT control investment decisions in terms of minimizing the ongoing cost of IT controls. Framing a decision inevitably sets boundaries. The focus on cost may have created a mental framework that restricts the potential solution set and that causes these executives to lose sight of important objectives and overlook the best solution options.

For example, consider how U.S. automakers framed the problem of improving efficiency in the 1940s to the 1970s. Many framed the problem as how many cars should be made in a single production run before changing to a different model. Their production run calculations assumed changeover time was fixed at approximately 6 to 8 hours. Their frame blocked out the idea that changeover time itself could be cut.

The focus on cost reduction may have created a mental framework that restricts the potential solution set.

The Japanese framed the question of manufacturing efficiency quite differently. They realized they could make the entire system more efficient if they reduced changeover time. They could better utilize invested capital, carry smaller inventories, and offer a larger variety of model options if they sped up changeover. Two decades later, while U.S. companies still used analyses that assumed changeovers took an entire shift, automakers in Japan had achieved changeover that took only minutes. One Toyota plant could change models in as little as 44 seconds.¹ As a result, Japanese auto manufacturers achieved competitive advantage through improved efficiency, agility, and return on invested capital.

¹ Russo and Schoemaker, “Decision Traps,” Fireside, 1989.

Reframing Ongoing Resource Decisions

Similarly, IT executives can reframe ongoing IT control resource decisions in terms of performance improvement potential, instead of cost reductions. If IT executives view IT controls as an effective way to improve IT operating performance through better management of IT operations, security, and audit processes, then they can more effectively allocate resources to those areas that are related to improvements in key performance measures.

The effective use of IT controls contributes, in part, to the superior operating results of IT departments that have the best overall performance. We have observed that top performers tend to have a rigorous and cultural commitment to process management, and they focus on process measurement and improvement as a strategic approach to improving IT service and performance. We have also observed that the top performers integrate IT processes and IT controls into their daily operations. They view IT controls as more than a requirement to pass an audit to meet regulations. They see IT controls as a way to help enforce consistent use of recognized processes and procedures that are proven to improve performance.

A more productive perspective is to view IT controls as an effective way to improve IT operating performance.

Studying the Results of Top Performers

The IT Process Institute conducted a study of how IT controls affect operations, security, and audit measures. We designed a study to create empirical evidence that will help IT organizations guide ongoing IT audit and control investment decisions. Our approach was to study top-performing IT organizations so that we could identify the specific IT controls that have the greatest impact on performance and quantify the potential performance improvement for organizations that have ongoing investment in control activities.

Our underlying assumption is that IT organizations can focus IT audit and control resources in specific areas that will generate positive return on investment through improved performance. Our theory is that IT audit- and control-related activities are not just a necessary cost that IT organizations must incur to achieve regulatory compliance. The effective use of IT control activities found in frameworks such as ITIL[®], COBIT[®], and ISO 20000 (formerly BS 15000) can improve operating performance.

To test this theory, the IT Process Institute formed a research team that included IT practitioners and researchers from Carnegie Mellon University, Florida State University, and the University of Oregon. We conducted an extensive Web-based survey of primarily North American IT organizations from August 15 to October 30, 2005. The survey included 97 required and 97 optional questions. Respondents from 98 IT organizations in many industries voluntarily completed the surveys. These organizations varied in size: 40 percent of respondents have more than 100 people in their IT organization, and 43 percent of respondents are director-, VP-, or C-level executives.

The survey asked a broad range of questions designed to support analysis of 63 COBIT control activities and 25 key operations, security, and audit performance measures. We looked at controls in six groups, including access controls, change controls, release controls, configuration controls, service level controls, and resolution controls. The number of performance measures for which respondents scored in the top 50th percentile of all respondents determined the top, medium, and low performers.

Top Performers Have More IT Controls

We analyzed the survey results and determined that the increased use of IT controls does correlate with higher performance across a broad range of operations, security, and audit performance measures. The top-performing IT organizations have more IT controls in place and have significantly higher performance measures that suggest better resource utilization.

The presence of a correlation between control activities and performance measures indicates that the best practices outlined in the ITIL and COBIT frameworks do improve performance measures.

Top-performing IT organizations have more IT controls in place.

Some IT Controls Have Bigger Impact

We assume that with limited resources, IT organizations can't focus with equal vigor on all the best practices found in the eight ITIL books and 312 COBIT controls.

Although a number of industry leaders prescribe various implementation paths through these best practices, we have not found empirical studies that are designed to identify a subset of these practices that create the biggest performance improvement.

In addition, although organizations must implement a broad range of IT controls to manage risk and meet an increasing number of regulatory requirements, we assume that a small set of controls will most significantly affect performance measures. Indeed, within the six groups of controls we call foundational controls, we identified a subset of 21 control activities that have the greatest impact on the broadest set of operations, security, and audit measures.

Top Performers Are Different in a Few Key Areas

The subset of foundational controls that most differentiate top from medium performers are change and configuration controls. Answers to the following survey questions separated the top performers from the medium performers:

- Do you monitor systems for unauthorized changes?
- Are there defined consequences for intentional unauthorized changes?
- Do you have a formal process for IT configuration management?
- Do you have an automated process for configuration management?
- Do you track your change success rate?
- Are you able to provide relevant personnel with correct and accurate information on the present IT infrastructure configurations, including their physical and functional specifications?

Top performers consistently use controls to enforce processes and avert high-risk activities. Not only do control activities proactively stabilize the IT environment, but they also sustain and continuously improve the control systems themselves.

Quantifying Performance Improvement Potential

The obvious question, then, is how much performance improvement is possible for IT organizations considering a focused investment in foundational control activities? To quantify improvement potential, we compared the performance measures of the respondents in the high-, medium-, and low-performing clusters.

Top performers with foundational controls in place have significantly better operational performance.

Top performers that have foundational controls in place have significantly better operational performance measures than medium and low performers:

- Top performers have a **12 percent lower rate of unplanned work** than medium performers, and 37 percent lower than low performers.
- Top performers have an **11 percent better change success rate** than medium performers, and 25 percent better than low performers.
- Top performers have a **first fix rate that is 45 percent greater** than medium performers, and 56 percent greater than low performers.
- Top performers support **2.5x more servers per system administrator** than medium performers, and 5.4x more than low performers.

Analysis of the top performers in this study shows that when IT organizations frame IT control resource decisions in terms of performance improvement potential and when they focus ongoing audit- and control-related resources on those foundational control activities that have been proven to improve performance measures, then they will generate a significant return on investment realized through improvements in a wide range of key performance measures.

Additional Resources

IT Controls Performance Research Report

This 70 page report provides a detailed analysis of how IT Controls improve audit, security, and operations performance. The report provides compelling empirical evidence for organizations wanting to optimize IT Controls investments.

The report provides useful guidance including how ITIL and COBIT practices correlate with performance measures, a list of 21 Foundational controls that have the largest impact, a list controls that differentiate top performers, detailed comparison of performance measures for top, medium, and low performers, and a compelling summary of performance improvement potential for those using IT controls.

IT Controls Performance Benchmark

This simple on-line tool is based on the findings of the IT Controls Performance Research Report. It asks 45 questions about the presence of specific IT controls, and 15 questions about specific performance measures that vary the most from organization to organization.

Use this benchmark to find out if your organization is using the foundational controls that matter most, and compare your performance measures to those of the top, medium, and low performers identified in the study.

The output is a simple and compelling 8 page report that includes a color coded comparison of your performance measures to the study participants, a color coded comparison of your use of foundational controls, a detailed comparison to those foundational controls that differentiate top performers, and a detailed comparison of your use of all controls to top, medium, and low performers.

About the ITPI

The IT Process Institute (ITPI) is an independent research organization that exists to support the membership of IT operations, security, and audit professionals. Our mission is to advance IT management science through independent research, benchmarking, and prescriptive guidance. Our vision is to pair industry-based volunteers with leading university-based researchers to identify and study top-performing IT organizations and enhance the efficiency and effectiveness of the industry.

The research report and benchmark are available for purchase at www.itpi.org.

© 2006 IT Process Institute. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form other than PDF by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written authorization of the IT Process Institute. Submit requests to info@itpi.org.

ITIL® is a Registered Trade Mark and a Registered Community Trade Mark of the Office of Government Commerce and is registered in the US Patent and Trademark Office. COBIT® is a registered trademark of the IT Governance Institute.