

# **LEVERAGING IT CONTROLS TO IMPROVE IT OPERATING PERFORMANCE**

**By  
Daniel Phelps and  
Kurt Milne**

**June 2008**

## **Disclosure**

Copyright © 2008 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) International Professional Practices Framework for Internal Auditing (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 978-0-89413-625-2

08276 06/08

First Printing

## TABLE OF CONTENTS

Executive Summary .....	1
Foreword .....	4
Acknowledgments .....	5
About the Authors .....	6
Preface .....	7
 Introduction .....	 8
 Chapter 2: Study Scope .....	 13
 Chapter 3: Summary of Key Findings .....	 19
 Chapter 4: Understanding the Impact of Foundational Controls .....	 23
 Chapter 5: Application of These Findings .....	 37
 Chapter 6: Performance Improvement Potential .....	 39
 Appendix A: Glossary of Terms .....	 61
 Appendix B: Clustering IT Organizations Based On Control Use, Performance, and Size .....	 62
 Appendix C: Identifying Foundational Controls .....	 70
 Appendix D: Assessing the Impact of Process Maturity .....	 75

### List of Tables

Table 1 .....	16
Table 2 .....	18

### List of Figures

Figure 1 .....	14
Figure 2 .....	41
Figure 3 .....	42
Figure 4 .....	43
Figure 5 .....	44
Figure 6 .....	45
Figure 7 .....	46
Figure 8 .....	47
Figure 9 .....	48
Figure 10 .....	49

**List of Figures (cont'd)**

Figure 11 .....	50
Figure 12 .....	51
Figure 13 .....	52
Figure 14 .....	53
Figure 15 .....	54
Figure 16 .....	55
Figure 17 .....	56
Figure 18 .....	57
Figure 19 .....	58
Figure 20 .....	63
Figure 21 .....	64
Figure 22 .....	65
Figure 23 .....	66
Figure 24 .....	67
Figure 25 .....	68
Figure 26 .....	70
Figure 27 .....	72
Figure 28 .....	75

## EXECUTIVE SUMMARY

The Institute of Internal Auditors Research Foundation (IIARF) and the Institute of Internal Auditors (IIA) Advanced Technology Committee invited the IT Process Institute (ITPI) to participate in the IT Audit Research Symposium held June 18, 2006, in conjunction with The IIA' International Conference in Houston, Texas. Subsequently, The IIARF commissioned ITPI to conduct a study of how information technology (IT) controls impact operational performance. The study was designed to give IT audit and operations professionals empirical data about which IT controls have the biggest impact on operational performance, and about the effect of higher levels of IT control process maturity. The study did not look at how IT controls reduce risk, but instead focused on how IT controls that are often mandated by regulatory requirements also improve performance if implemented at sufficient levels of process maturity.

A Web-based survey was completed by 330 executives from North American-based IT organizations. Data about 15 performance measures and the use and maturity of 53 IT controls was analyzed to reveal three key findings:

1. IT controls do improve operating performance, and some IT controls improve performance more than others. We found that just three controls predict 45 percent of the performance difference across those organizations that have fewer controls in place, and that tend to be smaller organizations. Those controls in order from highest to lowest impact include:
  - 1) A defined process to detect unauthorized access.
  - 2) Defined consequences for intentional, unauthorized changes.
  - 3) A defined process for managing known errors.

The amount of performance variation related to just three controls is significant. We recommend that all IT organizations implement these key controls in order to optimize performance improvement potential.

2. IT controls impact the performance of smaller and larger organizations in different ways. We found another set of nine controls that predict 60 percent of the performance variation of organizations with a greater number of controls in place, and that tend to be larger organizations. Those controls in order from highest to lowest impact include:
  - 1) A defined process to analyze and diagnose the root cause of problems.
  - 2) Providing IT personnel with accurate information about the current configuration.
  - 3) Changes are thoroughly tested before release.
  - 4) Well-defined roles and responsibilities for IT personnel.
  - 5) A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents.
  - 6) A defined process to identify consequences if service-level targets are not met.
  - 7) A defined process for IT configuration management.
  - 8) A defined process for testing releases before moving to the production environment.
  - 9) A configuration management database describes the relationships and dependencies between configuration items (infrastructure components).

We recommend that larger organizations with more than 200 IT staff or 5,000 total employees implement these three plus nine IT controls.

3. This study confirms that organizations with higher levels of IT control process maturity have higher levels of IT operational performance. The maturity of the IT control processes, as indicated by monitoring and management of process exceptions, also impacts the performance improvement potential of these foundational controls.

The performance improvement potential of using foundational controls at higher process maturity levels is significant. The organizations in the study that scored in the top 15<sup>th</sup> percentile of overall performance exhibit significantly higher performance on a range of key measures including change success rate, server to system administration ratio, first fix rate, as well as security and customer satisfaction measures.

Although there are a number of factors that contribute to performance that were not analyzed in this study, the large degree of performance variation that is predicted by the use of the foundational controls suggests that IT organizations that implement these key controls have significant performance improvement potential. IT audit and operations professionals should evaluate and consider use of these 12 foundational controls as baseline “hygiene” controls even if they pursue a top-down risk and control analysis.

These findings suggest eight specific ways that IT audit and IT operations professionals can leverage these findings to improve the return on the investment of IT control activities:

1. Reposition IT controls as a performance improvement tool. This study gives IT audit the opportunity to build a business case for IT control activities related to their performance improvement potential. This helps reposition IT controls from being an externally imposed incremental cost to being a proven strategy for improved performance.
2. Reposition IT operations’ relationship with IT audit. IT audit should be viewed as a partner who can help verify that the carefully designed procedures and controls that improve performance are actually followed throughout the organization. However, IT operations should own the implementation and management of controls that impact general operating processes and procedures.
3. Implement foundational controls at a target process maturity level. The foundational controls should be implemented at a level where process exceptions are detected and managed, and exceptions have consequences.
4. Use IT controls to initiate a systematic program of ongoing process improvement. Build on process definition and data collection requirements mandated by both internal and external audit to also set aggressive but achievable performance improvement goals.
5. Use compliance as a mandate to adopt a process orientation. IT executives should purposefully set the tone at the top that following documented processes and procedures is a basic job expectation for all IT personnel.
6. Engineer cultural changes using human resources and the thoughtful application of both the “carrot” and the “stick.” Work with operations and HR to engineer the appropriate mix of positive and negative incentives to enable lasting behavioral change.

7. Use this study to benchmark control maturity and operational performance. Work with IT operations to compare your organization to the top, medium, and low performers in this study. Use the results to identify areas for increased focus and process maturity.
8. Use the study measures as the foundation of an audit and operations shared performance dashboard. Focusing the measures on control activities that simultaneously reduce risk and improve operating performance is an ideal place to integrate IT audit and operations-monitoring activities.

## FOREWORD

This study should be of interest to all IT auditors. The IT audit community should focus on the risks both within an organization's IT environment as well as those arising through the organization's use of technology. This study provides insight into several key factors that auditors can utilize to bring an organization long-term benefits from IT audit and control activities.

The IT auditor, in concert with the entire internal audit community, is always seeking ways to add value to the enterprise through the execution and recommendations delivered from IT audits. However, in the past several years IT auditors have increasingly focused on the identification of risks and the compliance objectives related to regulations such as the U.S. Sarbanes Oxley Act of 2002. These increased and focused efforts have resulted in an overall increased awareness of the IT auditor's role and value to the organization. This study provides considerable insight to the IT audit community related to overall IT risk management and could have significant positive impacts on the business as a whole, through both a reduction of risk as well as increased IT business process effectiveness.

The IT audit community is focused on business and IT risks and the controls needed to mitigate those risks. This study helps the auditor to understand and evaluate key controls from both a completeness and accuracy standpoint as well as from an operational effectiveness standpoint. In fact, this study also provides guidance on which controls contribute to both traditional risk mitigation and operational excellence. As the IT auditor moves from risk assessment through audit execution, auditors are tasked with providing recommendations to close control gaps and/or suggest improvements to the IT process controls. Because this study is focused on the control aspects around IT operational process areas, it provides a performance-oriented basis for making specific control recommendations. In working with audited parties to create appropriate action plans, the IT auditor could reference this study, which describes the value derived from related control recommendations and provides a strong, proven basis for the recommendation.

A second key learning from this study is the impact of process maturity on how related controls effect the overall control environment. As the IT auditor more clearly understands the design of related process where the control resides, he or she really understands the maturity of the process. This study shows definitively that increased process maturity improves the overall ability of the organization to mitigate its risks and have adequate controls for its processes. As IT auditors read and understand the study, they will be able to bring enhanced value to related IT audit areas. This value will be mainly through recommendations that have a higher overall value to the organization through both the improvement of the control environment and adding to operational efficiency of the process.

Each IT auditor needs to understand the risks and controls that are resident within the audited IT environment as well as the process maturity of the process being audited. This study provides the auditor with powerful, quantified research that outlines the value that these controls bring not only to mitigating the traditional IT audit risks, but to improving the operating effectiveness of the IT organization, improving its value to the organization as a whole. The result is that the IT auditor is now better enabled to be a valuable partner to the enterprise.

Jeff Weber  
Managing Director  
Protiviti

## ACKNOWLEDGMENTS

This report reflects the current state of our ongoing exploration of the impact of IT controls on operating performance. We could never have learned so much about the application IT controls without the ongoing help and support of many people and organizations along the way. As we developed this study and wrote this report, we had wonderful discussions about bridging the gap between study and practice with a wide range of friends and colleagues.

Special thanks to The Institute of Internal Auditors Research Foundation (IIARF) for their vision and funding for this type of applied research. Specific thanks to Jeffrey Swerdlow, project director, and Herriot Prentice, director, Standards and Guidance, for ongoing insight. Additional thanks to The IIARF's BREA Committee, the Board of Trustees, and the member review team who gave pointed and invaluable feedback on the structure and presentation of the study's findings. Thanks also to Lily Bi, Joe Clooney, Ulrich Hahn, Steve Mar, Mark Salamasick, Don Sparks, and Doug Ziegenfuss.

We extend a special thanks to Gene Kim, chief technology officer at Tripwire, for tireless support and guidance throughout this effort. Gene's willingness to roll up his sleeves and help with every step of this project made this effort possible. Jeff Weber and Christopher Holm at Protiviti also gave invaluable guidance, offering an ever-ready sounding board for ideas and findings that emerged throughout the analysis of the study data. Jay Taylor at General Motors provided insight into how to share study findings in a way that is most relevant to IT auditors. Sasha Romanosky, Ph.D. student at Carnegie Mellon University, also provided a constant voice of reason, helping think through the logic of our research questions and findings. He also provided ongoing analysis support as we worked through the data associated with this study.

The team at GCR Insight, our survey and analysis firm, offered ongoing support and insight into this type of research. Special thanks to Jason Ball, who managed the lion's share of the survey and analysis work, and Dr. Scott Evans, for his creative and astute ideas about how to construct and test relevant and actionable research questions.

We also thank our feet-on-the-street practitioners, George Spafford at Pepperweed Consulting, and Steve Gerick at Information Technology ProPartners, for real-time input on IT audit and operations practices that work. Also, Scott Alldridge and Steve Darby at IP Services have given us an inside look at SAS70 audit results as well as the procedures and controls environment in a world-class IT service provider environment.

Thanks go out to the unending support of Ron Neumann, Temple Burke, and Mary Matthews at the IT Process Institute which allows us to focus on research.

Mollyann Brodie, vice president, director, Public Opinion and Media Research of the Henry J. Kaiser Family Foundation, and David Erickson of the Federal Reserve Bank of San Francisco deserve special thanks for their encouragement to think big and solve problems that help change the industry.

## ABOUT THE AUTHORS

### **Dr. Daniel Phelps - Primary Researcher**

Dan Phelps is the research lead on the IT Controls Performance Study. He is an information scientist with broad research interests in information systems and technology, particularly related to information assurance, community development, and best practices. His graduate work in information studies was done at Florida State University and in computer science at James Madison University.

### **Kurt Milne - Managing Director, IT Process Institute**

Kurt Milne is the managing director of the IT Process Institute (ITPI), and primary writer of this research report. He has over 15 years' experience in various engineering, marketing management, and business development positions at leading technology companies. His main areas of expertise include IT service management and IT controls, inventory and supply chain management, and computer integrated manufacturing. He is responsible for overall ITPI operations, including research, sponsorship, and membership. Kurt helped provide ongoing management of this research project and was the primary writer of the findings.

### **About the IT Process Institute**

The IT Process Institute is an independent research organization that exists to support the membership of IT audit, security, and operations professionals. Its mission is to advance IT management science through independent research, benchmarking, and the creation of prescriptive guidance. The IT Process Institute's vision is to pair industry-based volunteers with leading university-based researchers to identify and study top performing IT organizations in order to identify proven practices that enhance the efficiency and effectiveness of the industry. [www.itpi.org](http://www.itpi.org).

## PREFACE

This study is based on the assumption that organizational performance is something that can be understood, predicted, and shaped. In our research, we seek to identify operating variables that produce variations in performance. Due to the increased use of IT controls as a way to meet the requirements of various industry regulations, we seek to understand how the use of IT controls impacts the performance of IT processes and procedures. And, more specifically, our goal is to provide empirical evidence that helps IT audit and operations professionals focus resources on specific control activities that are shown to improve operating performance.

The study of organizational performance can be challenging. First, it is difficult to identify the true causal relationship between activities and results based on information generated by a survey. Second, we do not collect data on a wide range of activities and practices that impact performance results. Business strategy and the role IT plays in supporting that strategy vary widely. And, factors such as IT employee skill level, pay scale, and management style all may affect the performance of IT organizations. Third, it is only feasible to collect a limited amount of data about each organization in the study. We designed the study to collect data about controls we think are most likely to impact performance measures, based on the findings of a pilot study. However, there may be other types of controls that cause performance variation that are not included in our study. Fourth, there are problems with collecting survey data using questions designed to collect a single answer about both the use and maturity of IT controls, as well as performance measures. IT control use and maturity and resulting performance may vary across departments or locations within an IT organization, making it difficult to generalize a response to a survey question.

That said we believe we have overcome many of these challenges and designed a study that identifies practices that predict performance variation. This study follows a preliminary study conducted by the IT Process Institute in 2006, which identified a limited number of IT controls that best predict performance variation. In this second version of this work, we have modified survey questions to address some of the limitations of the previous work. For example, we have given survey respondents a range of answers about the process maturity of each control studied, instead of a yes or no answer about whether each control is in use. We have also modified the performance measures used to include those variables that are primarily impacted by the use and maturity of controls.

Based on our previous work and refined methods in this study, we are confident that the results can help internal auditors and IT operations managers understand the impact of the IT controls they have put in place in their IT organization. Our hope is that IT audit and operations professionals use these findings to apply resources in those areas in order to improve their own performance.

# CHAPTER 1

## INTRODUCTION

There are an increasing number of industry and federal regulations that impact the operations of IT organizations. More and more, many IT organizations across industries and in the public sector are focusing IT resources on compliance with these various regulations. Many of the regulations, such as Sarbanes-Oxley section 404, the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (Financial Modernization Act, 1999) in the U.S., and several European consumer data privacy regulations, explicitly mandate the control of various business processes and the control and protection of sensitive data. In order to demonstrate such control, IT organizations implement and manage various IT controls to address risks associated with software applications and the underlying IT server, network, and data management infrastructure that support the proper function of the applications.

Control is defined as the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected, and corrected.<sup>1</sup> IT controls provide for assurance related to the reliability of information and information services, and help mitigate the risks associated with an organization's use of technology.<sup>2</sup>

The primary purpose of IT controls is to mitigate specific risks that have been identified by the organization. A top-down approach to IT risk management starts with identifying individual risks that could jeopardize the integrity and security of software applications, IT infrastructure, and data sources that support key business processes. Then, the appropriate level of risk is determined for the organization, and specific IT controls are implemented to prevent, detect, and correct activities to mitigate the identified risks. Audit activities focus on testing and verifying that the controls actually work as designed to validate their effectiveness as risk reduction mechanisms.

But we wonder, what is the impact of these controls on how IT organizations manage the ongoing operation of production systems? There is widespread agreement that IT organizations are focusing and spending more on IT control activities to address compliance requirements. But IT organizations still have to run the shop while they implement and manage controls. Do IT controls enhance or detract from the primary objective of IT operations, which is to deliver and support business-aligned IT services and capabilities at a reasonable cost?

Different categories of IT controls might impact IT operating activities to various degrees. Application controls are embedded in applications to verify the accuracy, validity, and completeness of data, and do not overlap directly with most IT operational functions. Other controls, however, are embedded in IT processes and services that already exist in a normally functioning IT organization, such as systems development, change management, security, and operations.<sup>3</sup>

The IT controls that are embedded in operating processes are of particular interest, as IT organizations are often required to modify their operating practices in order to implement controls. IT audit criteria dictate that various processes and procedures run at a more rigorous level than they might otherwise without control and audit requirements applied.

For example, every IT organization makes changes to applications that enable key business functions, and the underlying servers, databases, and networks on which they run. The organization's typical way of

making changes to production systems may or may not be specified, documented, or repeatable. However, change management controls require the process and procedures related to making application and system changes follow documented procedures that are consistently followed, and that records are kept that can be used to verify specific actions were taken. Similarly, every IT organization regularly assigns and manages application and system passwords. IT access and identity controls mandate the use of defined processes and procedures that should be followed in order to address risks associated with granting or managing access.

However, regardless of the type of control or method of implementation, the overarching principle that drives IT control activities is that a control is based upon a specified way of doing things. And, to be effective, the control must be used consistently in the course of executing related processes and procedures. Controls that are documented but not consistently followed fail to meet basic requirements and adequately address the risks they are designed to mitigate.

### **IT Controls Impact on Operating Process and Procedures**

The impact of implementing IT controls in the IT production environment results from two primary mechanisms. First, the working function of various processes and procedures may change as the result of meeting control requirements. Implementing IT controls may require IT staff to change the way they do things as they perform their regular job functions. People may need to get authorization or approval for activities they previously executed without oversight. Systems may need new software to track workflow activities. Organizations may need to collect more data to store records about individual tasks and timestamps in order to create an audit trail. All of these changes potentially impact the working function and operating results of an IT organization.

Second, implementing IT controls in the IT production environment may also increase the consistency of how various activities are performed. IT organizations may not have a history of identifying and following specific procedures in many functional areas within IT. Many IT organizations have historically valued and rewarded individual contributors who innovate and try new ways of solving technical problems. The natural inclination of many technical professionals is driven by curiosity and motivation to understand and solve technical problems. However, IT controls require that everyone in the organization agree to follow documented practices and procedures. Activities that previously were influenced by personal preference or skill level may now be standardized across functional groups and geographically dispersed locations in order to meet control requirements and reduce audit costs. The increased consistency of practice may impact the performance of various operating processes.

The introduction of IT controls into an organization that does not have a culture that supports following documented processes and procedures can be problematic. Many organizations that have not historically had well documented process and work procedures are now turning to best practice frameworks such as the IT Infrastructure Library (ITIL ®), and control frameworks such as COBIT. However, they may not have a process-focused organizational culture, and may not have a commitment to process discipline that is needed to ensure that best practice activities and control are consistently performed. Organizations that do not have a history of following specified procedures may require remediating controls to shore up other controls, which will in turn increase the overall number of controls and cost of implementation, ongoing management, and audit. Additionally, a growing number of controls may tip the balance and unduly restrict operating processes and impede the basic operational functions in IT.

In broad terms, IT organizations may respond to general IT controls in one of two ways. Some IT organizations that have a culture that supports following defined processes and procedures may view IT

controls and IT audit activities at worst as a minor change that requires additional documentation, testing, and verification, and at best as an effective addition to a broader strategy of having defined processes. These control supportive organizations already follow prescribed operating procedures and collect data to verify control processes as part of ongoing operational efforts. As a result, IT controls support their general strategy for achieving performance goals.

Other organizations that have a culture that supports individual preference may view IT controls and IT audit activities as an externally imposed burden or impediment to achieving operating goals. They may focus on flexibility and responsiveness as an overall IT strategy that best meets the needs of the business. As a result, IT controls may at best require significant effort to document and train IT staff to follow prescribed processes and procedures, and at worst be at odds with their general strategy for achieving performance goals. As a result of new regulatory requirements, these organizations may view implementing and auditing IT controls as a “checkbox” activity that imposes a burden on already stretched IT resources, and may not view IT controls as something that can help them in their quest for higher levels of operating efficiency and effectiveness.

This bifurcation of IT organization “personality” poses some interesting questions about the impact of IT controls. Do IT controls improve operating performance? Do IT controls need to be implemented at a high level of process maturity to achieve performance improvement? Do controls improve performance more in organizations that already have a process culture and environment that support following documented processes and procedures?

For organizations that already have a processes and procedures orientation, IT controls and the audit of those controls simply may prove that optimally designed processes and procedures are actually being followed. In those organizations, we might expect to find that IT controls that are naturally implemented at a higher level of process maturity serve as a means to identify variance from approved procedures. For other organizations that do not have a controls orientation, IT controls and the audit of those controls may be naturally implemented at a lower level of process maturity, and only be viewed as an activity that is followed at the lowest level required to meet regulatory requirements.

## **Research Question and Objectives**

The overarching research question for this study is “What is the impact of IT controls on IT operating performance?”

The various lines of questions related to this overall question are:

- Do organizations that use IT controls have higher levels of IT operations performance than those that do not?
- If IT controls do improve performance, then are there specific IT controls that impact performance more than others? Which ones?
- Do IT controls need to be used at a minimum level of process maturity in order to impact performance?
- Finally, what is the performance improvement potential that is possible with the use of key IT controls implemented at the required level of maturity?

Our objective for this line of questioning is to help IT organizations allocate scarce resources in areas that are proven to improve performance in order to drive performance gain as well as risk reduction from IT control activities.

## Summary of Findings

We used data from 330 IT organizations to answer these questions. We found that IT controls do impact overall performance as measured by an index of 15 key performance metrics. There is a subset of the controls we studied that strongly predicts the highest levels of performance across the organizations that participated in the study. We found that three specific types of controls best predict performance differences across those organizations that have fewer controls in place, and that tend to be smaller organizations. Those controls in order from highest to lowest impact include:

1. A defined process to detect unauthorized access.
2. Defined consequences for intentional, unauthorized changes.
3. A defined process for managing known errors.

We found another set of nine controls that best predict performance across organizations with a greater number of controls in place, and that tend to be larger organizations. Those controls in order from highest to lowest impact include:

1. A defined process to analyze and diagnose the root cause of problems.
2. Providing IT personnel with accurate information about the current configuration.
3. Changes are thoroughly tested before release.
4. Well-defined roles and responsibilities for IT personnel.
5. A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents.
6. A defined process to identify consequences if service-level targets are not met.
7. A defined process for IT configuration management.
8. A defined process for testing releases before moving to the production environment.
9. A configuration management database describes the relationships and dependencies between configuration items (infrastructure components).

We also found that control process maturity matters. Those organizations that have controls implemented at a higher level of process maturity have higher performance than organizations with the same controls implemented at a lower level of process maturity. As a result, we recommend that organizations manage control processes at a level where process exceptions are monitored and managed to reduce causes of process variation.

Finally, we quantified the performance difference between the top, medium, and low performing organizations in the study.

The study data allows IT audit and operations groups to benchmark their control process maturity and performance against the other organizations in the study. IT audit and operations can use a maturity and performance dashboard to jointly monitor the impact and effectiveness of IT control efforts.

## Why These Findings are Important to the Internal Audit Profession

The IIA defines internal auditing as “*an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*”<sup>4</sup>

Understanding the performance impact of the IT controls that are being audited is a powerful way to “add value and improve an organization’s operations.” As IT audit approaches operations management with information about how well they are following documented controls, the results of this study can be used not only to help illustrate which IT control activities are good predictors of improved performance, but also show why consistently following documented processes and procedures is important to achieving performance improvement.

Better understanding of the positive impact of IT controls helps IT operations executives understand the benefits associated with the costs of managing and auditing controls. This “business-level” discussion helps increase the level of communication and strategic value of internal auditing, and builds management’s confidence in internal auditing’s assurance and consulting abilities.

## Report Outline

In Chapter 2 we summarize the scope of IT controls and performance measures used in our analysis. In Chapter 3, we summarize four key findings, including the identification of 12 foundational controls revealed by the analysis. In Chapter 4, we take a closer look at the six categories of controls we studied and explore why the foundational controls impact performance more than other controls. In each control area, we highlight specific recommendations based on the study findings that can be used by IT auditors. In Chapter 5, we suggest eight ways that IT auditors can use the study findings and this report to modify and improve working relationships with IT operations. In Chapter 6, we explore the performance improvement potential related to the 15 measures in the study.

We conclude with four appendixes. Appendix A is a glossary of terms used in this study. Appendix B presents details about the analysis used to identify five clusters of IT organizations in the study. Appendix C details the analysis used to identify the 12 foundational controls. Appendix D details the analysis of process maturity impact on performance and what process maturity measure is recommended based on analysis of the study data.

<sup>1</sup> COBIT 4.0 Control Objectives Management Guidelines Maturity Models (Rolling Meadows, IL: IT Governance Institute, 2005) p. 14.

<sup>2</sup> Global Technology Audit Guide, Information Technology Controls (Altamonte Springs, FL: The Institute of Internal Auditors, 2005), p. iii.

<sup>3</sup> COBIT 4.0 Control Objectives Management Guidelines Maturity Models (Rolling Meadows, IL: IT Governance Institute, 2005) p. 15

<sup>4</sup> IIA Web site, definition of internal auditing. <http://www.theiia.org/guidance/standards-and-practices/professional-practices-framework/definition-of-internal-auditing/?search=internal%20audit%20definition>

## CHAPTER 2

# STUDY SCOPE

Our overall research question with this study is “What is the impact of IT controls on IT operating performance?” To answer that question, we developed a data collection survey and analysis plan to test the hypothesis that there exists a subset of IT controls that impact IT operating performance to a greater extent than other IT controls.

This study repeats the general approach used for a pilot study conducted by the IT Process Institute in October 2005 titled “IT Controls Performance Study,” which forms the basis for this work. In this follow-on study, we have modified the survey tool and analysis approach to strengthen the findings of the previous work.

The data analyzed in this study was collected by GCR Insight, an independent market research firm based in Portland, Oregon. Data was collected through a Web-based survey that was distributed via e-mail between November 28, 2006, and January 31, 2007. E-mail invitations were sent to multiple e-mail lists, including GCR’s IT decision maker panel, a list of IIA North American members with IT audit-related job titles, IT Process Institute members, and Protiviti newsletter recipients.

### **Study Demographics**

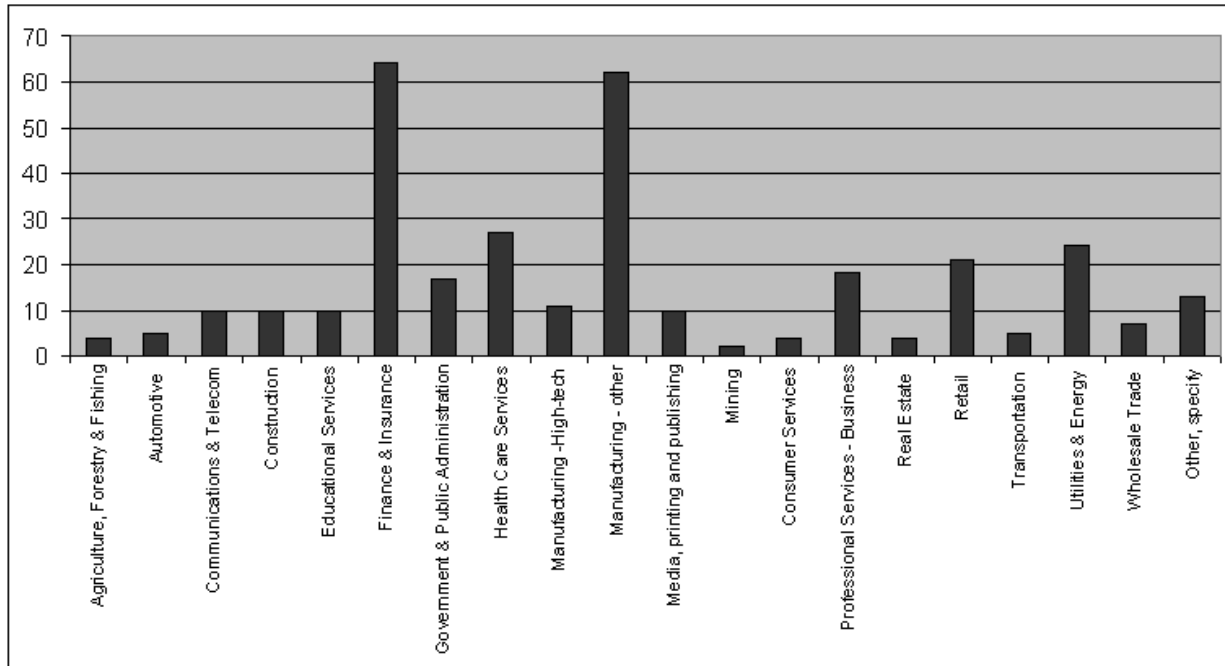
We used data from 330 organizations for analysis. Survey respondents were primarily at the director and executive levels. Fifty-three percent of respondents were IT director, IT vice president, or IT executive level; 35 percent were manager level; and 11 percent were individual contributors.

The data represented a range of organizational sizes based on total employee count: 54 percent were from large organizations with more than 5,000 employees; and 46 percent were from organizations with fewer than 5,000 employees.

Organizations represented have a broad range of annual revenue, including 42 percent between \$250M and \$1B; 41 percent between \$1B and \$10B; and 14 percent from companies with greater than \$10B.

A broad range of industries are represented with most in the financial and insurance, and manufacturing industries, as shown in Figure 1.

**Figure 1**  
**Study Respondent Industry Cross-section**



### Scope of IT Control Questions

To answer our research question about the impact of IT controls on overall IT operating performance, we collected data on 53 different controls in six categories. Based on our previous research, we selected those controls that are most likely to impact key operating processes when implemented at a high level of process maturity.

Identity and access controls – 10 controls related to how user accounts are created and managed.

1. A defined process is used to map or match user accounts to an authorized user.
2. A defined process is used to detect unauthorized access.
3. A defined process is used for the creation and management of user accounts.
4. A defined process is used to audit user accounts to ensure they map to authorized users.
5. A defined process is used for suspending and closing user accounts.
6. Developers are not given direct change access to production environments.
7. IT personnel have well-defined roles and responsibilities.
8. A defined process is used to review logs of violation and security activity to identify and resolve unauthorized access incidents.
9. A defined process is used to monitor user accounts to ensure they do not exceed their specified role.
10. A defined process is used for granting emergency system access.

Change controls – 15 controls related to how application, infrastructure, and security-related changes are managed in production.

1. A defined process for managing application-related changes.
2. A defined process for managing security-related changes.
3. A defined process for handling emergency change requests.
4. A defined process for managing IT infrastructure-related changes.
5. Monitor systems for unauthorized changes.
6. Defined consequences for intentional, unauthorized changes.
7. Enforced consequences for intentional, unauthorized changes.
8. Changes are thoroughly tested before release.
9. Changes are made only during scheduled maintenance windows.
10. Create and distribute a forward schedule of changes.
11. Track the number of authorized changes.
12. Track the success rate of approved changes.
13. Use of a change advisory board or committee.
14. Use historical change success information to identify potential risky changes.
15. Audit successful, unsuccessful, and unauthorized changes.

Configuration controls – seven controls related to how system configurations are managed.

1. A defined process is used for IT configuration management.
2. Provide IT personnel with accurate information about the current configuration.
3. Provide IT personnel with accurate information about the last approved or desired configuration.
4. Use of a configuration management database (CMDB).
5. The CMDB describes the relationships and dependencies between configuration items (infrastructure components).
6. The CMDB describes the relationships and dependencies between configuration items (infrastructure components) and the IT services they enable.
7. The CMDB describes the relationships and dependencies between the configuration items (infrastructure components) and the business services they support.

Release controls – five controls related to how production releases are tested and distributed.

1. A defined process is used for testing releases before moving to the production environment.
2. A defined process is used for building software releases.
3. A defined process is used for testing rollback plans before release to the production environment.
4. Maintaining an identical testing and production environment.
5. Approved releases maintained in a definitive software library.

Service-level controls – seven controls related to how service-level targets are set, monitored, and responded to when not met.

1. A defined process is used to monitor service-level performance.
2. A defined process is used to identify the consequences if service-level targets are not met.
3. A defined process is used to review and communicate service-level performance with customers.
4. A defined process is used to set service-level targets with IT customers.
5. Use of a service catalog that defines IT services offered to the business.
6. A defined process is used to update our service catalog.
7. Use of a formal service improvement program.

Resolution controls – nine controls related to how incidents and problems are managed.

1. A defined process is used for managing incidents/service outages.
2. A defined process is used for managing known errors.
3. Use of known errors to help resolve incidents.
4. A defined process is used for managing problems.
5. A defined process is used to analyze and diagnose the root cause of problems.
6. Track the percentage of incidents that are fixed on the first attempt.
7. Provide change history to personnel managing incidents and problems.
8. Identify service-level violations before they are reported by users.
9. Rebuild rather than repair systems based on predefined criteria.

Table 1 shows the Likert scale answer options on a 0 – 5 scale that was used for the 53 different IT control questions assessed in the survey. For our analysis, a control is considered “in use” if it scores 3, 4, or 5 on the scale.

**Table 1**  
**Likert Scale Used for IT Control Questions**

0 – Not used	1 – Documented, but not in use	2 – Documented, but only used inconsistently	3 – Used consistently, exceptions not detected	4 – Used consistently, exceptions detected	5 – Used very consistently, exceptions have consequences
-----------------	-----------------------------------	--	---	---	---

Responses include a broad range of controls used in the IT organizations. Ninety percent of the organizations studied have between seven and 53 controls in use. A large number of respondents indicated 50 to 53 controls in use.

**Scope of Performance Measure Questions**

To answer our research question about the impact of IT controls on overall IT operating performance, we collected data on 15 different performance measures. Performance measures were selected based on criteria including:

- Are the measures widely used in practice?
- Are they a key performance indicator?
- Is the measure clearly tied to IT and business value?
- Is the measure logically dependent on IT controls (i.e., a dependent variable)?

The 15 measures include:

**Operations Rates**

1. Change Success Rate (%)
2. Emergency Change Rate (%)
3. Late Project Rate (%)
4. Server/System Admin (ratio)

#### Support Rates

5. Incident First Fix Rate (%)
6. Incidents Fixed Within SLA Rate (%)
7. Large Outage Mean Time to Repair (hours)

#### Security and Audit

8. Security Breaches That Did Not Result in Loss (%)
9. Security Breaches Corrected (%)
10. Security Breaches Auto Detected (%)
11. Repeat Audit Findings (%)

#### Customer Satisfaction

12. End-user Satisfaction (1-5 scale)
13. Business Management Satisfaction (1-5)
14. IT Staff Customer Awareness (1-5)
15. IT Staff Customer Communication (1-5)

### **Identifying Performance of Each Organization in the Study**

The 15 performance measures are combined into a single variable called “top-half count” which is used throughout the study as the measure of overall IT operational performance. This approach is conceptually similar to identifying an overall score for a decathlon, which combines the scores for 10 individual track-and-field events. The top-half score was determined by comparing a respondent’s performance measures to the other organizations in the study. For each measure, an organization’s individual score is compared to the median score for all participants. If the participant scored in the top 50<sup>th</sup> percentile, or top half of all respondents, then a single point is awarded. The top-half score for an organization is the sum of top-half points for each measure. An equal weight is given to each individual measure. An organization that scored in the top half of all 15 measures would have a top-half score of 15. An organization that did not score in the top half of any measure would have a top-half score of zero.

We selected the label of top, medium, and low performers based on their top-half count. The top performers were selected as those in roughly the top 15<sup>th</sup> percentile of all participants. The rest were identified as medium and low performers. The distribution of organizations in the study includes:

- Low performers – top-half count of 0 to 6 – 122 organizations (37% of total)
- Medium performers – top-half count of 7 to 10 – 157 organizations (47% of total)
- Top performers – top-half count of 11 to 15 – 52 organizations (16% of total)

### **Analysis of Control Use Impact on Performance**

To determine the impact of control use on performance, we identified organizations with similar control use and performance characteristics. We then determined which controls best predicted different levels of performance between the clusters.

A summary of the analysis approach we used includes:

**Table 2**  
**Four-step Analysis Plan**

Analysis Step	Methodology
1 – Cluster participants by control use and performance	Group IT organizations in the sample based on the presence of IT controls (independent variables) and a performance index measure (dependent variable) using cluster analysis techniques.
2 – Identify foundational controls	Identify a subset of “foundational controls” that best predict performance by using multi-step linear regression with clusters that have different levels of control use and performance.
3 – Assess impact of control process maturity	Assess the impact of process maturity by analyzing clusters with similar control use, but different performance levels.
4 – Quantify performance improvement potential	We compared the performance levels of those organizations with the highest performance with organizations with average and low performance, as determined by different percentiles of the top-half count overall performance measure.

### Underlying Assumptions/Assertions

The underlying assumptions and assertions that our research questions and analysis build on include:

- Organizational performance is something that can be understood, predicted, and shaped.
- Increased process repeatability and predictability of results contributes to performance improvement, not degradation.
- Key performance measures are sensitive to some controls more so than others.
- Some control activities impact operating performance more than others.
- We can gain understanding of what is working by analyzing sample data from a cross-section of organizations.
- A specific IT organization can achieve performance improvement by implementing the IT controls identified as having the biggest impact on performance in the sample of IT organizations in this study.

## CHAPTER 3

# SUMMARY OF KEY FINDINGS

### First Key Finding

The first key finding from the study is that IT controls impact the performance of the organizations in the study. However, the degree of performance impact of IT controls varies across different groups of IT organizations in the study. Cluster analysis identified five groups of organizations based on their control use and performance. These groups were roughly split between those organizations with fewer controls in place, which are generally smaller organizations, and those organizations with more controls in place, which are generally larger organizations. We label organizations with more than 200 IT staff and 5,000 employees as larger organizations.

Our interpretation of this finding is that IT controls impact smaller and larger organizations in different ways. The IT operating environment of smaller and larger organizations is different in several key ways that might explain the variance in IT control impact. First, the smaller organizations in this study have fewer controls in use; therefore, there is a smaller set of controls that have potential impact on performance.

Second, smaller IT organizations typically rely less on documented processes and procedures. They may be more likely to use tacit knowledge and organizational learning than standardized operating practices. In smaller organizations, various IT professionals may have informal channels of communication, which allows them to communicate ongoing activities without formalized processes. As a result, smaller organizations may have fewer formal IT operating procedures in place than larger organizations that rely on more formal communication channels.

Third, larger IT organizations tend to be more geographically dispersed, and have more siloed IT functions, both of which require greater reliance on IT process and procedures that may be impacted by the use of IT controls. These larger organizations that rely on documented procedures and controls may also have a culture that naturally supports greater process consistency, which is shown to explain in part the performance difference of organizations in this study.

Note – more details about how the clusters were identified are outlined in Appendix B.

### Second Key Finding

The second key finding is that just three of the 53 controls studied predict 46 percent of the performance variation in the companies with fewer controls in use. Table 3 shows the three foundational controls and their impact on performance variation, as well as the percentage of low, medium, and high performers that have the control in use at level 4 or 5. For example, having a process to detect unauthorized access predicts 32 percent of the performance variation in smaller organizations. Forty-four percent of low performers have this control in place at level 4 or 5, and 88 percent of top performers have it in place at level 4 or 5.

**Table 3**  
**Performance Variation Predicted by Three Foundational Controls**

Foundational Control	Amount of performance variance predicted by foundational control	Low Performers	Medium Performers	Top Performers
		% that have implemented the control at level 4 or 5		
1. A defined process to detect unauthorized access	32%	44%	73%	88%
2. Defined consequences for intentional, unauthorized changes	10%	39%	64%	79%
3. A defined process for managing known errors	3%	36%	48%	77%

This amount of performance variation predicted by just three of the 53 IT controls analyzed in this study is a significant finding. For operational research where there is a wide range of potential factors that may impact performance, this level of performance prediction by just three of controls is very significant.

Note – details about how these foundational controls were identified are outlined in Appendix C.

### Third Key Finding

The third key finding is that nine of the 53 controls in this study predict 60 percent of the performance variation in two clusters of organizations with more controls in place. Table 4 shows the nine controls and their impact on performance variation, as well as the percentage of low, medium, and high performers that have the control in use at maturity level 4 or 5.

**Table 4**  
**Performance Variation Predicted by Nine Foundational Controls**

Foundational Control	Amount of performance variance predicted by foundational control	Low Performers	Medium Performers	Top Performers
		% that have implemented the control at level 4 or 5		
1. A defined process to analyze and diagnose the root cause of problems	32.7%	26%	45%	67%
2. Provide IT personnel with accurate information about the current configuration	12.4%	29%	43%	67%
3. Changes are thoroughly tested before release	7.2%	44%	62%	75%
4. Well-defined roles and	2.8%	45%	63%	79%

Foundational Control	Amount of performance variance predicted by foundational control	Low Performers	Medium Performers	Top Performers
		% that have implemented the control at level 4 or 5		
responsibilities for IT personnel				
5. A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents	1.8%	36%	62%	79%
6. A defined process to identify consequences if service-level targets are not met	1.0%	26%	31%	58%
7. A defined process for IT configuration management	1.2%	42%	43%	60%
8. A defined process for testing releases before moving to the production environment	0.8%	42%	66%	77%
9. A Configuration Management Database (CMDB) describes the relationships and dependencies between configuration items (infrastructure components)	0.9%	23%	25%	48%

For operational research where there are a wide range of factors that may impact performance, this level of performance prediction by nine of the controls is very significant.

**Recommendation:**

Make sure that larger IT organizations have these nine controls in place. Even if you follow a top-down approach to identifying risks and controls, specify these three controls as basic “hygiene” controls that every organization should have. Use this study to justify the effort based on expected performance improvement.

Note – details about how these foundational controls were identified are outlined in Appendix C.

#### Fourth Key Finding

The fourth key finding is that maturity of control processes matters. Analysis of control process maturity levels for organizations that have a similar number of controls in place at different levels of maturity shows that higher levels of process maturity explain part of the difference in performance.

Some larger companies with a high number of controls in use did not have high levels of performance. They are incurring the cost of implementing, managing, and auditing controls without getting the performance improvement benefit. Higher levels of process maturity that include monitoring and

responding to process exceptions will decrease variance in process outcomes. As variance is reduced, process capability increases, which generally increases quality and productivity.

This study indicates that those organizations that monitor and respond to process exceptions (our level 4 and 5 process maturity) will perform better than those that have control processes implemented where exceptions are not monitored (our level 3 process maturity). Having and enforcing consequences for not following key control processes is a critical step needed to set the “tone at the top” and develop a process-focused IT organizational culture.

Two general approaches to managing consequences to influence behavior include both positive consequences that reward desired behavior and negative consequences that discourage undesired behavior. The approach to managing consequences as a strategy to encourage IT operations personnel to follow documented processes and procedures should be tailored to the culture of each IT organization.

**Recommendation:**

Recommend that IT organizations implement the foundational controls identified in this study at a target process maturity level of 4 or 5 in order to achieve performance gains. Do not assume that defined processes are consistently followed. Help IT operations identify and implement appropriate detective controls to actively look for and respond to process exceptions. Suggest that IT executives clearly communicate that following these processes and procedures is a basic job expectation. Also suggest that IT executives work with the organization’s HR department to identify a response if processes and procedures are knowingly not followed by employees.

Note – details about assessment of control maturity are outlined in Appendix D.

## CHAPTER 4

# UNDERSTANDING THE IMPACT OF FOUNDATIONAL CONTROLS

We identified 12 of the 53 controls in the study that best predict performance variations across top, medium, and low performing organizations. The controls that predict top levels of performance include controls in all six categories of controls. In this chapter we look at the controls that do and do not impact performance to hypothesize about what is causing the performance impact.

### Identity and Access Controls

Identity and access controls are key controls that help secure an organization against both internal and external security threats. Controlling access to applications, networks, and databases that transaction critical or private information is a key focus for most security and audit organizations.

We assessed the performance impact of 10 controls related to how user accounts are created and managed. We also asked about segregation of duties, access to production systems, detecting unauthorized access, and auditing access activities.

Table 5 lists the 10 access controls studied, including the three controls that predict performance variation, listed in order of the percentage of top-performing IT organizations that have the controls in place. The controls are listed with the percentage of low, medium, and top performers that have the controls in place at level 4 or 5 process maturity.

**Table 5**  
**Access Controls - Percentage of Respondents With**

Identity and Access Controls	Low Performers	Medium Performers	Top Performers
	% that have implemented the control at level 4 or 5		
1. A defined process is used to map or match user accounts to an authorized user.	45%	70%	92%
2. **A defined process is used to detect unauthorized access.	44%	73%	88%
3. A defined process is used for the creation and management of user accounts.	78%	86%	88%
4. A defined process is used to audit user accounts to ensure they map to authorized users.	41%	67%	88%
5. A defined process is used for suspending and closing user accounts.	60%	80%	83%
6. Developers are not given direct change access to production environments.	50%	69%	83%

Identity and Access Controls	Low Performers	Medium Performers	Top Performers
	% that have implemented the control at level 4 or 5		
7. *IT personnel have well-defined roles and responsibilities.	45%	63%	79%
8. *A defined process is used to review logs of violation and security activity to identify and resolve unauthorized access incidents.	36%	62%	79%
9. A defined process is used to monitor user accounts to ensure they do not exceed their specified role.	45%	55%	77%
10. A defined process is used for granting emergency system access.	51%	69%	75%

\*\* foundational controls for organizations with fewer controls in place

\* foundational controls for organizations with a greater number of controls in place

Three identity and access controls predict higher levels of performance.

- 1) For organizations with fewer overall controls in place, having a well-defined process for detecting unauthorized access predicts 32 percent of performance variation. This is the single most significant predictor of performance variation for organizations with fewer controls in place.

This control is significant because it generally requires a range of other controls that are prerequisite. In order to be able to detect unauthorized access, various other controls need to be in place such as defining and granting authorized access, including creation and management of user accounts, and mapping accounts to authorized users. Only after controls are in place to manage usual access attempts can unauthorized or unusual access attempts be detected. Our analysis shows that these other controls are pervasive for top, medium, and low performers, but do not predict performance variation. Since they are prerequisite for detecting unauthorized access, we consider them necessary but not sufficient predictors of performance.

**Recommendation:**

For smaller organizations with fewer controls in place, make sure tools and prerequisite controls are in place to enable detection of unauthorized access attempts. Not having had previous unauthorized access attempts is not justification for not having detection capabilities in place.

- 2) For IT organizations with a greater number of controls in place, having well-defined roles and responsibilities predicts 2.8 percent of performance variation.

Having well-defined roles and responsibilities and segregation of duties are common controls that ensure that a single person cannot initiate a fraudulent change. However, having segregation of duties forces IT organizations to clearly define processes so that everyone can identify who is responsible for what and when. Separating development, from QA and test, from those that make modifications to live production systems may improve change success rate and reduce downtime, as well as prevent internal fraud. When processes are well defined, they generally are more predictable and less variable. This standardization of roles and responsibilities is shown to improve overall operating performance.

**Recommendation:**

Make sure IT operations management clearly understands the performance improvement potential related to well-defined roles and responsibilities. IT operations may view the segregation of duties controls as inhibiting their ability to work quickly. However, use this study to help show them that improving definition of who does what when is a proven way to improve IT operating performance.

- 3) Also for organizations with more controls in place, having a defined process to review security violations and unauthorized access incidents predicts 1.8 percent of performance variation. Unlike the smaller organizations in the study where detecting unauthorized access predicts performance, the larger organizations need a process in place to respond to unauthorized access attempts. The process to respond to unauthorized access attempts predicts higher levels of performance for more complex organizations, while the process to detect unauthorized access predicts higher performance at smaller, less complex organizations. We can assume that smaller organizations follow up on access attempts, and that larger organizations have a greater complexity of systems and access points that require a defined process for escalation and resolution.

**Recommendation:**

Verify that larger IT organizations have clearly defined processes to respond to, escalate, deal out appropriate consequences, and resolve unauthorized access attempts. Detecting unauthorized access is not enough. Do not assume IT operations support and security have process interlocks to adequately respond to unauthorized access events.

## Change Controls

Change controls are another critical category of controls that provide assurance that modifications to critical applications, servers, networks, or databases are authorized and managed to minimize risk. These controls are used to assure that systems function as specified before and after the system modifications are made, and that the changes do not create a security weakness. Change controls are also key to managing operational risk. Up to 80 percent of service outages are caused by changes.

We assessed the performance impact of 15 controls related to how organizations make modifications to production systems. We asked about which processes are defined and automated. We also asked about which metrics are tracked, how emergency changes are managed, and how changes are categorized and scheduled.

Table 6 lists the 15 change controls studied, including the two controls that predict performance variation, that are listed in order of the percentage of top-performing IT organizations that have the controls in place. The controls are listed with the percentage of low, medium, and top performers that have the controls in place at level 4 or 5 process maturity.

**Table 6**  
**Change Controls - Percentage of Respondents With**

Change Controls	Low Performers	Medium Performers	Top Performers
	% that have implemented the control		
1. Enforced consequences for intentional, unauthorized changes.	42%	66%	88%
2. A defined process for managing application-related changes.	57%	74%	85%
3. A defined process for managing security-related changes.	59%	69%	85%
4. A defined process for handling emergency change requests.	58%	77%	85%
5. A defined process for managing IT infrastructure-related changes.	54%	66%	81%
6. **Defined consequences for intentional, unauthorized changes.	39%	64%	79%
7. *Changes are thoroughly tested before release.	44%	62%	75%
8. Track the number of authorized changes.	39%	57%	75%
9. Monitor systems for unauthorized changes.	50%	67%	73%
10. Changes are made only during scheduled maintenance windows.	46%	64%	73%
11. Audit successful, unsuccessful, and unauthorized changes.	42%	53%	71%
12. Create and distribute a forward schedule of changes.	41%	59%	69%
13. Track the success rate of approved changes.	40%	53%	67%
14. Change advisory board or committee.	42%	51%	63%
15. Use historical change success information to identify potentially risky changes example.	28%	29%	52%

\*\* foundational controls for organizations with fewer controls in place

\* foundational controls for organizations with a greater number of controls in place

Two change controls predict higher levels of performance in this study.

- 1) For organizations with fewer overall controls in place, having defined consequences for intentional unauthorized changes predicts 10 percent of performance variation. As a contrast, the survey data indicates that the presence of a range of other formal change oversight controls does not predict higher levels of performance.

One possible explanation is that at smaller organizations, following a documented change process may be viewed by many IT staff as an inhibitor to getting critical work completed. Compensating controls that clearly identify consequences for unauthorized changes may be required to modify behavior and achieve the performance benefit of a standardized change process.

Interestingly, enforcing consequences for intentional authorized change is more pervasive across all three levels of performance than defining consequences for intentional unauthorized change. This study indicates that defining consequences has a bigger impact on performance than enforcing consequences.

IT employees generally want to do the right thing. Clearly defining expectations about following defined change control processes and procedures, and communicating the consequences of intentionally skirting the process, is enough to set the tone at the top and send signals about what is important to the organization. Focusing efforts on enforcing consequences that may not have already been defined and communicated may be less effective than clearly communicating what is important to set the tone at the top.

For organizations with fewer controls in place, which tend to be smaller organizations that may not have a history of documenting and following processes and procedures, the combination of clear communication of what is expected with clear consequences for not complying appears to be a powerful combination.

**Recommendation:**

Make sure IT operations management clearly identifies the desired change management processes and procedures, as well as consequences for individuals that do not follow the formal process. Taking this step will help ensure that controls are followed, and that performance improvement expected with a more rigorous change management process is actually achieved.

- 2) For IT organizations with a greater number of controls in place, having a process to thoroughly test changes before production release predicts 7.2 percent of performance variation.

Testing changes in a complex, multilayered, multi-location environment is recognized to improve change success rate and reduce rollback rates. This preventative control requires that organizations develop and maintain a preproduction test environment in order to make testing effective. This control is also an effective complement to having test and production release activities conducted by different people, as specified by segregation of duties requirements.

Large multilayered computing environments are complex. Making untested changes to “in-scope” production systems is unpredictable unless changes have been tested in a preproduction test environment that is similar enough to the production environment to identify potential problems of planned changes. Even with change approval, change tracking, and multifunction change oversight, testing changes before they are made in production assures highest levels of system function, availability, and security.

**Recommendation:**

Require that all changes to “in-scope” applications and underlying systems are tested in a preproduction test environment. Use this study to help operations justify the cost of building and maintaining a preproduction test environment for “in-scope” applications and systems. An effective measure to jointly track with operations is the percentage of changes to in-scope systems that were tested in a preproduction environment.

## Configuration Controls

Configuration controls are another category of controls that can significantly improve the operating environment, as well as reduce risk. Minimizing the number of approved configurations and monitoring for configuration drift are proven ways to minimize downtime and improve the ability to detect security incidents.

We assessed the performance impact of seven controls related to how system configurations and data about configurations are managed. We asked about which processes are defined and automated. We also asked about relationship data, and what configuration data is available to other IT functional processes.

Table 7 lists the seven configuration controls studied, including the three controls that predict performance variation, shown in order of the percentage of top-performing IT organizations that have the controls in place. The controls are listed with the percentage of low, medium, and top performers that have the controls in place at level 4 or 5 process maturity.

**Table 7**  
**Configuration Controls - Percentage of Respondents With**

Configuration Controls	Low Performers	Medium Performers	Top Performers
	% that have implemented the control at level 4 or 5		
1. *We provide IT personnel with accurate information about the current configuration.	29%	43%	67%
2. *A defined process is used for IT configuration management.	42%	43%	60%
3. We provide IT personnel with accurate information about last approved or desired configuration.	33%	39%	60%
4. We have a configuration management database (CMDB).	28%	31%	52%
5. *Our CMDB describes the relationships and dependencies between configuration items (infrastructure components).	23%	25%	48%
6. Our CMDB describes the relationships and dependencies between configuration items (infrastructure components) and the IT services they enable.	25%	25%	48%
7. Our CMDB describes the relationships and dependencies between the configuration items (infrastructure components) and the business services they support.	24%	27%	46%

\* foundational controls for organizations with a greater number of controls in place

Three configuration controls predict higher levels of performance in this study.

- 1) For organizations with a higher number of overall controls in place, providing IT personnel with accurate information about current system configuration predicts 12.4 percent of performance variation. This is the most pervasive configuration control, with 67 percent of top performers having this control in place at process maturity level 4 or 5.

What is the current state of an application, server, network, or database? Knowing the answer to that simple question is critical to successfully completing a wide range of routine operations tasks. Whether someone is investigating a service outage, or preparing for an operating system patch or application upgrade — knowing the configuration state of the application and underlying server, database, and network ensures successful task completion.

Interestingly, providing personnel information about the last approved or desired configuration is not a predictor of performance variation. Knowing if a system is in compliance with baseline configuration is a key control for many organizations. Both practices are similarly pervasive at top performing organizations. Knowing the desired or baseline state or configuration of an application or

system is necessary information to determine when an unauthorized change has occurred. However, knowing the current configuration provides more useful information for production resources that are responsible for managing the ongoing operation of the applications and underlying systems.

**Recommendation:**

Providing information about what the configuration currently is appears to have a bigger impact on production performance than providing information about what the configuration should be. However, we suggest IT auditors ensure that IT operations provides information to personnel about both what system configurations are and should be in order to meet dual objectives of control and performance improvement.

- 2) For organizations with a higher number of overall controls in place, having defined processes for IT configuration management predicts 1.2 percent of performance variation.

Configuration management includes a broad set of practices and controls that ensure that systems are managed and maintained to perform in a known and risk-reduced state. Configuration management includes identifying and standardizing on a few tested and approved system configurations. With multiple levels of interdependent system components (application, OS, middleware, server, database, network), there are an exponential number of possible combinations of configuration settings. Identifying optimal and approved settings for various interdependent systems is critical for maintaining proper function.

Configuration management also includes managing information about the current and desired state of the systems, as well as which systems are dependant on other properly functioning systems. The distributed and networked nature of modern computing ensures that systems must rely on the availability and proper function of other connected systems. IT personnel may or may not be able to easily identify which systems depend on or support other systems. There are specialized software applications that map the route of transactions as they flow through multiple dispersed layers of application, server, database, and network. In a large geographically dispersed organization with multiple datacenters, the map can illuminate a surprisingly complex path for simple transactions.

Controlling the state of systems and having information about each interdependent system predicts top levels of performance at large organizations. These practices are critical for assuring the availability, integrity, and security of the production environment.

**Recommendation:**

Sound configuration management practices are a cornerstone for ensuring proper function of applications and automatically detecting unauthorized access and change activities. Use this study to suggest that the IT organization simplify and standardize system configurations.

- 3) For organizations with a higher number of overall controls in place, having a Configuration Management Database (CMDB) that describes the relationship and dependencies between infrastructure components predicts 0.9 percent of performance variation.

We tested for the various types of uses of CMDB in this study, as the CMDB has been a capability of significant and growing focus for the past several years. There are two key functions of a CMDB. One is to manage and maintain accurate information about various system components, known as Configuration Items (CI). This includes current, past, and desired state information. The other key function is to identify the dependency relationships between CIs and IT and business services. We tested the presence or use of the different levels of dependency information. The study indicates that the top, medium, and low performers have similarly low average use of CMDB dependencies; CI to CI, CI to IT service, and CI to business service. However, the presence of CI to CI relationship and dependency information was the one that predicts performance variation.

It is generally recognized that a CMDB is an enabler of practices that improve other control processes. The transformational power of having a CMDB is using the data about configuration items and their relationships that enables more effective processes and controls. In other words, having a CMDB is not a control, but a CMDB makes other controls better.

For example, risk assessment is a key element of change management controls. However, assessing the impact of a change on dependent systems can be very difficult unless there is a record of what system dependencies are. Those organizations in the study that have CMDBs with CI to CI relationship data have higher performance than those that do not.

**Recommendation:**

Building a CMDB is a current area of focus for many IT organizations. IT audit can support IT operations efforts to justify and build a CMDB that includes CI to CI relationship data by indicating that CMDB is shown to improve IT control processes. The CMDB that is integrated with and enables key IT controls can be used as the primary source of record for many types of audit data.

The three configuration management controls identified as predictors of performance variation provide a solid profile of proven configuration management controls. Knowing what state the production system is in, managing systems to fit a tested risk-reduced state, and knowing the dependencies between production systems are three foundational configuration management controls that should be implemented to optimize performance.

## Release Controls

Release controls are similar to change controls in that they help ensure that modifications to the production environment follow predefined and managed processes and procedures. Change controls focus on tracking, approval, and scheduling modifications, whereas release controls focus on the activities that actually touch or modify the production systems.

We assessed the performance impact of five controls related to how production releases are tested and distributed. We asked about which processes are defined and automated. We also asked about maintaining an identical test environment and maintaining releases in a defined library.

Table 8 lists the five release controls studied, including the one control that predicts performance variation, in order of the percentage of top-performing IT organizations that have the controls in place. The controls are listed with the percentage of low, medium, and top performers that have the controls in place at level 4 or 5 process maturity.

**Table 8**  
**Release Controls - Percentage of Respondents With**

Release Controls	Low Performers	Medium Performers	Top Performers
	% that have implemented the control at level 4 or 5		
1. *A defined process is used for testing releases before moving to the production environment.	42%	66%	77%
2. We maintain an identical testing and production environment.	39%	55%	75%
3. Approved releases maintained in a definitive software library.	40%	58%	71%
4. A defined process is used for building software releases.	45%	64%	69%
5. A defined process is used for testing rollback plans before release to the production environment.	33%	40%	63%

\*\* foundational controls for organizations with fewer controls in place

\* foundational controls for organizations with a greater number of controls in place

One release control predicts higher levels of performance in this study.

- 1) For organizations with a higher number of overall controls in place, having a defined process for testing releases before moving into production predicts 0.8 percent of performance variation. At larger organizations with more complex and distributed computing environments, testing releases in a preproduction environment helps assure that unknown dependencies or issues are identified before modifications are made in the production environment.

It is generally recognized that it is less expensive to identify problems and make changes before releases are moved into the production environment. However, there is ongoing debate about how practical and cost effective it is to build a test environment that is similar enough to the production environment to matter. The survey analysis did not identify maintaining an identical testing and production environment as a predictor of performance variation. Although it may not be feasible to recreate the production environment in total, the study findings indicate that developing and using a preproduction test environment that is “sufficiently similar” to production can improve performance.

**Recommendation:**

Encourage production to develop a preproduction test environment that is “sufficiently similar” to the production environment, for all in-scope applications and underlying systems. Work to set goals of having 100 percent of changes to in-scope systems tested in the preproduction environment.

**Service-level Controls**

Service level controls help ensure that IT is delivering capabilities to the level needed by the business. We assessed the performance impact of seven controls related to how service-level targets are set, monitored, and responded to when not met. We asked about which processes are defined and automated. We also asked about managing service levels with customers and having a service improvement program.

Table 9 lists the seven service-level controls studied, including the one control that predicts performance variation, in order of the percentage of top-performing IT organizations that have the controls in place. The controls are listed with the percentage of low, medium, and top performers that have the controls in place at level 4 or 5 process maturity.

**Table 9**  
**Service-level Controls - Percentage of Respondents With**

Service-level Controls	Low Performers	Medium Performers	Top Performers
	% that have implemented the control at level 4 or 5		
1. A defined process is used to monitor service-level performance.	28%	43%	73%
2. *A defined process is used to identify consequences if service-level targets are not met.	26%	31%	58%
3. We have a service improvement program.	27%	28%	58%
4. A defined process is used to review and communicate service-level performance with customers.	30%	36%	56%
5. A defined process is used to set service-level targets with IT customers.	29%	37%	54%
6. We have a service catalog that defines IT services offered to the business.	30%	25%	52%
7. A defined process is used to update our service catalog.	26%	25%	48%

\*\* foundational controls for organizations with fewer controls in place

\* foundational controls for organizations with a greater number of controls in place

One service-level control predicts higher levels of performance in this study.

- 1) For organizations with a higher number of overall controls in place, having a defined process for identifying consequences if service-level targets are not met predicts one percent of performance variation. This is a rather interesting if not intuitive finding. The processes related to defining and updating services in a catalog, of defining target service levels, and monitoring service levels to target did not predict top levels of performance across the IT organizations in the study. However, using a defined process to identify the consequences if service-level targets are not met did predict performance variation.

Again, we find a consequences-related control that predicts top levels of performance more so than other related controls. We find that the control that relates to monitoring service levels is more pervasive with 73 percent of top performers monitoring service levels. However, it is the process used to identify consequences if targets are not met — which is used by 58 percent of top performers — that has the bigger impact.

**Recommendation:**

Make sure production has processes in place to identify consequences if service-level targets are not met. Putting “teeth” in the service-level agreement will help optimize all the efforts of defining services and setting targets and monitoring service levels.

## Resolution Controls

Identifying, responding to, and resolving service disruptions is a critical set of control activities. We assessed the performance impact of nine controls related to how incidents and problems are managed. We asked about which processes are defined and automated. We also asked about specific metrics used, using known errors and root cause analysis, rebuilding vs. repairing, and identifying issues before service levels are violated.

Table 10 lists the nine controls studied, including the two controls that predict performance variation, in order of the percentage of top-performing IT organizations that have the controls in place. The controls are listed with the percentage of low, medium, and top performers that have the controls in place at level 4 or 5 process maturity.

**Table 10**  
**Resolution Controls - Percentage of Respondents With**

Resolution Controls	Low Performers	Medium Performers	Top Performers
	% that have implemented the control at level 4 or 5		
1. A defined process is used for managing incidents/service outages.	45%	61%	79%
2. **A defined process is used for managing known errors.	36%	48%	77%
3. We use known errors to help resolve incidents.	36%	39%	75%
4. A defined process is used for managing problems.	47%	55%	73%
5. *A defined process is used to analyze and diagnose the root cause of problems.	26%	45%	67%
6. Track the percentage of incidents that are fixed on the first attempt.	39%	46%	62%
7. Provide change history to personnel managing incidents and problems.	29%	43%	62%
8. We identify service-level violations before they are reported by users.	28%	32%	60%
9. We rebuild rather than repair systems based on predefined criteria.	26%	29%	46%

\*\* foundational controls for organizations with fewer controls in place

\* foundational controls for organizations with a greater number of controls in place

Two resolution controls predict higher levels of performance in this study.

- 1) For organizations with fewer overall controls in place, having a defined process for managing known errors predicts three percent of performance variation. Managing known errors is considered a form of knowledge management, and focuses on storing information about causes of common or recurring system failures.

**Recommendation:**

Make sure production has a process and capability to store and retrieve information about known or recurring system errors. Being able to quickly identify a known error and easily identify a recommended fix is a powerful way to improve overall performance.

- 2) For organizations with a higher number of overall controls in place, having a defined process to analyze and diagnose the root cause of problems predicts 32.7 percent of performance variation. This is the most significant predictor of performance variation in the study.

Many IT organizations implement well-defined processes to respond to service outages and incidents, as this process area is a primary touch point between IT and business users. It is generally recognized that improving incident response processes improves customer satisfaction. The survey data shows that 79 percent of top performers have incident management processes in place.

However, identifying and eliminating the root cause of problems is what drives down the number of incidents. Is it better to be good at responding to service outages or be good at fixing problems that drive down the number of service outages? This study indicates that having a process in place to analyze and identify the root cause of problems has a very significant impact on overall performance.

**Recommendation:**

Encourage IT operations to not overlook root cause analysis and problem management processes. Help raise awareness that resolving problems and avoiding future service outages is a better way to reduce risk than being good at responding to incidents.

## CHAPTER 5

# APPLICATION OF THESE FINDINGS

What can IT audit do with these findings? In addition to the recommendations that are highlighted for each of the foundational controls in the previous chapter, there are eight key takeaways that can help IT audit optimize their role and relationship with IT operations.

### 1) Reposition IT controls as a performance improvement tool.

Most IT executives have operational responsibility. At the highest level, IT risk management and use of IT controls helps them achieve their objectives by identifying and mitigating risk. However, the day-to-day impact of IT control and audit activities may be perceived as only adding documentation, approval, and data collection requirements. Showing that key IT controls implemented at a higher level of process maturity can positively impact their key operating measures helps reposition IT controls from being an overhead cost to being a strategy for improved performance. This shift in thinking can help IT executives reframe important audit and control resource allocation decisions.

### 2) Reposition IT operations' relationship with IT audit.

IT audit can help bridge the gap between external requirements and enterprise risk assessments, and IT operating processes and procedures. However, IT leaders should take an active role in developing IT controls so that they improve operating performance as well as reduce risk. IT audit can help conduct risk assessment and identify control objectives. But, IT operations should own the implementation and management of controls that impact general operating process and procedures. If changes to operating procedures are made only to pass an audit, at best the organization misses an opportunity to engineer performance improvement, and at worst may implement procedures that inhibit operating performance.

IT audit should be viewed as a partner who can help verify that the carefully designed procedures and controls are actually followed throughout the organization. The consistency of practice that results from well designed controls should reduce risk but also help achieve performance breakthrough.

### 3) Implement foundational controls at a target process maturity level.

Analysis reveals that 12 of the controls in this study predict performance in a broad sample of organizations. We can infer that these controls can also impact performance at other organizations as well. The foundational controls should be implemented at a level where process exceptions are detected, and exceptions have consequences. Not all IT processes need to achieve this level of maturity; however, foundational control processes should. Getting everyone to follow documented process and procedures — at a level of maturity where expectations can be easily identified and managed — creates an environment that boosts process performance.

### 4) Use IT controls to initiate a systematic program of ongoing process improvement.

Build on process definition and data collection requirements mandated by both internal and external audit to also set aggressive but achievable performance goals. Make sure enhanced data collection that is required to meet process audit requirements is used to measure both process and outcomes

metrics, and is focused on monitoring and identifying process exceptions. Work with IT operations to help prioritize process improvement efforts and leverage control data to help identify ways to refine and improve processes to meet performance goals.

- 5) Use compliance as a mandate to adopt a process orientation.

IT executives we have studied have made a decision to adopt a process approach to managing IT as a strategy for achieving higher service levels at lower cost. The repeatability and predictability of key processes that are managed at a maturity level where exceptions are detected improves both operating performance and reduces risk. Achieving compliance with new regulations can be used as a mandate to set the tone at the top that following documented processes and procedures is a basic job expectation.

- 6) Engineer cultural changes using human resources, and the thoughtful application of both the “carrot” and the “stick.”

This study identified multiple places where having consequences ignited performance improvement. However, “consequences” shouldn’t be read as “punishment.” Work with operations and HR to engineer the appropriate mix of positive and negative incentives to enable lasting behavioral change.

- 7) Use this study to benchmark control maturity and operational performance.

Work with IT operations to compare your organization to the top, medium, and low performers in this study. The data in this study provides a fast baseline benchmark for your organization. IT audit can help operations benchmark the process maturity of key IT controls and key operating performance measures. Use the results to identify areas for increased focus and process maturity.

- 8) Use the study measures as the foundation of an audit and operations shared performance dashboard.

IT audit and operations can use a set of shared measures to manage ongoing controls. Focusing the measures on control activities that simultaneously reduce risk and improve operating performance is an ideal place to start jointly measuring results.

## CHAPTER 6

# PERFORMANCE IMPROVEMENT POTENTIAL

We have identified foundational controls that best predict top levels of performance. We have also determined that the process maturity level helps predict performance. The overall implication of these findings is that organizations that implement foundational controls at a high level of process maturity can achieve higher levels of performance.

In this chapter, we will complete the last step in our analysis by looking at the performance difference of low, medium, and top performing organizations in the study. Grouping study participants based on overall performance provides a powerful tool for organizations to assess their own performance improvement potential. Feedback from IT audit and operations professionals on the findings of the pilot study indicated that showing the difference in performance based on low, medium, and top performance was especially helpful in understanding what might be accomplished by focusing resources on the foundational control activities.

We segmented study participants into top, medium, and low performance based on different percentiles of top-half count. Our performance segmentation includes:

Low performers – top-half count of 0 to 6 – 122 organizations (37% of total)

Medium performers – top-half count of 7 to 10 – 157 organizations (47% of total)

Top performers – top-half count of 11 to 15 – 52 organizations (16% of total)

Table 11 shows a summary of all performance measures

**Table 11**  
**Performance Measure Summary for Three Performance Groupings**

	Low Performers		Medium Performers		Top Performers	
	Mean	Median	Mean	Median	Mean	Median
<b>Overall Performance Measures</b>						
Top-half Count	5.14	6.00	8.86	9.00	11.77	11.50
<b>Foundational Control</b>						
Foundational Control Count	6.89	7.00	8.97	9.00	10.38	11.50
Foundational Control Maturity	2.69	2.67	3.28	3.33	3.80	3.96
<b>Operations Measures</b>						
Change Success Rate (%)	84.79	90.00	91.95	95.00	94.60	98.00
Emergency Change Rate (%)	18.04	15.00	11.41	10.00	8.08	5.00
Late Project Rate (%)	34.96	25.00	21.91	15.00	17.56	10.00
Server/System Admin (ratio)	60.36	15.00	86.14	27.00	113.65	48.00
<b>Support Measures</b>						
First Fix Rate (%)	72.62	80.00	84.02	90.00	88.85	90.00
Incident SLA Rate (%)	74.63	80.00	90.17	95.00	93.69	97.00
Large Outage MTTR (hrs)	11.61	4.00	7.52	3.00	4.86	2.00

	Low Performers		Medium Performers		Top Performers	
	Mean	Median	Mean	Median	Mean	Median
<b>Overall Performance Measures</b>						
<b>Security and Audit Measures</b>						
Security Breaches No Loss (%)	92.21	98.00	97.18	100.00	98.65	100.00
Security Breaches Corrected (%)	66.81	80.00	83.04	99.00	83.56	100.00
Security Breaches Auto Detected	46.33	40.00	72.70	80.00	81.35	90.00
Repeat Audit Findings (%)	32.19	25.00	25.59	16.00	15.61	2.50
<b>Customer Satisfaction Measures</b> (Note - averages have more meaning for these measures)						
End-user Satisfaction (1-5 scale)	3.43	4.00	3.70	4.00	4.29	4.00
Business Mgmt. Satisfaction (1-5)	3.15	3.00	3.51	4.00	4.31	5.00
IT Staff Customer Awareness (1-5)	3.52	4.00	3.94	4.00	4.60	5.00
IT Staff Cust. Communication (1-5)	3.29	3.00	3.53	3.00	4.17	4.00

Overall top performers, which represent the top 15<sup>th</sup> percentile of participants, exhibit significantly higher performance on a range of key measures that indicate the overall effectiveness and efficiency of IT operating performance.

These segments are used throughout this study to illustrate the difference in performance for these three groups for each of the performance measures used to calculate the top-half count measure. Figure 2 shows the three performance segments based on top-half count.

**Figure 2**  
**Top-half Count for Three Performance Groupings**

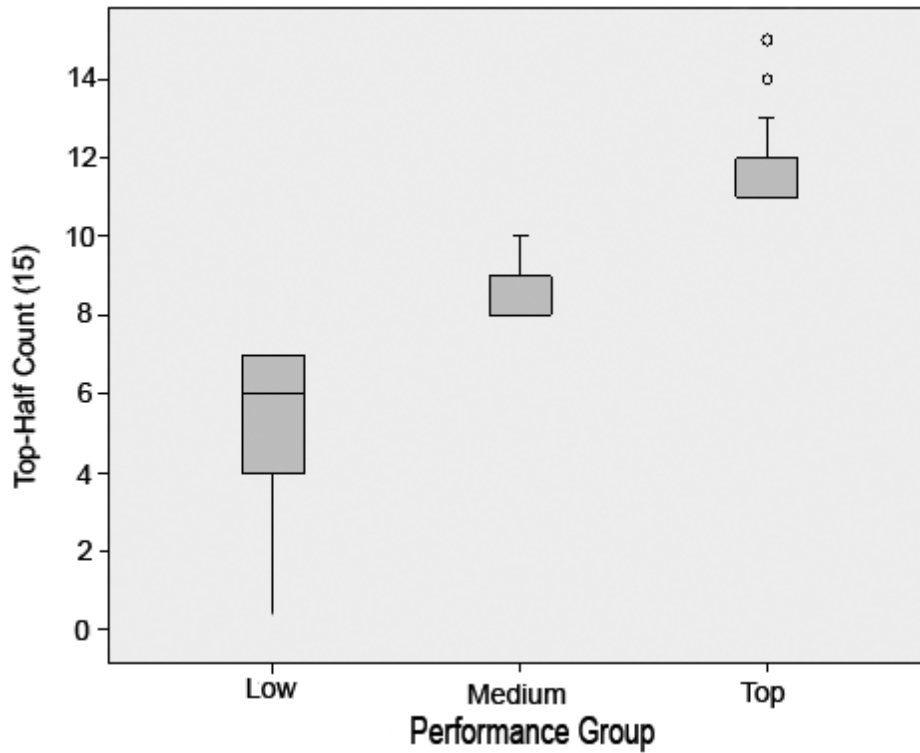


Figure 3 shows the foundational control count for each of the three performance groupings.

**Figure 3**  
**Foundational Control Count for Three Performance Groupings**

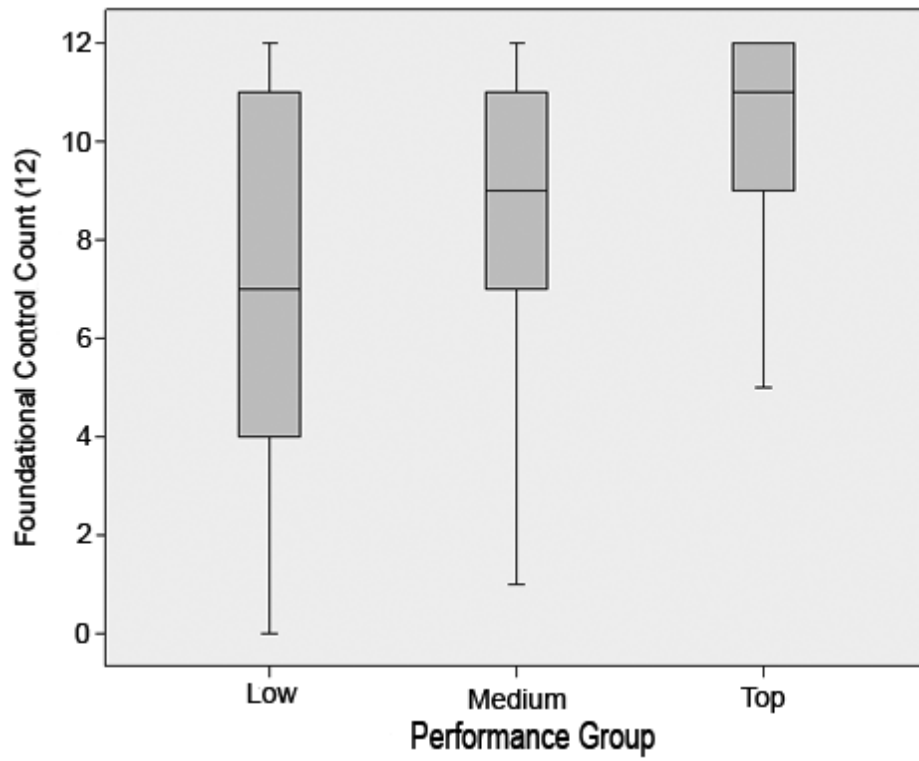
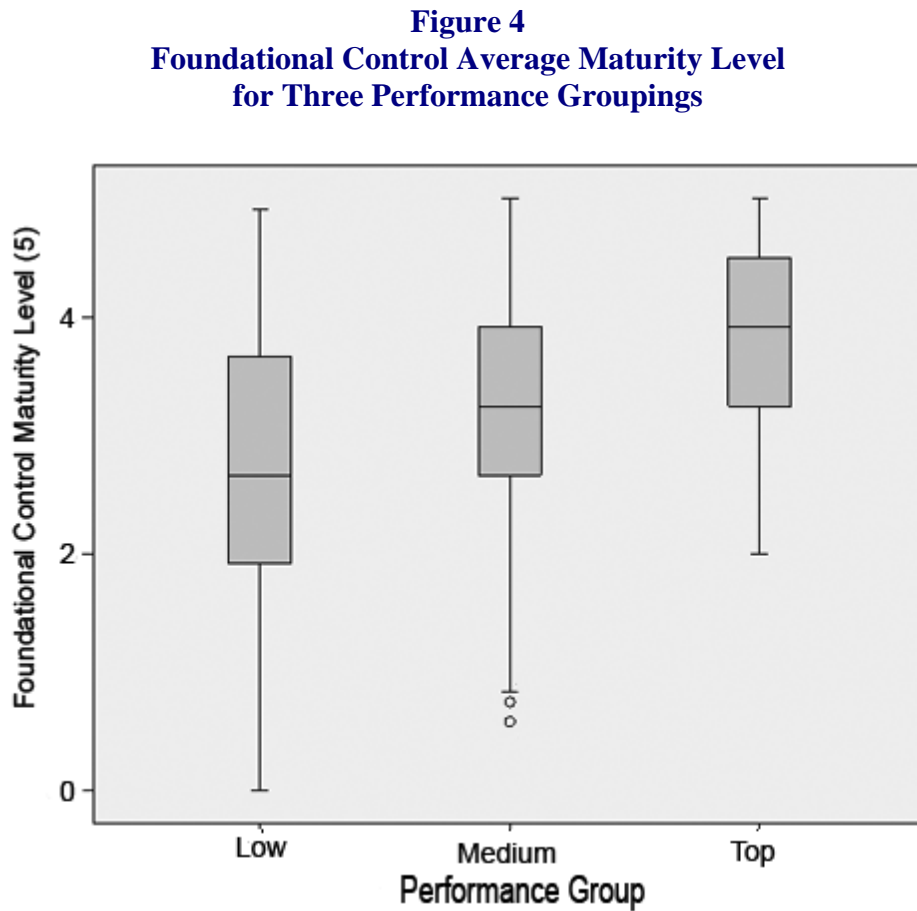


Figure 4 shows the foundational control average maturity level for the three performance groupings.

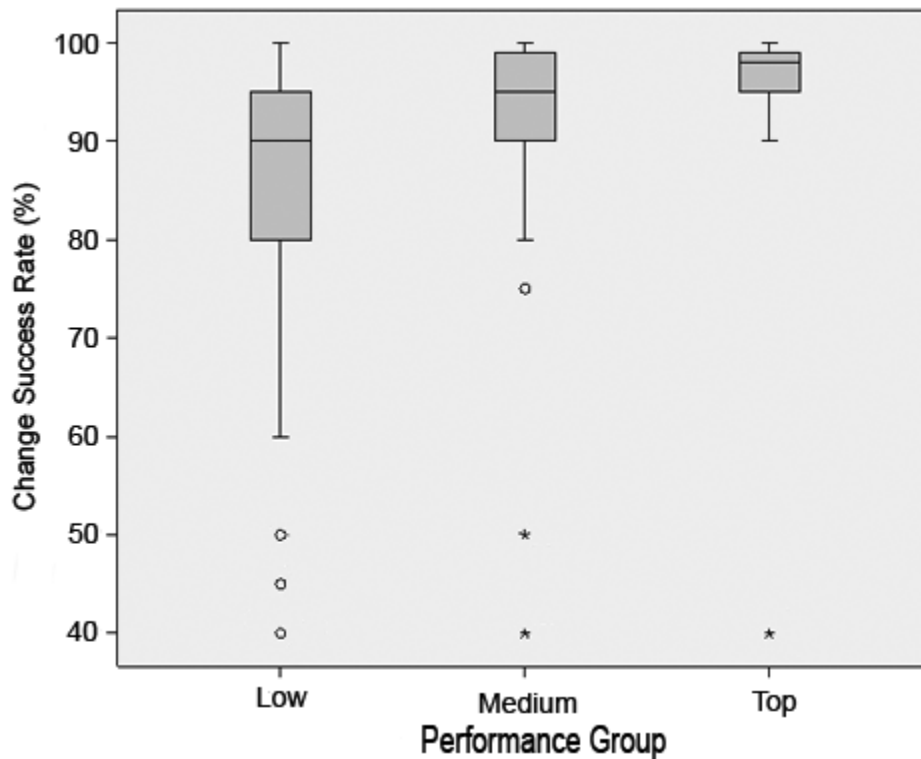


The remainder of this chapter assesses the performance difference for these three groups for each of the performance measures that make up the top-half count measure. Table 13 shows a summary of the mean and median for each of the performance groupings for comparison.

## Operations Measures

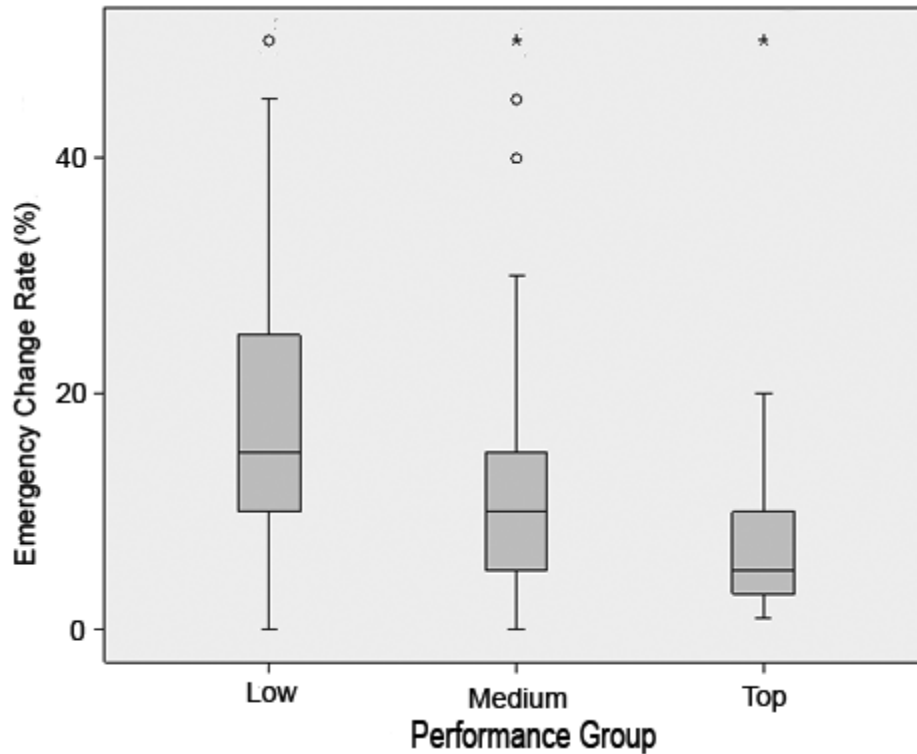
Top performers have an average 95 percent change success rate that is three percent better than medium performers and 12 percent better than low performers who average 92 percent and 85 percent. Change success rate is important as failed changes are a leading cause of downtime and service disruption. Top performing organizations have higher changes success rate which means they have less risk introduced into the production environment.

**Figure 5**  
**Change Success Rate - Low, Medium, and Top Performers**



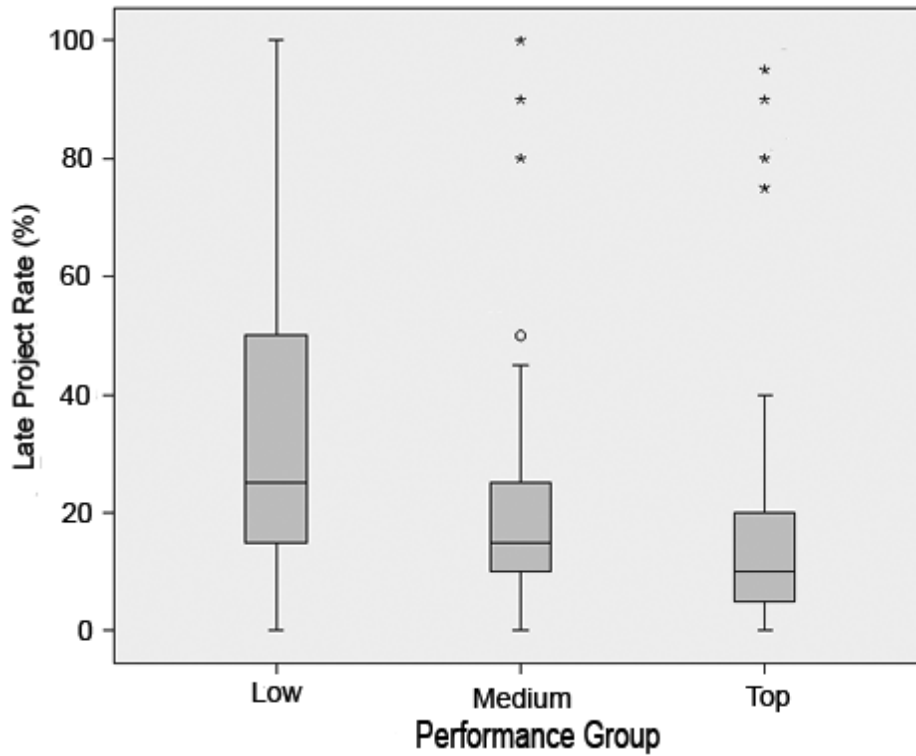
Top performers have an average eight percent emergency change rate that is 29 percent lower than medium performers and 55 percent lower than low performers who average 11 percent and 18 percent. Emergency change rate is an indicator of how many changes are implemented without cross-functional review at a regularly scheduled change review meeting, which can mean that emergency changes do not get the full careful review that normal process changes receive.

**Figure 6**  
**Emergency Change Rate - Low, Medium, and Top Performers**



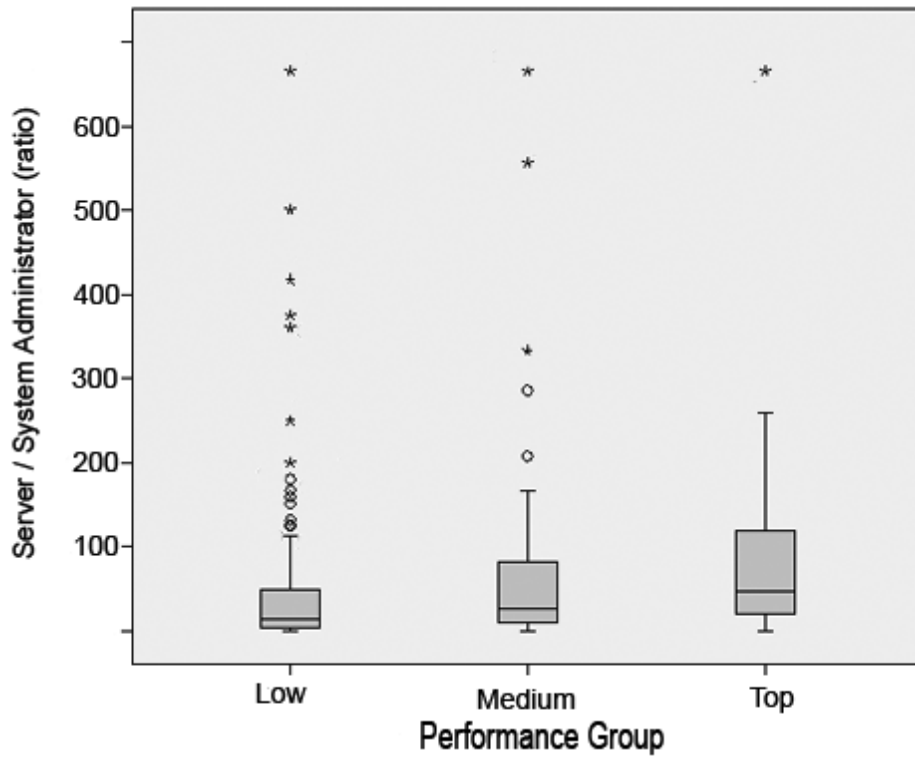
Top performers have an average 17 percent late project rate that is 20 percent lower than medium performers and 50 percent lower than low performers who average 22 percent and 34 percent. Late project rate is an indicator of how well IT organizations utilize development and release resources, and can also indicate how well IT reacts to changing business demands.

**Figure 7**  
**Late Project Rate - Low, Medium, and Top Performers**



Top performers have an average server to system administrator ratio of 114 that is 32 percent better than medium performers and 88 percent better than low performers whose average ratios are 86 and 60. Server to system administrator ratio can be an effective measure of how well organizations utilize administrator resources. More importantly, this ratio is often higher at organizations that have optimized configuration, build, and release strategies, which reduce overall server administration and support requirements.

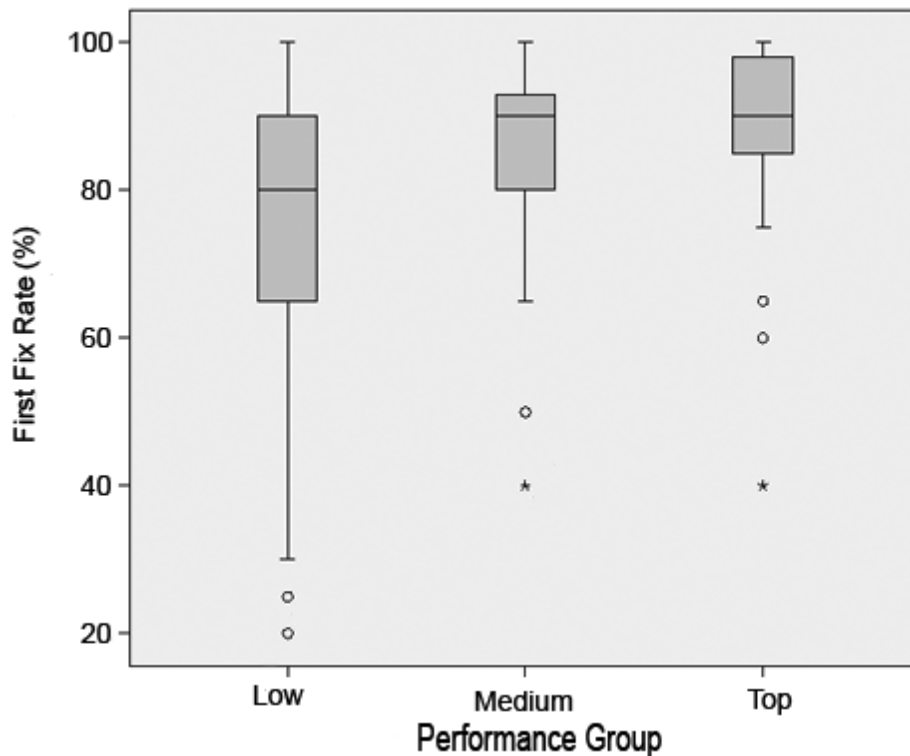
**Figure 8**  
**Server to System Administration Ratio - Low, Medium, and Top Performers**



## Support Measures

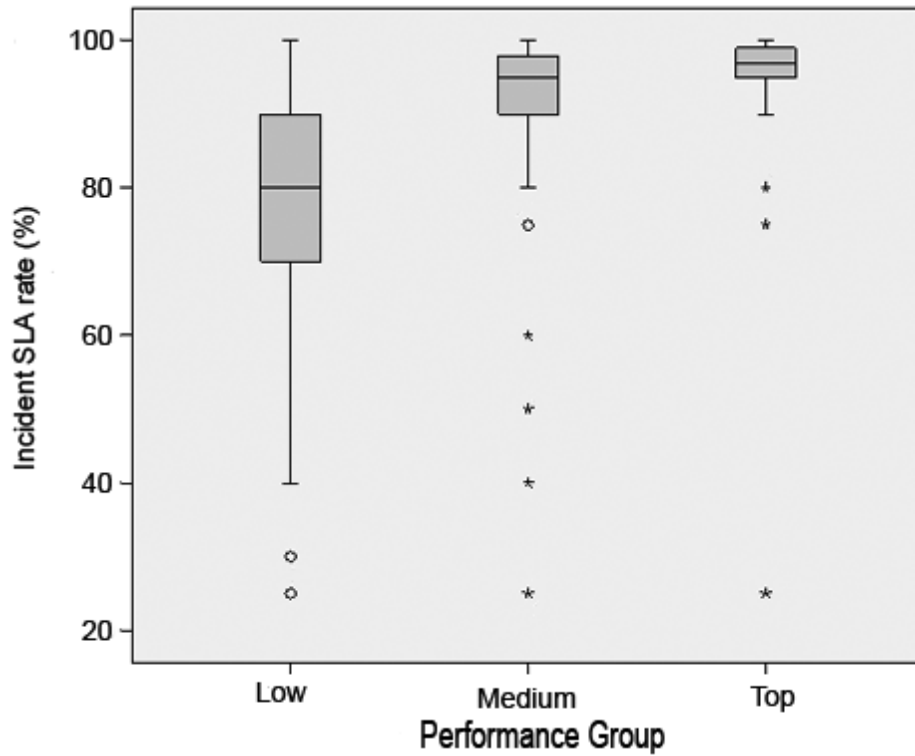
Top performers have an 89 percent average first fix rate that is six percent higher than medium performers and 22 percent higher than low performers who average 84 percent and 73 percent. First fix rate measures how often organizations restore service without engaging second- or third-level support resources. Top performing organizations have fewer interruptions for second- and third-level support resources, which means they can stay focused on planned work.

**Figure 9**  
**First Fix Rate - Low, Medium, and Top Performers**



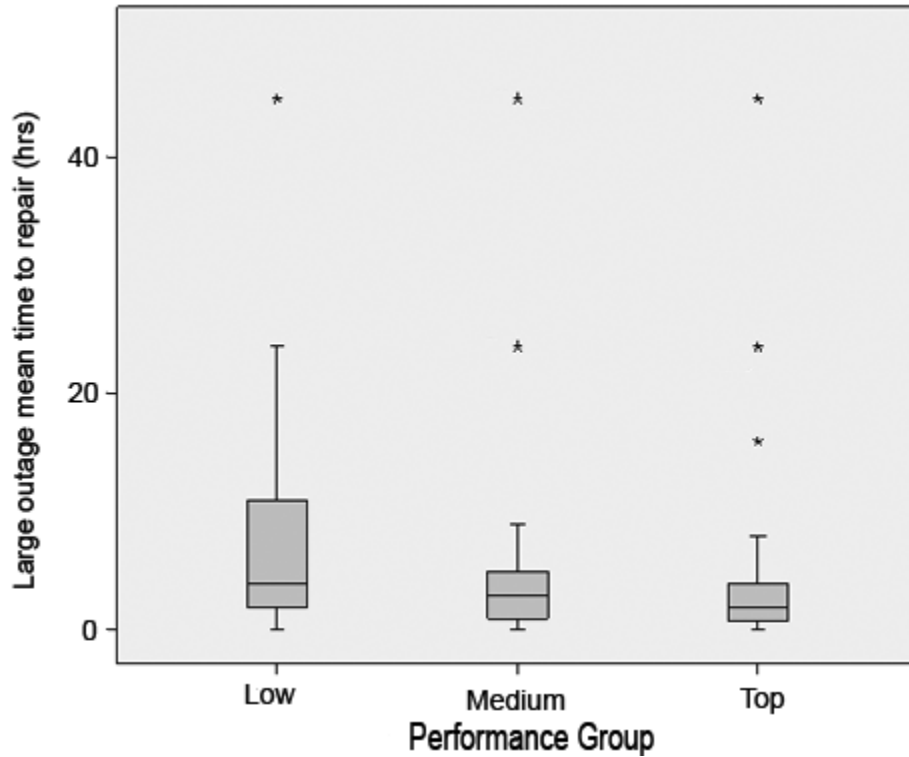
Top performers have a 94 percent average rate of incidents resolved within limits set in a service-level agreement (SLA) that is four percent higher than medium performers and 26 percent higher than low performers who have 90 percent and 74 percent. SLA fix rate measures how often organizations restore service within the terms of service-level agreements, which is an important customer facing metric.

**Figure 10**  
**Incident SLA Rate - Low, Medium, and Top Performers**



Top performers have an average 4.9 hour mean time to repair large outages, which is 35 percent lower than medium performers and 58 percent lower than low performers who average 7.5 and 11.6 hours. Large outages typically involve six to 25 personnel, and can have significant customer impact at organizations that have customer facing IT systems. The ability to dispatch resources and quickly diagnose and repair large outages is an indication that an IT organization has integrated functions and processes.

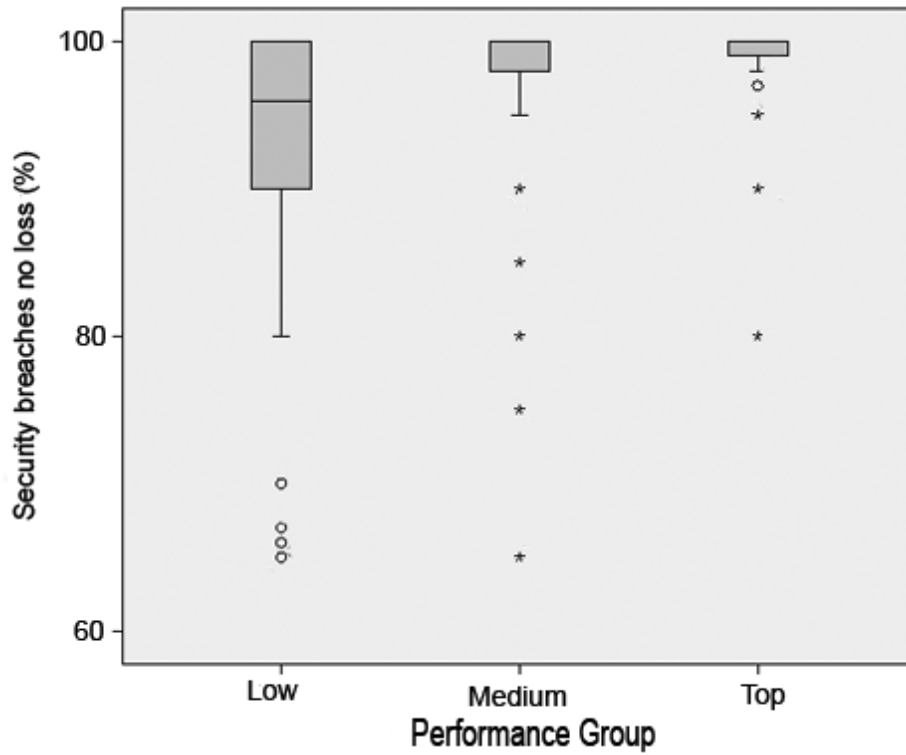
**Figure 11**  
**Large Outage Mean Time to Repair - Low, Medium, and Top Performers**



**Security Measures**

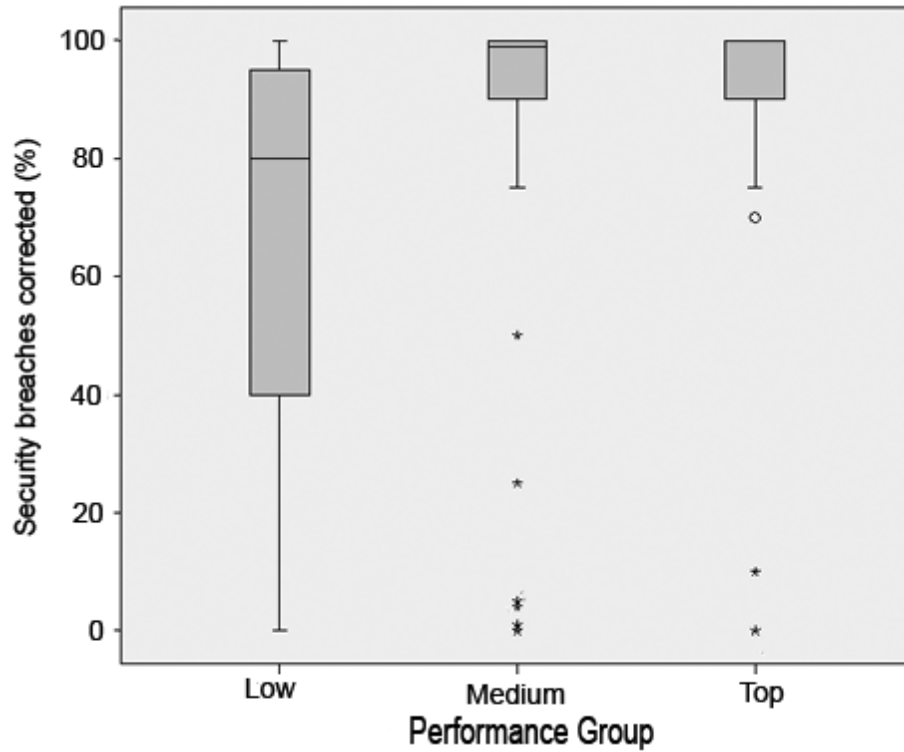
Top performers have a 99 percent average of security breaches that do not result in loss, which is two percent higher than medium performers and seven percent higher than low performers who average 97 percent and 92 percent. Top performers identify and resolve issues faster, which reduces the number of incidents that result in loss.

**Figure 12**  
**Security Breaches No Loss - Low, Medium, and Top Performers**



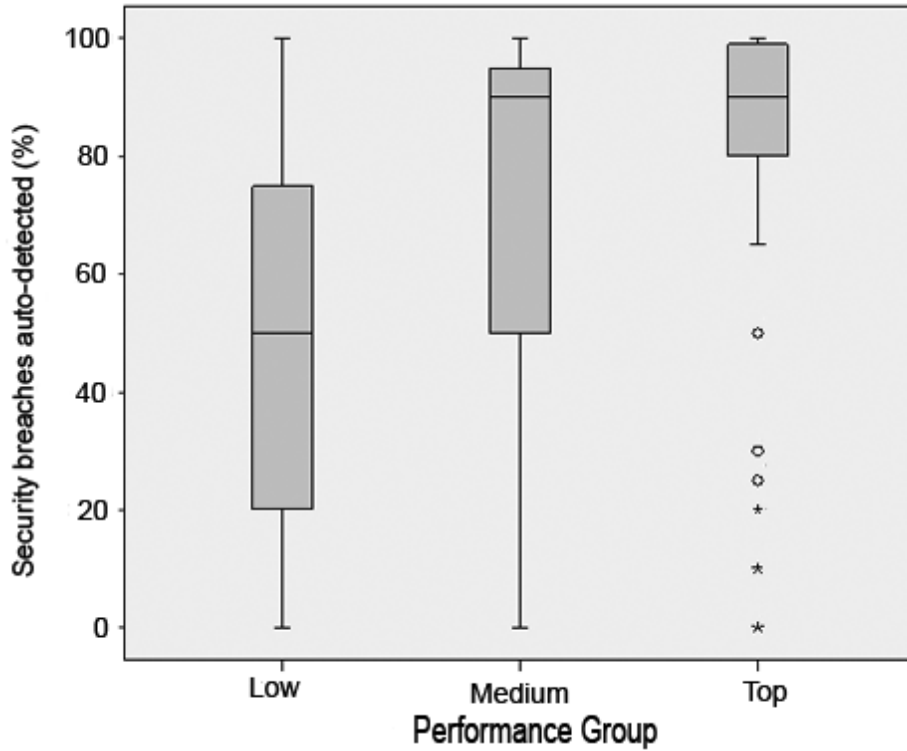
Top performers have an 84 percent average of security breaches that are investigated and corrected, which is one percent higher than medium performers and 25 percent higher than low performers who average 83 percent and 67 percent. Investigating and correcting security breaches is critical for ongoing hardening of IT infrastructure and sensitive data.

**Figure 13**  
**Security Breaches Detected - Low, Medium, and Top Performers**



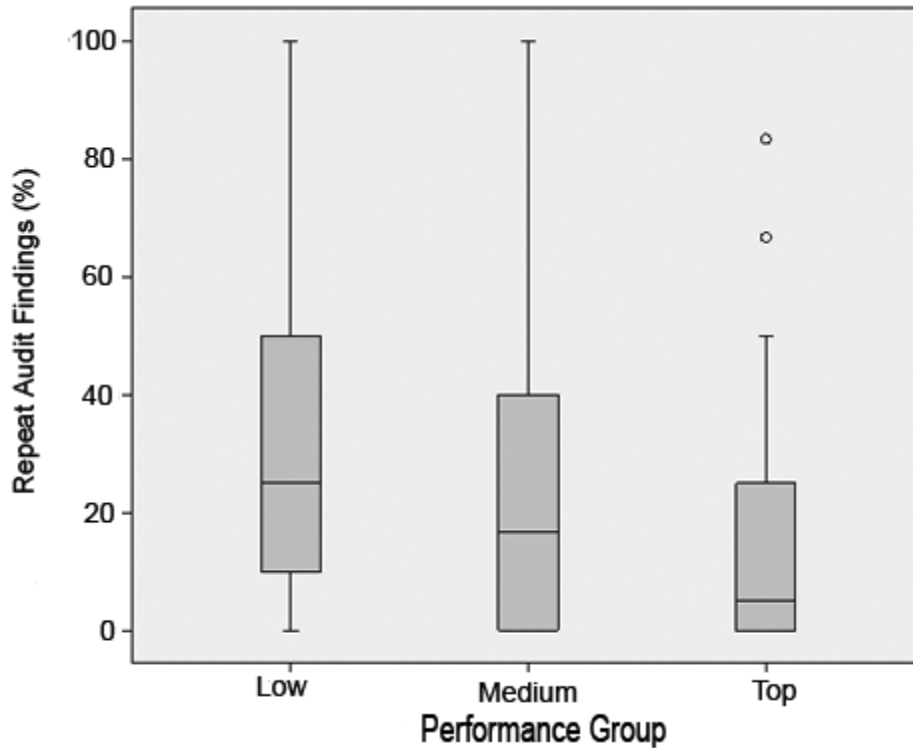
Top performers have an 81 percent average of security breaches that are automatically detected, which is 12 percent higher than medium performers and 76 percent higher than low performers who average 72 percent and 46 percent. Auto detection of security breaches is an excellent measure as it indicates that organizations have a range of preventative and detective controls in place, and are able to identify an abnormal or unapproved event or change to critical systems.

**Figure 14**  
**Security Breaches Auto Detected - Low, Medium, and Top Performers**



Top performers have an average repeat audit finding rate of 15 percent, which is 39 percent lower than medium performers and 52 percent lower than low performers who average 25 percent and 32 percent. A lower rate of repeat audit findings is a good indicator of how well organizations can implement and modify controls that impact IT operating processes.

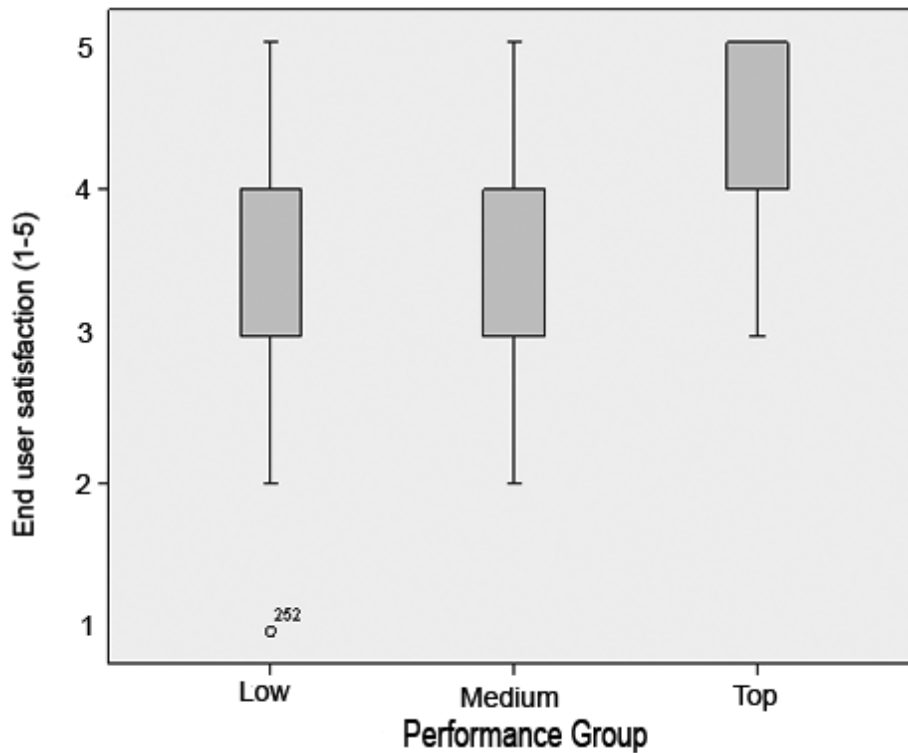
**Figure 15**  
**Repeat Audit Findings - Low, Medium, and Top Performers**



## Customer Satisfaction Measures

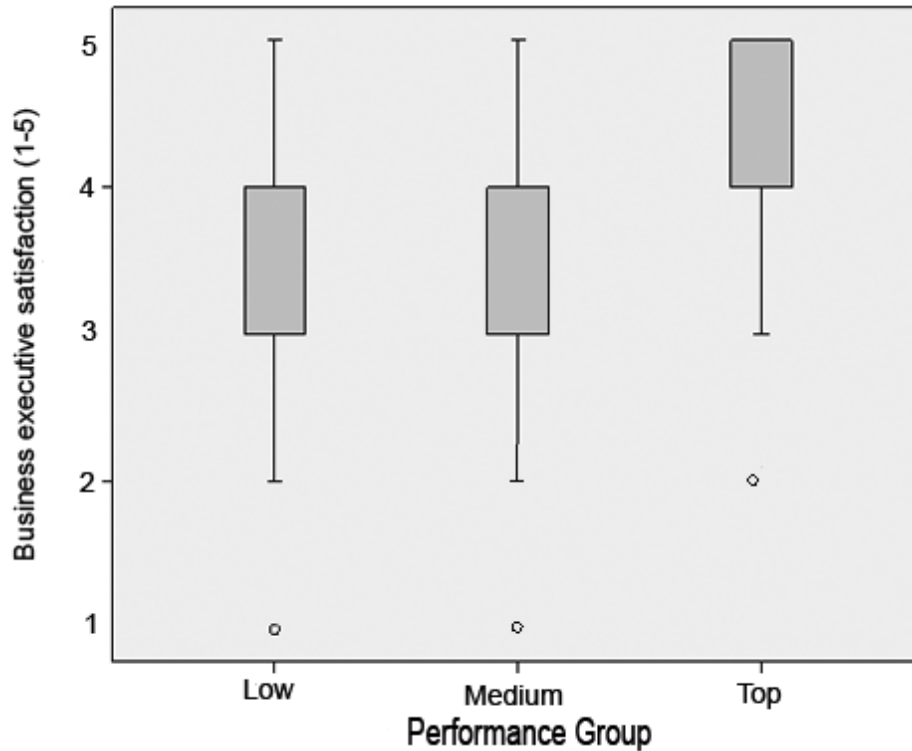
Top performers have an average customer satisfaction score of 4.3 (on 1-5 scale) that indicates how well IT staff are aware of how their customers perceive them, which is 16 percent higher than medium performers and 25 percent higher than low performers who average 3.7 and 3.4. End-user customer satisfaction is one element of a balanced set of customer satisfaction measures that indicates how well end users view their service from the IT organization.

**Figure 16**  
**End-user Satisfaction - Low, Medium, and Top Performers**



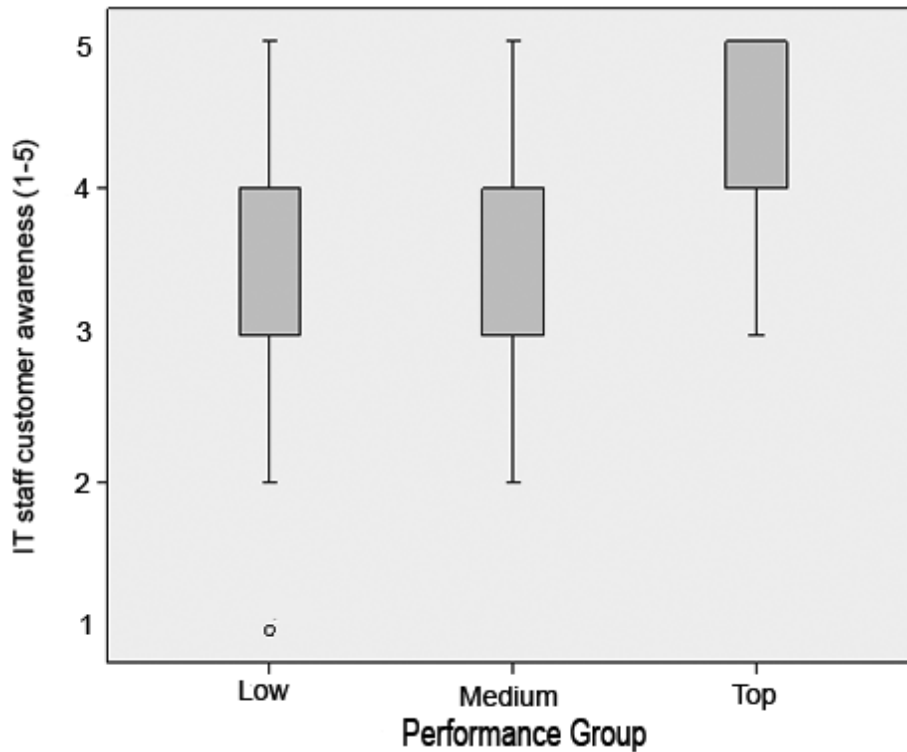
Top performers have an average business management satisfaction score of 4.3 (on 1-5 scale) that indicates how well IT staff are aware of how their customers perceive them, which is 23 percent higher than medium performers and 37 percent higher than low performers who average 3.5 and 3.1. Business management customer satisfaction helps gauge the IT organization's agility in meeting the changing needs of line of business managers.

**Figure 17**  
**Business Management Satisfaction - Low, Medium, and Top Performers**



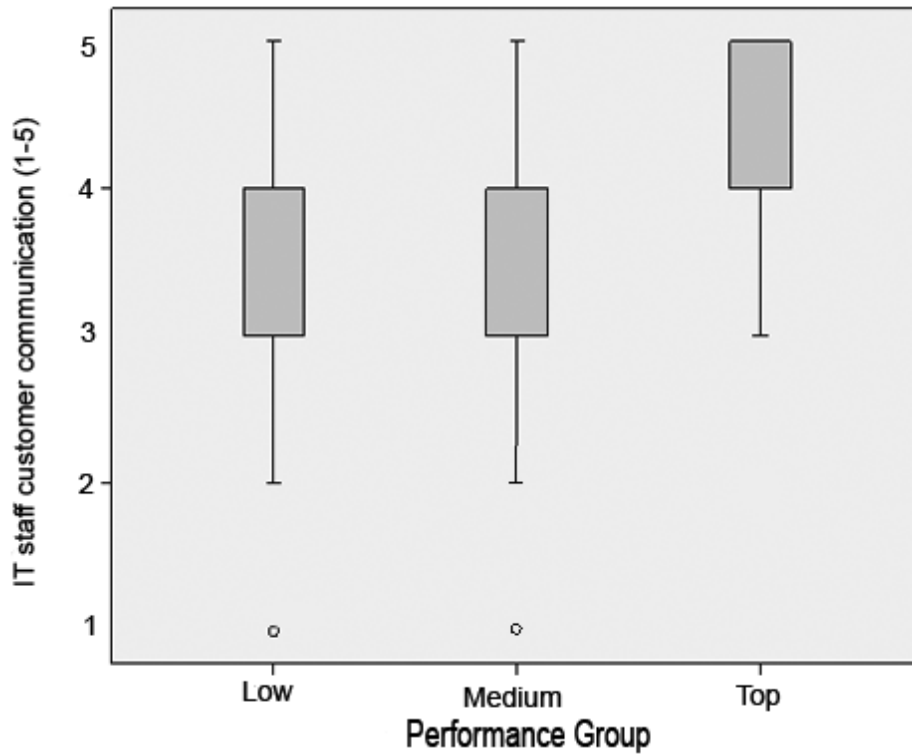
Top performers have an average IT staff customer awareness score of 4.6 (on 1-5 scale), which is 17 percent higher than medium performers and 31 percent higher than low performers who average 3.9 and 3.5. Internal awareness of customer perception is critical to user and business manager satisfaction, and can also indicate how well IT stays aligned with the changing needs of the business.

**Figure 18**  
**IT Staff Customer Awareness - Low, Medium, and Top Performers**



Top performers have an average customer communication score of 4.2 (on 1-5 scale), which is 18 percent higher than medium performers and 27 percent higher than low performers who average 3.5 and 3.3. How well IT communicates with customers is an important indicator of how IT listens and responds to the needs of both business managers who fund it and end users who consume IT services.

**Figure 19**  
**IT Staff Customer Communication - Low, Medium, and Top Performers**



The list of measures used in the performance index and questions used to collect the measure data in the survey are listed in Table 12.

**Table 12**  
**List of Performance Measure Questions**

Measure	Question Asked in Survey
<b>Operations Measures</b>	
Change Success Rate (%)	What percentage of approved changes is successful? Change Success Rate includes changes that were not backed out, that do not cause service outage/incident, and the change was done within the scheduled amount of time.
Emergency Change Rate (%)	What percentage of all IT changes were emergency changes?
Late Project Rate (%)	On average, what percentage of those IT projects did not meet timeline expectations (i.e., were late)?
Server/System Admin (ratio)	How many component servers (i.e., servers, network devices, firewalls, etc.) are supported by those in the server administration role?
	What percentage of IT employees and third-party service providers (FTE) are dedicated to the server administration role?
<b>Support Measures</b>	
First Fix Rate (%)	On average, what percentage of incidents/service outages are fixed on the first attempt? (i.e., First Fix Rate)
Incident SLA Rate (%)	On average, what percentage of incidents/service outages are resolved within SLA limits?
Large Outage Mean Time to Repair (hours)	How quickly do you repair/restore service for a large incident – six to 25 IT staff mobilized to?
<b>Security and Audit Measures</b>	
Security Breaches No Loss (%)	What percentage of security breaches do not result in some form of loss (e.g., financial, reputation)?
Security Breaches Corrected (%)	What percentage of security breaches are successfully investigated and corrected?
Security Breaches Auto Detected (%)	What percentage of security breaches are automatically detected?
Repeat Audit Findings (%)	How many repeat IT audit findings did you have in the last annual audit?
	How many total IT audit findings did you have in the last

Measure	Question Asked in Survey
	annual audit?
<b>Customer Satisfaction Measures</b>	
End-user Satisfaction (1-5 scale)**	How satisfied would you say end users are with the quality of IT services? We'll use a 5-point scale where a "1" means the IT staff is <i>not at all aware</i> and a "5" means they are <i>extremely aware</i> .
Business Management Satisfaction (1-5)	Using your best judgment, how satisfied are business executives with IT's agility and flexibility in meeting changing business requirements?
IT Staff Customer Awareness (1-5)	Using your best judgment, how aware is the IT staff of how they are perceived by the customer community (both end users and business executives)?
IT Staff Customer Communication (1-5)	How effective is IT's ongoing communication and interaction with the customer community?

## APPENDIX A

# GLOSSARY OF TERMS

**Control Count**

The count of controls that are considered “in use” as measured by counting the number of control questions that scored 3, 4, or 5 on a 0 to 5 Likert scale.

**Control Maturity Level**

The average of answers to Likert scale control questions.

**Control Maturity Level 4 and 5**

The count of Likert scale control questions answered at level 4 or 5.

**Control Maturity Level 5**

The count of Likert scale control questions answered at level 5.

**Larger Organizations**

Those organizations with greater than 5,000 employees and more than 200 IT staff.

**Likert Scale**

The most common type of response scale used in survey research that allows a respondent to specify their level of agreement with a statement.

**Low Performer**

A term used to describe organizations with a top-half count between 0 and 6, which includes 122 organizations or 37 percent of those in the study.

**Medium Performer**

A term used to describe organizations with a top-half count between 7 and 10, which includes 157 organizations or 47 percent of those in the study.

**Smaller Organizations**

Those organizations with up to 5,000 employees and 200 IT staff.

**Top Performer**

A term used to describe organizations in the top 15<sup>th</sup> percentile of performance, based on a top-half count of 11 to 15, which includes 52 organizations or 16 percent of those in the study.

**Top-half Count**

The count of measures scored in the top 50<sup>th</sup> percentile of all survey respondents.

## **APPENDIX B**

# **CLUSTERING IT ORGANIZATIONS BASED ON CONTROL USE, PERFORMANCE, AND SIZE**

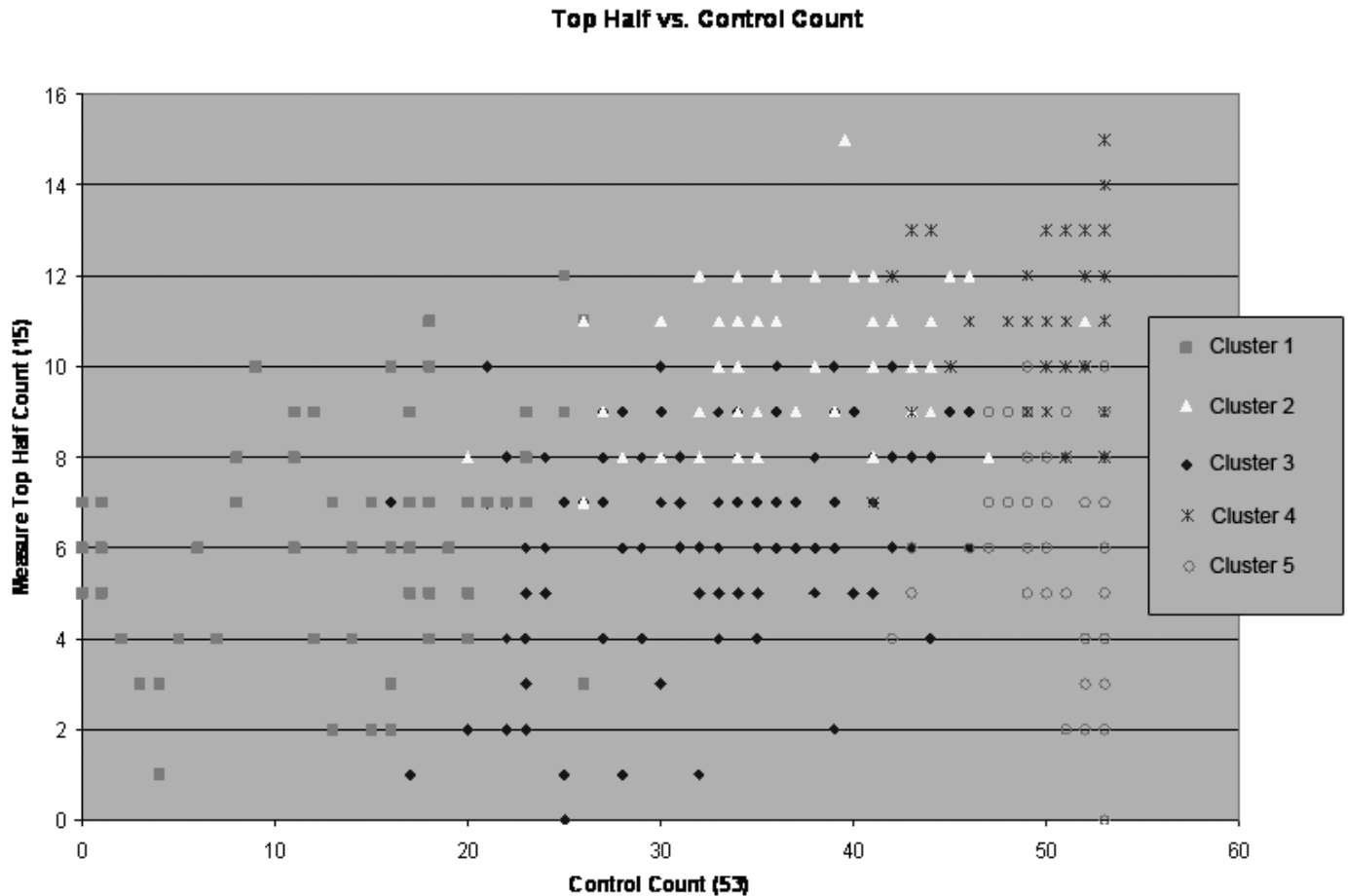
In order to test the overall study hypothesis that “there exists a subset of IT controls that impact IT operating performance to a greater extent than other IT controls,” we designed our study and survey to use regression analysis. Regression analysis is used to examine the relation of multiple independent variables, in this case the 53 IT controls, to a single dependent variable, in this case the top-half count overall performance index. In the pilot study, we found that there were multiple clusters or subgroups of organizations that have different relationships between IT controls and performance index. We conducted a correlation analysis for the organizations in this study and confirmed that there was not a single common relationship between control use and performance. We hypothesized that we had two or more underlying groups with different relationships between control use and performance, which was similar to our findings in the pilot study.

### **Using Cluster Analysis**

We used cluster analysis in an effort to uncover the latent groupings for use in regression analysis. Cluster analysis is a descriptive, multivariate, exploratory technique that groups cases or variables based on measures of similarity, and is often used to assist in the identification of latent groups of cases or variables within a dataset. A two-step clustering algorithm was used to identify study participants with similar patterns of control usage and performance. The first step in the cluster analysis is used to identify participants with similar control use. Control-use clustering identified three clusters of organizations with similar control-use profiles. Identifying these three separate clusters confirmed the idea that the study sample was not a homogeneous group based on control use. The second clustering step analyzed performance in addition to control use. The cluster analysis was repeated using the three control-use clusters and a variable that indicates which IT organizations scored in the top 25<sup>th</sup> percentile of all organizations based on top-half count. This included organizations with a top-half count of 10 or higher.

The two-variable cluster analysis resulted in the identification of five clusters that were differentiated based on both control usage and performance. Figure 20 shows a scatter plot of top-half count versus control count with the five clusters identified.

**Figure 20**  
**Five-cluster Scatter Plot Top-half Count Versus Control Count**



The complex relationships based on Likert scale scores and an additional top 25<sup>th</sup> performance variable is difficult to plot. Think of plotting groupings in 40 dimensions. Instead, we can look at control count and top-half count in two dimensions, to more easily visualize the five clusters. However, while this representation of the cluster solution is easy to visualize, it does not have hard limits between clusters, and thus the clusters overlap on the plot.

To gain additional insight about the profile of these five clusters, we can also look at how they differ based on control use, control maturity, and performance. Figure 21 shows the control use of the five clusters. Controls are considered “in use” if they are at level 3, 4, or 5 on the Likert scale. There is low, moderate, and high usage of controls. Transition from low to moderate control use is separated at roughly 25 controls in use. The transition from moderate to high control use is separated at roughly 45 controls in use.

**Figure 21**  
**Control Count for Five Clusters**

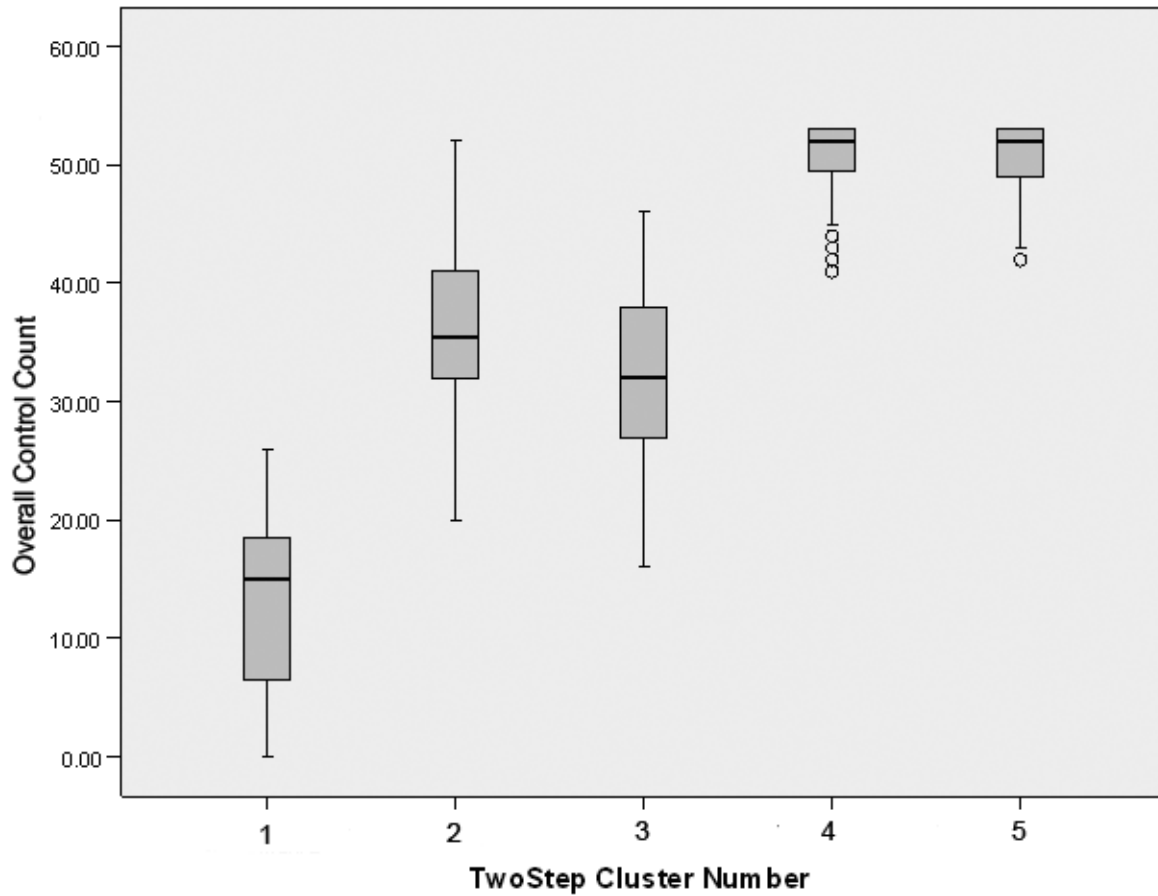


Figure 22 shows the control maturity of the five clusters. Control maturity is the average of Likert scales scores for all controls. There is low, moderate, and high control maturity. The control maturity for the first cluster has a 25<sup>th</sup> to 75<sup>th</sup> percentile range of 1.18 to 1.83. The control maturity of the second and third cluster is a similar moderate level and has a 25<sup>th</sup> to 75<sup>th</sup> percentile range of approximately 2.5 to 3.2. The fourth and fifth clusters have a similar high level of maturity with 25<sup>th</sup> to 75<sup>th</sup> percentile range of approximately 3.9 to 4.4. Transition from low to moderate control maturity is separated at roughly 2.15. The transition from moderate to high control maturity is separated at roughly 3.5 control average maturity level.

**Figure 22**  
**Control Maturity Level for Five Clusters**

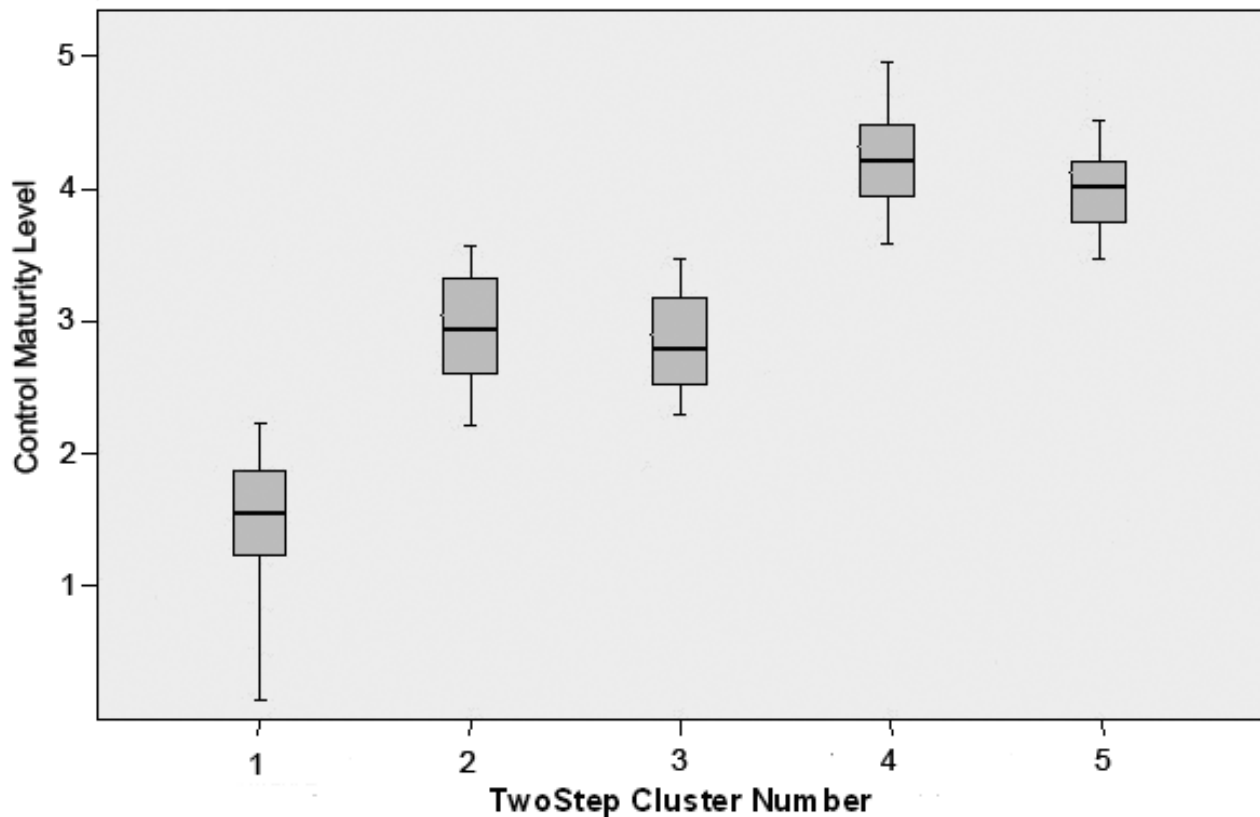
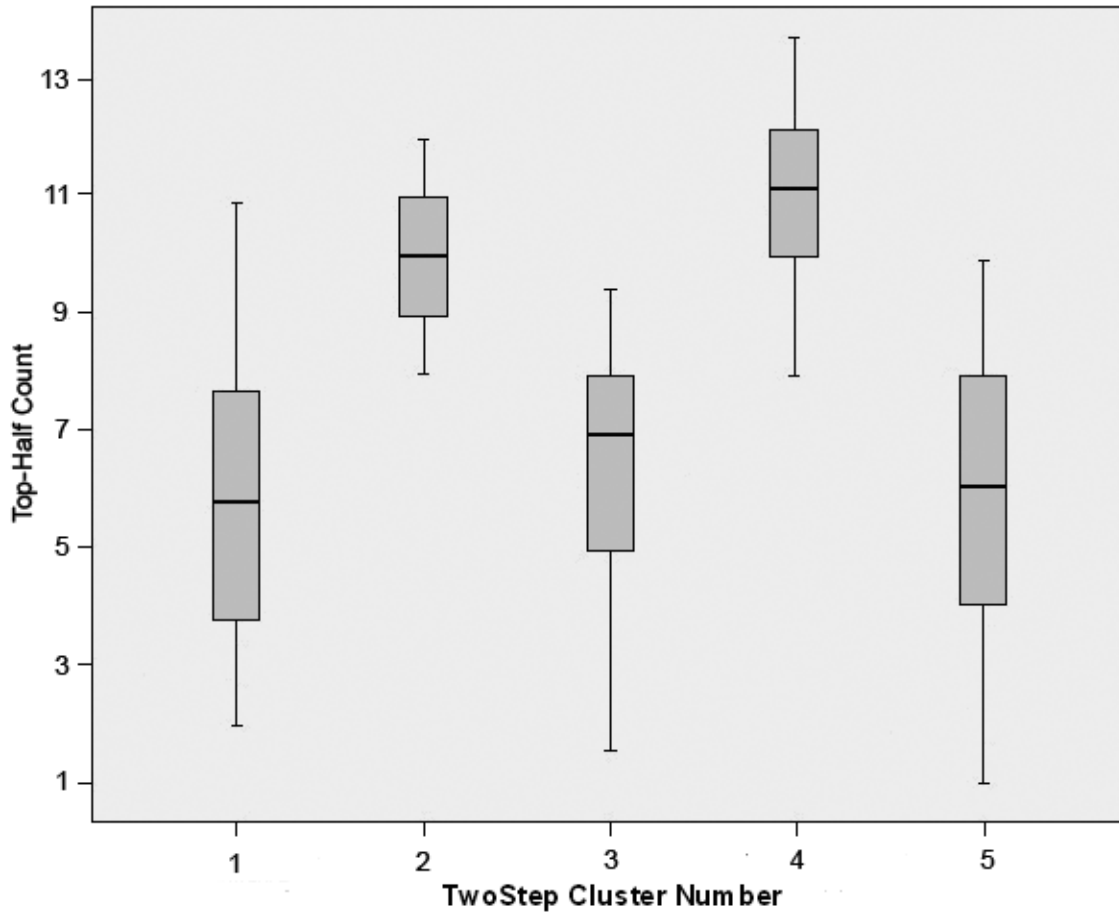


Figure 23 shows the performance top-half count for the five clusters. The top-half count is the number of measures the organization scored in the top 50<sup>th</sup> percentile of all respondents. We see that there are low and high levels of performance based on top-half count. The transition from low to high performance corresponds with a top-half count of nine.

**Figure 23**  
**Top-half Count for Five Clusters**



In addition to clustering, which separates these organizations by control maturity and performance, these five groups were examined to look for additional segmentation that would help identify profiles that explain the heterogeneous population. We used firmographic data to develop profiles that help describe additional differences in the clusters in order to identify appropriate clusters to group together for use in the regression analysis. We analyzed linear affects of various measures for the five clusters.

We determined that the clusters differed based on organization size as measured by both number of employees and number of IT staff. Organizational and IT staff size was the only measure that showed consistent differences in the five groups. Figure 24 shows the number of employees for the organizations that make up the five clusters. We see that the number of employees for clusters one and two are similar. We consider smaller organizations those with up to 5,000 employees.

**Figure 24**  
**Employees in the Organization for Five Clusters**

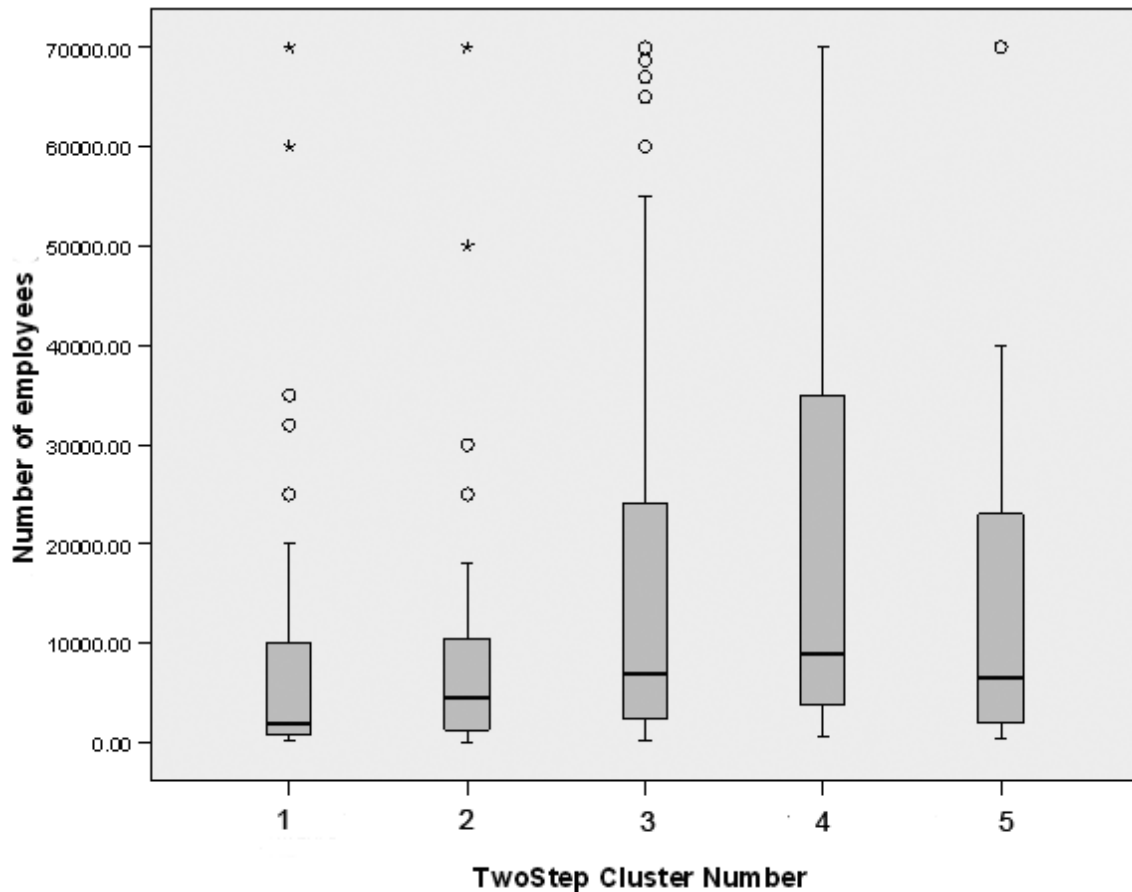
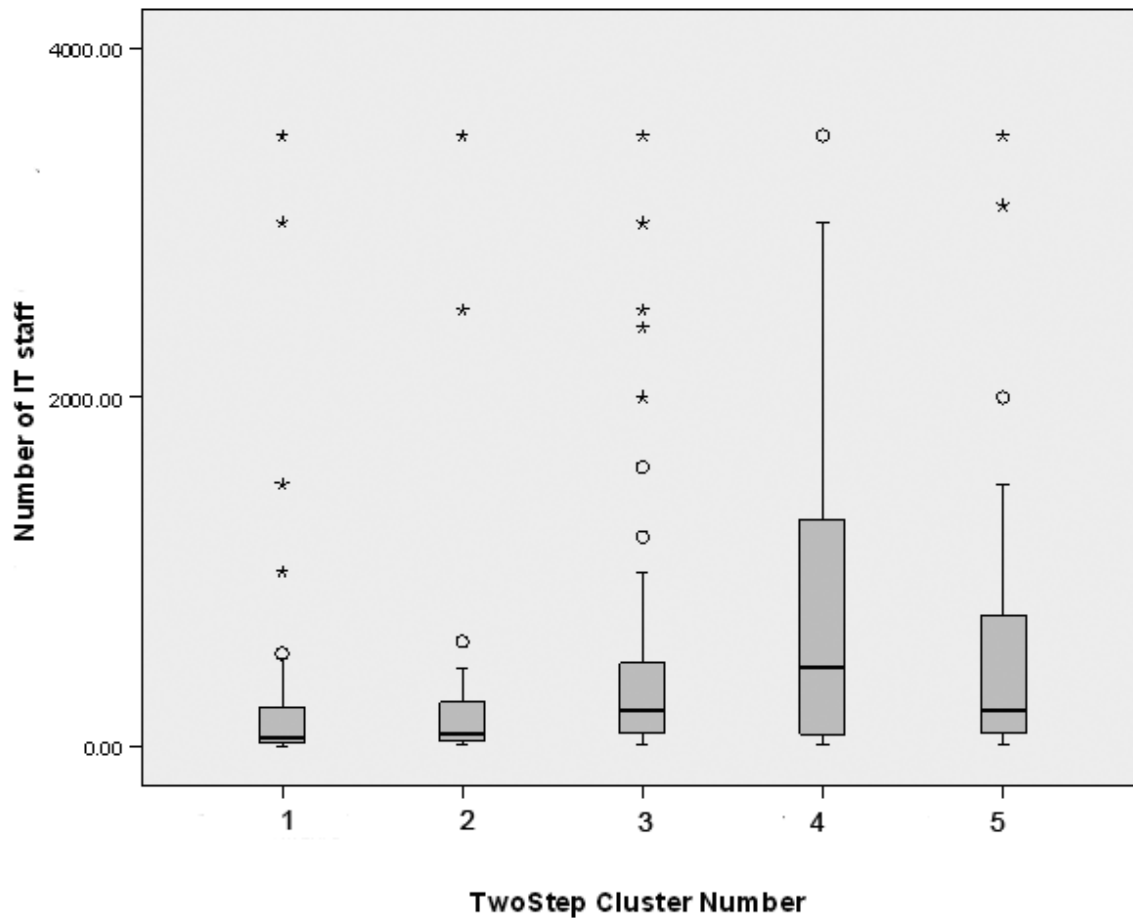


Figure 25 shows the number of IT staff in the organizations for each of the five clusters. We see that the IT staff size for clusters one and two are also similar. We consider smaller organizations as those with IT staff of up to 200 full-time equivalent employees.

**Figure 25**  
**IT Staff for Five Clusters**



This differentiation of the clusters based on employee and IT staff size was important to our understanding of the differences in the way controls impact performance in the different clusters. As IT groups grow in size, there is a natural propensity for internal functions to become segregated, which creates the need for more controls. Smaller organizations have organizational learning and develop tacit knowledge about how things are done and who does what. Larger organizations are often geographically dispersed and rely on more formal documented processes and procedures in order to effectively coordinate activities of a larger number of resources that need to work together to manage IT systems.

Table 13 includes a summary of how the five clusters in the study sample are identified and grouped for regression analysis.

**Table 13**  
**Profile Summary for Five Clusters**

	<b># in Cluster (% of total)</b>	<b>Control Use (average)</b>	<b>Control Maturity (average)</b>	<b>Performance Top-half count (average)</b>	<b>Organization Size</b>
<b>Smaller – low use/low performance</b>	60 (18%)	Low (13.3)	Low (1.42)	Low (6.2)	Small
<b>Smaller – moderate use/high performance</b>	46 (14%)	Moderate (36.3)	Moderate (2.95)	High (10.0)	Small
<b>Larger - moderate use/low performance</b>	114 (34%)	Moderate (32)	Moderate (2.79)	Low (6.3)	Large
<b>Larger - high use/high performance</b>	47 (14%)	High (50.1)	High (4.29)	High (10.5)	Large
<b>Larger - high use/low performance</b>	63 (19%)	High (50.5)	Moderate (4.09)	Low (6.0)	Large

### Summary of Findings

We identified five clusters of IT organizations based on control use and performance. Two of the clusters are from organizations with fewer controls, and are generally smaller organizations. Three are from organizations with more controls in use, and are generally larger organizations. This provides us with two overall sample groups for regression analysis of the impact of IT controls on performance. Our theory based on this clustering is that IT control use as predictor of performance may be different for smaller and larger organizations.

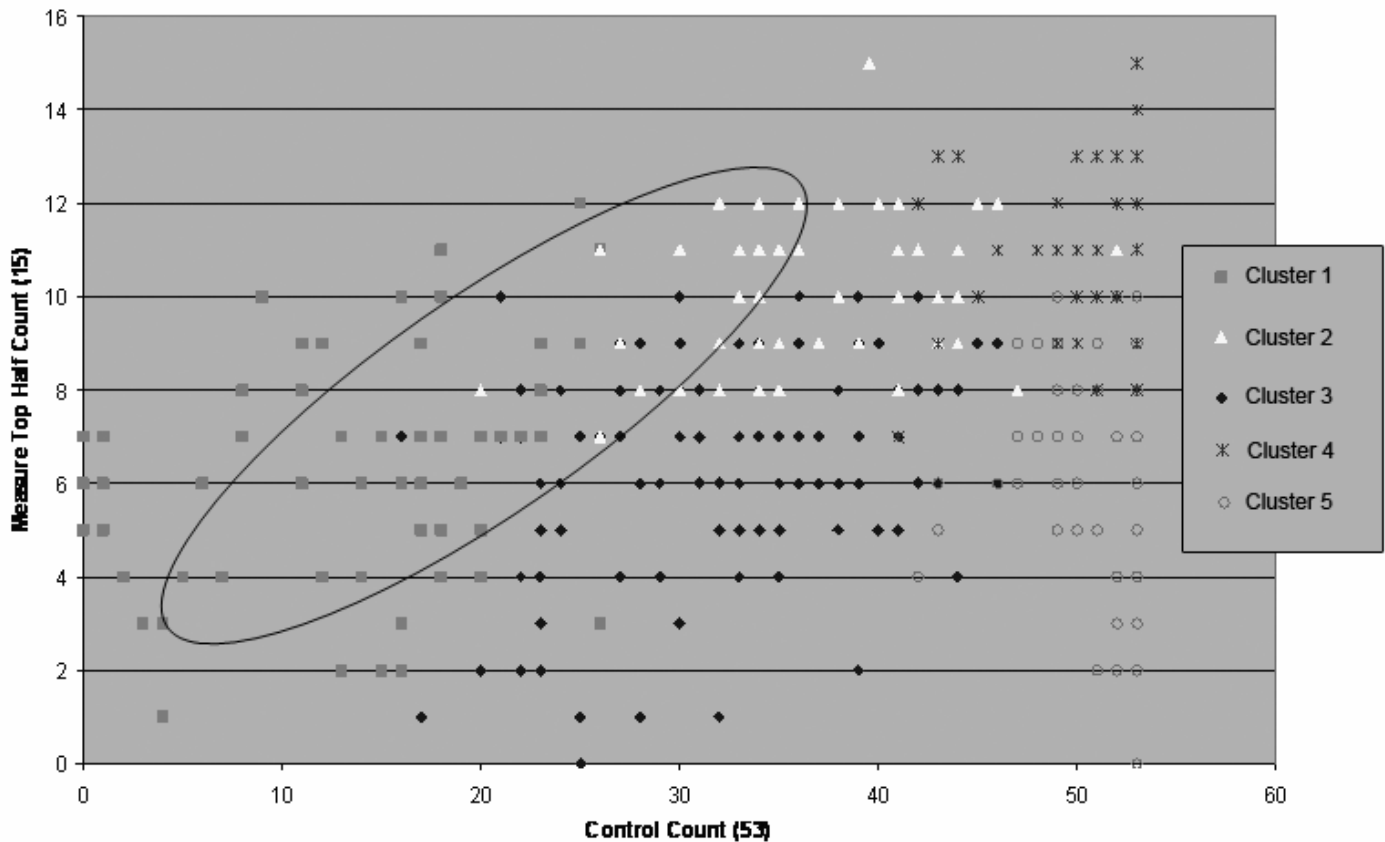
## APPENDIX C IDENTIFYING FOUNDATIONAL CONTROLS

We used stepwise linear regression to determine which IT controls predict different levels of performance for the two clusters of smaller organizations in the study, and for two of the three clusters of larger organizations in the study. The full list of the 53 control variables was used as the input to the regression algorithm, and the top-half count was used as the dependent variable.

Figure 26 highlights the two smaller organization clusters analyzed, represented by squares and triangles. The smaller organization clusters have low to moderate control use and control maturity, and low to high performance.

**Figure 26**  
**Two Smaller Organization Clusters Used in Regression**

**Top Half vs. Control Count**



In each step of the regression, the IT control variables were automatically added or removed to identify the set of controls that best accounts for the greatest variance in the top-half count. This analysis identified three controls that had best predicted variations in the top-half count performance measure. The adjusted r-squared value shows the proportion of variability in the performance top-half count that is accounted for by the statistical model. Table 14 shows the three controls in order of most to least significant impact.

**Table 14**  
**Three Foundational Controls for Smaller Organizations**

Adjusted R squared	Control
.329	A defined process to detect unauthorized access
.428	Defined consequences for intentional, unauthorized changes
.458	A defined process for managing known errors

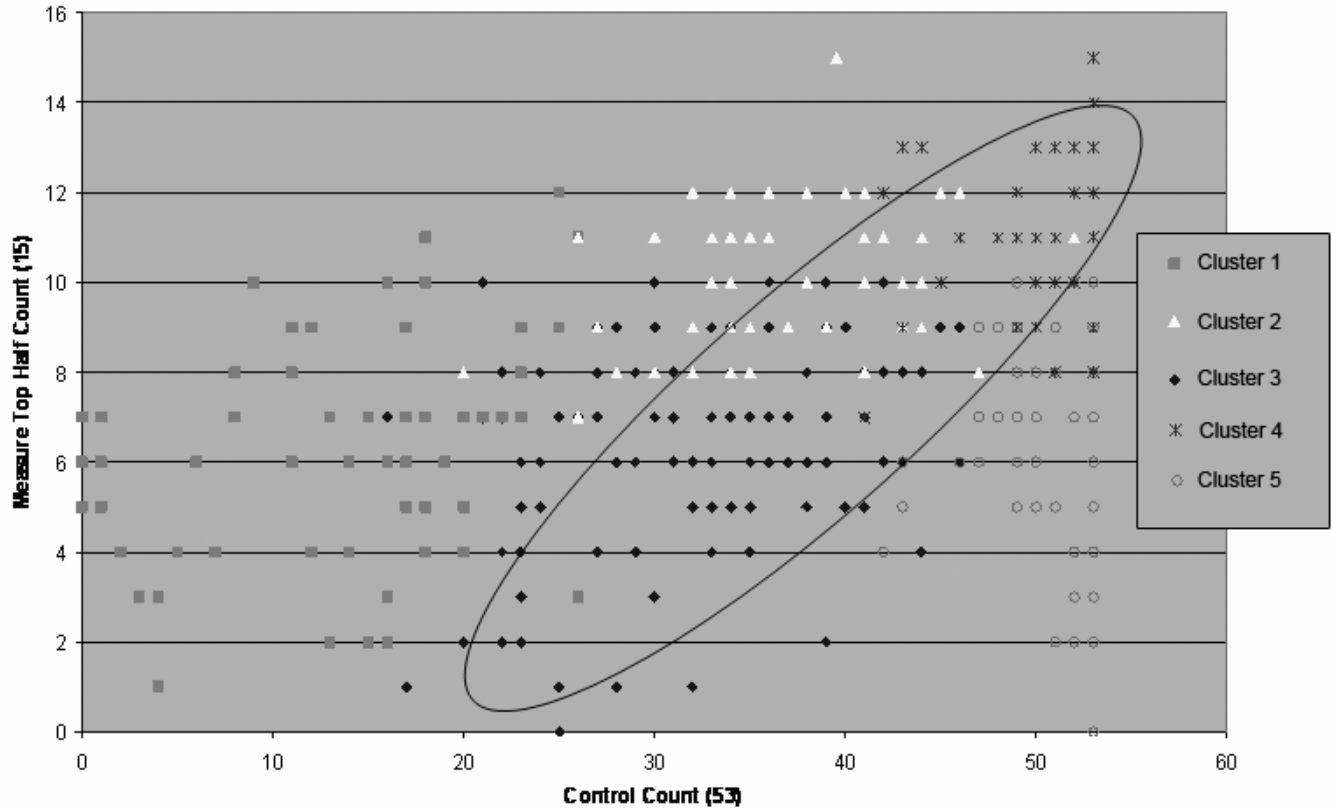
The most significant control, “a defined process to detect unauthorized access,” predicts 32.9 percent of the variation in the top-half count performance measure for smaller organization clusters. The next most significant control, “defined consequences for intentional, unauthorized changes,” predicts 9.9 percent of the performance variation, and together these two predict 42.8 percent of the variation. The third most significant control, “a defined process for managing known errors,” predicts three percent of the performance variation.

A combined adjusted r-squared value of .458 indicates that all three controls combined predict 45.8 percent of the performance variation of the two smaller organization clusters. For operational research where there is a wide range of factors that may impact performance, this level of performance prediction by just three of the controls is significant.

Figure 27 highlights the two larger organization clusters analyzed represented by diamonds and x's. These two larger organization clusters have moderate to high control use and control maturity, and low to high performance.

**Figure 27**  
**Two Larger Organization Clusters Used in Regression**

**Top Half vs. Control Count**



Regression analysis identified nine controls that had a statistically significant impact on the top-half count performance measure for two of the larger organization clusters. The adjusted r-squared value shows the proportion of variability in the performance top-half count that is accounted for by the statistical model.

Table 15 shows the nine controls in order of most to least significant impact.

**Table 15**  
**Nine Foundational Controls for Larger Organizations**

Adjusted R squared	Control
.327	A defined process to analyze and diagnose the root cause of problems
.451	Provide IT personnel with accurate information about the current configuration
.523	Changes are thoroughly tested before release
.551	Well-defined roles and responsibilities for IT personnel
.569	A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents
.579	A defined process to identify consequences if service-level targets are not met
.591	A defined process for IT configuration management
.599	A defined process for testing releases before moving to the production environment
.608	CMDB describes the relationships and dependencies between configuration items (infrastructure components)

The most significant control, “a defined process to analyze and diagnose the root cause of problems,” predicts 32.7 percent of the performance variation in the larger organization clusters. The next most significant control, “provide IT personnel with accurate information about the current configuration,” predicts 12.4 percent of the performance variation, and together these two predict 45.1 percent of the variation. The third most significant control, “changes are thoroughly tested before release,” predicts an additional 7.2 percent of the performance variation. The fourth most significant control, “well-defined roles and responsibilities for IT personnel,” predicts 2.8 percent of the performance variation.

A combined adjusted r-squared value of .608 indicates that the nine controls combined predict 61 percent of the performance variation of the two larger organization clusters. For operational research where there is a wide range of factors that may impact performance, this level of performance prediction by nine of the controls is very significant.

Analysis of the three foundational controls identified for the smaller organizations indicates that most of the larger organizations also have the three controls in use. Seventy-one percent of lower performance cluster have the initial three foundational controls in place, while 99 percent of the higher performance cluster have them in place. Our conclusion is that the three initial foundational controls identified for smaller organizations are prerequisite for larger organizations.

## Summary and Recommendations

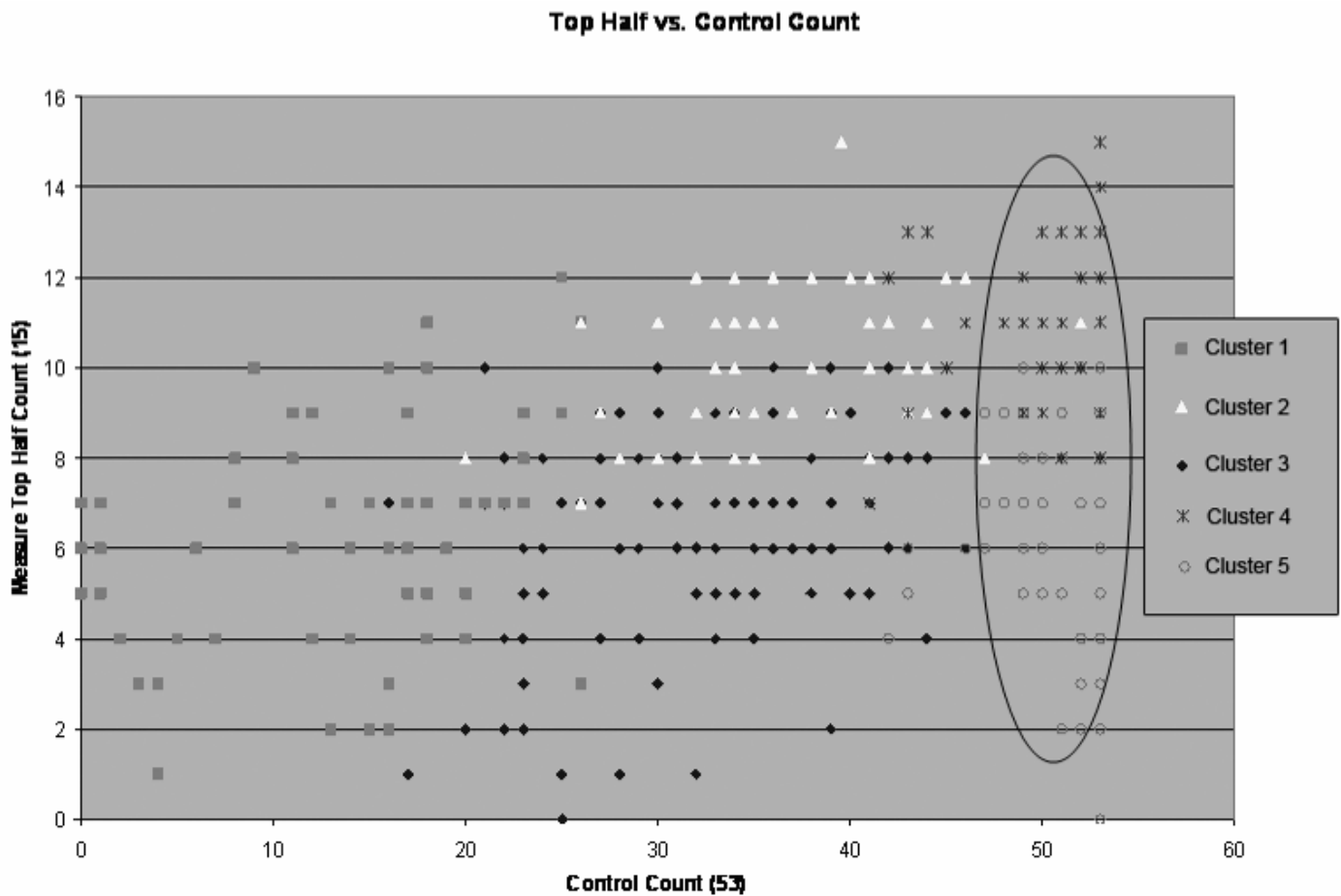
Stepwise regression identified three controls that predict 46 percent of the performance variation in the two clusters of smaller organizations in the study. This is a significant finding. Smaller organizations should implement these three foundational controls, with a predicted result of overall performance improvement. Based on the Likert scale which was used to score control use, we also recommend that processes should be implemented at a level 4 or 5 maturity. That is, these key controls should have measures in place to monitor and manage process exceptions, with clearly identified consequences for individuals who knowingly do not follow process.

Stepwise regression identified nine controls that predict 60 percent of the performance variation in the two clusters of larger organizations. This is a very significant finding. Larger organizations should implement these nine foundational controls, with a predicted result of overall performance improvement. We consider the three foundational controls identified for smaller organizations as prerequisite for larger organizations. Based on the Likert scale used to score control use, we also recommend that these 12 foundational controls be implemented at a level 4 or 5 maturity. That is, these key controls should have measures in place to monitor and manage process exceptions, with clearly identified consequences for individuals who knowingly do not follow process.

## APPENDIX D ASSESSING THE IMPACT OF PROCESS MATURITY

Analysis in Appendix B and Appendix C indicates that there are 12 foundational controls: three that predict performance variations between two clusters of smaller organizations, and nine that predict performance variations between two clusters of larger organizations. In this appendix, we look at various explanations of the performance difference of the fifth cluster of larger organizations with high control use and low performance, as compared to the other larger organization clusters with high use and high performance. Figure 28 highlights the two clusters that we analyze in this appendix, represented by circles and x's.

**Figure 28**  
**Two Larger Organization Clusters Used in Process Maturity Analysis**



One of the questions raised by our five-cluster solution was why two of the large organization clusters that both have high control use have very different levels of performance? Does the maturity of controls in use, or more specifically the maturity of foundational controls in use, help explain their performance differences?

Several potential explanations of the performance difference of these two clusters are related to the overall control count and maturity measures. We can work through various explanations of the potential cause of performance difference between these two larger organizations high use clusters by analyzing the various use and maturity measures. Table 16 shows the six overall and foundational control measures used in this analysis.

**Table 16**  
**Overall Average Maturity Levels for**  
**Two Larger Organization Clusters**

	Larger – High Use, Low Performance	Larger – High Use, High Performance	Statistically Different?
Overall Control Count Maximum score (53)	50.4	50.8	No
Overall Average Maturity Level Maximum score (5.0)	4.09	4.29	Yes
Overall Maturity 5-count Maximum score (53)	16.9	26.4	Yes
Foundational Control Count Maximum score (12)	11.70	11.72	No
Foundational Average Maturity Level Maximum score (5.0)	4.10	4.40	Yes
Foundational Maturity 5-count Maximum score (12)	3.87	6.38	Yes

Analysis indicates that the two clusters have the same overall and foundational control count. However, the overall and foundational control maturity measures are different for these clusters.

Our interpretation of these findings is that there are some organizations with foundational controls in use (but not at the highest levels of maturity) that do not get performance gain that the other organizations with highest levels of maturity receive. Many organizations have implemented controls recently to meet new regulatory requirements. Those controls may be implemented at a level of maturity required to pass audit, but not yet at a level of maturity that has been internalized by the organization to impact performance.

To determine which maturity measure best predicts performance variation in top-half count we calculated the correlation coefficient for the count of foundational controls implemented at 1) levels 3, 4, or 5, 2) levels 4 or 5, and 3) at level 5.

The foundational control maturity level 4 and 5 measure had the highest correlation coefficient at .1629, as compared to 0.143 for the foundational control count, and 0.137 for the foundational control maturity level 5.

Our conclusion from this analysis is that the foundational control maturity level 4 and 5 is the best maturity measure for use by IT organizations looking to improve performance related to the use of foundational controls.

## **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 978-0-89413-625-2**

**Item #2006.dl**

**Free to IIA Members**

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