

Research Summary

Not All IT Controls Are Created Equal

Understanding the Performance Improvement Potential of Foundational Controls



Advancing the Science
of IT Management

IT Process Institute
www.itpi.org

Executive Summary

IT organizations have an increased focus on implementing IT controls and passing IT audits in order to comply with various regulatory requirements, such as those related to Sarbanes-Oxley section 404.

The primary purpose of identifying and managing an IT operating procedure or process as a control is to reduce a specific risk. However, one theory is that a secondary benefit exists: the processes around improved repeatability, predictability, and auditability of key operating processes can also produce measurably better results.

To test this theory, the IT Process Institute conducted a survey to study the performance impact of a broad range of IT controls. We found that companies with higher performance levels had more controls than lower performing peers. We also found a subset of what we call “foundational controls” that have the largest impact on performance.

This paper summarizes the research findings of that study with a focus on the IT controls found to have the biggest impact on IT performance, and on the performance improvement potential that can be achieved by implementing more rigorous IT controls in those areas.

In response to the onslaught of regulations, the demands of meeting industry best practices, and the need to enforce internal policies, IT organizations have an increased focus on implementing IT controls and passing IT audits. As a result of making improvements to comply with various regulatory requirements, IT operating processes that previously were defined, but perhaps not consistently followed, are now managed to become repeatable, predictable, and verifiable via an audit.

The primary purpose of identifying and managing an operating procedure or process as a control is to reduce a specific risk. However, one theory is that a secondary benefit also exists: that by improving repeatability, predictability, and auditability of key operating processes, the processes produce better operating results.

There are a wide range of benefits related to processes that are repeatable, predictable, and verifiable via an audit:

- Consistent procedures produce consistent results.
 - This is beneficial to large organizations that want consistent results across dispersed IT operating units.
 - Predictable results are also desirable for key processes, such as change management, that have a significant impact on performance.
- Resources are more efficient.
 - If people clearly understand their roles, responsibilities, and work procedures, they are more efficient in their efforts.
 - Less time is spent understanding upstream and downstream work, and in handoffs with other process participants.
- Ongoing compliance costs are reduced
 - It is easier to demonstrate that procedures are consistently followed if they actually are consistently followed.
 - Repeatable processes and consistent results get a lower level of scrutiny by auditors.

Testing the theory

To test this theory, the IT Process Institute conducted a Web-based survey of 98 companies in North America to study the performance impact of a broad range of IT controls. The study respondents were from a cross-section of industries and represented varying organization sizes. The survey instrument consisted of 97 core questions that collected information on both controls in use and on operational measures.

The survey was designed to test our theory about the impact of increased rigor of IT processes that are managed as IT controls, from the perspective of whether the improved process control impacted operating performance.

We defined 25 performance measures in three categories: operations, security, and audit. Each of the measures had a business benefit associated with improved performance, in the form of improved utilization of resources (people and assets), reduced ongoing operating costs, better alignment with needs of the business, and reduced audit, compliance, and security costs.

Overall, we looked at the relationship between 65 specific control activities, and the 25 operations, security, and audit performance measurement questions. We found that companies with higher performance levels had more controls than lower performing peers. We also found a subset of what we call “foundational controls” that have the largest correlation with performance.

Foundational Controls

Although IT organizations must implement a broad range of IT controls to manage risk and meet an increasing number of regulatory requirements, we looked to identify a subset of controls that have a greater effect on performance measures.

Using statistical analysis, we identified a subset of 21 foundational controls, out of the total 65 controls analyzed in the study, which have the greatest correlation with the operations, security, and audit performance measures. These controls fall in six categories, which include:

Access Controls

- Have a formal process for requesting, establishing, and issuing user accounts
- Have an automated means of mapping user accounts to authorized users
- Ensure that IT personnel have well-defined roles and responsibilities
- Regularly review logs of violation and security activity to identify and resolve incidents of unauthorized access

Change Controls

- Track the change success rate
- Monitor systems for unauthorized change
- Have defined consequences for intentional unauthorized changes
- Use historical change success rate information to avert potentially risky changes

Configuration Controls

- Have a formal process for IT configuration management
- Have an automated process for configuration management
- Provide relevant personnel with accurate information on the present IT infrastructure configurations, including their physical and functional specifications

Release Controls

- Have a standardized process for building software releases
- Maintain an identical testing environment to your production environment for release testing purposes
- Have a definitive software library (DSL) that supports a repeatable build strategy

Service Level Controls

- Regularly review the service catalog
- Have a service improvement program
- Have a formal process to define and monitor service levels

Resolution Controls

- Track the percentage of incidents that are fixed on the first attempt (first fix rate)
- Use a knowledge database of known errors and problems to resolve incidents
- Rebuild, rather than repair, to resolve an incident
- Have a defined process for managing known errors

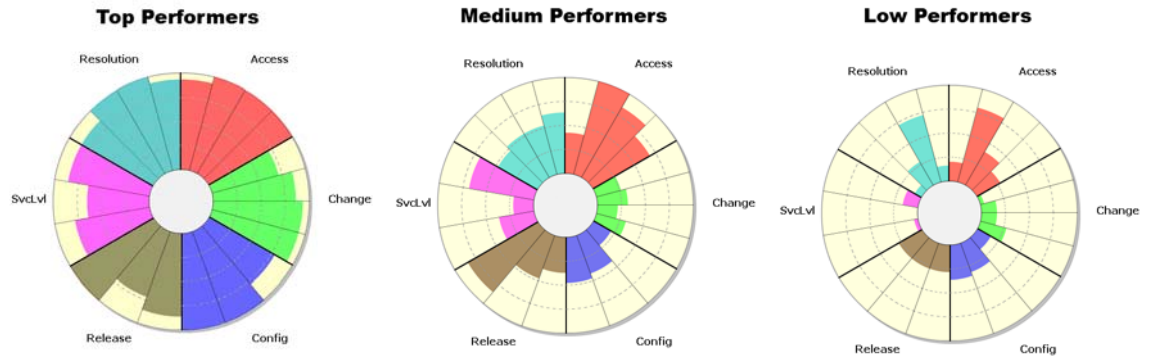
Varying Use of Foundational Controls

We used a cluster analysis technique to group respondents by both their use of the 21 foundational controls and their performance by counting how many times they scored in the top 50th percentile (within the 25 performance measures defined above).

Summary of three groups:

- The top performers had an average of 95 percent of foundational controls in use, and had a median 12 measures in the top 50th percentile of respondents.
- The medium performers had 52 percent of foundational controls in use, and had 11 measures in the top 50th percentile.
- The low performers had 26 percent of foundational controls in use, and had nine measures in the top 50th percentile.

Polar vector diagrams help illustrate which controls differentiate the top performers. These diagrams show the percentage of each foundational control implemented by the respondents in each of the three clusters.



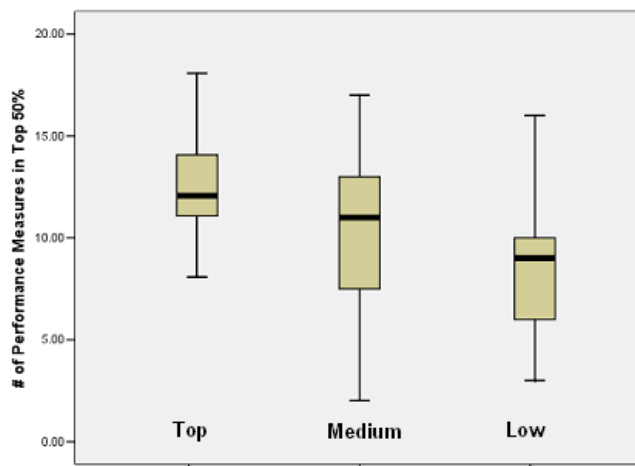
The outside of the circle represents 100 percent of respondents having implemented a particular control, and the inside circle represents 0 percent. The intermediate marks show 25 percent, 50 percent, and 75 percent.

The six categories of foundational controls are shown in different colors, with access controls starting at the 1 o'clock position, followed by change, configuration, release, service level, and resolution controls.

This provides a visual verification that the members of the top-performing group implemented more of each of the foundational controls than the medium or low-performing groups.

Varying Levels of Performance

The levels of performance of these three groups varied significantly. To quantify performance difference, we compared the performance measures of the respondents in the top, medium, and low-performing clusters. The difference in the number of top 50th percentile measures for these three groups varies as shown below.



Organizations with more foundational controls in place have significantly better operational performance.

When we shared these results with IT practitioners, a range of alternative explanations were considered. Typical reactions were that these top performers may not be

representative of large complex IT organizations, or that perhaps they had fewer configuration items and software applications to support.

However, demographic information about the study participants does not support these alternative explanations for their top performance. We found that:

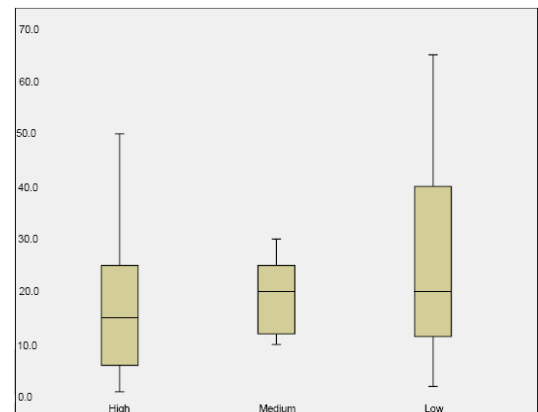
- Top performers deliver and support 4.5 times more IT services to the business than medium performers.
- Top performers support 2.6 times more applications and software solutions than medium performers.
- Top performers authorize and implement 5 times more IT changes than medium performers.
- Top performers are very comparable in size to medium performers, although slightly larger than low performers.
- Top performers are found in the same IT-intensive industries as medium and low performers.

When comparing performance levels of top, medium, and low cluster groups, our findings suggest that foundational controls do make a substantial contribution to these performance improvements.

Top performers that have foundational controls in place have significantly better operational performance in some key performance measurement areas.

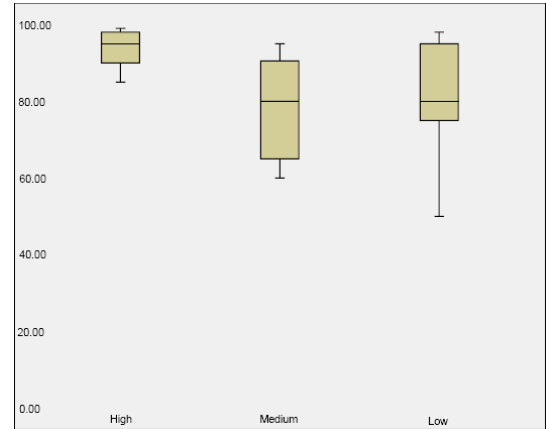
Top performers have a **12 percent lower rate of unplanned work** than medium performers and 37 percent lower than low performers.

Unplanned work is also known as “fire fighting.” Lower unplanned work rate allows top-performing organizations to focus more resources on planned work that supports the priorities of the business.



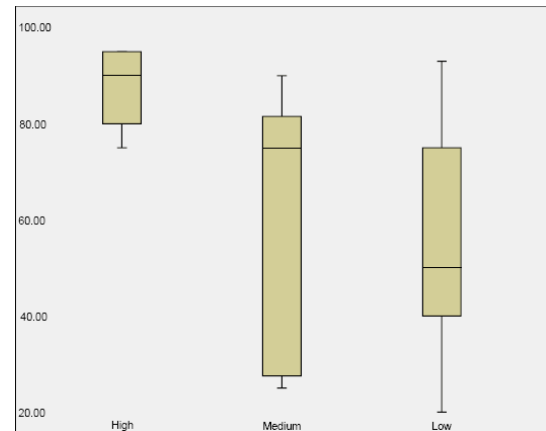
Top performers have an **11 percent better change success rate** than medium performers and 25 percent better than low performers.

Change success rate is important as failed changes are a leading cause of downtime and service disruption. Top-performing organizations have a higher change success rate, which means they have less risk introduced into the production environment.



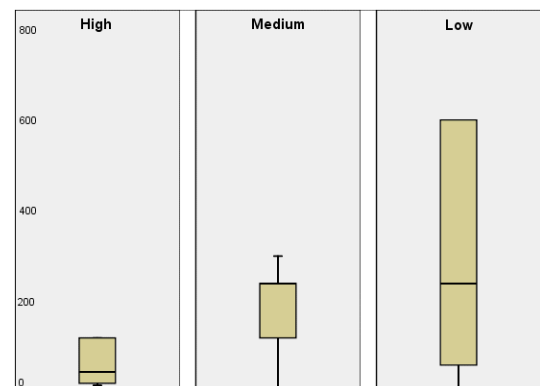
Top performers have a **first-fix rate that is 45 percent greater** than medium performers and 56 percent greater than low performers.

First-fix rate is important as it 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.



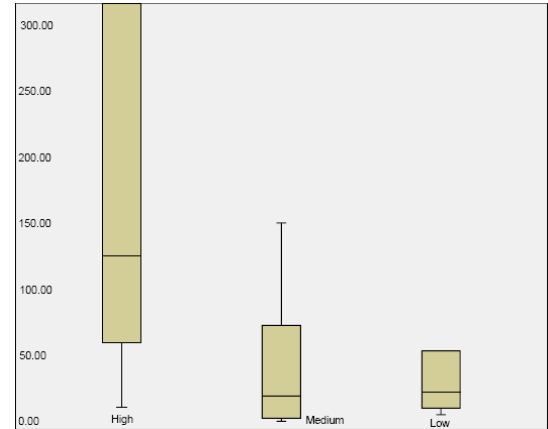
Top performers have **87 percent lower mean time to repair** (minutes) for large outages than medium performers, and 85 percent lower than low performers.

Low mean time to repair indicates that services are restored quickly. Top performers have significantly lower mean time to repair, which, combined with higher first-fix rate, indicates better IT resource utilization and better overall service levels.



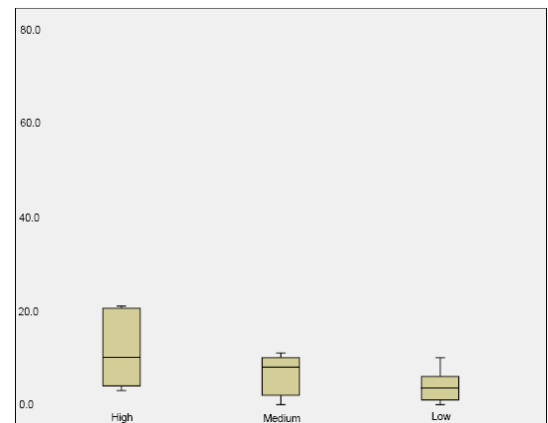
Top performers support **2.5 times more servers per system administrator** than medium performers, and 5.4 times more than low performers.

Server-to-system-administrator ratio is a rough gauge of how much IT infrastructure can be supported with limited resources. Top-performing IT organizations have significantly higher server-to-system-administrator ratios, which indicates much better resource utilization.



Top performers set aside **1.9 times more hours per week for scheduled maintenance** than medium performers, and 4.8 times more than low performers.

Making changes only during scheduled maintenance hours is an effective way to deliver service within service level agreements. Top performers have more time scheduled for changes to production, and are more likely to only make changes during scheduled maintenance periods.



Applied Findings and Conclusions

The implications of these findings are significant for IT executives and practitioners who are responsible for both compliance and for managing operating results.

When organizations identify and manage operating processes as IT controls in order to meet compliance requirements, they should be managed to meet the primary purpose of reducing risk. However, in the areas we have identified as foundational controls, the processes should also be managed with the expectation that improved consistency, repeatability, and predictability also help achieve better operating results.

IT should look beyond IT controls as a “check box” activity, and invest resources into leveraging defined and repeatable processes as a general strategy for achieving improved results.

With a focus on the controls as a way to improve operating performance, IT personnel and managers are more likely to follow procedures and process that are required to pass audit. Understanding how these IT controls improve performance also helps IT audit build a business case for audit activities in IT.

Additional Resources

IT Controls Performance Research Report

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

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

IT Controls Performance Benchmark

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

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

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

For more information about the IT Controls Research Report and IT Controls Performance Benchmark visit www.itpi.org.

About the ITPI

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

© 2007 IT Process Institute. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form other than PDF by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written authorization of the IT Process Institute. Submit requests to info@itpi.org.

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