

# Executive Snapshot

## Process maturity matters: The key to unlocking the power of IT controls

Includes ten applied findings from a study of 330 IT organizations that reveals specific IT Controls that can significantly improve IT operating performance if implemented at a high level of process maturity

Based on a study funded by the Institute of Internal Auditors Research Foundation



Advancing the Science  
of IT Management

IT Process Institute  
[www.itpi.org](http://www.itpi.org)

## Executive Summary

A recent study conducted by the IT Process Institute and funded by the Institute of Internal Auditors Research Foundation finds that IT controls improve the performance of a range of key IT operating processes. In addition, there is a small set of foundational controls that impact performance more than others across the organizations in the study. The findings indicate that implementing these controls at a high level of process maturity appears to be the key that unlocks the performance improvement potential of these controls. Data that quantifies the different levels of performance of companies studied suggests significant performance improvement potential related to the implementation of foundational controls.

The findings from this study highlight ten powerful ideas that can be applied to achieve the dual objectives of risk reduction and performance improvement in IT.

The complete research report of these findings will be available from the Institute of Internal Auditors in 2007.

© 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](mailto:info@itpi.org).

## ***Introduction***

What if IT controls reduce risk as designed, but at the same time also improve IT operating performance?

Many IT organizations view IT Controls as an externally imposed regulatory cost and burden on already stretched IT resources. But what if IT controls are also a powerful tool to improve service levels and reduce costs? Then controls would simultaneously meet the objectives of the IT auditor and the VP of information systems. And, what if there were a small number of IT controls that have the biggest impact on IT performance? IT organizations could focus their efforts on these few foundational controls in order to get performance improvement, and as a result, see a tangible return on investment for IT control activities.

A recent study conducted by the IT Process Institute and funded by the Institute of Internal Auditors Research Foundation found that there is a set of foundational controls that impact performance more than others across the top, medium and low performing organizations in the study. In addition, the findings indicate that implementing these controls at a high level of process maturity appears to be the key that unlocks the performance improvement potential of these controls.

The implications of these findings are significant: IT organizations can use IT controls as a way to improve performance. This gives IT executives a focused target with big payoff. They can use compliance and controls projects as a reason to move their organizations to a more process focused orientation.

**What if IT controls improve IT operating performance as well as reduce risk as designed?**

Executives can leverage the compliance and controls mandate to set the tone at top that following documented process and procedures in key functional areas is a strategy for performance improvement. The requirement of needing IT controls to meet various regulatory requirements offers a unique opportunity to make organizational and cultural changes so that everyone in the organization understands they are expected to follow documented process and procedures.

The process focused approach to managing key IT processes represents a shift away from a technology focus, to a focus on process consistency and repeatability. IT and business executives that are tired of IT related surprises can identify and manage process exceptions as a way to improve predictability of both activities and results.

This paper presents a summary of the study of how IT controls improve performance at 330 North American IT organizations in 2007.

## ***Identifying Foundational Controls***

The overarching research question for this study is “What is the impact of IT controls on IT operating performance?” More specifically, if IT controls improve performance, are there specific IT controls that improve performance more than others?

The research reveals that just twelve of the fifty-three controls analyzed predict sixty percent of the performance variance of the organizations studied. These Foundational Controls include specific activities in the areas of access controls, change controls, release controls, configuration controls, resolution controls, and service level controls.

**Just twelve of the fifty-three controls analyzed predict sixty percent of the performance variance.**

Three of these IT controls predict 45% of the performance of one group of organizations that have lower overall control use, which tend to be smaller organizations. The other nine controls predict 60% of the performance of a second group of organizations that tend to be larger organizations, that have higher overall control use and performance. This is a significant finding for operations research, where a wide range of other factors may also cause performance variation.

The three controls that predict 45% of performance variation for primarily smaller companies with fewer controls in place include:

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

Nine controls that predict 60% of performance variation for primarily larger companies with a greater number of controls in place include:

1. A defined process to analyze and diagnose the root cause of problems
2. Provide 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. CMDB describes the relationships and dependencies between configuration items (infrastructure components)

The three foundational controls that best predict performance for organizations with fewer controls in place are also implemented by most of the larger organizations in the study, and therefore do not produce performance variation in larger organizations. However, we consider these three pre-requisite for organizations with overall greater number of controls in place. Together, we consider this set of twelve IT controls as foundational controls that best predict performance variation in the organizations in this study.

The impact of implementing IT controls in an information systems production environment comes from the IT organization modifying their processes and procedures to implement general controls which are embedded in IT processes. Implementing IT controls may require IT staff to change the way they do things as part of their regular job functions. Systems may need new software to manage specific risks. Organizations may need to collect more data to store records about individual activities in order to provide an audit trail. All of these things potentially impact the working function and operating results of an IT organization.

The impact of implementing IT controls in an operational environment is also the result of consistently following the specified way of doing things. IT organizations may not have a history of identifying and following specific operating procedures in many functional areas within IT. Although many organizations are now turning to best practice frameworks such as the IT Infrastructure Library (ITIL ®), they may not have an organizational culture that encourages and rewards following documented procedures.

The impact of implementing IT controls in the IT production environment is partly the result of consistently following a specified way of doing things.

Several factors may help explain why IT organizations with fewer controls in place have different control impact characteristics than those with more controls in place. First, a smaller set of controls have less potential impact on various performance measures. Second, smaller IT organizations typically rely less on documented processes and procedures. They may be more likely to use tacit knowledge, individual heroics, and organizational learning than standardized operating practices. Third, larger IT organizations tend to be more geographically dispersed and have more siloed IT functions, both of which require greater reliance on more formalized IT processes and procedures that may be impacted by the use of IT general controls. These larger organizations that rely on documented procedures and controls may also have a culture that naturally supports greater consistency of implemented controls, which is shown to explain in part the performance difference of organizations in this study.

Overall, smaller organizations have fewer IT controls and thus the controls are less of a predictor of overall performance than other factors which were not analyzed in this study.

## **Process maturity matters**

Another key finding of this study is that maturity of control activities matters, and it matters a lot. Some companies with a high overall control usage, and high foundational control usage did not measure high levels of performance. Analysis of the maturity levels of controls for these IT organizations reveals that both the process maturity level of all controls, and more specifically the foundational controls, helps explain in part their lagging performance. Our survey questions asked to what degree each of 53 controls are implemented on a 0 to 5 maturity scale as follows:

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
-----------------	--------------------------------------	--	---	---	--

Analysis of the level of maturity for different groups of IT organizations in the study indicates that use of controls at a process maturity level 4 or 5 on this scale appears to enable greatest performance gain from the foundational controls.

IT organizations may respond to IT controls in one of two ways. Some IT organizations with a culture that supports the use of documented 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 process orientation and process improvement. Other organizations with a culture that supports individual innovation and achievement may view IT controls and IT audit activities as an externally imposed burden that at best require significant effort to document and train IT staff to follow prescribed process 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 “check box” 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 of higher levels of operating efficiency and effectiveness.

**Controls implemented at a process maturity level 4 or 5 on this scale enables the greatest performance gain from the foundational controls.**

Our interpretation of the data is that those organizations that implement control processes at a high level of maturity, which includes identifying and managing process exceptions (our level 4 and 5 process maturity), perform better than those that have only informal controls driven by regulatory compliance (our level 3 process maturity). As a result of our assumptions about process maturity, and our analysis findings, we recommend that IT organizations implement foundational controls at a target process maturity level of 4 or 5 (“managing by exception”) to achieve performance gains.

## ***Performance improvement potential***

The performance improvement potential of using foundational controls at higher process maturity levels is significant. Overall top performers, which represent the highest performing 15<sup>th</sup> percentile of participants in this study, exhibit significantly higher performance on a range of 15 key measures that indicate the overall effectiveness and efficiency of IT operating performance in our study.

Highlights of the striking performance differentials include:

- Top performers have an average 95% change success rate, which is 3% better than medium performers and 12% better than low performers.
- Top performers have an average 17% late project rate, which is 20% lower than medium performers and 50% lower than low performers.
- Top performers have an average server to system administrator ratio of 114, which is 32% higher than medium performers and 88% higher than low performers.
- Top performers have an 89% average first fix rate, which is 6% higher than medium performers and 22 % higher than low performers.
- Top performers automatically detect 81% of security breaches, which is 12% higher than medium performers and 76% higher than low performers.
- Top performers have average composite customer satisfaction score of 4.3 (on 1-5 scale), which is 18% higher than medium performers and 30% higher than low performers.
- And, top performers have an average repeat audit finding rate of 15% which is 39% lower than medium performers and 52% lower than low performers.

## ***Top-ten applications of these findings***

The findings from this study highlight ten powerful ideas that can be applied to achieve the dual objectives of risk reduction and performance improvement.

- 1) Recognize that certain controls can improve IT performance. This shift in thinking can help IT executives reframe important resource allocation decisions. IT application and operations groups can more actively manage IT controls that impact key processes, to achieve performance gains.
- 2) Reposition IT's 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 create a positive performance effect as well as meet risk reduction objectives. Form a partnership with IT audit and use them as resource to help verify that your carefully designed procedures and controls are actually followed throughout the organization, in order to achieve performance ignition.
- 3) Make sure foundational controls are in place. Data shows this handful of controls predict performance in a broad sample of organizations. We can infer that these controls can also impact performance in your organization as well.

- 4) Implement foundational controls at a target process maturity level. 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.
- 5) Synchronize compliance and controls initiatives with 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 goals, measure both process and outcomes metrics, identify process exceptions, prioritize improvements, refine and improve processes to meet performance goals.
- 6) Don't settle for a check-box mentality. IT audit can help identify control objectives. But IT organizations should design and own the processes that meet the dual objectives of control and performance. If you accept changes to IT operating procedures that are designed to only pass an audit, at best you miss an opportunity to engineer performance improvement, and at worst you may implement procedures counter to performance objectives.
- 7) Use good process design practices to achieve high levels of process repeatability both for auditability and to drive out variation in results. Collect data that leaves an audit trail and which also enables process exception identification, root cause analysis, gathering of key performance indicators, and process capability improvement.
- 8) Don't be afraid to update control definitions and processes to meet operating measure objectives in parallel with risk and control objectives. Just because your operating process is linked to a control requirement doesn't mean it can't be updated regularly as process improvements are identified.
- 9) 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 IT management, and a strategy for achieving higher service levels at lower cost. Achieving compliance with new regulations provides an opportunity to set the tone at the top set a new direction for IT efforts.
- 10) Engineer cultural changes using human resources, and the thoughtful application of both the "carrot" and the "stick." Hire people with a natural process orientation, and reward and promote process oriented people instead of fire fighting heroes.

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

The IT Process Institute is an independent research organization that exists to support the membership of IT operations, security, and audit professionals. Our mission is to advance IT management science through independent research, benchmarking, and prescriptive guidance. Our vision is to pair industry-based volunteers with leading university-based researchers to identify and study top-performing IT organizations and enhance the efficiency and effectiveness of the industry. V062807