Prioritizing IT Controls for Effective, Measurable Security

Daniel Phelps
Gene Kim
Kurt Milne

October 2006

ABSTRACT: This article summarizes results from the IT Controls Performance Study conducted by the IT Process Institute. The article describes what differentiates high performing organizations in IT and security from others and identifies six foundational controls that are deployed by these organizations.

INTRODUCTION

How can you tell if your security and IT controls are really effective? How do you measure security effectiveness? How do you prove that IT security controls help increase IT operating effectiveness and efficiency and that they don't just slow the business down? How can you differentiate high performing security and IT operations organizations from those that are low performing?

These are all questions that historically did not have great answers. Most of the better answers resembled platitudes instead of actionable advice (for example, "Make sure the business cares about security").

Coming up with better answers is what Kevin Behr and Gene Kim set out to do in 2000 when they co-founded the IT Process Institute. They wanted to advance the quantitative science in IT operations and security to help organizations answer these very questions and to create meaningful guidance that was tested with the same empirical rigor that, for example, pharmaceuticals use for conducting drug trials.

Their hypothesis was that if they could analyze high performing IT and security organizations and what they did, they could discover and recommend specific actions, with fair confidence that these actions would produce measurable results.

The IT Process Institute is dedicated to researching, benchmarking, and developing prescriptive guidance for IT organizations. The IT Process Institute has partnered over the years with organizations such as the SANS Institute, the Software Engineering Institute at Carnegie Mellon University, and the Institute of Internal Auditors to capture and codify how high performers became great, the result of which is The Visible Ops Handbook [<a data-cke-saved-href="/articles/best-

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

practices/deployment-and-operations/deployment-and-operations-references" href="/articles/best-practices/deployment-and-operations/deployment-and-operations-references" itpi04"="">ITPI 04]. As of July 2006, this handbook has sold over 40,000 copies, and is increasingly accepted as a useful, prescriptive, project-based approach to implementing the processes described by the IT Infrastructure Library (ITIL) [ITIL 00], [ITIL 01]. (See Integrating Security and IT for more information about Visible Ops and ITIL.)

From the outset, high performing organizations were easy to spot. By 2001, Behr and Kim had identified eleven organizations that had similar outstanding performance characteristics. These organizations had the best security as indicated by

- high service levels, measured by high mean time between failures and low mean time to repair
- the earliest and most consistent integration of security controls into IT operational processes, measured by control location and security staff participation in the IT operations life cycle
- the best posture of compliance, measured by the fewest number of repeat audit findings and lowest staff count required to stay compliant
- high efficiencies, measured by high server to system administrator ratios and low amounts of unplanned work (new work that is unexpectedly introduced when a change is made)

Kim and Behr suspected that what differentiated the high performers from everyone else were two things: A culture of change management and a culture of causality. For this and many other reasons, they wanted to demonstrate that building a culture of change management and causality was good for every organization, supported by compelling business reasons and evidence. And that there were very real business consequences of not building such a culture.

As they analyzed the high performers, they began to think, “What if we could show that these high performers are doing something differently, that what they do results in real performance differences, and that this can be replicated in any IT organization?”

To prove that the hypotheses outlined in Visible Ops were both valid and practical, ITPI began a project in 2003 called the IT Controls Performance Study. During this study, conducted over the last three years, ITPI benchmarked IT organizations to answer two questions:

1. What are high performing IT organizations doing differently?

2. How much better are they than typical IT organizations?

Study analysts found many expected, but also surprising, results described below.

HOW GOOD HIGH PERFORMING IT ORGANIZATIONS REALLY ARE

Benchmarks and survey results revealed that the high performers outperform everyone else not by a factor of two, but often by a factor of five to ten [Kim 06]. Survey analysis identified a group of organizations that were high performing in both security and IT operations. This group comprised 13% of total survey respondents.

From a security perspective, here’s what happened when high performing organizations experienced a security breach:

- Security breaches were far less likely to result in loss events (such as financial, reputational, and customer). Loss events in high performers were 29% less likely than in medium performers and 84% less likely than in low perfomers.
- They were far more likely to detect breaches using automated controls. Compared to high performers, medium performers were 60% less likely to detect a breach through automated controls; low performers 79% less likely. In other words, high performers had the right controls in place to detect security breaches; low performers would typically find out from external sources (such as customers and newspaper headlines).
- They detected breaches far more quickly. High performers had a mean time to detect measured in minutes, compared to hours for medium performers and days for low performers.

Top performers also allocated three times more budget to security as a percentage of total IT operational expense. These metrics show that high performing organizations are delivering considerably more value to the business than medium and low performers.

- From an operational perspective, the performance gap between the high performers and everybody else was even more surprising:
- High performers were completing 8 times as many projects as medium and low performers.
- High performers were managing 6 times as many applications and IT services.

- High performers were authorizing and implementing 15 times as many changes.
- When top performers managed IT assets, they had 2.5 times higher server to system administrator ratios than medium performers and 5.4 times higher ratios than low performers.
- When top performers implemented changes, they had one-half the change failure rate of medium performers and one-third the change failure rate of low performers.
- The percentage of work that was unplanned in top performers was 12% lower than in medium performers and 37% lower than in low performers.

Why is this surprising? When the lean manufacturing researchers at the Massachusetss Institute of Technology benchmarked over 100 automotive manufacturing plants around the globe, they found a performance difference of 2x between high and low performers: high performing plants had one-half the defects, one-half the floor space, one-half the cycle time, one-half the inventory, etc. [Womack 91]. In comparison, in the IT organizations that were benchmarked, analysis revealed a much higher difference in performance between high and low performers.

IT security is responsible for properly managing business risk and assuring confidence in business systems and the protection of customer- and business-critical information. Low performers cannot do either and consequently garner extremely low satisfaction ratings with the business and cannot get budget to do anything new. On the other hand, by delivering great security and exceptional operational performance, high performers earn the right to spend more money and are allocated a higher share of the total operating budget.

WHAT DIFFERENTIATES HIGH PERFORMERS FROM EVERYONE ELSE

The second big surprise was discovering the extent to which specific controls differentiated high performers from medium performers. In analyzing what foundational controls were most present in high performing organizations and least present in medium performers, the questions that mapped to IT controls where this gap was largest were

1. Do you monitor systems for unauthorized changes?
2. Are there defined consequences for intentional, unauthorized changes?

These IT change controls were almost universally present in the high performers and virtually absent for everyone else, indicating that they are likely the key levers for medium and low performers to become high performers.

Rounding out the top six foundational controls that were most present in high performers and least present in medium performers were the following:

1. Do you have a formal process for IT configuration management?
2. Do you have an automated process for configuration management?
3. Do you track your change success rate (percentage of changes that succeed without causing an incident, service outage, or impairment [ITPI 04])?
4. Are you able to provide relevant personnel with correct and accurate information on the present IT infrastructure configurations?

These controls validate the Visible Ops methodology, as they are the controls needed to foster a culture of causality. In other words, these controls help the organization not only look one step ahead to avert risky changes but also look one step behind and trace the source of outages and service impairments to change. A configuration management process to track and record change success rates aids in the change management and incident management processes.

FINDING THE FOUNDATIONAL CONTROLS OF THE HIGH PERFORMERS

Study analysts hypothesized that high performers were using a common subset of ITIL processes; they were not doing all of ITIL but had selected the subset that really mattered. Analysts coined this subset the “foundational controls,” which they conjectured would have a disproportionately large impact on the performance measures of operations, security, and audit.

To find which controls mattered most, analysts developed a candidate list of 63 controls by selecting the six leading ISO 20000 [ISO 05c] control categories within ITIL that are considered to be “where to start” when implementing controls. These categories were access, change, resolution, configuration, release, and service levels. Analysts then selected 63 COBIT [ITGI 07a] control objectives within these areas. (See also Integrating Security and IT for more information about ISO 20000, ITIL, and COBIT.)

The survey also included 25 questions on operations, security, and audit performance measures. Questions addressed topics such as IT user satisfaction, unplanned work, security sufficiency, and audit compliance disruption level.[1]

The study revealed that the Pareto Principle applies to IT controls: 20% of the controls provide 80% of the benefit. Each of the six control categories could be reduced to three or four foundational controls. These foundational controls had the same impact on performance measures as the full set of controls. The study identified a total of 21 foundational controls and analysis indicated that these 21 controls delivered the majority of the performance benefits.

But is it true that organizations with more foundational controls have better security and higher performance? To determine this, study analysts used a statistical technique called "clustering." This technique is often used by marketing organizations to analyze purchasing patterns and group them into buying demographics. They used clustering to group similar populations with similar control environments and performance. Specifically, they were looking for a cluster that was achieving the highest levels of performance.

Figure 1 shows a representation of the controls of the three clusters that emerged. Each wedge on the polar vector diagrams represents one of the foundational controls. The size of each wedge represents the percentage of the cluster members that responded "yes" to questions that mapped to that control.

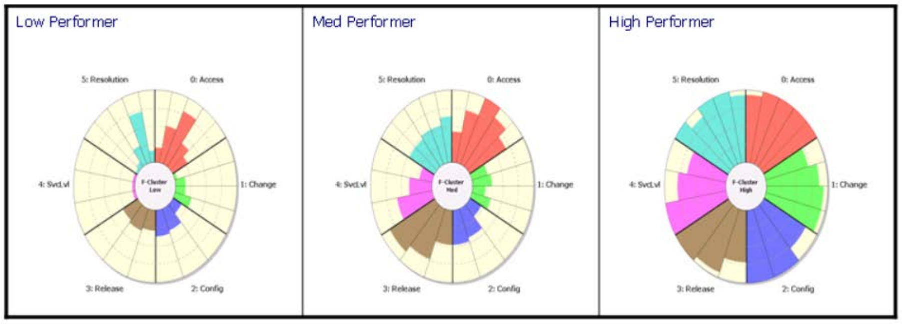

Figure1. Three clusters: low, medium and high performers

[1] hese were Likert-scale questions asking survey respondents to answer the following: "How satisfied are your end users with IT services?"; "How sufficient do you believe your IT security is?"; "What is your level of pain for the following activities: patching, audit, and compliance?" Respondents answered from 1 (causes no disruptions to IT services and no cost increases) to 5 (causes substantial, recurring disruption to IT services and increased IT costs).

Note that almost all of the members of the high performing cluster had all of the foundational controls and that almost all of the members of the low performing cluster had no controls except for access and resolution.

The controls profile of low performers is particularly interesting because it matches study analysts' intuition and experience: most low performing organizations do not have any security controls except for access controls (i.e., issuing and revoking passwords). In addition, the primary work system is reactive resolution controls (i.e., trouble ticketing systems). Security managers, almost by tradition, have hung their hat on access controls; and yet, increases in the amount of foundational access controls are not linked with increased IT operating effectivness or efficiency, or security effectiveness.

On the other hand, the minority of security managers that hinge their strategy on change controls have shown success. According to the IT Controls Performance Study, change controls help create real value in IT operating effectiveness and efficiency.

As mentioned earlier, the study found two discriminant controls. These two controls were in use by all high performers and practically no medium or low performers. These controls are highlighted in Figure 2, which shows the high performers' cluster controls overlaid with the medium performers' (indicated by the solid black line).

Those controls are (1) Do you monitor systems for unauthorized changes? and (2) Are there defined consequences for intentional unauthorized changes?

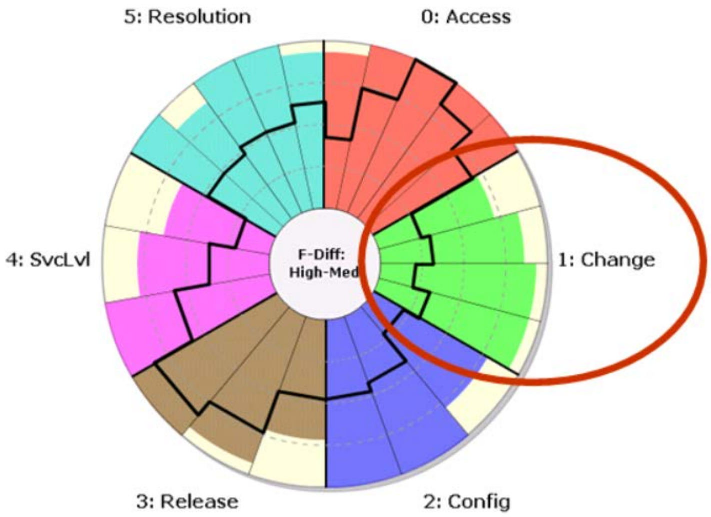

Figure 2. High versus medium performer cluster: what is different?

The study also revealed that there are three things high performing security and IT organizations never do. Specifically, they

- never let developers make changes in production
- never let the change management process get bureaucratic
- never let users exceed their role in the change process

How do they accomplish these things? Through the foundational IT controls, creating a culture of change management. This can be accomplished using Visible Ops [ITPI 04].

CONCLUSION: MOVING FROM GOOD TO GREAT

To move from good to great, Visible Ops prescribes, and the IT Controls Performance Study strongly confirms, the first step is to create a culture of change control and a culture of causality. Begin by establishing tone at the top of the organization that all change follows the change management policy and process. To be successful with this foundational control, leaders must consistently promote and enforce a policy of zero tolerance for unauthorized changes. Additional steps include

- establish a change management culture supported by documented policy
- learn from past successes and failures
- monitor all change (not just authorized change)
- implement technology (such as automated controls) to support the process and make it easy for people to do the right thing
- ensure the organization has preventive, detective and corrective controls

The security and IT industries have long sought the holy grail, reaching for the magic control that will provide both security and positive ROI for the business. While many professionals have focused on access as the path to this holy grail, this research shows that access controls are not a meaningful enabler of security excellence, nor do they strategically contribute to operational efficiency and excellence.

Security is most effective as a strategic contributor to IT operations. Having zero successful security incidents is simply not a perfect score in security, as it does not differentiate between complete control and complete ignorance. Security controls and practices need to be measured to determine their ability to

- support the fulfillment of business commitments

- integrate into daily IT operational processes
- use automation to detect potential events
- reduce the percentage of security incidents that result in loss events
- support the successful investigatation of security events

Taken together, these measures are more powerful indicators of security success than the traditional measure of whether or not an incident occurred.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

DM-0001120