



Configuration Control for
Virtual & Physical Infrastructures

Linking Information Security and Operations Effectiveness To Business Performance:

A Nine Year Study Of High Performing IT Organizations:

Gene Kim, CISA, TOCICO Jonah
CTO, Tripwire, Inc.
9/10/2008
genek@tripwire.com

Are There Really Dead Bodies In IT And Security?

- Having studied high- and low-performing IT organization, I have come to believe that there is a common cause for...
 - High performing IT operations
 - High performing information security
- Because of the criticality of IT to projects and operations, poor IT performance should significantly contribute to probability of...
 - Material weaknesses for SOX-404
 - Loss of confidential information (cardholder data, patient records, SSL certificates)
 - Achievement of business goals and business performance
 - Success of CEOs and CFOs

There is growing body of decisive evidence that all these things are true...

Surprise #1: How Good The High Performers Are

- High performers contribute more to the business
 - **8 times more** projects and IT services
 - **6 times more** applications
- When high performers implement changes...
 - **14 times more** changes
 - **One-half** the change failure rate
- When high performers manage IT resources...
 - **One-third** the amount of unplanned work
 - **5 times higher** server/sysadmin ratios
- When high performers are audited...
 - **Fewest** number of findings

High performers also have 3x higher budgets, as measured by IT operating expense as a function of revenue

Source: IT Process Institute, May 2006

High Performing Information Security Organizations

- High performers find their security breaches before the newspapers do...
 - Loss events are **29% less likely** than in medium performers, and **84% less likely** as low performers
 - Failure to detect of the security breach by an automated control is **60% less likely** than medium performers, and **79% less likely** than low performers
 - Time to detect is **minutes** for top performers, **hours** for medium performers, and **days** for low performers
- Top performers also allocate up to **3x more budget** to security, as a function as IT operational expense



Source: IT Process Institute, May 2006

And Maybe Even Affects The Tenures Of CEOs and CFOs...

- In 2008, Dr. Vernon Richardson and team studied the 10-K filings and disclosures for 184 public firms, dividing them into three categories:
 - A = Firms with material weakness: IT related
 - B = Firms with material weakness: non-IT related
 - C = Clean firms (no material weakness)
- Control groups were constructed to ensure similar demographics across categories:
 - Market capitalization (average \$19B) and industry SIC code
 - The control groups with no material weaknesses were selected to match these groups, along with CEO/Chairman sharing role, etc...

Source: Forthcoming Paper: Richardson, Masli, Watson, Zmud, *Sarbanes-Oxley Information Technology Material Weaknesses And The Disciplining Of The CEO, CFO And CIO*



Comparison Of Turnover For CEOs and CFOs...

- When firms with IT-related material weaknesses are compared with the other two groups, there are some startling differences in executive turnover...

N=184	vs. non-IT related material weakness	vs. no material weakness
CEO	2.0x higher	4.0x higher
CFO	1.7x higher	3.0x higher
CIO	2.2x higher	2.2x higher

Why would IT material weaknesses so heavily impact executive turnover compared to non-IT material weaknesses?

Source: Forthcoming Paper: Richardson, Masli, Watson, Zmud, *Sarbanes-Oxley Information Technology Material Weaknesses And The Disciplining Of The CEO, CFO And CIO*

Comparison Of Turnover For CEOs and CFOs...

- When firms with IT-related material weaknesses are compared with the other two groups, there are some startling differences in executive turnover...

N=184	vs. non-IT related material weakness	vs. no material weakness
CEO	2.0x higher	8.0x higher
CFO	1.7x higher	3.6x higher
CIO	2.2x higher	2.2x higher

Why would IT material weaknesses so heavily impact executive turnover compared to non-IT material weaknesses?

Source: Forthcoming Paper: Richardson, Masli, Watson, Zmud, Sarbanes-Oxley Information Technology Material Weaknesses And The Disciplining Of The CEO, CFO And CIO

Two Questions

- What about your job causes you to feel uncomfortable?
- In your interactions with your business peers and management, what situations don't feel right to you?



Information Security and Compliance Risks *

- Information security practitioners are always one change away from a security breach
 - Front page news
 - Regulatory fines
 - Brand damage
- High profile security failures are increasing external pressures for security and compliance
 - Sarbanes-Oxley (SOX) Act of 2002, the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), emerging privacy laws, and the Payment Card Industry Data Security Standard (PCI DSS)



An Uncomfortable Question *

- Business executives need little convincing that managing information security is necessary to achieve their goals
- Even when information security is adequately funded, why does information security fail to effectively prevent and quickly detect and recover from security breaches?

We believe that the root cause is failing to effectively integrate information security into the daily work of IT operations, software/service development, compliance, project management and internal audit...

Words often used to describe information security:

"hysterical, irrelevant, bureaucratic, bottleneck, difficult to understand, not aligned with the business, immature, shrill, perpetually focused on irrelevant technical minutiae..."

Operations And Security Already Don't Get Along *

Operations Hinders Security...

- Deploying insecure components into production
- Making production IT infrastructure hard to understand
- Lack of information security standards
- Poor availability of IT services
- Using shared accounts to simplify access
- Do not address known security vulnerabilities quickly

Security Hinders Operations...

- Creates bureaucracy
- Generates large backlog of reviews
- Implementation of information security requirements presents delays
- Correcting issues costs too much, takes too long, & reduces feature set



Information Security Must Help Break A Core, Chronic Conflict In IT *

- Every IT organization is pressured to simultaneously:
 - Respond more quickly to urgent business needs
 - Provide stable, secure and predictable IT service
- When information security is integrated into development activities, development projects can implement security requirements earlier, requiring less rework, faster time to market and lower costs
- When information security is integrated into IT operations, IT operations can better manage risks, prevent incidents from occurring, and quickly detect and correct incidents (ideally, before anyone is affected). IT operations can better protect organizational commitments



Source: The authors acknowledge Dr. Eliyahu Goldratt, creator of the Theory of Constraints and author of The Goal, has written extensively on the theory and practice of identifying and resolving core, chronic conflicts.

Common Traits of the Highest Performers

Culture of...

Change management

- Integration of IT operations/security via problem/change management
- Processes that serve both organizational needs and business objectives
- Highest rate of effective change

Causality

- Highest service levels (MTTR, MTBF)
- Highest first fix rate (unneeded rework)

Compliance and continual reduction of operational variance

- Production configurations
- Highest level of pre-production staffing
- Effective pre-production controls
- Effective pairing of preventive and detective controls

Source: IT Process Institute



Seven Habits of Highly Effective IT Organizations

They...

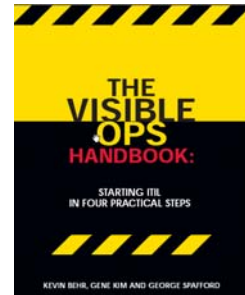
1. Have a culture that embraces change management.
2. Monitor, audit, and document all changes to the infrastructure.
3. Have zero tolerance for unauthorized changes.
4. Have specific, defined consequences for unauthorized changes.
5. Test all changes in a preproduction environment before implementing into production.
6. Ensure preproduction environment matches production environment.
7. Track and analyze change successes and failures to make future change decisions.

- **All high performers have created Cultures of...**
 - **Change Management**
 - **Causality**
 - **Planned Work**



Visible Ops: Playbook of High Performers

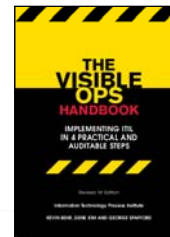
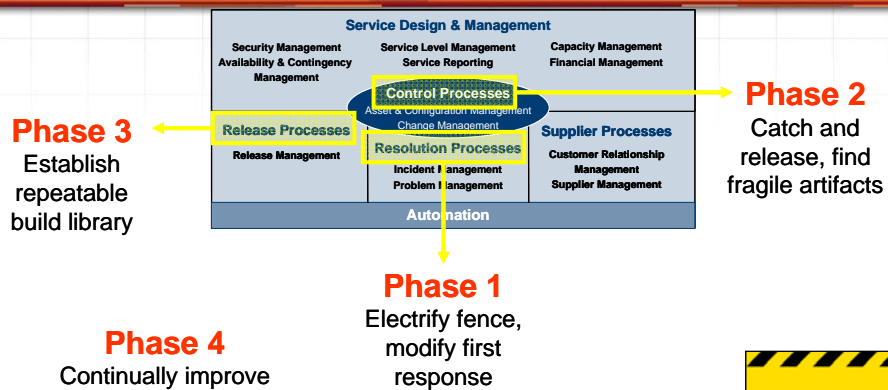
- The IT Process Institute has been studying high-performing organizations since 1999
 - What is common to all the high performers?
 - What is different between them and average and low performers?
 - How did they become great?
- Answers have been codified in the Visible Ops Methodology
- The “Visible Ops Handbook” is now available from the ITPI



www.ITPI.org



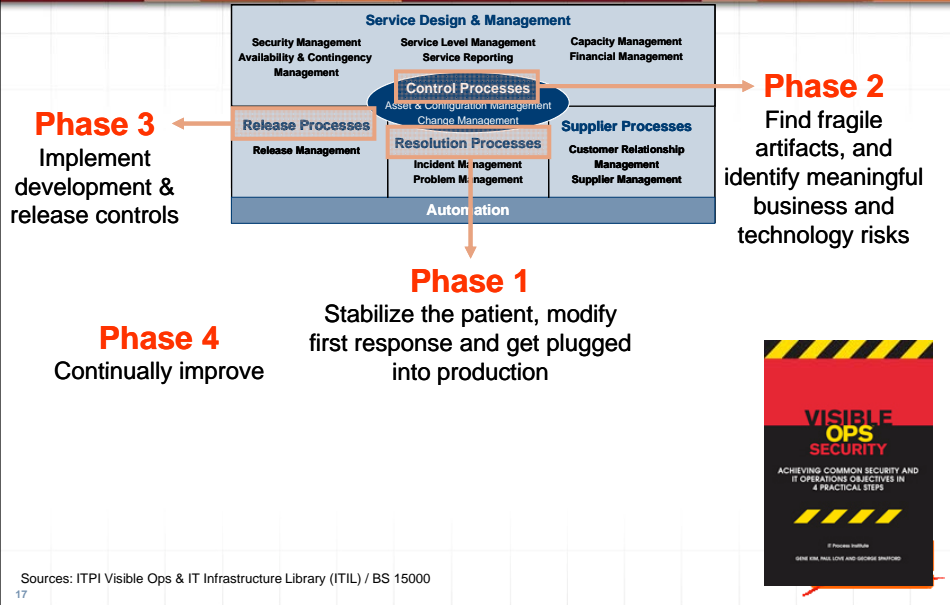
Visible Ops Security: Linking Security and IT Operations Objectives In 4 Practical Steps *



Sources: ITPI Visible Ops & IT Infrastructure Library (ITIL) / BS 15000

16

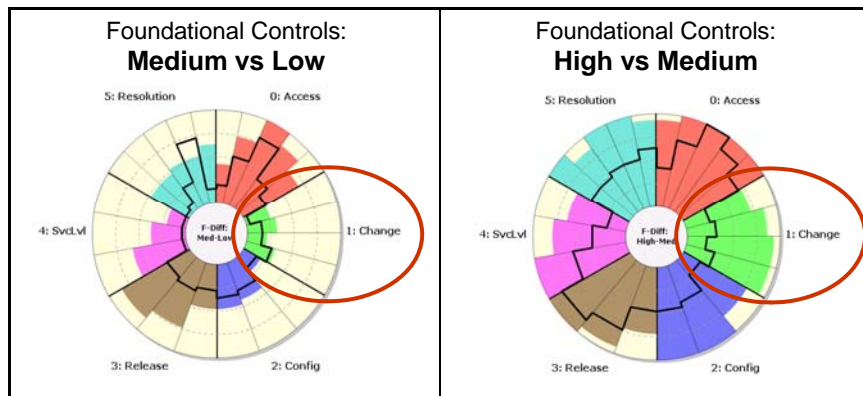
Visible Ops Security: Linking Security and IT Operations Objectives In 4 Practical Steps



Surprise #2: What The High Performers Do Differently

Top Two Differentiators between Good and Great

1. Systems are monitored for unauthorized changes
2. Consequences are defined for intentional unauthorized changes



Source: IT Process Institute, May 2006

Does Research Validate The Theory?

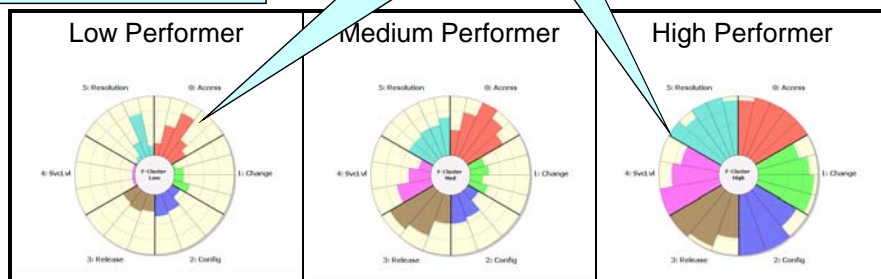
1 The ITPI identified 23 "foundational controls" and used cluster analysis techniques to identify the relationship between the use of Foundational Controls and performance indicators of the companies studied

Three clusters emerged.

3 Almost all of the members of the high performing cluster had all of the foundational controls.

4 Almost all of the members of the low performing cluster had no controls, except for access and resolution.

2 Each wedge in the pie represents one of the foundational controls. Each bar represents the percentage of the cluster members that responded 'yes' to that control.



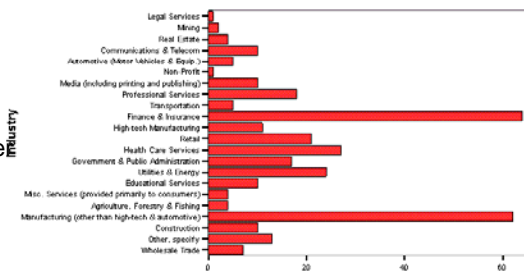
Source: IT Process Institute, May 2006

tripwire

2007: Larger Repeat Benchmark With Even More Fascinating Results

- In 2007, the ITPI and the Institute of Internal Auditors repeated the benchmark to answer the following questions:
 - Are the results still valid for a larger sample?
 - Can the set of foundational controls be reduced even further?
- 350 organizations were benchmarked
- There were two even bigger surprises in the study

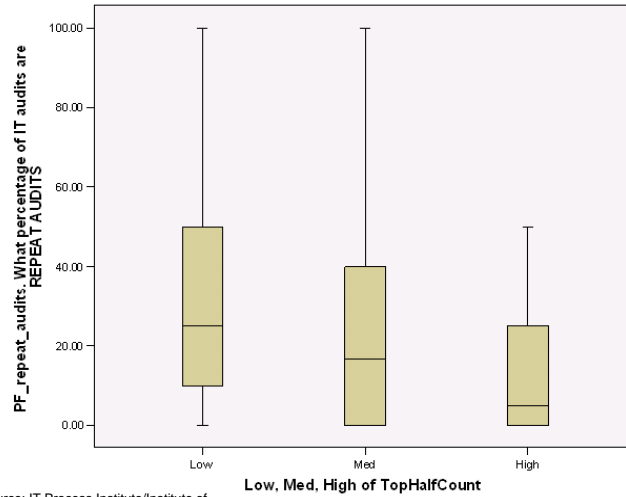
N = 350	IT Employees	IT Budget
Average	587	\$236 million
Min	2	\$1 million
Max	3,500	\$15 billion



Source: IT Process Institute/Institute of Internal Auditors (May 2007) Number of Organizations

High Performers Have Fewer Repeat Audit Findings

High performers not only have **fewer repeat audit findings**, and spend **less time on audit and compliance activities**

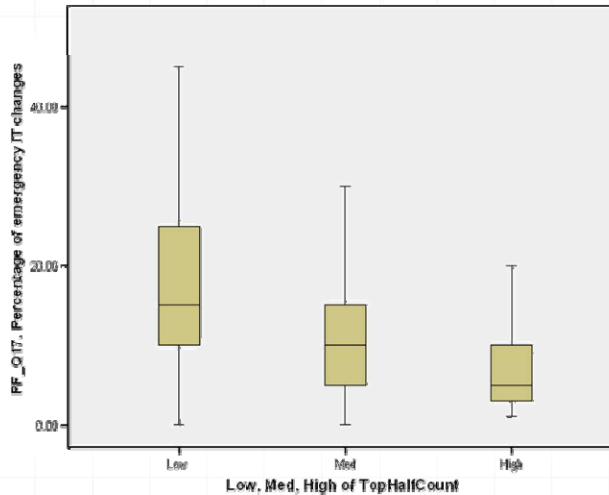


Source: IT Process Institute/Institute of Internal Auditors (May 2007)



High Performers Make Fewer Emergency IT Changes

High performers not only **avoid testing changes in production**, they insist that **even emergency changes are reviewed and approved**

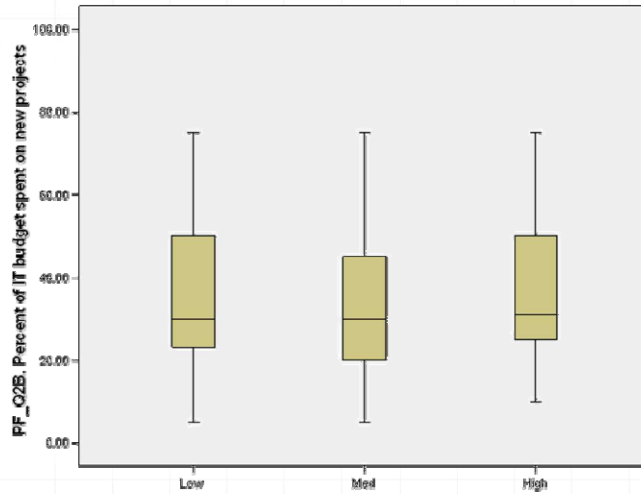


Source: IT Process Institute/Institute of Internal Auditors (May 2007)



High Performers Complete More Projects

High performers get **budget for more new projects**, and **they complete 6-8 times more of them**



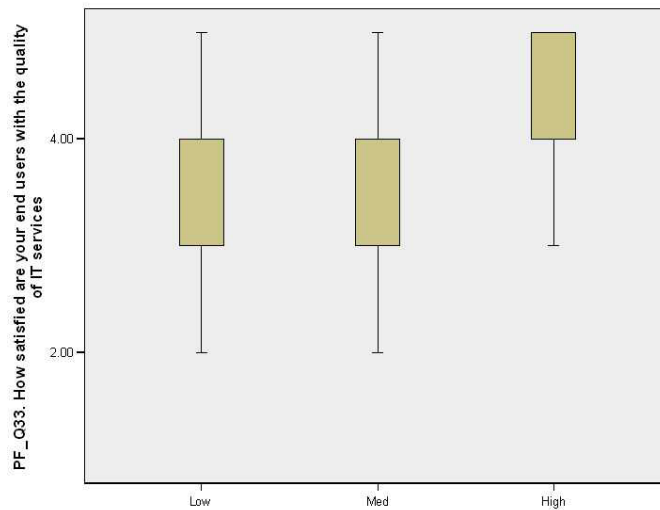
Source: IT Process Institute/Institute of Internal Auditors (May 2007)

Low, Med, High of TopHalfCount



High Performers Have Happier Users

High performers **keep the business happier**



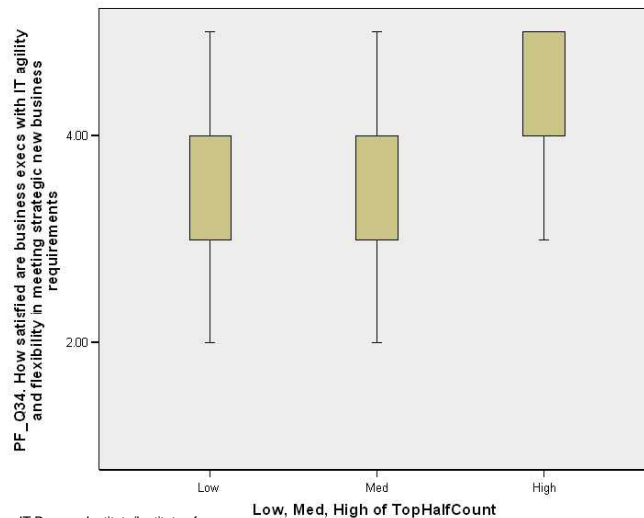
Source: IT Process Institute/Institute of Internal Auditors (May 2007)

Low, Med, High of TopHalfCount



High Performers Are More Responsive

High performers **satisfy executives** with superior agility and results



Source: IT Process Institute/Institute of Internal Auditors (May 2007)



High Performers Speak with One Voice: Maturity in Change Discipline Is Key



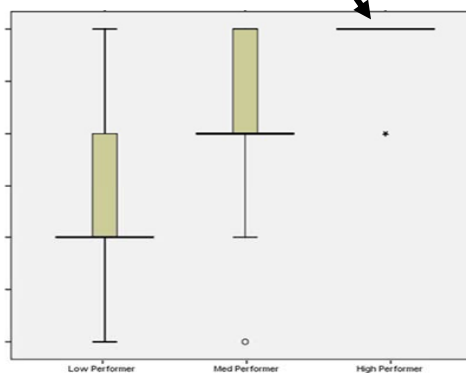
- High performers **clearly stand apart** in their commitment to **change discipline**
- While low- and medium-level performer responses overlap slightly, high performers are virtually **unanimous** in signaling the **criticality** of a **highly mature approach to change control**:

A process is defined and followed, and there are consequences for unauthorized changes

A process is defined and followed, but no consequences for unauthorized changes

A defined process, but not followed and no consequences for unauthorized changes

No defined process for change control



Slide 28

© 2008 Enterprise Management Associates, Inc.

High Performers Speak with One Voice: Monitoring and Enforcement of IT Change Control

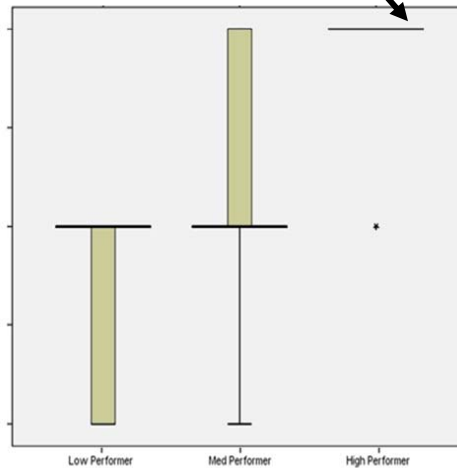


- This **same** degree of unanimity is shown in high performer commitment to monitoring and enforcing change control:

Changes are monitored and change monitoring is used to enforce change control

Changes are monitored, but monitoring information is **not** used to enforce change control

No monitoring for changes



- “You can’t manage what you don’t know”...so if change discipline is critical, so is change monitoring and control enforcement

Slide 29

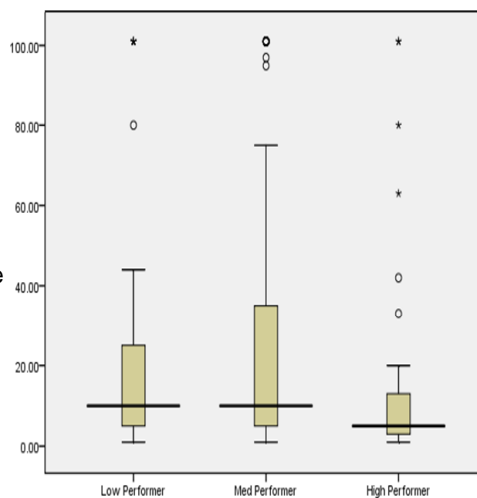
© 2008 Enterprise Management Associates, Inc.

Performance in IT Risk Management: Percentage of Disruptive IT Security Events



- While low and medium performers show similar responses, **high performers stand apart**

- High performers had about **half** the rate of disruptive IT security events experienced by low and medium performers



- High performers also had significantly less variability in the range of percentages reported

- This translates a **highly important**

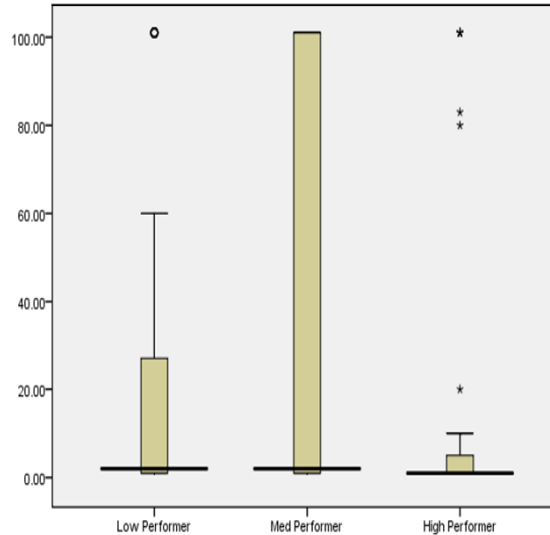
Slide 30

© 2008 Enterprise Management Associates, Inc.

Percentage of Information Leakage or Exposure Incidents in IT



- Here again, high performers stand apart
- **Much** less variability and significantly lower range of responses among high performers compared to low and medium performers



Slide 31

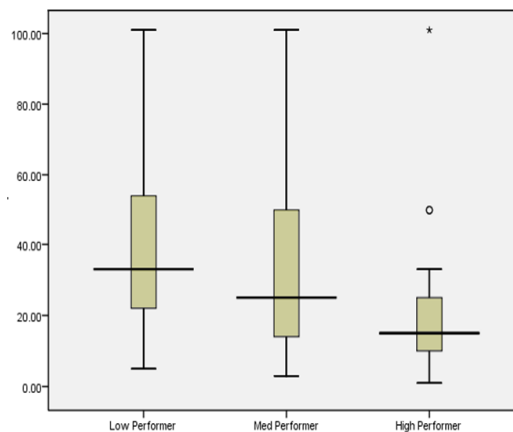
© 2008 Enterprise Management Associates, Inc.

Comprehensive IT Risk Control: Percentage of Unplanned IT Work



- IT risk management is **more than security or compliance!**
- Example: Managing risks to the **business values** of IT

- Need we say it again? Once more, high performers stand apart
- Again, some overlap in responses of low and medium performers, but a



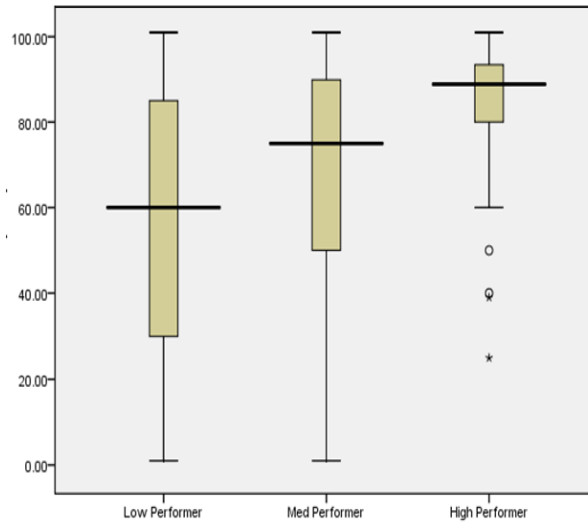
Slide 32

© 2008 Enterprise Management Associates, Inc.

Percentage of IT Projects Delivered On Time and Within Budget with Expected Features



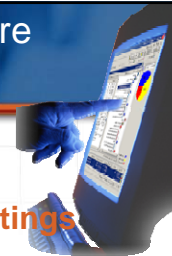
- In addition to less variability in responses, high performers experience significant gains
- High performers have a 50% increase in median percentage (from 60% to 90%) compared to low performers.



Slide 33

© 2008 Enterprise Management Associates, Inc.

Higher Performing IT Organizations Are More Stable, Nimble, Compliant And Secure

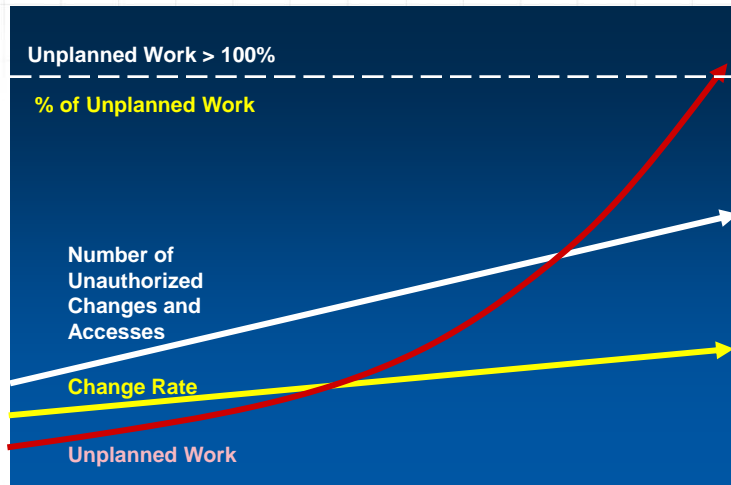


- High performers **have higher user satisfaction ratings**
- High performers **are rated much higher by business executives for agility and results**
- High performers **complete 6-8 times more projects**
- High performers have **fewer repeat audit findings and lower audit costs**
- High performers make **fewer emergency IT changes**
- High performers **find and fix security breaches faster**

Source: IT Process Institute/Institute of Internal Auditors (May 2007)



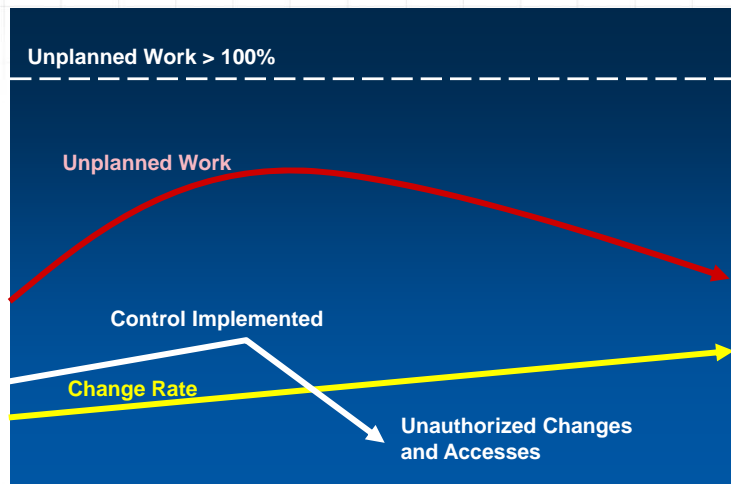
Weak IT Controls Drive Up IT Costs



Source: The Visible Ops Handbook, © IT Process Institute



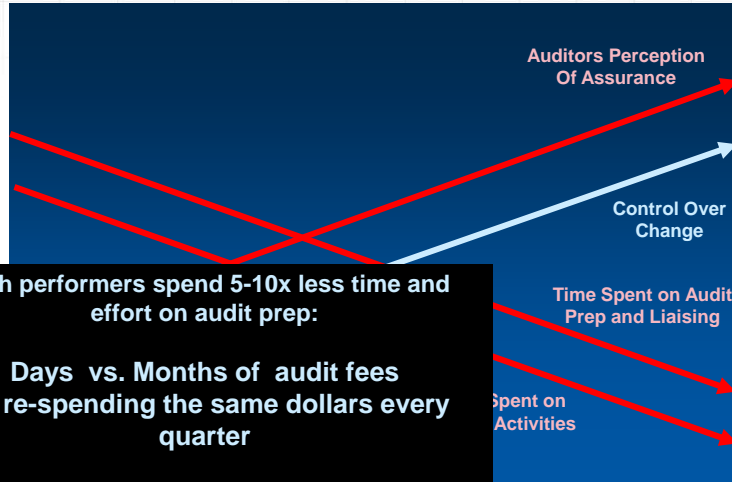
Strong IT Controls Reduce Unplanned Work



Source: The Visible Ops Handbook, © IT Process Institute



Visible Ops Phase 1 Increasing Auditability



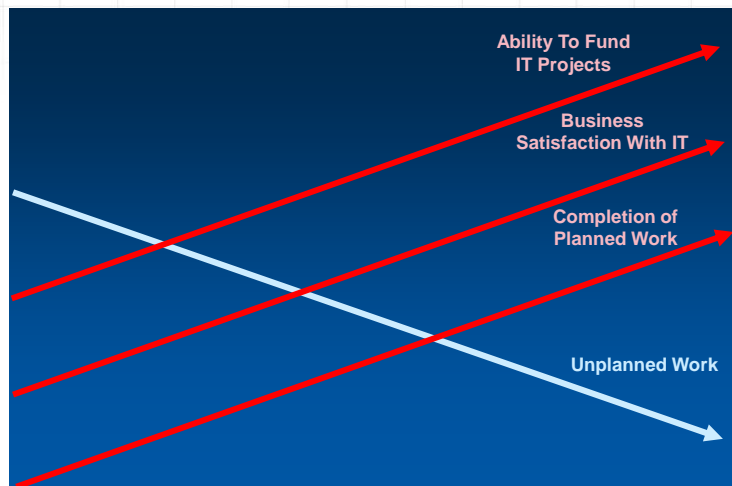
High performers spend 5-10x less time and effort on audit prep:

Days vs. Months of audit fees
No re-spending the same dollars every quarter

With Tripwire and change authorization system, auditors can sample change control effectiveness with little effort from IT!



Visible Ops Phase 1 Operational Excellence and Strategic Excellence

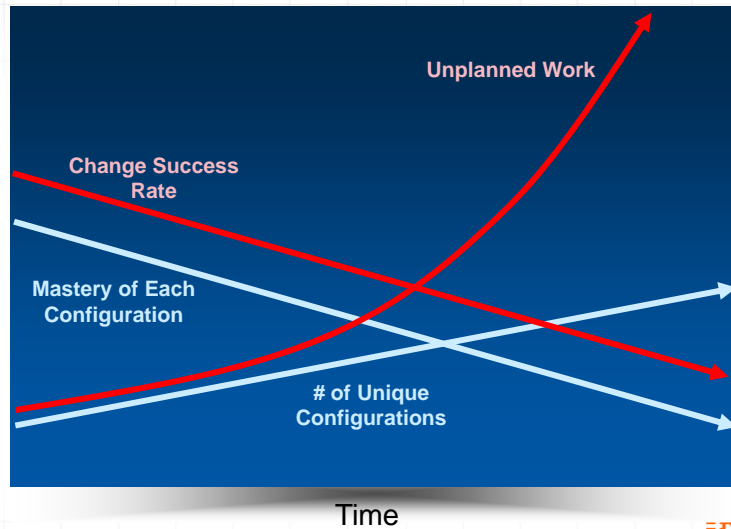


Time

Source: The Visible Ops Handbook, © IT Process Institute



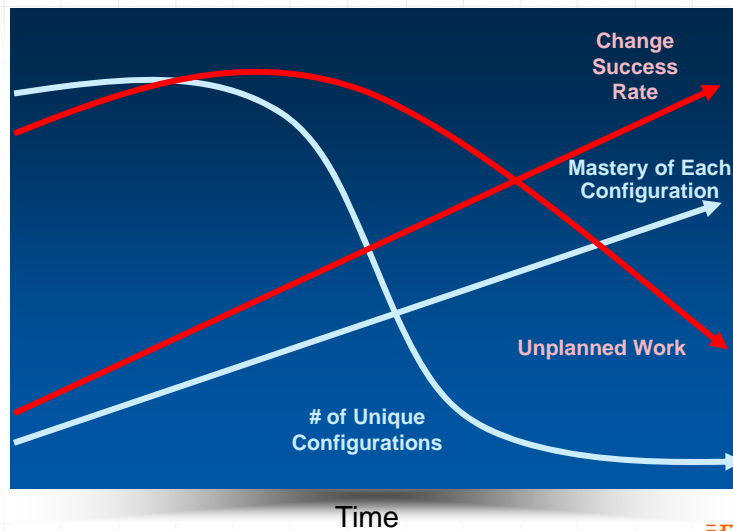
Visible Ops Phase 2 Drifting Configurations



Source: The Visible Ops Handbook, © IT Process Institute



Visible Ops Phase 2 Find Fragile Artifacts



Source: The Visible Ops Handbook, © IT Process Institute



Top 5 Mistakes IT Executives Make

Not locking down change

"We can't – we won't be able to get anything done."

Not electrifying the fence

"We don't need to – we trust our own people."



The continual desire for a technical solution

Technology is easier to justify and implement than people and process improvements

Reward personal heroics instead of repeatable discipline

"If one person can save the entire boat, one person can probably sink it, too."

The biggest failure is accountability while the biggest obstacle is a commitment to the process

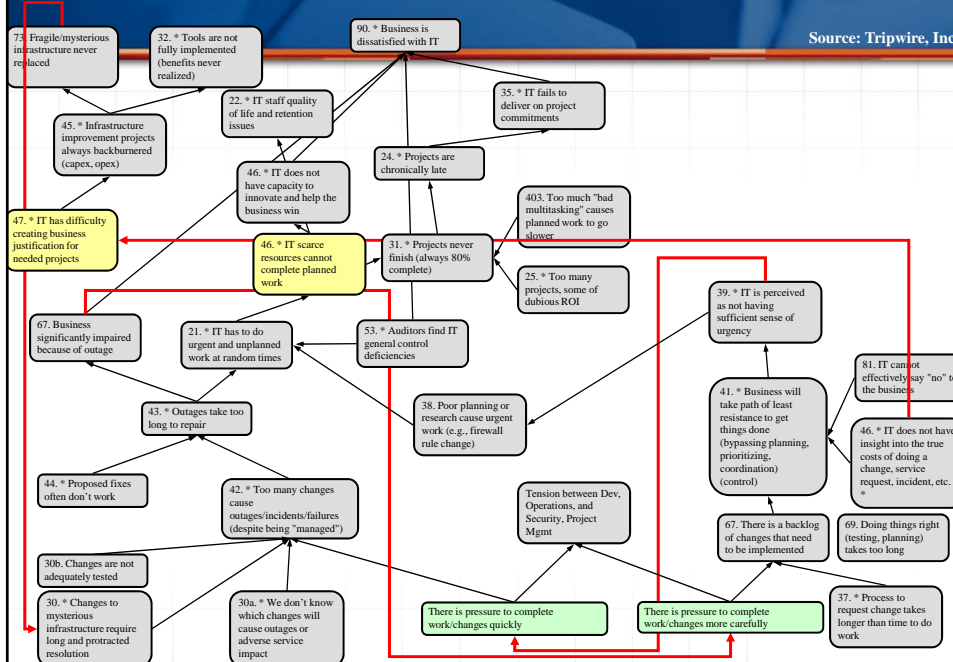
The only acceptable number of unauthorized change is "zero"



Source: The Visible Ops Handbook, © IT Process Institute

Current Reality: Does This Feel Familiar?

Source: Tripwire, Inc.



What Does A CEO Want From A CIO?



Gerry Ablaza

CEO, Globe Telecom

2004 Asian Business Leader of the Year

2004 Asian Telecom CEO of the Year

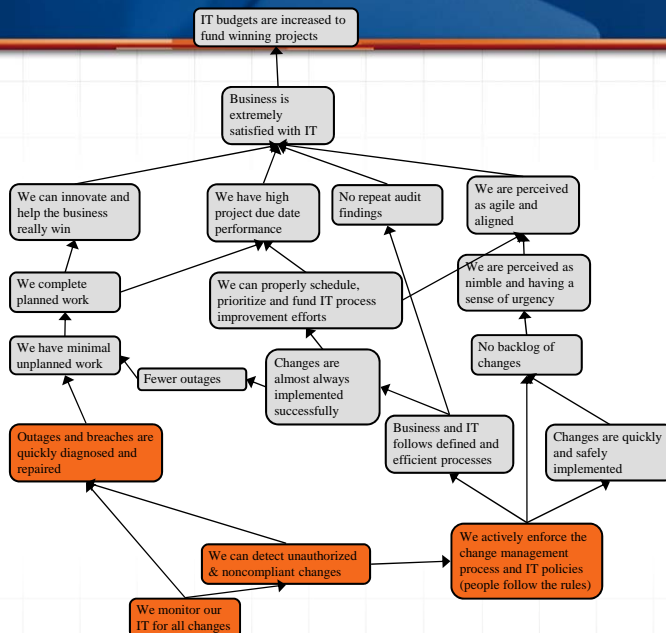
“ At night I want him to make sure that I can sleep peacefully. ”

“ When I wake up in the morning, I want him to excite me with new possibilities for our business. ”



Create A Better Reality In 30+90 Days!

Source: Tripwire, Inc.



Use Tripwire Configuration Audit and Control and satisfy your CIO (and CEO) and customers.

We can help give you everything you need to create this desired reality!



Resources

- ITPI Visible Ops Handbook
 - Kevin Behr, CTO, IP Services, Inc.
 - Gene Kim, CTO, Tripwire, Inc.
 - George Spafford, Spafford Global Consulting
- ITPI IT Controls Performance Study
 - Gene Kim, CTO Tripwire, Inc.
 - Kurt Milne, ITPI
 - Dr. Dan Phelps, Florida State University
 - Dr. Grant Castner, University of Oregon
- Get your copy of VisOps
Email: tripwire.com/visibleops
- More Info:
Email: highperformer@tripwire.com

