



The Leader in
Configuration Audit & Control

Foundational Controls: Ways To Focus ITIL Process And COBIT Controls

An Eight Year Study Of High Performing IT Organizations

Gene Kim, CISA
CTO, Tripwire, Inc.
Denver ISACA/ISSA
5/15/2008
genek@tripwire.com



**The Leader in
Configuration Audit & Control**

Morning Session

The background of the slide features a close-up, high-speed photograph of a water drop hitting a surface, creating a series of concentric ripples. The drop is in the center-right of the frame, with a small crown-like shape at its base. The water is clear and bright. In the lower portion of the image, a computer keyboard is visible, with a white "Ctrl" key in focus. The overall color palette is light blue and white, with a dark blue vertical bar on the left side and a horizontal orange bar across the middle.

Ctrl

Acknowledgements

- This presentation is based on the IT Controls Performance Study performed by the IT Process Institute
 - Gene Kim, CTO, Tripwire, Inc.
 - Kurt Milne, Managing Director, IT Process Institute
 - Dr. Dan Phelps, College of Information, Florida State University
 - Dr. Grant Castner, Lundquist College of Business, University of Oregon
- We thank the IT Process Institute team for all their efforts throughout this 2.5 year project
 - Kevin Behr, Scott Aldridge, Ron Neumann, Mary Matthews, George Spafford.
- ...as well as the IT Controls Performance Study Advisory Board:
 - Julia Allen, Jennifer Bayuk, Anita Montgomery, Andy Moore, Fred Palmer, Bill Philhower, Mike Prospect, Dr. Jeff Stanton, Brent Tanner, Jay Taylor,



Introductory 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?

Problem Statement

- IT management has a difficult job
 - IT effectiveness and efficiency, compliance and security
 - Deliver measurable ROI for all IT projects
- ITIL and COBIT frameworks exist, but does not give guidance on where to start
 - Most guidance based on anecdote and belief
 - Best practice is often not tested
- When IT management cannot bring quantitative science to bear on these problems, what often results is:
 - Failed initiatives and projects,
 - Increased suspicion from the business,
 - Short tenures for IT executives.

“IT people are valuable, and therefore worthy of study.”
Dr. Tom Longstaff, ITPI Advisory Board

Agenda

- Problem statement
- Background of research since 1999
- Findings from the April 2006 IT Controls Performance Study (ITPI)
 - ✓ Top surprises
 - ✓ Methodology
 - ✓ Performance benefits
- Experiences from the “90 day guaranteed IT performance improvement” program

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)

The screenshot displays two news articles. The top article, titled "Breach at TJX shows IT security still lacking in retail industry", reports that forty banks in Massachusetts have compromised credit cards. Below it is an article from the Kennebec Journal titled "Hackers swipe seed company's customers' data", which includes a sub-headline "Monster's Security Breach Larger than Thought" and a date of August 29, 2007. The bottom article, dated March 2, 2007, is titled "Westerly Hospital data breach affects 2,000" and states that social security numbers and other private data for 2,000 patients were posted online. The screenshot also shows various interface elements like comments, recommendations, and sharing options.

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

Not Using A Top-Down, Risk-Based Approach

- Information security will often significantly impede the achievement of business goals when they:
 - Use a technology-centric and bottom-up approach. Jay Taylor states, “There is no such thing as IT risk.” Instead, failure of technology to operate as designed may create business risk.
 - Best evidence of this is during the first several years of SOX-404. During testing, IT findings represented the largest category of findings, totaling more than the combined findings in revenue, procure-to-pay and tax categories.

Most of the IT findings could not have caused an undetected material error. So, why were they tested in the first place?

- Why this often occurs: Often, a vulnerability scan is performed on the entire IP network range, and the organization panics to correct the 2000 pages of vulnerabilities, sorted by how easy they are to exploit

Source: Jay Taylor, General Director, IT Audit, General Motors: “GAIT For Business and IT Risk”, Institute of Internal Auditors, 2008.

Source: KPMG study: “Sarbanes-Oxley 404: Lessons Learned”, ISACA Luncheon Sessions, April 20, 2005.



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

Seven Habits of Highly Effective IT Organizations

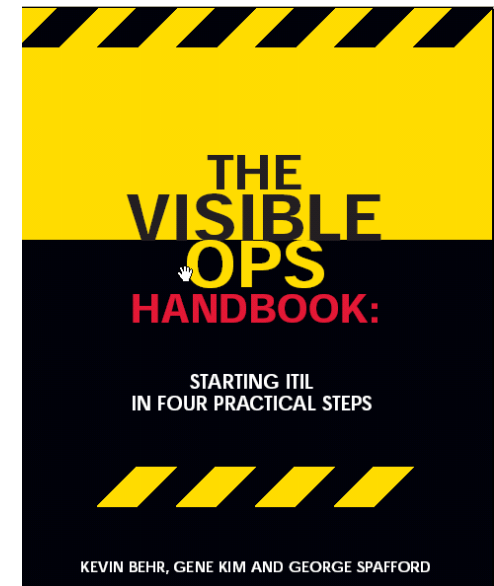
They...

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

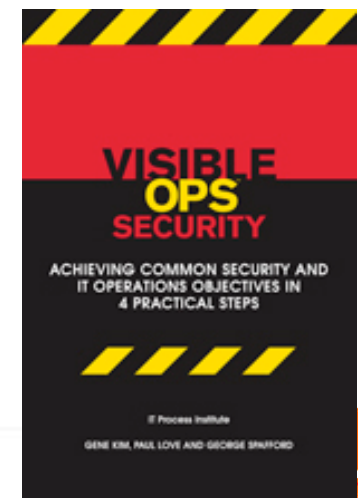
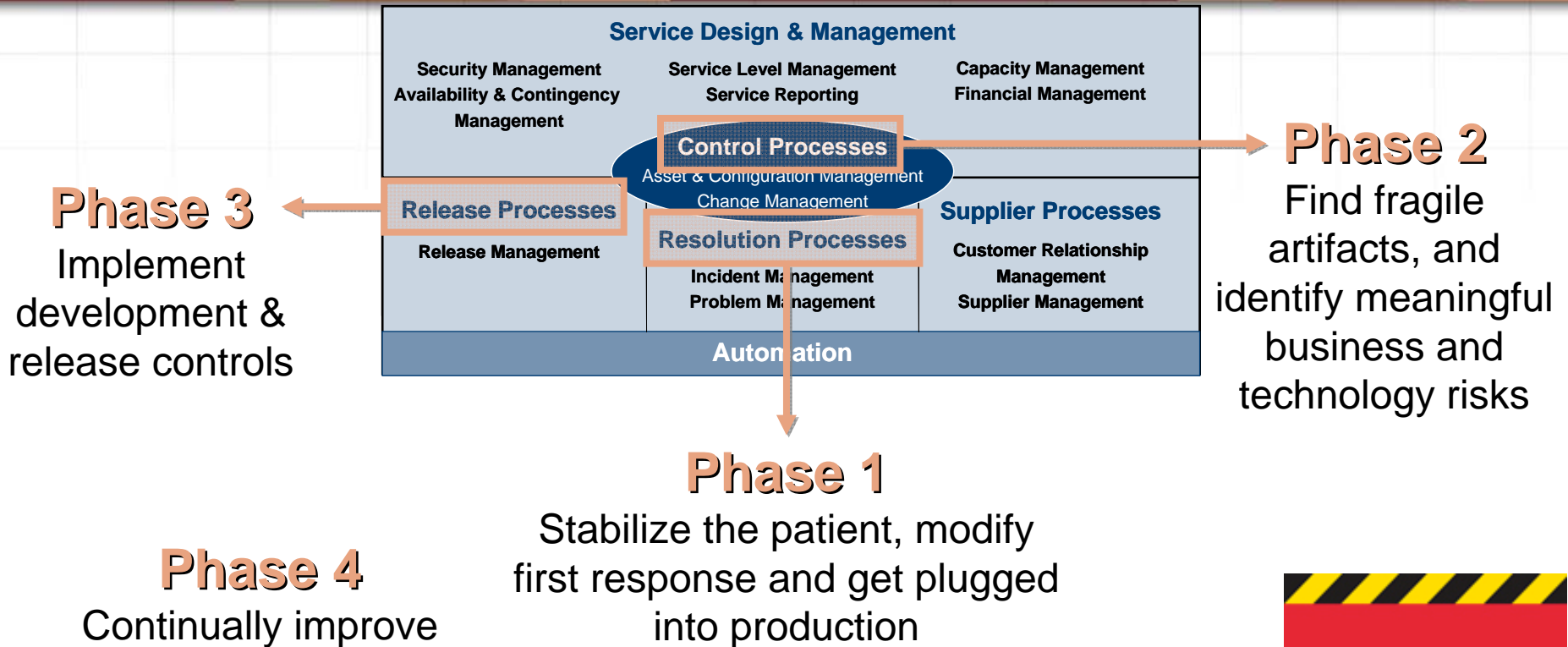
- The IT Process Institute has been studying high-performing organizations since 1999
 - What is common to all the high performers?
 - What is different between them and average and low performers?
 - How did they become great?
- Answers have been codified in the Visible Ops Methodology
- The “Visible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



www.ITPI.org



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



Surprise #1: How Good The High Performers Are

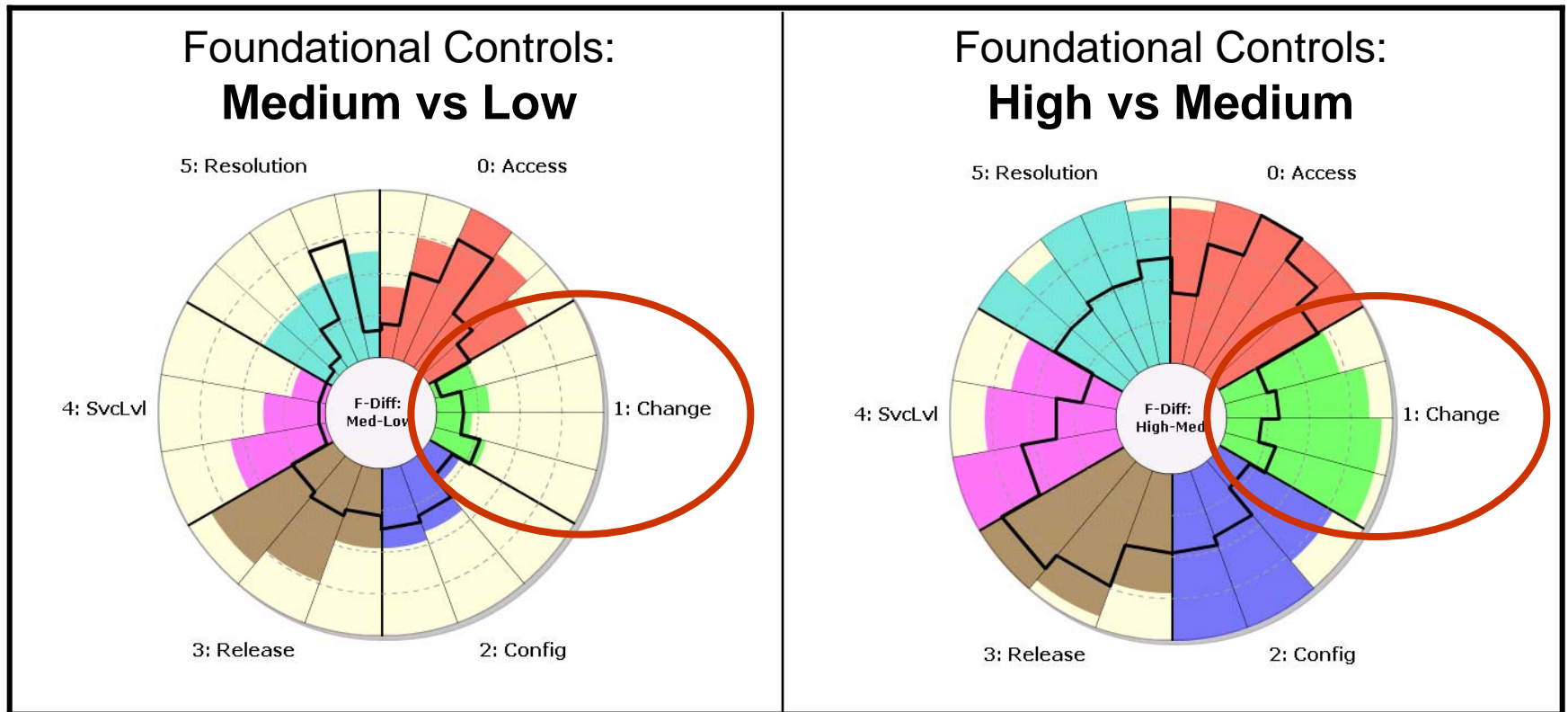
- High performers contribute more to the business
 - **8 times more** projects and IT services
 - **6 times more** applications
- When high performers implement changes...
 - **14 times more** changes
 - **One-half** the change failure rate
- When high performers manage IT resources...
 - **One-third** 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

Surprise #2: What The High Performers Do Differently

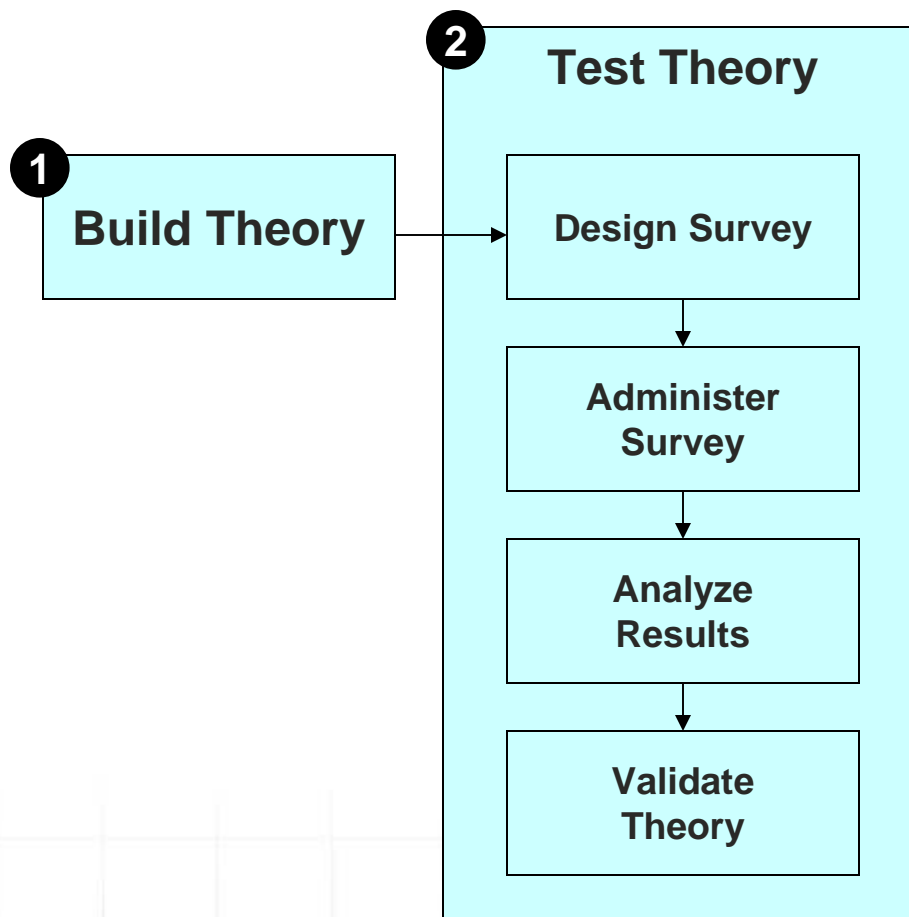
Top Two Differentiators between Good and Great

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



The IT Controls Performance Study

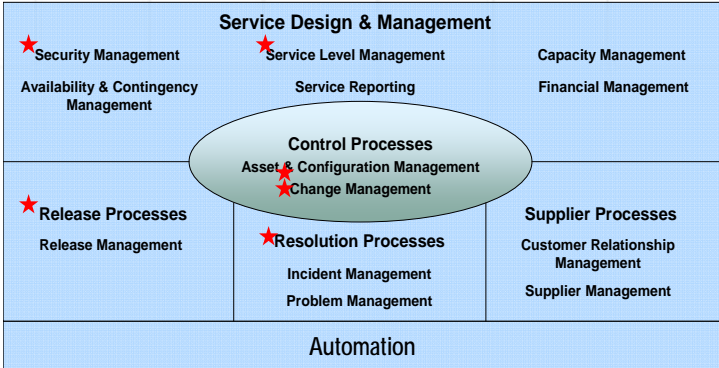
- Science is built on a combination of “theory building” and “theory testing”



Research Team:
Gene Kim, CTO, Tripwire
Kurt Milne, Managing Director, ITPI
Dr. Dan Phelps, Florida State University
Dr. Grant Castner, University of Oregon

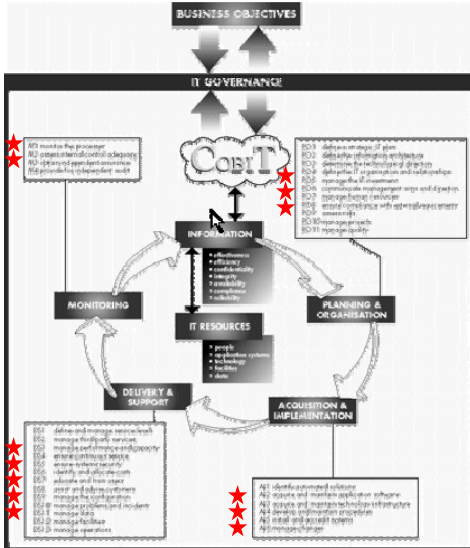
Design Survey: Pick IT Controls

1 We selected the 6 leading BS15000 areas within ITIL that are conjectured to be “where to start.”
 These were **Access, Change, Resolution, Configuration, Release, Service Levels**



Source: IT Infrastructure Library (ITIL) / BS 15000

2 We then selected 63 COBIT control objectives within these areas.



Source: COBIT, IT Governance Institute/ISACA



The 63 IT Controls

Access

Do you have a formal process for requesting, establishing, and issuing user accounts?

Do you have an automated means of mapping user accounts to an authorized user?

For each employee/resource, do you record a list of system access rights?

Do you audit user accounts to ensure that they map to an authorized employee?

Do you have procedures to keep authentication and access mechanisms effective?

Do you have a formal process for suspending and closing user accounts?

Do you have processes for granting and revoking emergency access to relevant staff?

Do IT personnel have well-defined roles and responsibilities?

Do you have an automated process for defining and enforcing user account roles?

Do user accounts ever allow actions that exceed their specified role?

Do you monitor accounts to detect when they exceed their specified role?

Do you rigorously enforce separation of duties between

Change

Do you have a formal IT change management process?

Do you use tools to automate the request, approval, tracking, and review of changes?

Do you track your change success rate?

Do you track the number of authorized changes implemented in a given period?

Do you track how many changes are denied the first time they are considered by the change authority?

Do you monitor systems for unauthorized changes?

Are their defined consequences for intentional unauthorized changes?

Do you have a change advisory board or committee?

Do you have a change emergency committee?

Do you use change success rate information to avert potentially risky changes?

Do you distribute a forward schedule of changes to relevant personnel?

Do you conduct regular audits of successful, unsuccessful, and unauthorized changes?

Are changes thoroughly tested

Configuration

Do you have a formal process for IT configuration management?

Do you have an automated process for configuration management?

Do you have a configuration management database (CMDB)?

Does the CMDB describe relationships and dependencies between the configuration items (infrastructure components)?

Does your configuration management database specify to which business service each configuration item supports?

Are you able to provide relevant personnel with correct and accurate information on the present IT infrastructure configurations, including their physical and functional specifications?

Do you monitor and record the time it takes to correct configuration variance?

Release

Do you have a standardized process for building software releases?

Do you use tools to automate the build of new releases of software applications?

Do you use automated software-distribution tools?

Do you test all releases before rollout to a live environment?

For release testing purposes, do you maintain an identical testing environment to your production environment?

Do you have a definitive software library (DSL)?

Service Level

Do you have someone (a service level manager) who is responsible for monitoring and reporting on the achievement of the specified service performance criteria?

Do you have a service catalog?

Do you regularly review your service catalog?

Do you regularly review service level agreements? Do you have a service improvement programme?

Do you ever renegotiate the defined consequences in the service level agreement?

Do you have a formal process to define service levels?

Does your service level agreement cover ALL of the following aspects: availability, reliability, performance, growth capacity, levels of user support, continuity planning, security, and minimum level of system functionality?

Resolution

Do you have a defined process for managing incidents?

Do you have an automated process for managing incidents?

Do you track the percentage of incidents that are fixed on the first attempt (first fix rate)?

Do you use a knowledge database of known errors and problems to resolve incidents?

During an incident, do you ever rebuild rather than repair?

Do you have a defined process for managing problems?

Do you have an automated process for managing problems?

Do you follow a structured method for analyzing and diagnosing problems?

Do you have a defined process for managing known errors?

Do you proactively identify problems and known errors before incidents occur?

Is there integration between your problem management and change management processes?

Is there integration between your problem management and configuration management

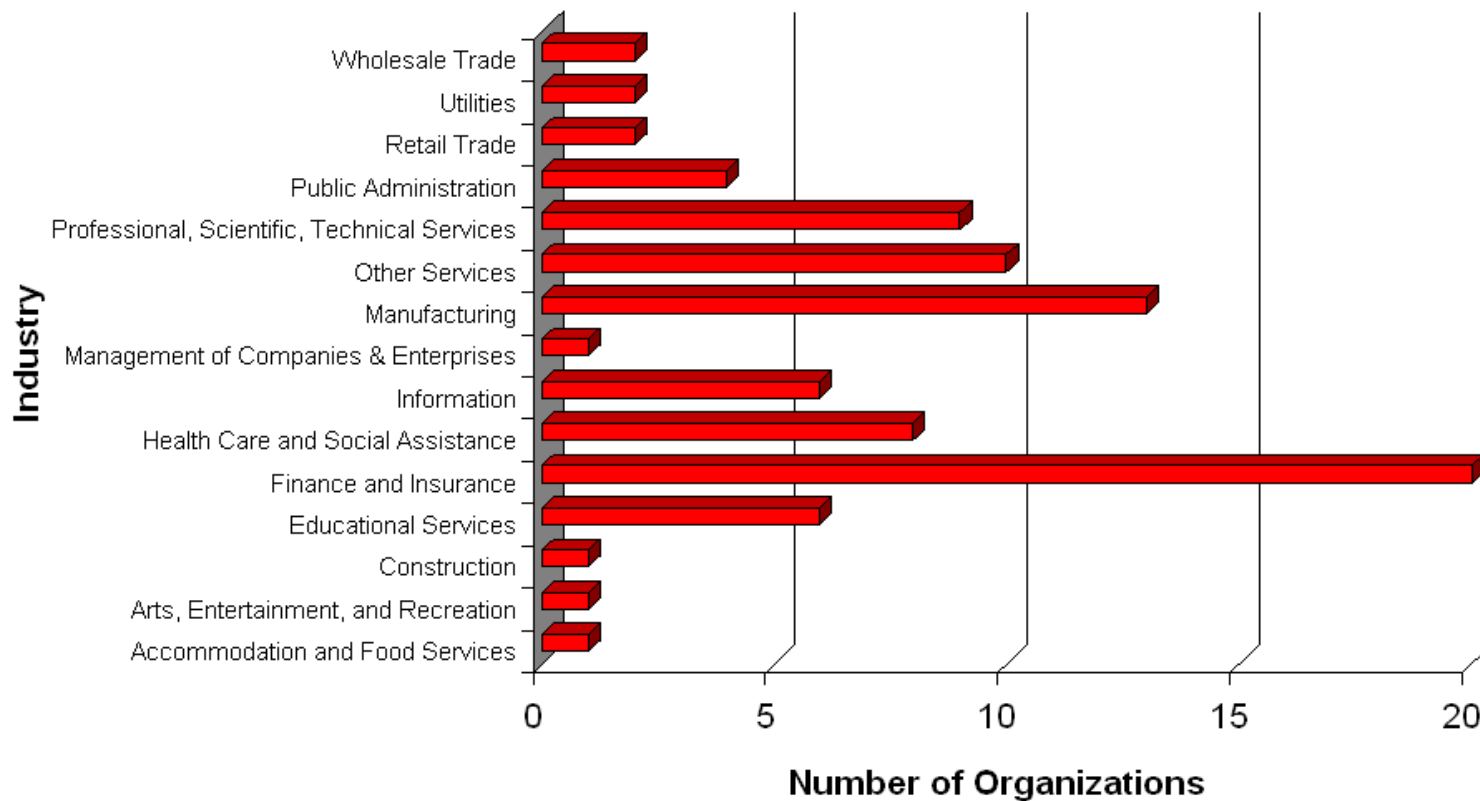
The resulting controls that we selected were in the following control categories:

- **Access Controls: 17 controls**
- **Change Controls: 13 controls**
- **Configuration Controls: 7 controls**
- **Release Controls: 6 controls**
- **Service Level Controls: 8 controls**
- **Resolution Controls: 12 controls**



ITPI Survey: Demographics

	IT Employees	IT Budget
Average	483	\$114 million
Min	3	\$5 million
Max	7,000	\$1,050 million



Design Survey: Pick 25 Performance Measures

- What are the primary goals of IT?
 - Build and deliver projects for the business
 - Operate and maintain existing IT assets

Operational Measures	Security Measures	Audit Measures
1 - User IT Satisfaction 2 - IT Ops Spend / Total Ops Spend 3 - Unplanned Work 4 - Change Success Rate 5 - First Fix Rate 6 - Weekly Maintenance 7- Server / Sys Admin Ratio 8 - IT Ops Spend / IT Staff 9 - App Developer Staff / IT Staff 10 - Network Sysadmin Staff / IT Staff 11 - Patching Disruption Level 12 - Outsourcing Disruption Level	13 - Security Sufficiency 14 - Security Spend / IT Ops Spend 15 - Security Operations Integration 16 - Security Staff / IT Staff 17 - % Security Breaches that results in loss 18 - % security Breaches that are corrected 19 - % Security Breaches auto detected 20 - % Security Breaches from internal source 21- Access Detection Speed 22 - Security Disruption Level	23 - IT Audit Controls / IT Staff 24 - IT SOX / IT Staff 25 - Audit Compliance Disruption Level



Design Survey: To Find Answers To Five Research Questions

<i>Research Question</i>	<i>Answer</i>
1. Do IT controls correlate with improved performance measures?	???
2. Which controls impacts the performance measures the most?	???
3. Do Foundational Controls users have higher performance?	???
4. Which Foundational Controls differentiate top performers?	???
5. What is the potential performance improvement when using Foundational Controls?	???

Question 1: Do IT Controls Correlate With Improved Performance Measures?

- Do the 6 control categories correlate with improvements in the 25 performance measures?
 - Answer: Yes, they do!
 - None of the control categories improved all the performance measures
 - Some control categories improved some of the performance measures
 - Some performance measures were improved by additions of any control category
 - But, where should you focus?



Question 2: Which Controls Impacts The Performance Measures The Most?

- Are there a subset of foundational controls that deliver 80% of the benefits?
 - Answer: Yes, there are!
 - Each of the six control categories could be reduced to 3 or 4 foundational controls that impact the measures as the full set
 - Examining the resulting foundational controls usually elicits an “a-ha” moment



The 21 Foundational Controls

Access	Change	Config
<ul style="list-style-type: none"> ▪Do you have a formal process for requesting, establishing, and issuing user accounts? ▪Do you have an automated means of mapping user accounts to an authorized user? ▪Do IT personnel have well-defined roles and responsibilities? ▪Do you regularly review logs of violation and security activity to identify and resolve incidents of unauthorized access? 	<ul style="list-style-type: none"> ▪Do you track your change success rate? ▪Do you monitor systems for unauthorized changes? ▪Are their defined consequences for intentional unauthorized changes? ▪Do you use change success rate information to avert potentially risky changes? 	<ul style="list-style-type: none"> ▪Do you have a formal process for IT configuration management? ▪Do you have an automated process for configuration management? ▪Are you able to provide relevant personnel with correct and accurate information on the present IT infrastructure configurations, including their physical and functional specifications?

Release	Service Levels	Resolution
<ul style="list-style-type: none"> ▪Do you have a standardized process for building software releases? ▪For release testing purposes, do you maintain an identical testing environment to your production environment? ▪Do you have a definitive software library (DSL)? 	<ul style="list-style-type: none"> ▪Do you regularly review your service catalog? ▪Do you have a service improvement program? ▪Do you have a formal process to define service levels? 	<ul style="list-style-type: none"> ▪Do you track the percentage of incidents that are fixed on the first attempt (first fix rate)? ▪Do you use a knowledge database of known errors and problems to resolve incidents? ▪During an incident, do you ever rebuild rather than repair? ▪Do you have a defined process for managing known errors?



Exercise 1:
Foundational Controls Exercise

138403

Question 3: Do Foundational Controls Users Have Higher Performance?

- Do organizations with higher number of foundational controls outperform those organizations with fewer foundational controls?
 - Answer: Yes, they do!
 - Create two populations: top and bottom 25th percentile of number of foundational controls
 - Measure their performance based on: # of performance measures in the top 50th percentile
 - Top significantly outscores bottom on performance measures



Step 4: Which Foundational Controls Differentiate Top Performers?

- Are there foundational controls that high performers are using that everyone else isn't?
 - Answer: Yes!
 - Use cluster analysis to find natural groupings: three clusters emerged based on their control usage...
 - High, medium and low performing can be accurately predicted based on high, medium and low controls...
 - Create sorted list of controls most present in high performers and most absent in med/low performers...



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

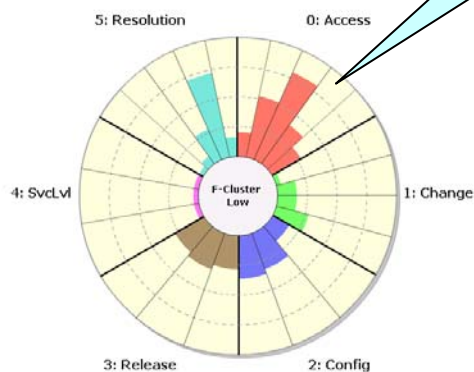
Three clusters emerged.

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

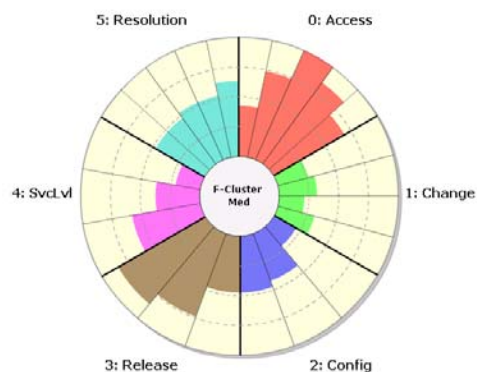
4 Almost all of the members of the low performing cluster had no controls, except for access and resolution.

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.

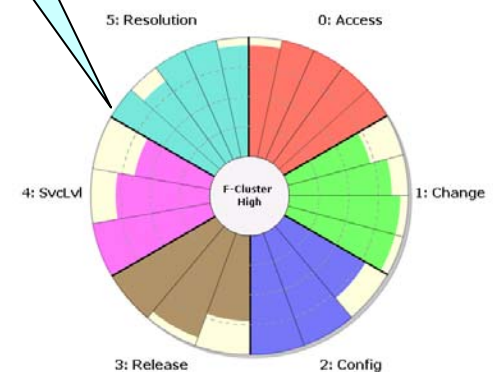
Low Performer



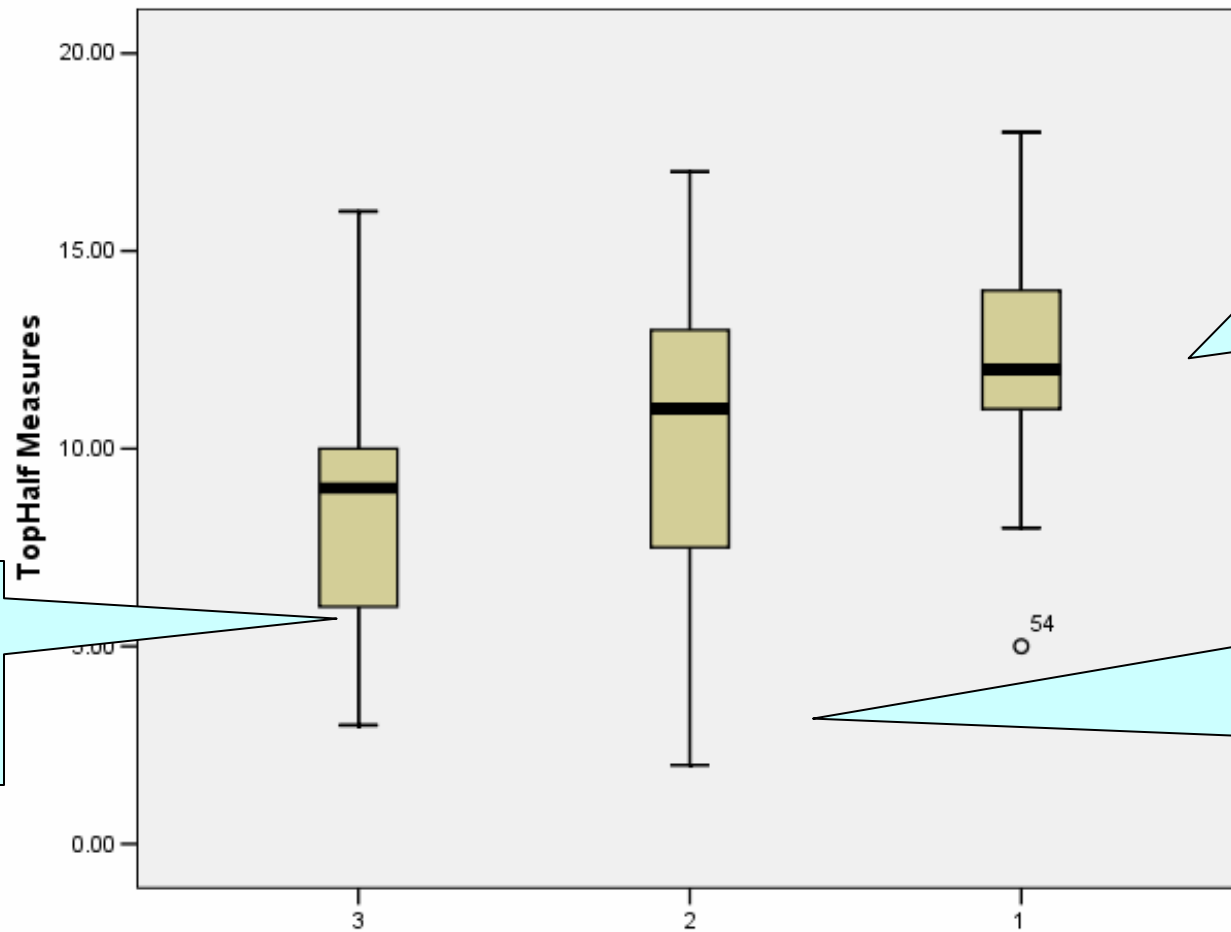
Medium Performer



High Performer



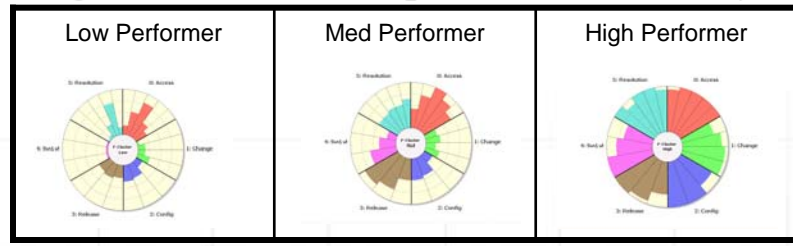
Show Your Work: High Controls = High Performer!



2 The low performers had the lowest performance and higher variance.

1 The high performing cluster had the highest performance measures, and also the lowest variance.

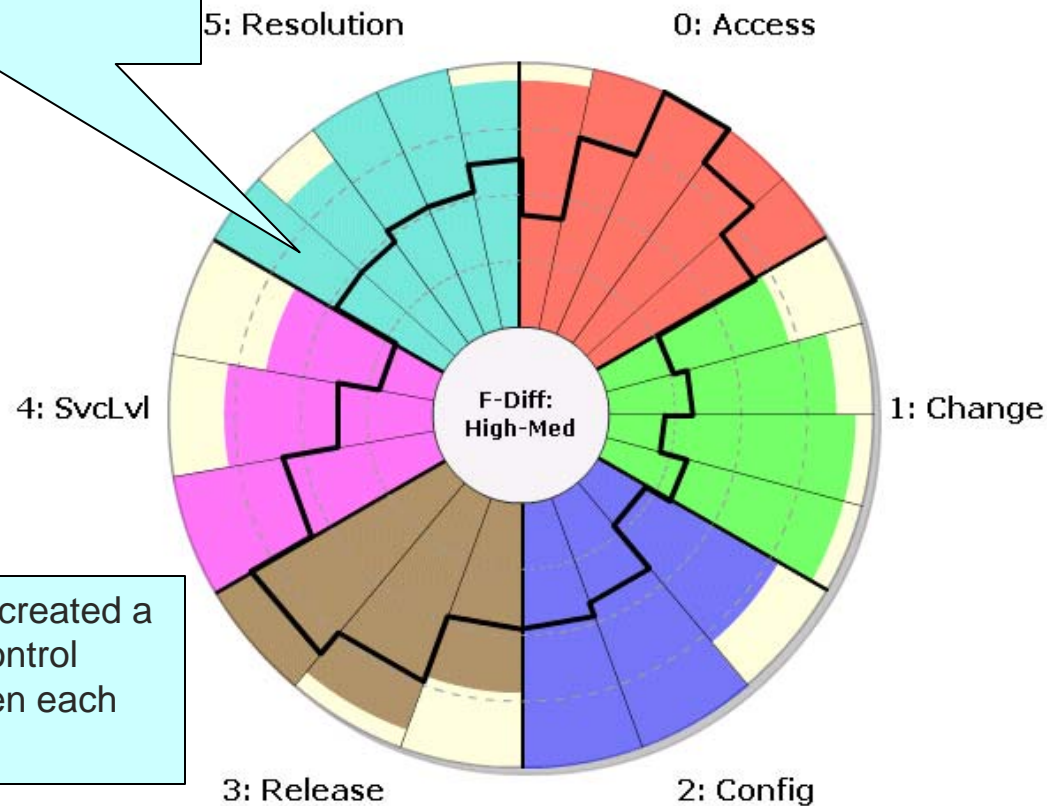
3 Medium performers had more controls but had the highest variance in performance. t



Does Research Validate The Theory?

1 What controls are present in the high performers but *not* in the low and medium performers?

Foundational Controls: High vs Medium



2 Researchers then created a sorted list of the control differences between each set...

Does Research Validate The Theory?

Foundational Control	% high with the specified control	% medium with the specified control	Difference	<p>Note that virtually every top performer monitors their systems for unauthorized changes... ...and has defined consequences for unauthorized changes! Organizations that have these controls are almost always great.</p>
C23 Do you monitor systems for unauthorized changes?			72	
C24 Are there defined consequences for intentional unauthorized changes?	93	32	61	
C31 Do you have a formal process for IT configuration management?			58	
C32 Do you have an automated process for configuration management?	79	21	58	
C20 Do you track your change success rate?	86	32	54	
C36 Are you able to provide relevant personnel with correct and accurate information on the present IT infrastructure configurations?	100	47	53	

**Visible Ops:
Electrify the Fence**

**Visible Ops:
Create Consequences for
Touching the Fence**



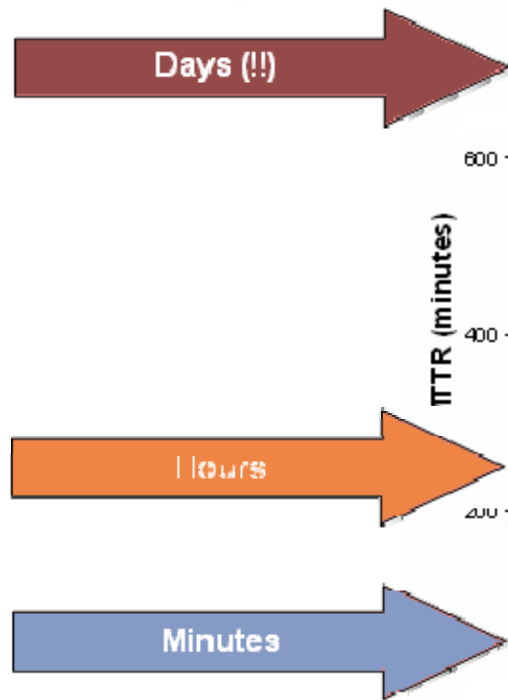
Step 5: What Is The Potential Performance Improvement When Using Foundational Controls?

- How much better are high performers than everyone else?
 - Answer: Much, much better...
 - The Lean Manufacturing researchers found a 2x difference in most performance measures between high performing and average
 - We found a significantly larger performance differential...

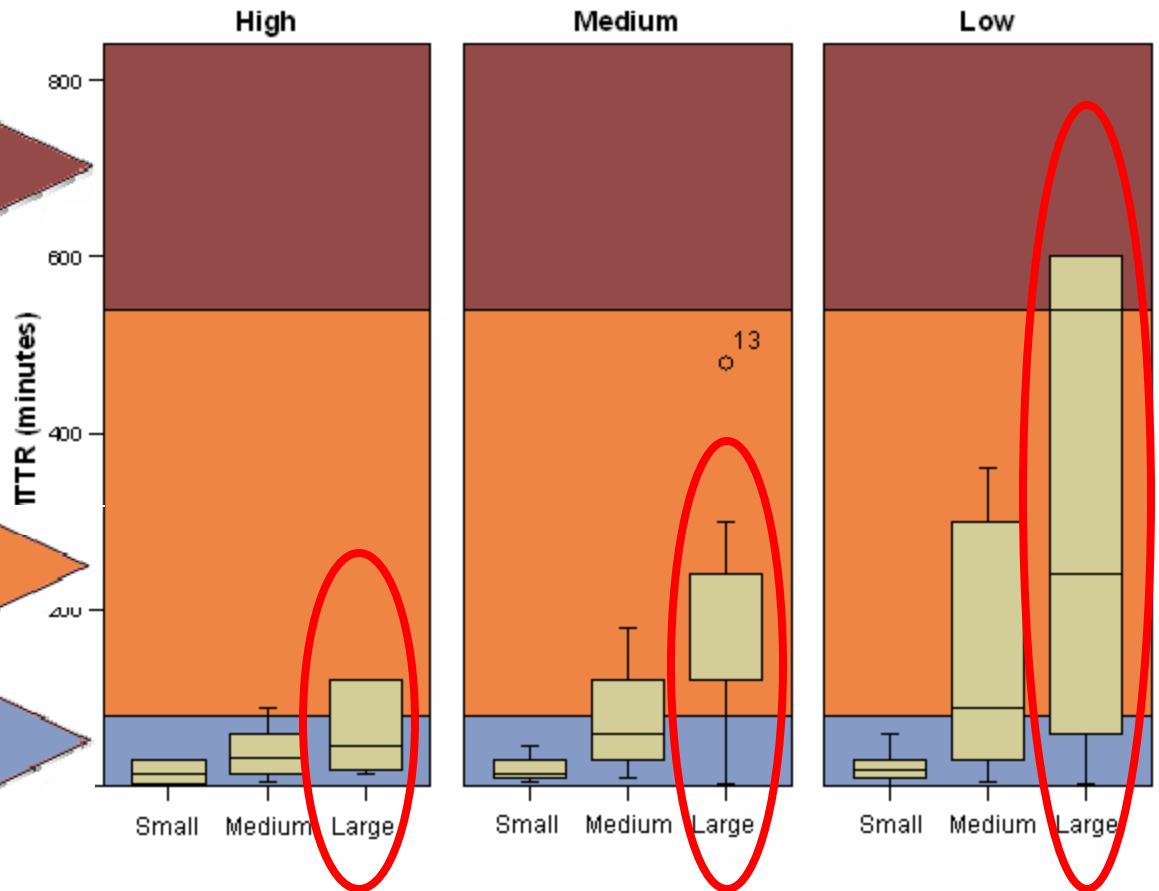


High Performers Can Bound Maximum MTTR

But look at the huge differences for large outages!



MTTR by Cluster

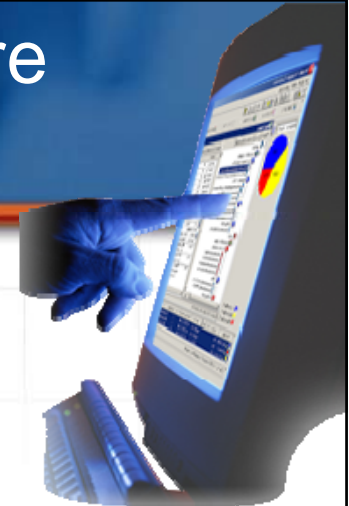


(Large outages required 25-50 people to fix!)

And Security High Performance, Too

- When top performers have a security breach...
 - 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 **3x more budget** to security, as a function as IT operational expense

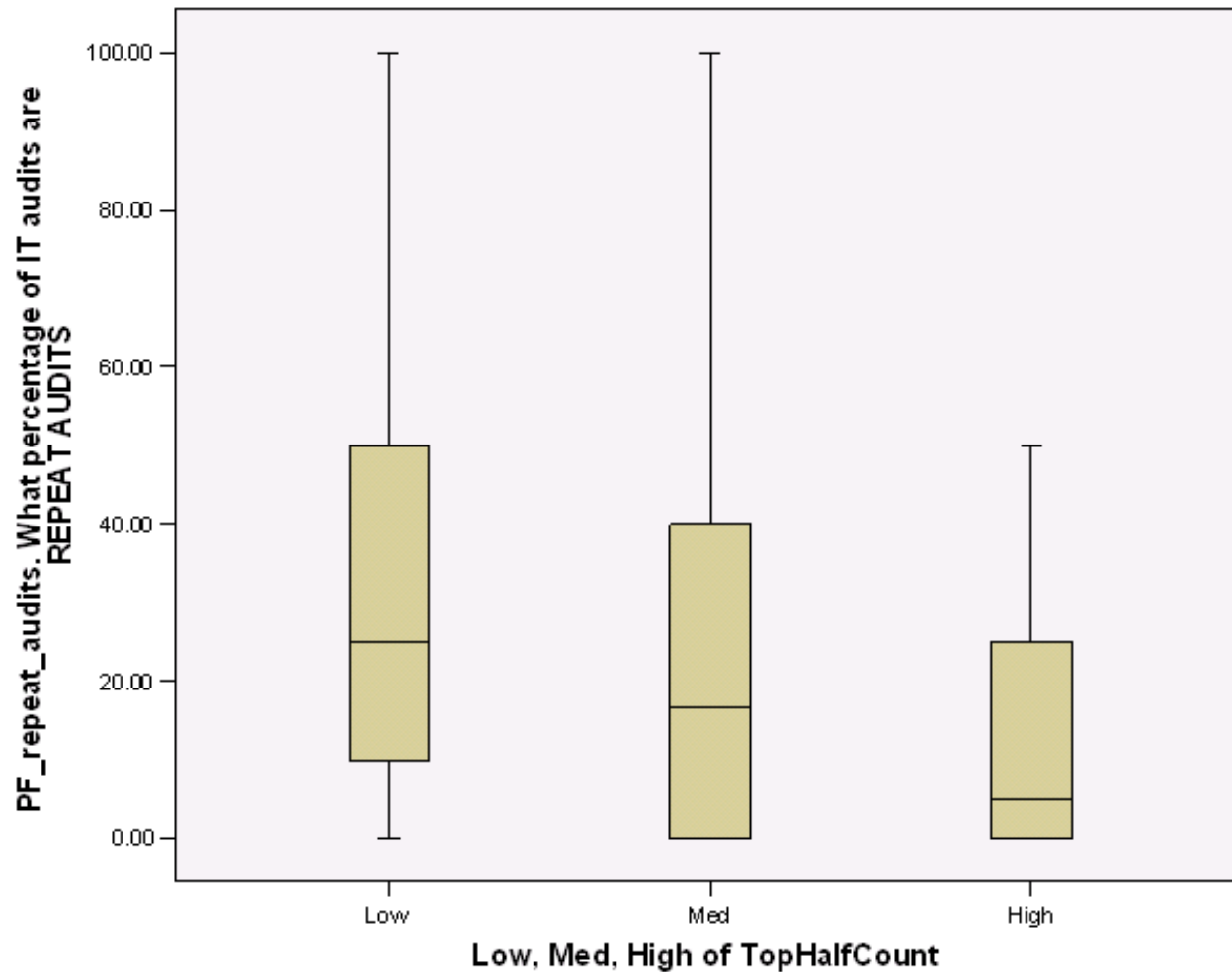
Higher Performing IT Organizations Are More Stable, Nimble, Compliant And Secure



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

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**

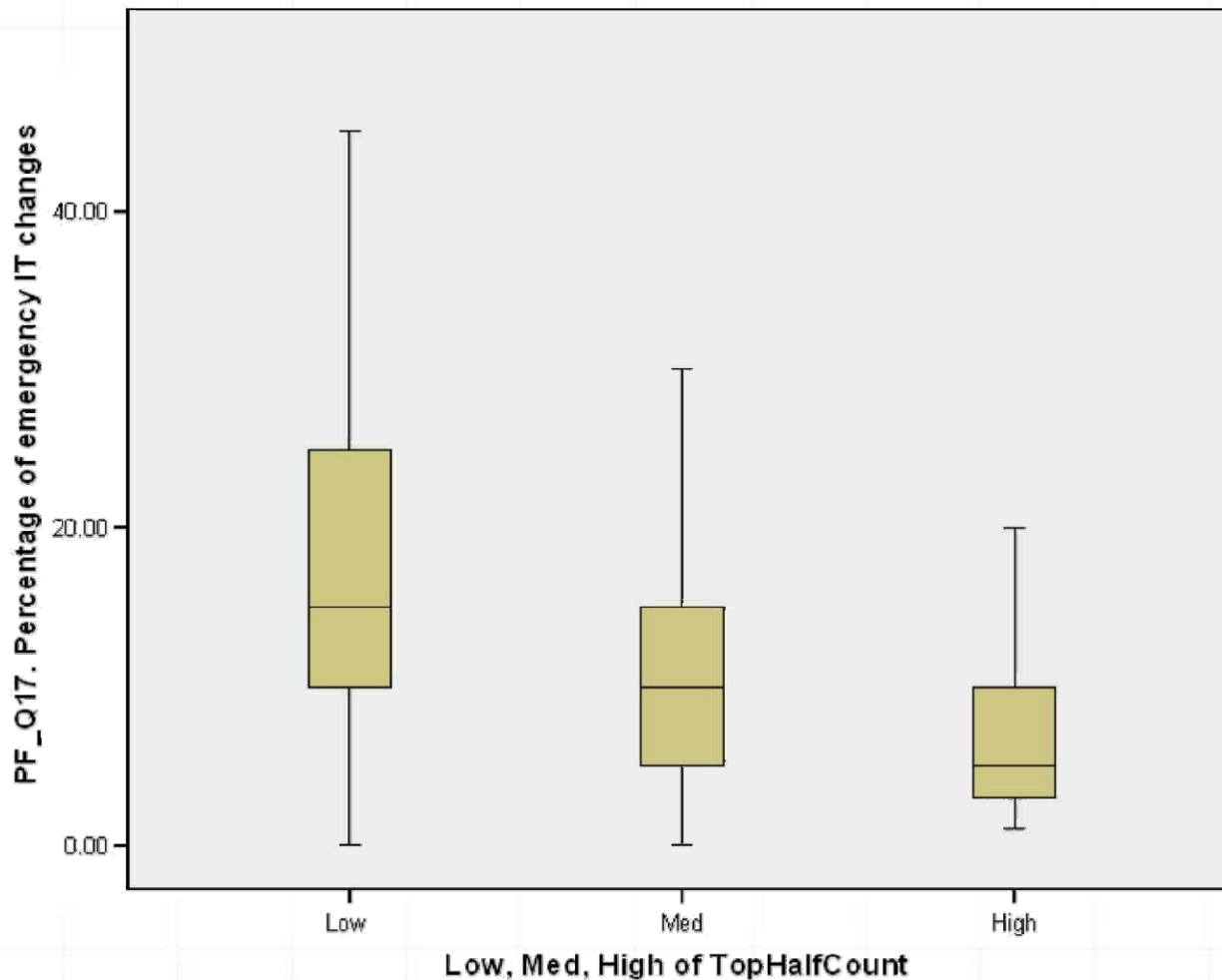


Source: IT Process Institute/Institute of Internal Auditors (May 2007)



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**

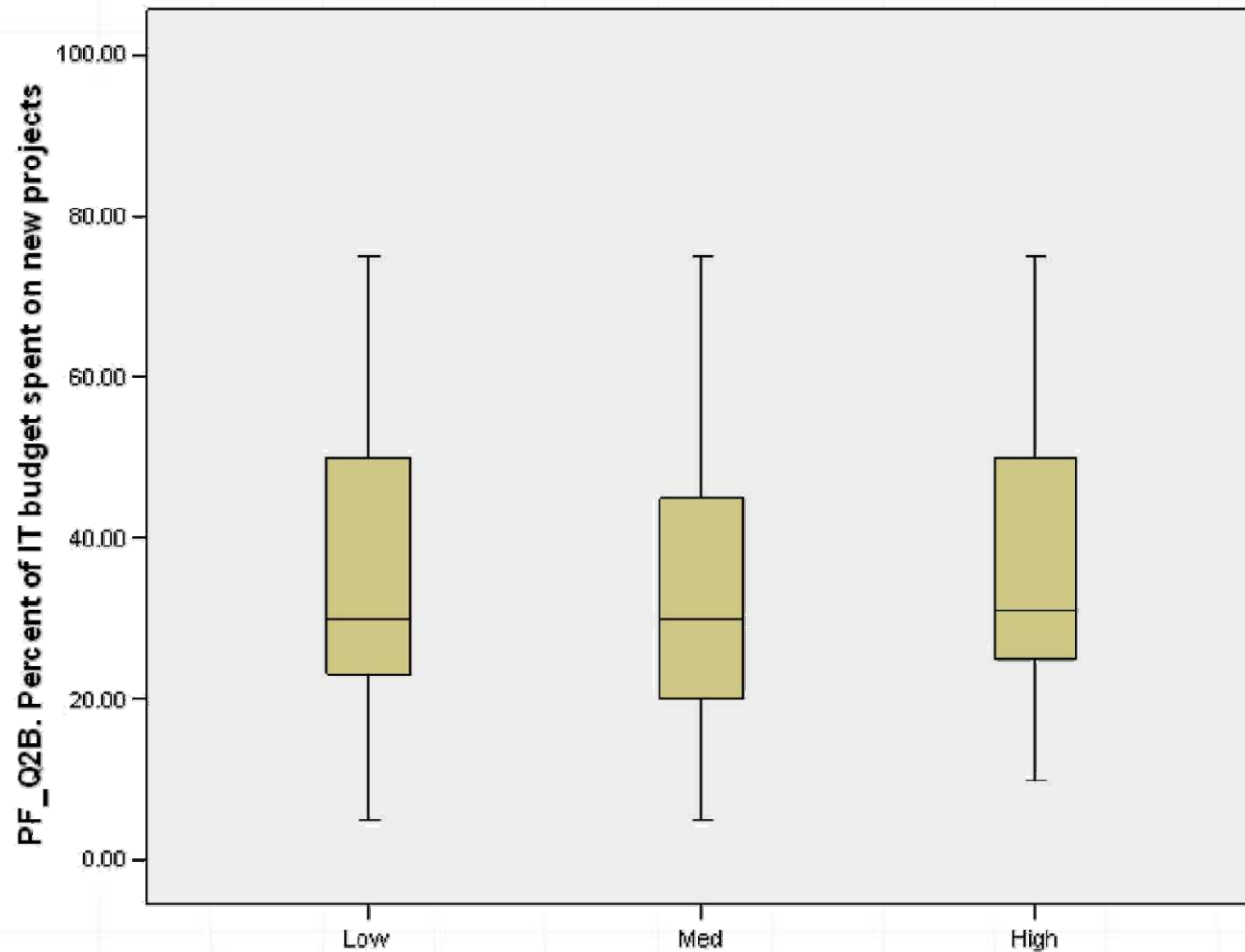


Source: IT Process Institute/Institute of Internal Auditors (May 2007)



High Performers Complete More Projects

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



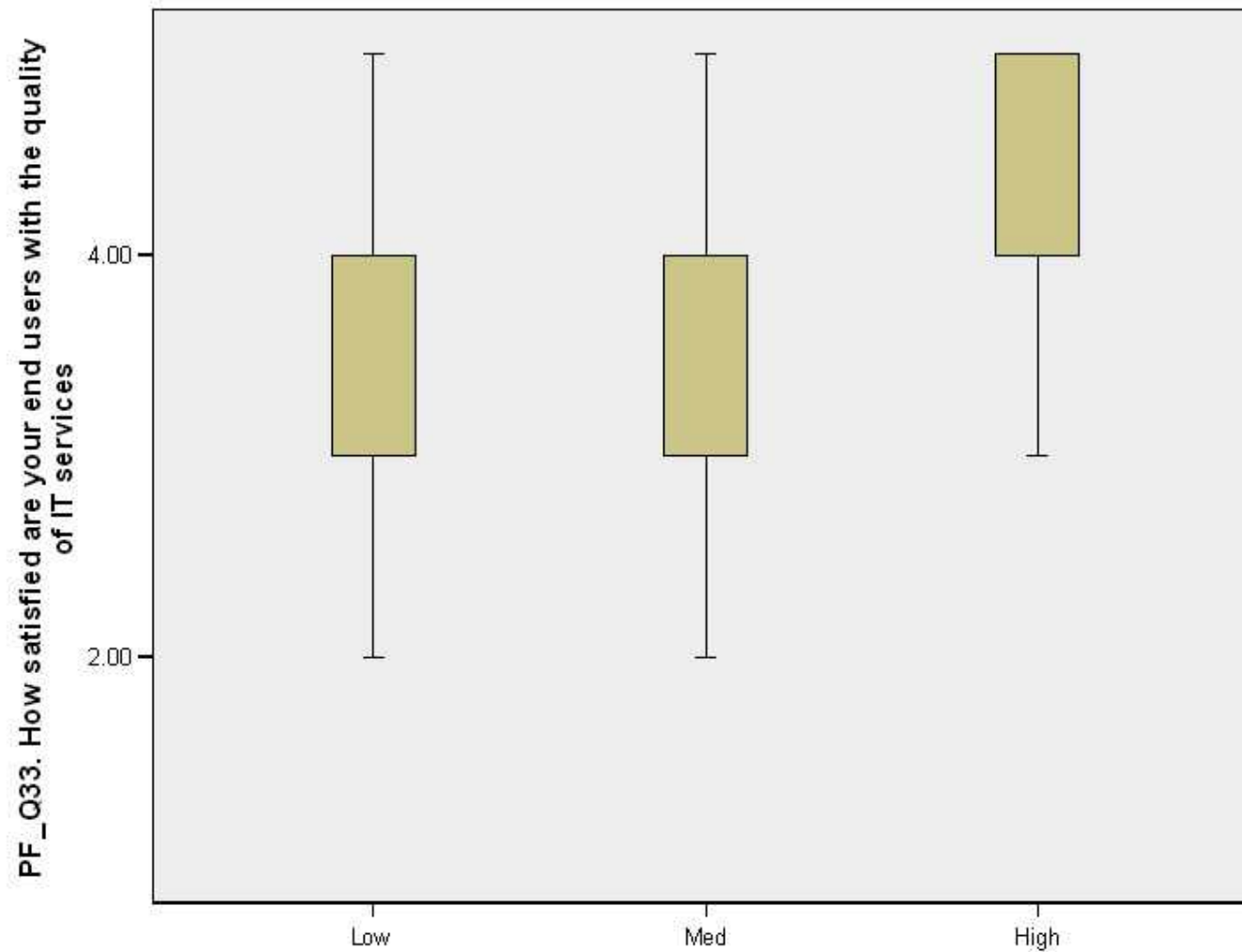
Source: IT Process Institute/Institute of Internal Auditors (May 2007)

Low, Med, High of TopHalfCount



High Performers Have Happier Users

High performers **keep the business happier**



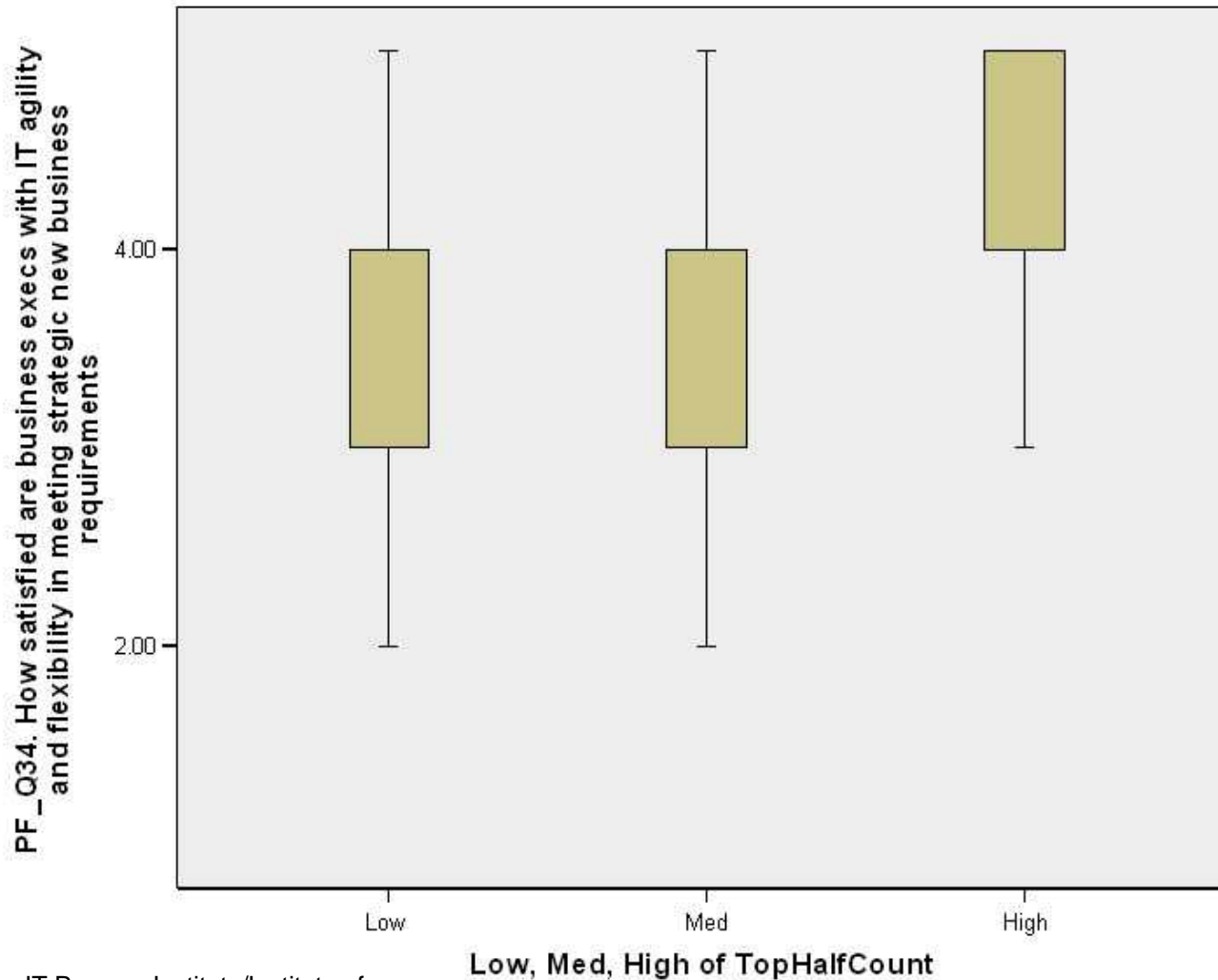
Source: IT Process Institute/Institute of Internal Auditors (May 2007)

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)



Discuss Findings and Validate Theory

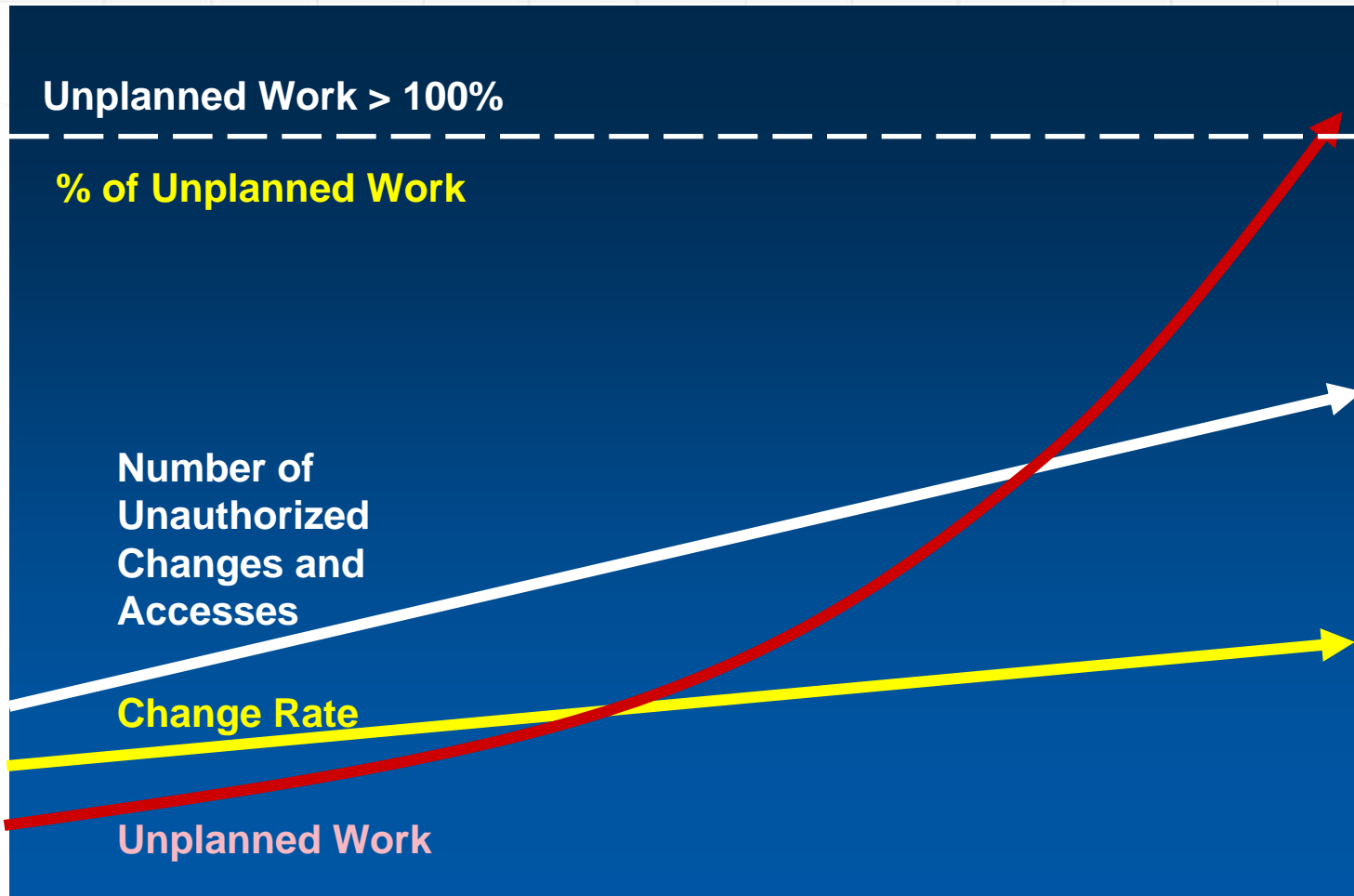
- Do the findings confirm deeply held intuitions and reveal surprising new insights?
 - Answer: Yes!
- Do the findings support the theory?
 - Answer: Yes!



2007: IT Controls Study II and CCR Study

- Two more studies that benchmarked almost 1000 IT organizations confirmed the findings, and further reduced the scope of “what seems to matter”
- The Change, Configuration and Release Study in 2007 found that the following three activities predicted 60% of performance:
 - Process discipline
 - Standardized configuration strategy
 - Controlled access to production systems

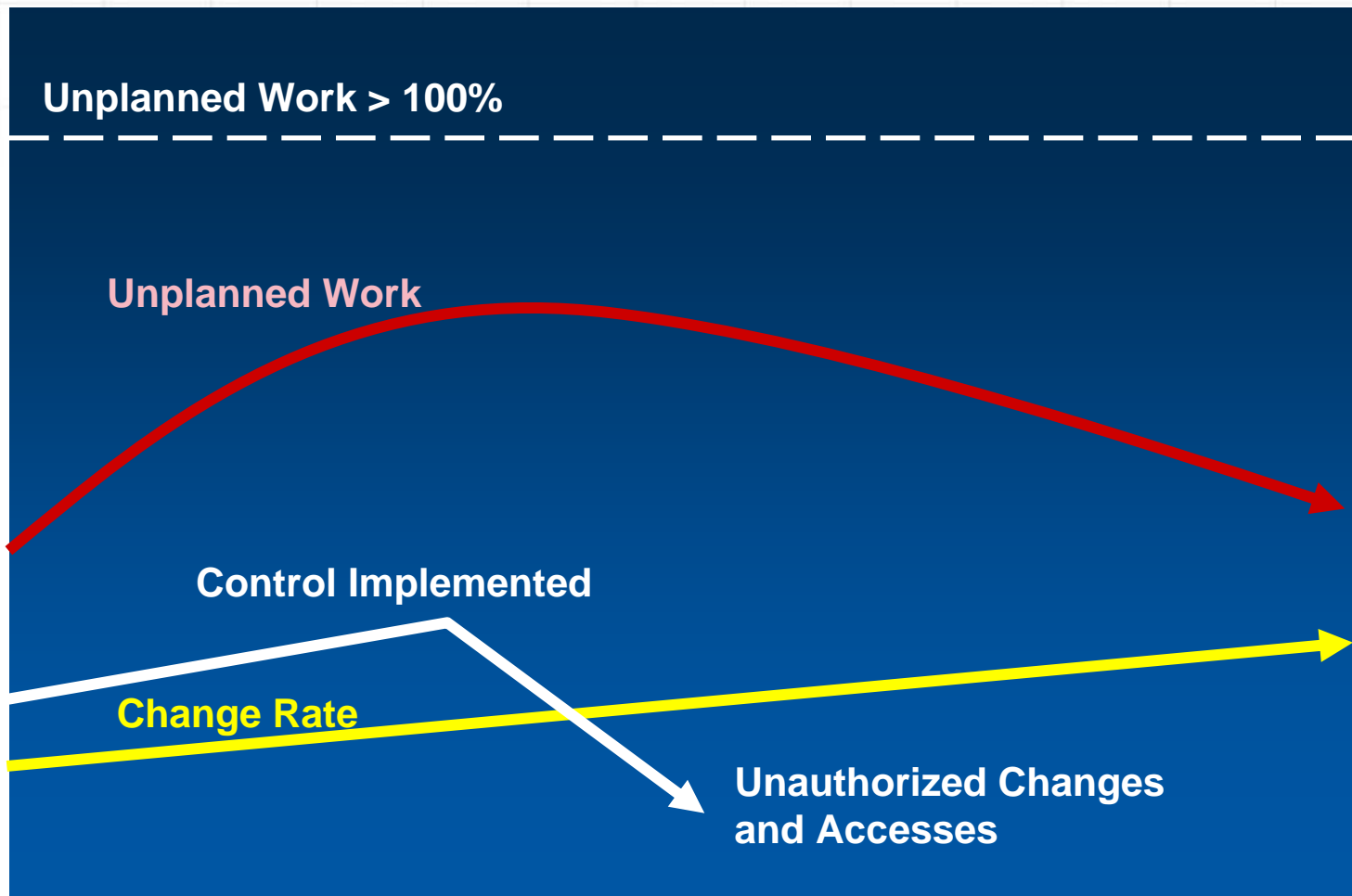
Weak IT Controls Drive Up IT Costs



Source: The Visible Ops Handbook, © IT Process Institute



Strong IT Controls Reduce Unplanned Work

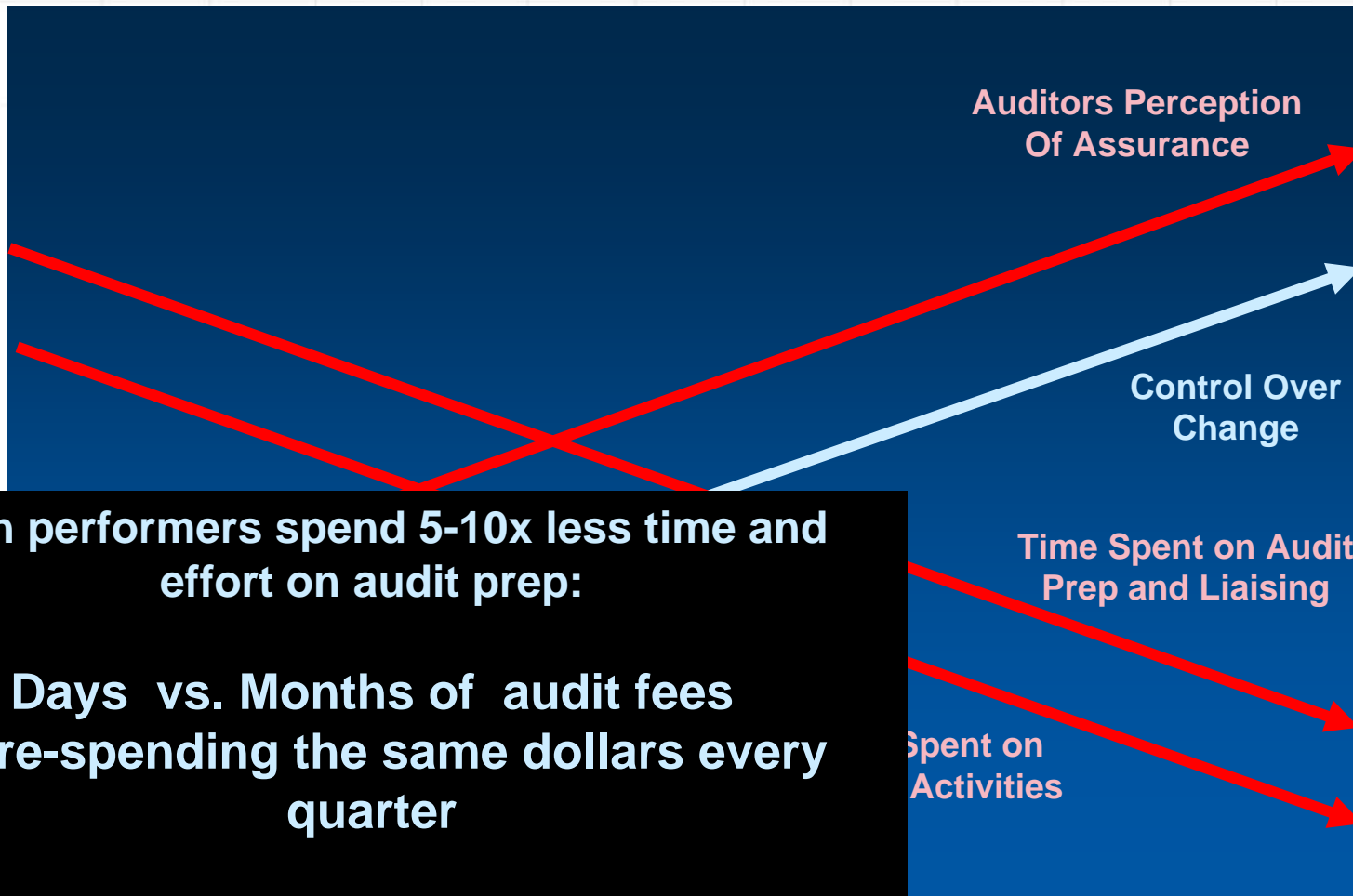


Source: The Visible Ops Handbook, © IT Process Institute



Visible Ops Phase 1

Increasing Auditability



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

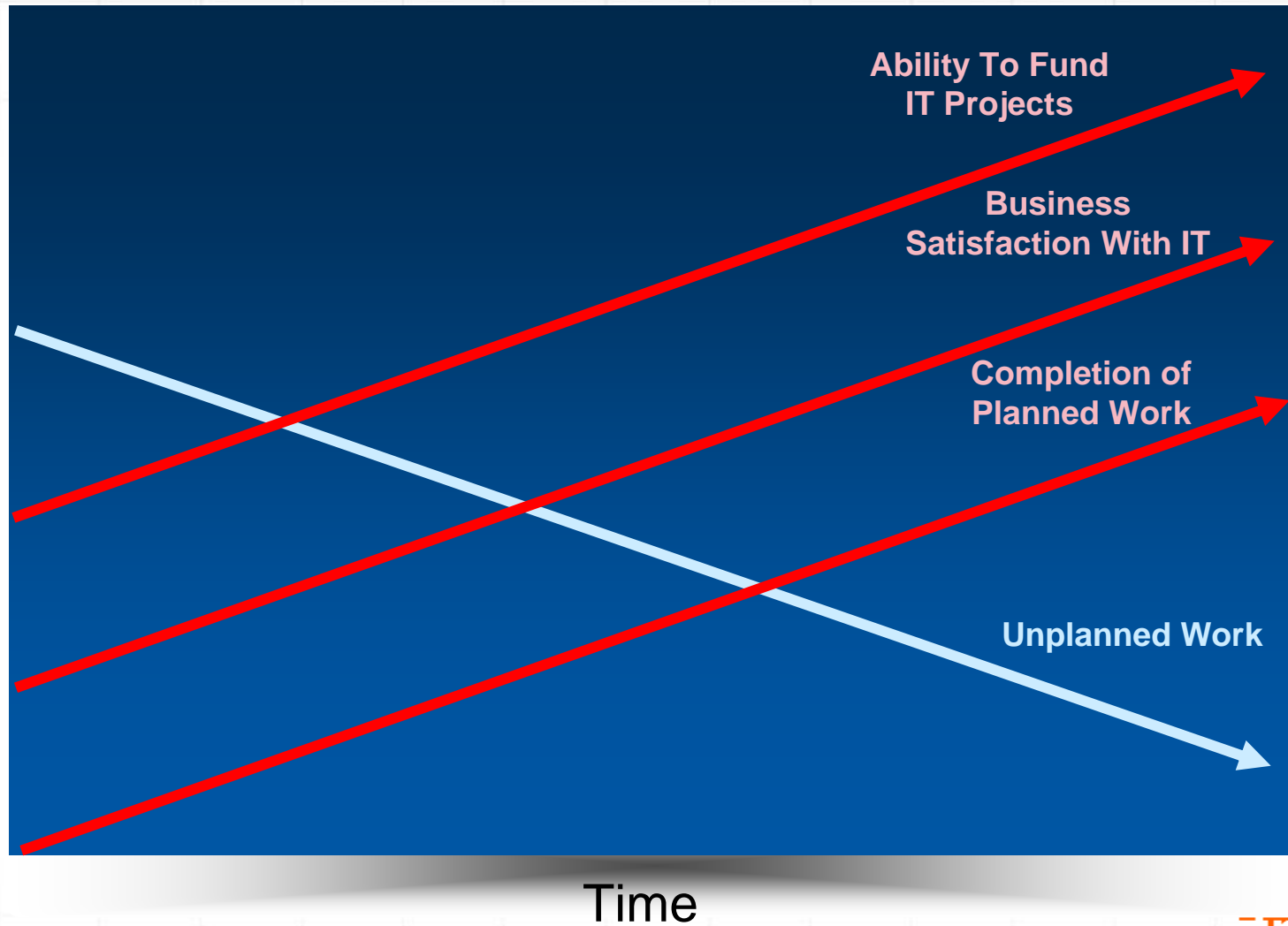
Days vs. Months of audit fees
No re-spending the same dollars every quarter

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

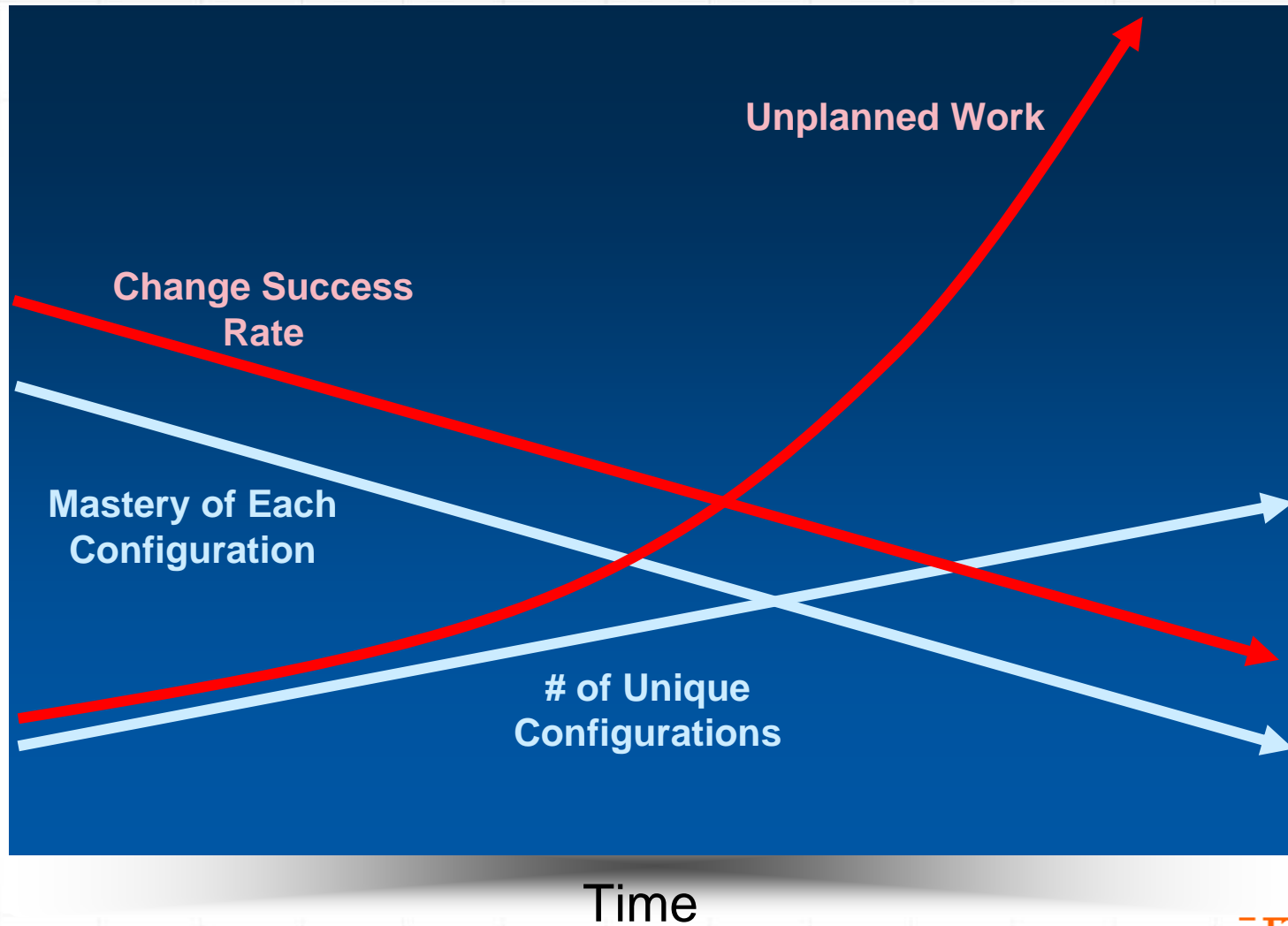


Source: The Visible Ops Handbook, © IT Process Institute



Visible Ops Phase 2

Drifting Configurations

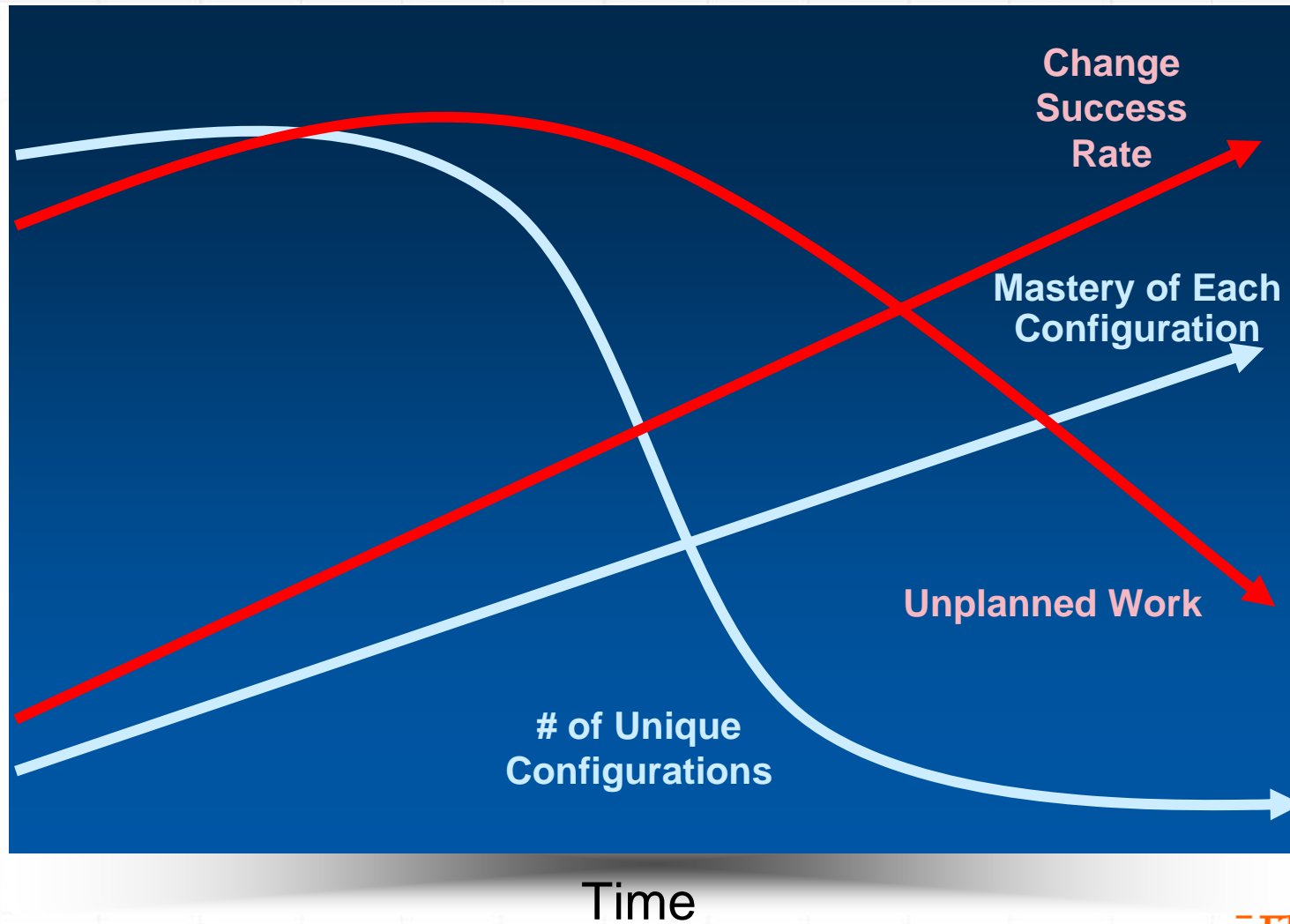


Source: The Visible Ops Handbook, © IT Process Institute



Visible Ops Phase 2

Find Fragile Artifacts



Source: The Visible Ops Handbook, © IT Process Institute



Does Research Validate The Theory?

Foundational Control	% high with the specified control	% medium with the specified control	Difference	<p>Note that virtually every top performer monitors their systems for unauthorized changes... ...and has defined consequences for unauthorized changes! Organizations that have these controls are almost always great.</p>
C23 Do you monitor systems for unauthorized changes?			72	
C24 Are there defined consequences for intentional unauthorized changes?	93	32	61	
C31 Do you have a formal process for IT configuration management?			58	
C32 Do you have an automated process for configuration management?	79	21	58	
C20 Do you track your change success rate?	86	32	54	
C36 Are you able to provide relevant personnel with correct and accurate information on the present IT infrastructure configurations?	100	47	53	

**Visible Ops:
Electrify the Fence**

**Visible Ops:
Create Consequences for
Touching the Fence**



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”

A Note About Scoping Risks And Controls

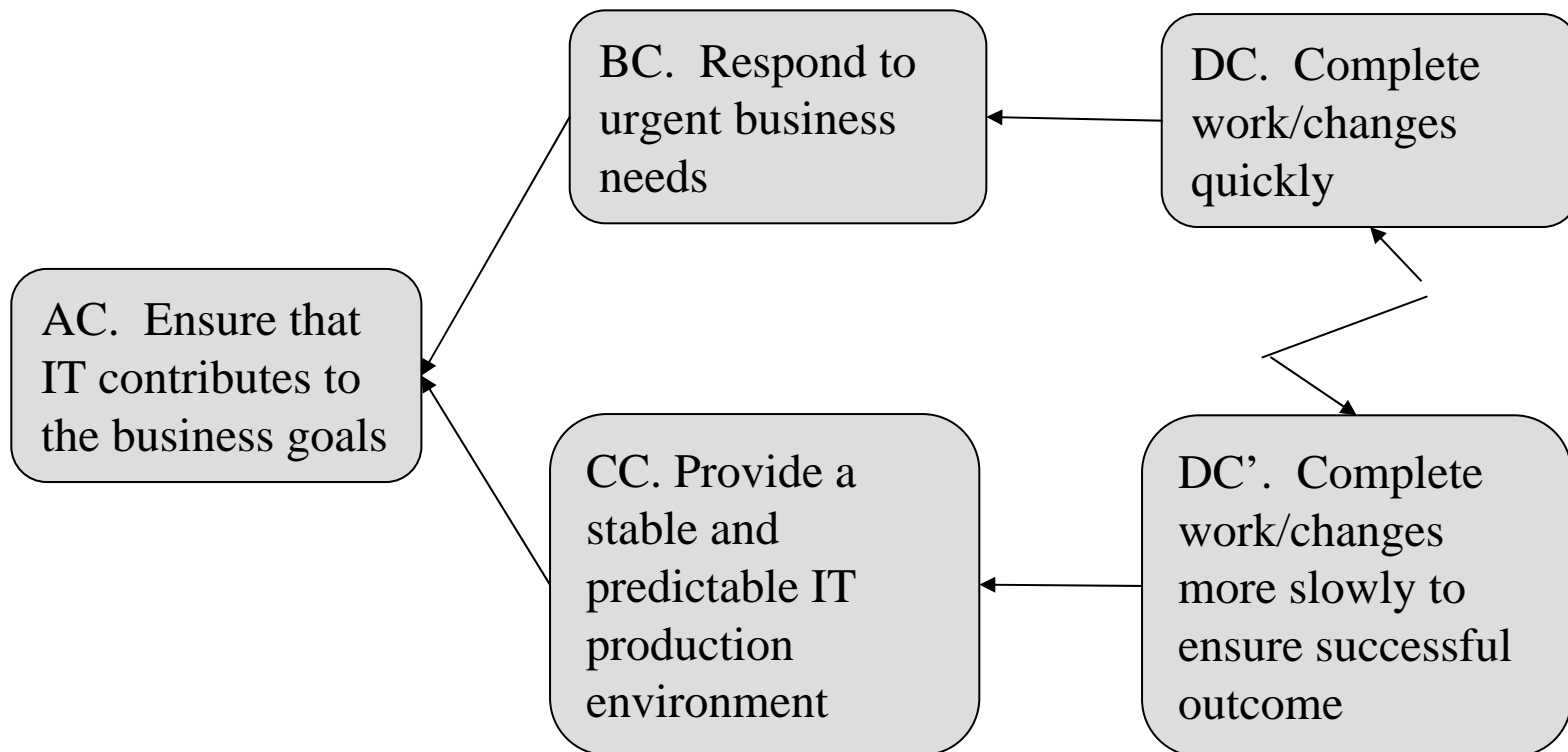
- Phase 2 of Visible Ops Security describes how to:
 - Zoom out to rule out: Understand which business processes have reliance on IT functionality, by understanding the end-to-end process
 - Understand how IT general control process risks jeopardize critical IT functionality
 - Find and fix IT control issues
- Examples for financial reporting
 - Payroll processes for an international subsidiary with 50 employees, where salaries change once per year
 - Grain levels that are centrally located
- Examples for data privacy
 - Point of sales and order entry systems that does automated processing of customer credit card authorization transactions
 - Point of sales for a hotel chain that does paper-based credit card authorizations
 - A 911 call center for a major metropolitan city that processes incident tickets and dispatches alerts to hundreds of other locations

We want to align the risks to what matters to the business, so we are helping them achieve their goals.



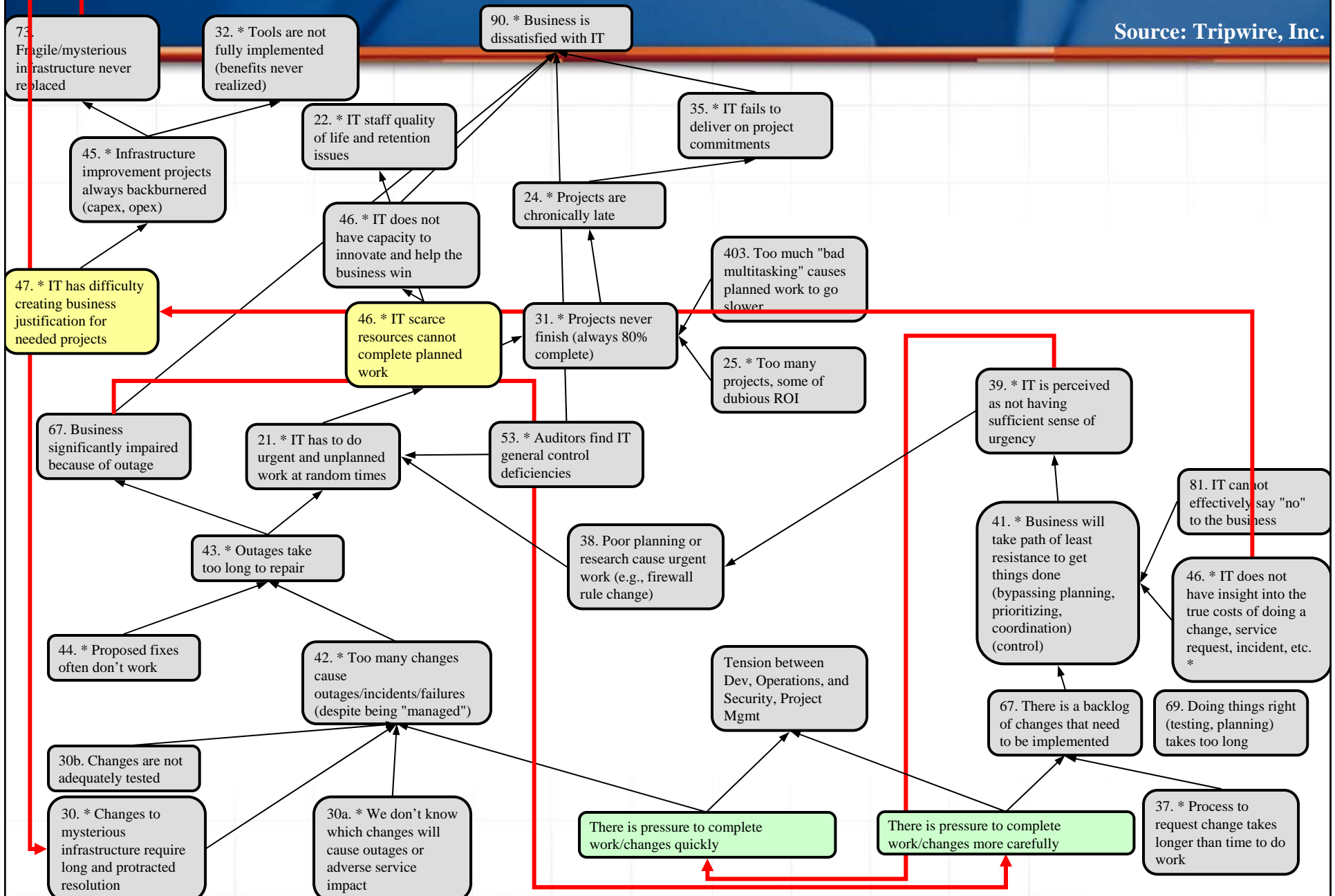
Warm Up For Exercise 2:
Metrics That Matter
And Designing An Intervention

Core Conflict: IT



Current Reality: Does This Feel Familiar?

Source: Tripwire, Inc.



Undesired Effects

- Developers must have daily production access
- Production issues require developer intervention (e.g., break/fix, fix transactions, direct data edits, etc.)
- Auditors find control weaknesses
- IT operations unable to support mission-critical application (e.g., “what is Error 520?”)
- Data errors cause issues (e.g., inaccurate financial reports, dosage errors, routing errors, payment issues)
- Developers can’t work on planned work
- Business has to wait even longer for needed projects
- Urgent project to fix audit issues
- Repeat audit findings cause unwanted attention from management



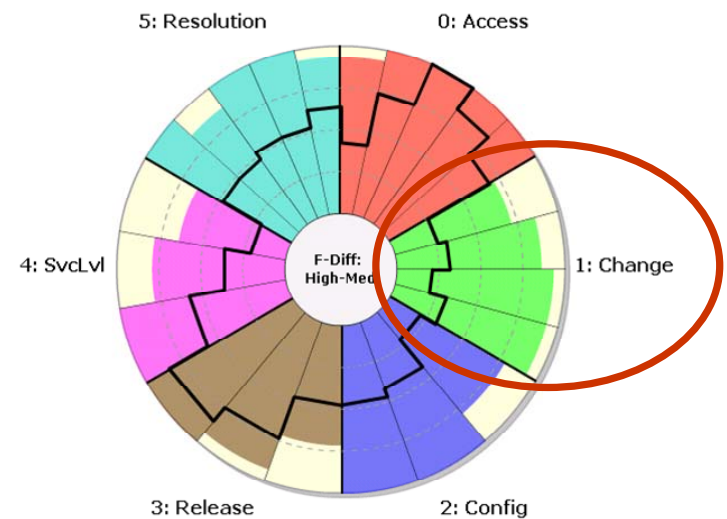
Exercise 2:
Metrics That Matter
And Designing An Intervention

Steps To Reduce Developer Access

- Remove developer logins
 - Often can't be done overnight
- Address control weakness
 - Put in change monitoring controls to track all changes made during emergency access
 - Create procedures to substantiate that only authorized changes were made
- Increase IT operations capabilities to restore service
 - Co-pilot restoration procedures
 - Reduce reliance over time
- Use saved developer cycles to address application issues that cause incidents

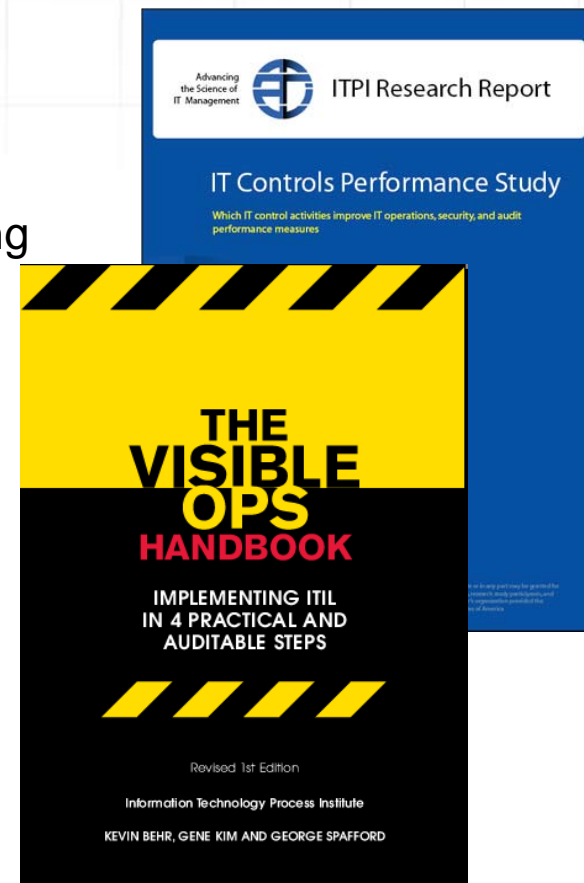
Got Change? Get Control.

- Implement the foundational controls of high performers
 - Use Tripwire to automatically monitor for unauthorized changes across the stack
 - Create consequences for intentional unauthorized changes
 - Manage by fact – not “gut feel”
- Achieve industry-leading credibility
 - Service levels
 - Security
 - Compliance
 - Efficiency and reduced unplanned work



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



Interested?

- Give us a business card, and we will provide you with a complementary copy of:
 - Visible Ops Handbook
 - IT Controls Performance Study executive summary
- Interested in the VIP Program?
 - Email highperformer@tripwire.com and genek@tripwire.com



**The Leader in
Configuration Audit & Control**

Lunch Session

The background of the slide features a high-speed photograph of a water drop hitting a surface, creating a series of concentric ripples. The drop is in the center, with a stem-like structure extending upwards. The ripples are light blue and white. In the lower portion of the image, a close-up of a computer keyboard is visible, with a white key labeled "Ctrl" in blue text. A thick orange horizontal bar is positioned across the middle of the slide, partially overlapping the keyboard image.

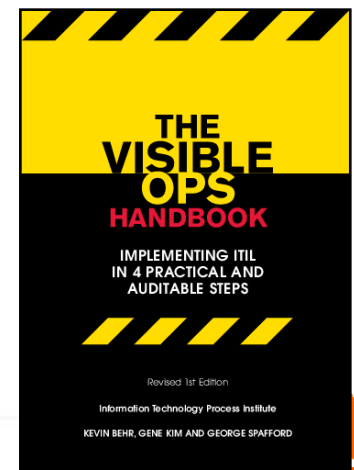
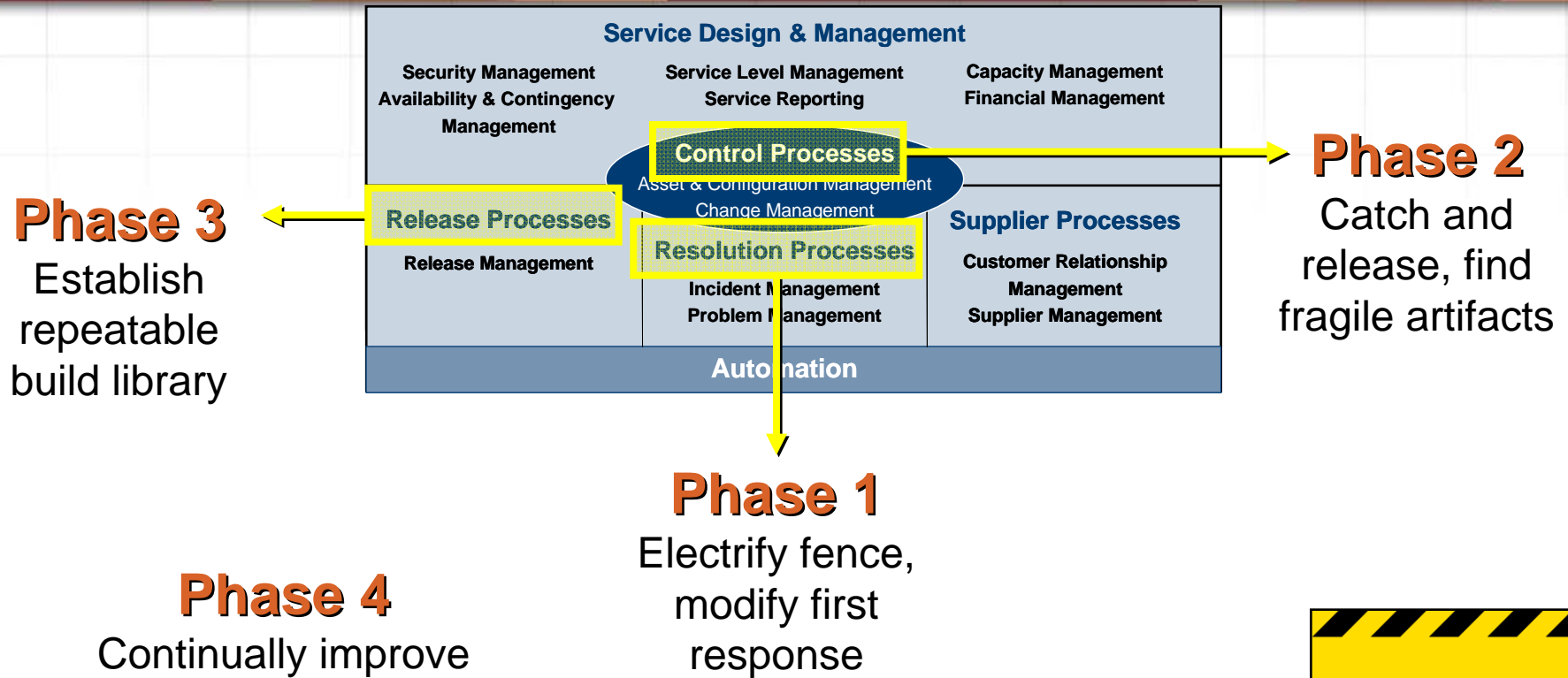
Ctrl

Visible Ops Security Goals

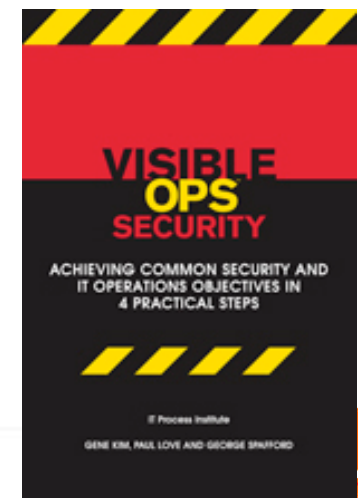
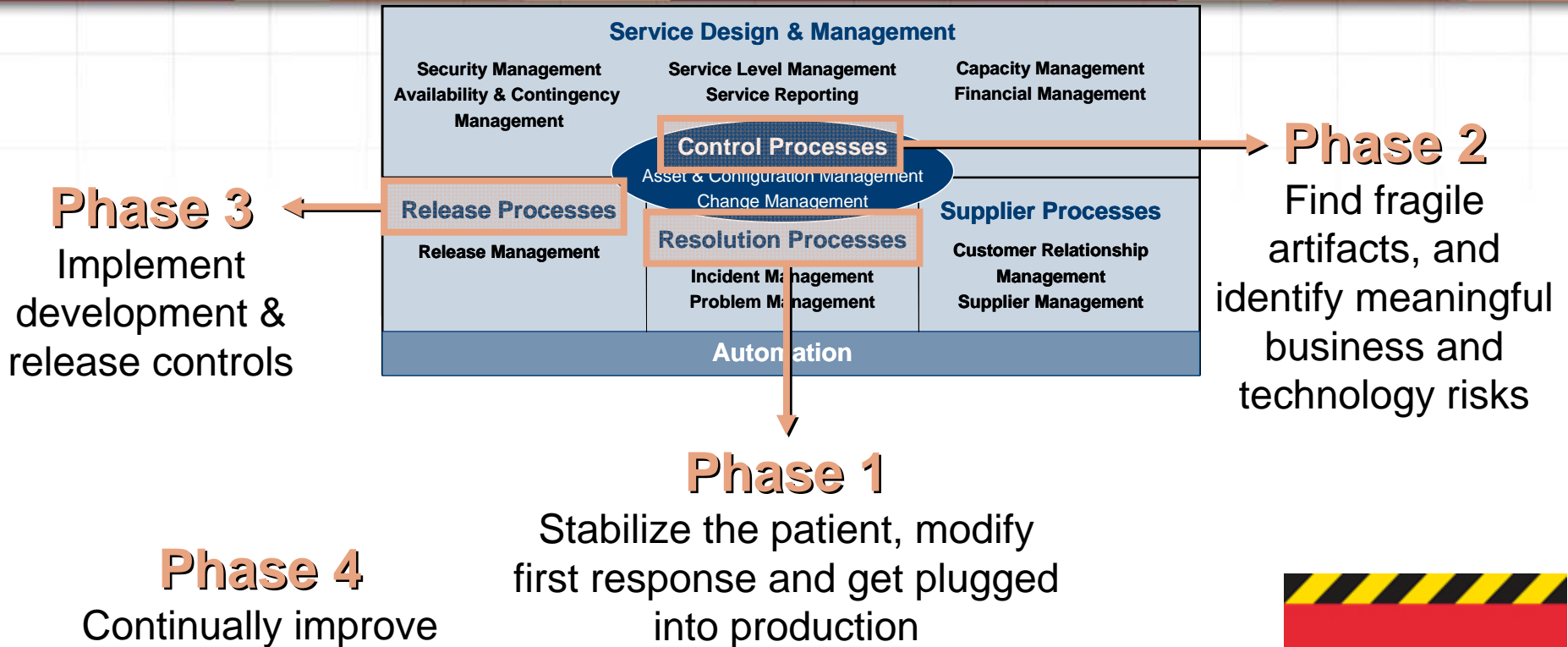
- Build those information security controls to reinforce a culture of controls, by being plugged into and generate value into the daily operational processes of...
 - IT operations
 - Software and service development
 - Project management
 - Internal audit
- To enable virtualized computing environments to be just as secure (if not more secure) than the physical computing environment

High performing information security organizations have the following attributes: business aligned, plugged in, add value, understand priorities, understand business context, and foster cooperation

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



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



The Seven Practical Steps To Integrate Security Into Operations

- Step 1: Gain situational awareness
- Step 2: Reduce and monitor privileged access
- Step 3: Define and enforce VMM configuration standards
- Step 4: Integrate and help enforce change management processes
- Step 5: Create library of trusted virtualized builds
- Step 6: Integrate into release management
- Step 7: Ensure that all activities (physical and virtual) go through change management

Step 1: Gain Situation Awareness

- Situational awareness: “the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regard to the mission.”
- Questions we want to answer:
 - Who are the business and IT units, and how are they organized? (e.g., the centralized IT services group, an IT outsourcer, etc.)
 - What are the relevant regulatory and contractual requirements for the business process enabled by virtualization? (e.g., SOX-404, PCI DSS, FISMA, etc.)
 - What are the technologies and IT processes being used? (e.g., SAP, Oracle, J2EE, VMware ESX, etc.)
 - Are there any high-level risk indicators from the past? (e.g., repeat audit findings, frequent outages, etc.)
 - What IT services are being enabled by virtualization? (e.g., e-commerce, point of sale, financial reporting, order entry, etc.)

Merely getting licensing information on VM servers to information security can be helpful!

Step 2: Reduce And Monitor Privileged Access

- We know where infrastructure that poses the largest risk to business objectives are: now it's time to ensure that access is properly restricted
- We look for administrators who have high levels of privilege and reduce access (applications, databases, OS, network, firewall, etc.)
- They can introduce likelihood of errors, downtime, fraud and security incidents
 - Can affect mission critical IT services
 - Can modify logical security settings
 - Can add, remove and modify VMs

“To err is human. To really screw up requires the root password.”—Unknown

Step 2: Reduce And Monitor Privileged Access

- Implement preventive controls:
 - Reconcile admins to authorized staff and delete any ghost accounts
 - Ensure reasonable number of admins (i.e., 25 is too many, one is too few)
 - Issue and revoke accounts upon hiring, firing, reassignment
- Implement detective controls:
 - Monitor privileged user account adds, removes and changes
 - Reconcile each user account change to an authorized work order
 - Reconcile each user account to an HR record
 - Implement account re-accreditation procedures

“Hope is not a strategy. Trust is not a control.”

Step 3: Define And Enforce Configuration Standards

- Virtually all IT infrastructure has configuration and logical security settings that are designed to limit the risk of human error, fraud and security incidents
- Our goal is to create known, trusted, stable, secure and risk-reduced configuration states
- External configuration guides include:
 - Center For Internet Security
 - VMWare: “VMware Infrastructure 3, Security Hardening”

“Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement. The security issues related to vulnerability and configuration management get worse, not better, when virtualized.”

Source: Gartner, Inc. “Security Considerations and Best Practices for Securing Virtual Machines” by Neil MacDonald, March 2007.

Step 3: Define And Enforce Virtualization Configuration Standards

- Implement preventive controls:
 - Help IT management and infrastructure managers define a configuration security policy
 - Mandate that all virtualization technologies use these secure configuration settings
 - Define a time-limit for implementation and how quickly corrective actions must be implemented
- Implement detective controls:
 - Monitor configuration settings wherever they are stored (e.g., Unix or Windows files, Windows registry settings, etc.).
 - Test configuration settings against organizational policies and report on any variance.
 - Verify that corrective actions are properly implemented in the required time.

Step 4: Help Enforce Change Management Processes

- Integrating information and change management have similar missions: both groups are trying to manage risk.
- Information security needs change management to gain situational awareness of production changes and to influence decisions and outcomes.
- Even if the organization achieved the mythical “perfectly secure state,” any change can quickly take us out of that secure state.
- Add value in the change management process by:
 - Helping assess the potential information security and operational impact of changes
 - Improving procedures for change authorization, scheduling, implementation and substantiation
 - Ensuring that change requests comply with information security requirements, corporate policy, and industry standards

Step 4: Help Enforce Change Management Processes

- Implement preventive controls
 - Get invited to the Change Advisory Board (CAB) meetings
 - Ensure “tone at the top” and help define consequences
- Implement detective controls
 - Build and electrify the fence
 - Substantiate that all changes are authorized
 - Look for red flags and indicators

“[As auditors,] the top leading indicators of risk when we look at an IT operation are poor service levels and unusual rates of changes.” – Bill Philhower

Step 5: Create A Library Of Trusted Builds

- Our goal is to make it easier to use known, stable and secure builds than unauthorized and insecure builds
- This is especially important in the virtualized environment, when deploying a new server is as easy as copying a file
- Implement preventive controls:
 - Defined process of how to assemble hardened and stable builds (e.g., application, database, OS)
 - Work with any existing server provisioning teams to add any standard monitoring agents
 - Ensure that application and service account passwords are changed before deployment (e.g., database logins)

Step 5: Create A Library Of Trusted Builds

- Implement detective controls:
 - Verify that deployed infrastructure matches trusted, known good (and risk reduced) states
 - Verify that virtual image configurations against internal and external configuration standards
 - Monitor the approved virtual image library to ensure for all adds, removes and changes (i.e., directory where .vmdk files reside)
 - Reconcile all adds, removes and changes to an authorized change order. This can be manual (e.g., signed change order from virtualization manager) or automated (e.g., Remedy work order)

Step 6: Integrate Into The Release Management Processes

- Release management and information security both require standardization and documentation
 - Checklists
 - Detections and reduction of variance
- How many things can go wrong between software packaging, installation, configuration, tuning and deployment?
- Implement preventive and detective controls:
 - Develop shared templates with release management, QA and project management and integrate into their checkpoints
 - Integrate automated security testing tools (e.g., vulnerability scanning, configuration assessment). Ideally, they will match those that run in production
 - Compare preproduction and production images, and reduce any variance (there are few excuses not to with virtualized images)

Step 7: Ensure That All Activities Go Through Change Management

- Ensure that “only acceptable number of unauthorized changes is zero”
 - Under what conditions are virtual machine activations, deactivations and restarts a change that requires approval? (e.g., delivers a new IT service, is a CI that enables a service that has security or regulatory requirements, has outage risk to a mission-critical service, etc.)
 - Who must approve standard and emergency changes for virtual machines?
- Virtualization bypasses many physical controls (e.g., data center access, network cabling, VLAN configuration), so we must ensure that we can rely on compensating processes
- Scenario: Materials management business process runs on virtualized IT service, which is in-scope for SOX-404. VM is accidentally deleted three days before end of quarter, preventing business from closing its books.

A Note About Scoping Risks And Controls

- Phase 2 of Visible Ops Security describes how to:
 - Zoom out to rule out: Understand which business processes have reliance on IT functionality, by understanding the end-to-end process
 - Understand how IT general control process risks jeopardize critical IT functionality
 - Find and fix IT control issues
- Examples for financial reporting
 - Payroll processes for an international subsidiary with 50 employees, where salaries change once per year
 - Grain levels that are centrally located
- Examples for data privacy
 - Point of sales and order entry systems that does automated processing of customer credit card authorization transactions
 - Point of sales for a hotel chain that does paper-based credit card authorizations
 - A 911 call center for a major metropolitan city that processes incident tickets and dispatches alerts to hundreds of other locations

We want to align the risks to what matters to the business, so we are helping them achieve their goals.

About Gene Kim

Gene Kim is the CTO and founder of Tripwire, Inc. In 1992, he co-authored Tripwire while at Purdue University with Dr. Gene Spafford. Since then, Tripwire has been adopted by more than 5,500 enterprises worldwide. Since 1999, he has been studying high performing IT operations and security organizations, which led Gene to co-found the IT Process Institute (ITPI) in 2004, an organization dedicated to research, benchmarking and developing prescriptive guidance for IT operations, security management, and auditors.

This same year Gene co-authored the "Visible Ops Handbook: Implementing ITIL in Four Practical And Auditable Steps" which has since sold over 75,000 copies. And, he was a principal investigator on the IT Controls Performance Study project, completed in 2006.

Gene currently serves on the Advanced Technology Committee for the Institute of Internal Auditors where he is part of the GAIT task force, which has created guidance on how to scope IT general controls for SOX-404. Most recently, he was given the Outstanding Alumnus Award by the Department of Computer Sciences at Purdue University for achievement and leadership in the profession.

