The importance of context
Security measures as a dependent variable

Data reveals foundational practices that optimize security and operations

Kurt Milne
Managing Director, IT Process Institute
kurt.milne@itpi.org

Gene Kim
CTO, Co-Founder, Tripwire, Inc.
genek@tripwire.com, @RealGeneKim

Where Did The High Performers Come From?

Agenda

- Present research background
- IT Process Institute
- Share study methodology findings
  - VEESC 2006
  - IT Controls performance study 2007 (IIARF funded)
  - Change configuration and release 2008
  - Virtualization maturity 2009
- Study limitations and feedback

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

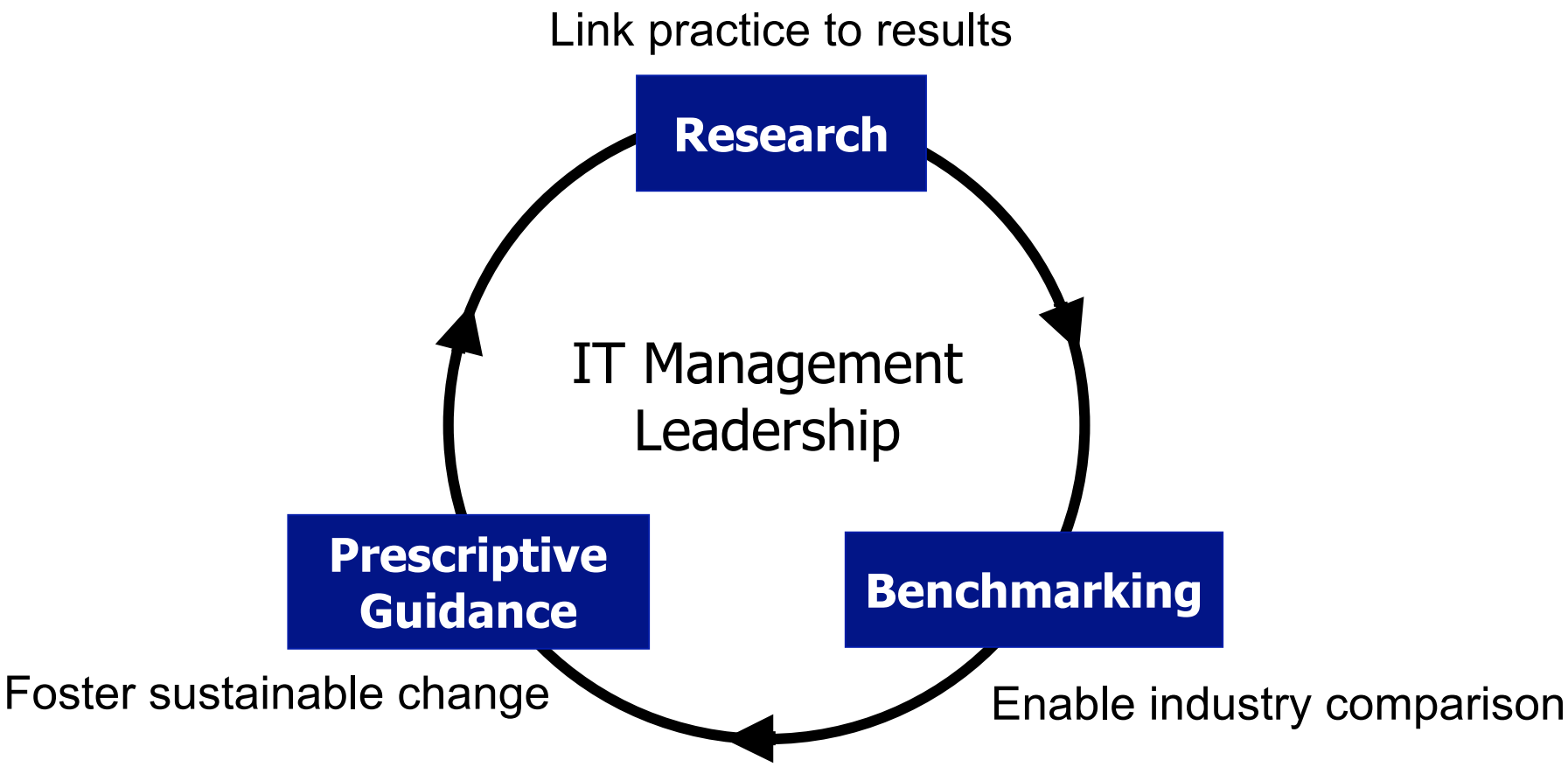
- Highest service levels (MTTR, MTBF)
- Highest first fix rate (unneeded rework)

Compliance and continual reduction of operational variance

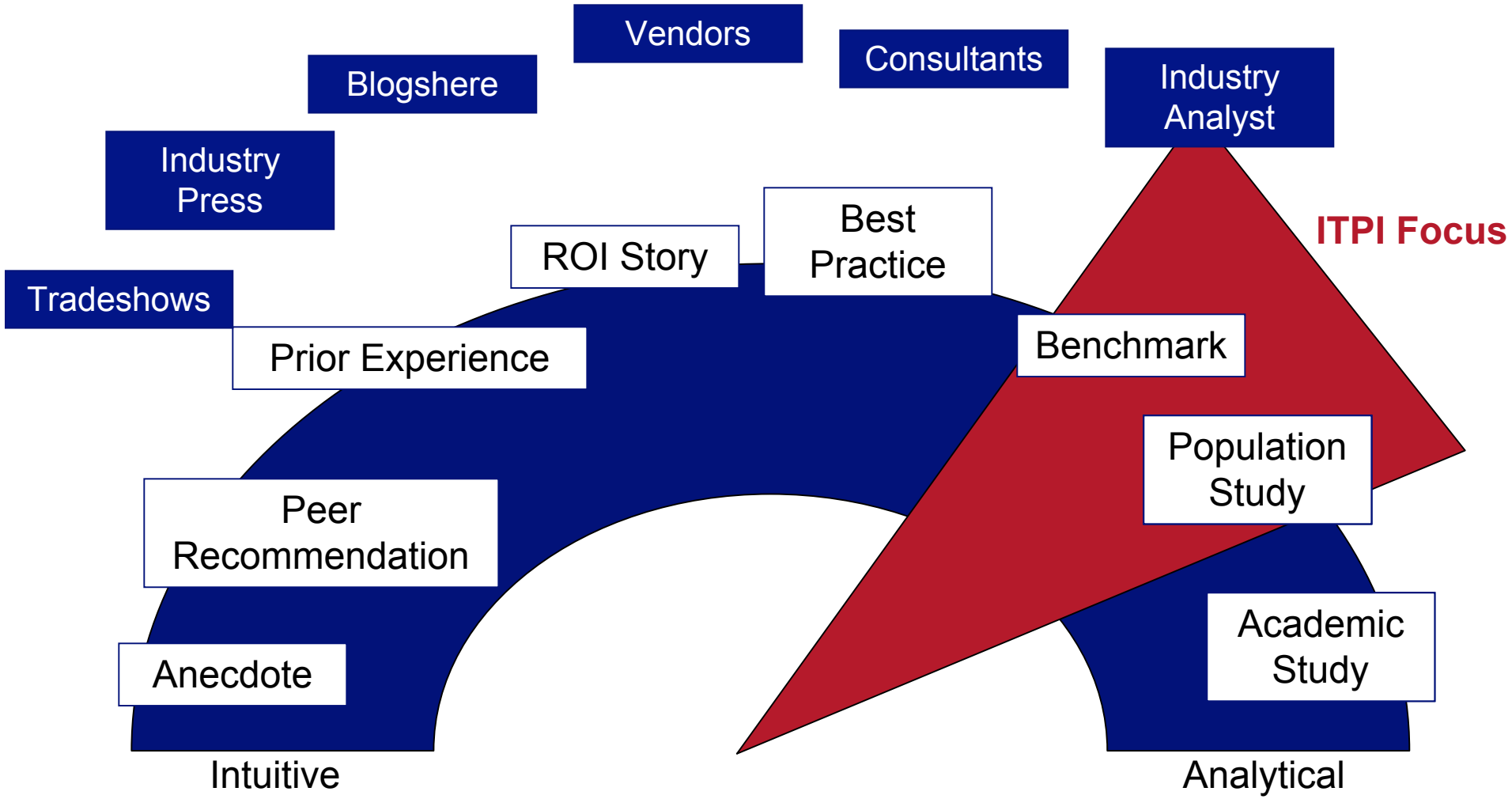
- Production configurations
- Highest level of pre-production staffing
- Effective pre-production controls
- Effective pairing of preventive and detective controls

Source: IT Process Institute

Mission - advancing the science of IT management



Data driven management - spectrum of influence

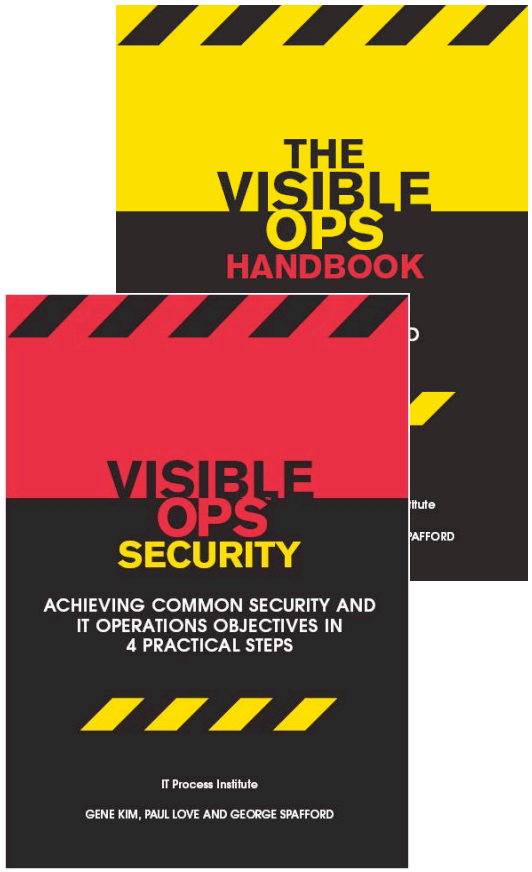


Vision: Quality Systems Approach

- Simple Mathematical function - Y = 2x+1
- Complex system – 300 step semiconductor fab
  - Settings at each step may potentially impact attributes of final product –i.e. CPU speed
  - How do you identify where to set equipment knobs at which process steps to optimize CPU speed?
  - Run controlled experiments – and identify correlation.
- Complex system – enterprise production environment
  - Hundreds of services
  - Many nodes, switches, configurations etc. etc. etc.
  - If you implement a new security control, how do you know it is working?
  - If it is not working
    - Do you consider it a sunk cost and pull it back out?
    - Or leave it on the ever growing pile of IT systems.

Prescriptive Guides

- 2006 - Visible Ops Handbook
  - Over 100,000 sold
  - Stop managing by "hair on fire"
- 2008 - Visible Ops Security
  - Meet dual objectives of security and operations



Surprise #1: Higher Performing IT Organizations

- High performers maintain a posture of compliance
  - **Fewest** number of repeat audit findings
  - **One-third** amount of audit preparation effort
- High performers find and fix security breaches faster
  - **5 times** more likely to detect breaches by automated control
  - **5 times** less likely to have breaches result in a loss event
- When high performers implement changes…
  - **14 times more** changes
  - **One-half** the change failure rate
  - **One-quarter** the change failure rate
  - **10x faster** MTTR for Sev 1 outages
- When high performers manage IT resources…
  - **One-third** the amount of unplanned work
  - **8 times more** projects and IT services
  - **6 times more** applications

Source: IT Process Institute, May 2007

Operations And Security Already Don't Get Along

Operations Hinders Security…

- Deploys insecure components into production
- Creates production IT infrastructure hard to understand
- Has no information security standard
- Creates self-inflicted outages
- Uses shared privileged accounts
- Can't finish projects
- Can't quickly address known security vulnerabilities

Security Hinders Operations…

- Creates bureaucracy
- Generates large backlog of reviews
- Creates delays through information security requirements
- Brings up project issues that cost too much, takes too long, & reduces feature set

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…"

Surprise #2: Three Controls Predicts 60% Of Performance

- To what extent does an organization define, monitor and enforce the following?
  - Standardized configuration strategy
  - Process discipline
  - Controlled access to production systems

Source: IT Process Institute, May 2006

2006: The ITPI IT Controls Performance Study

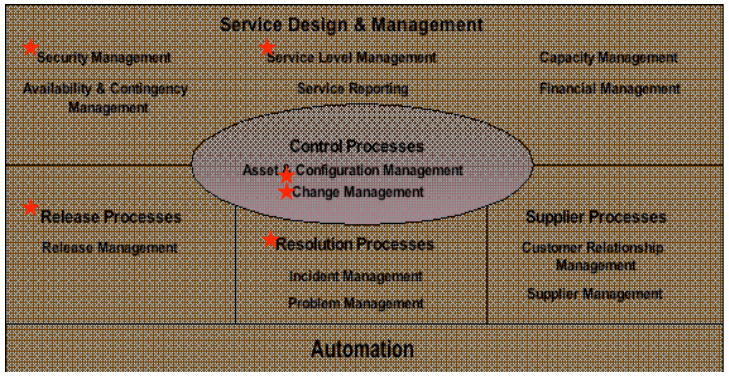
- ITPI launched the IT Controls Performance Study to find answers to the following questions:
  - Do high performers really exist?
  - Are all ITIL processes and COBIT controls created equal?
  - What controls have the highest impact on performance?
- 98 organizations were benchmarked (later expanded to 350)
- There were two huge surprises in the study

N = 98	**IT Employees**	**IT Budget**
Average	483	$114 million
Min	3	$5 million
Max	7,000	$1,050 million

2006: Design Survey: Pick IT Controls

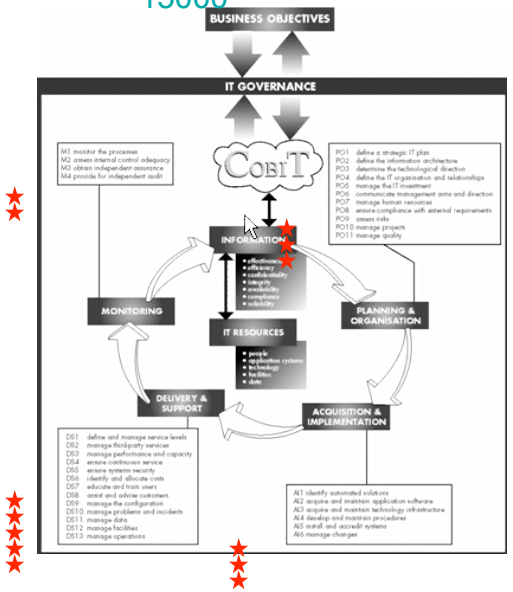
1. We selected the 6 leading BS15000 areas within ITIL that are conjectured to be “where to start.”

   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

2006: The 63 IT Controls

Access

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

Do you h ave 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 k eep 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 con sequences 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 s chedule 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 managemen t 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 specif ications?

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 aut omated 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 incide nt, 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

2006: Performance Differences

- 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
  - One-quarter first fix failure rate
- When high performers have security breaches
  - 5 times more likely to detect breaches by automated control
  - 5 times less likely to have breaches result in a loss event
- 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

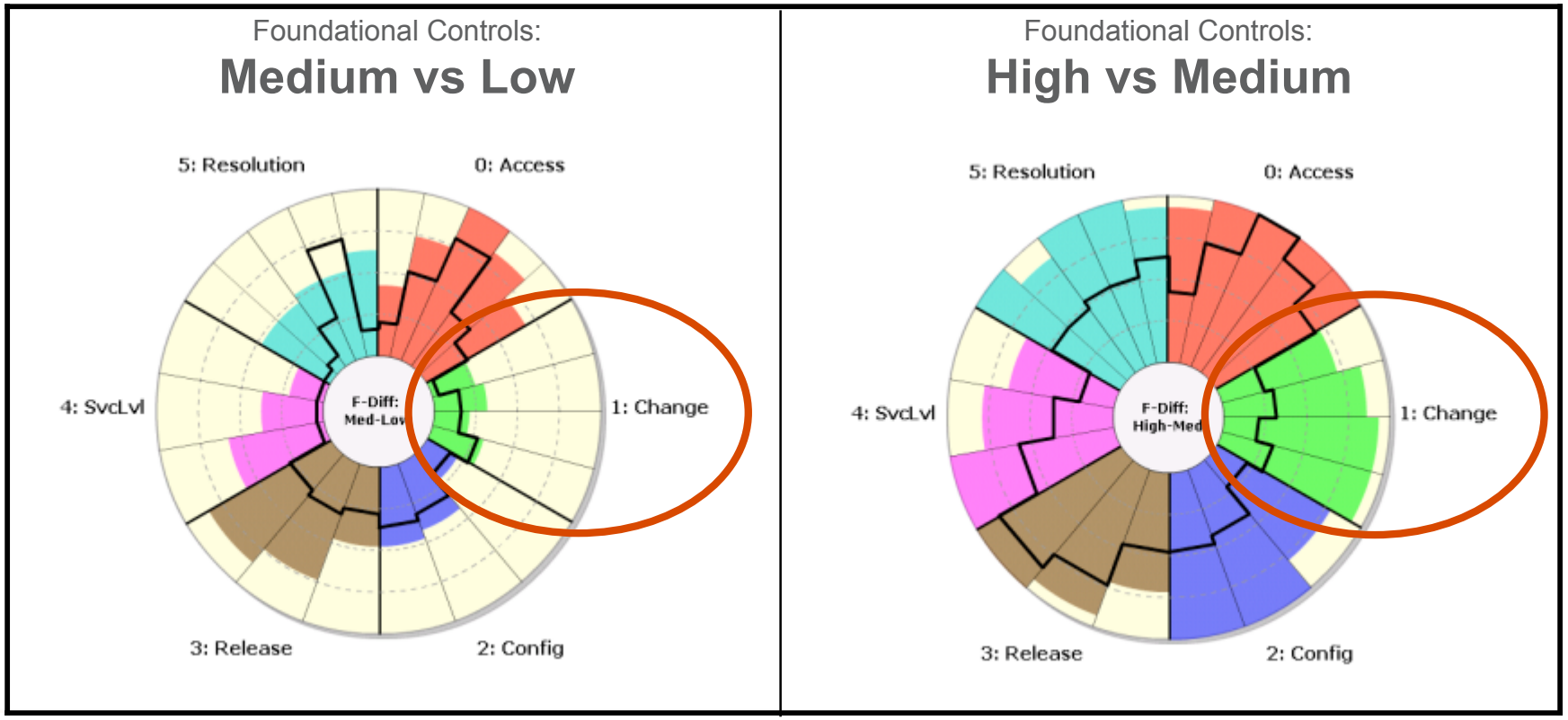
High performers also have 3x higher budgets, as measured by IT operating expense as a function of revenue

Source: IT Process Institute, May 2006

2006: Control Differences

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

2006: Three Clusters Of Respondents

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

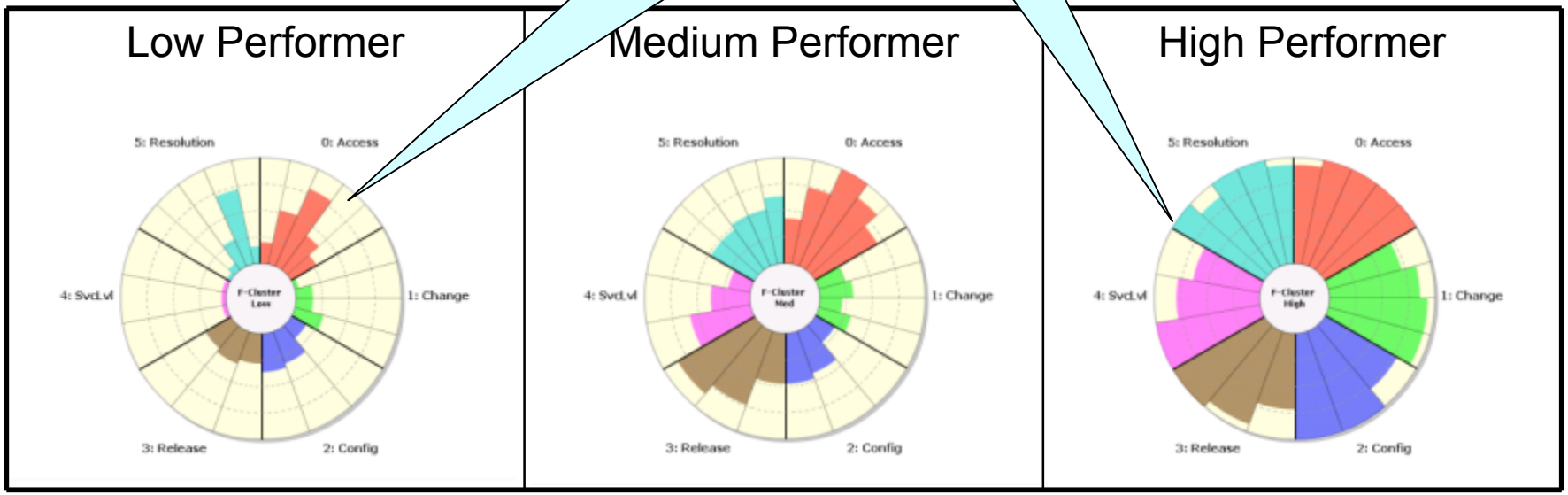
   Three clusters emerged.

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.

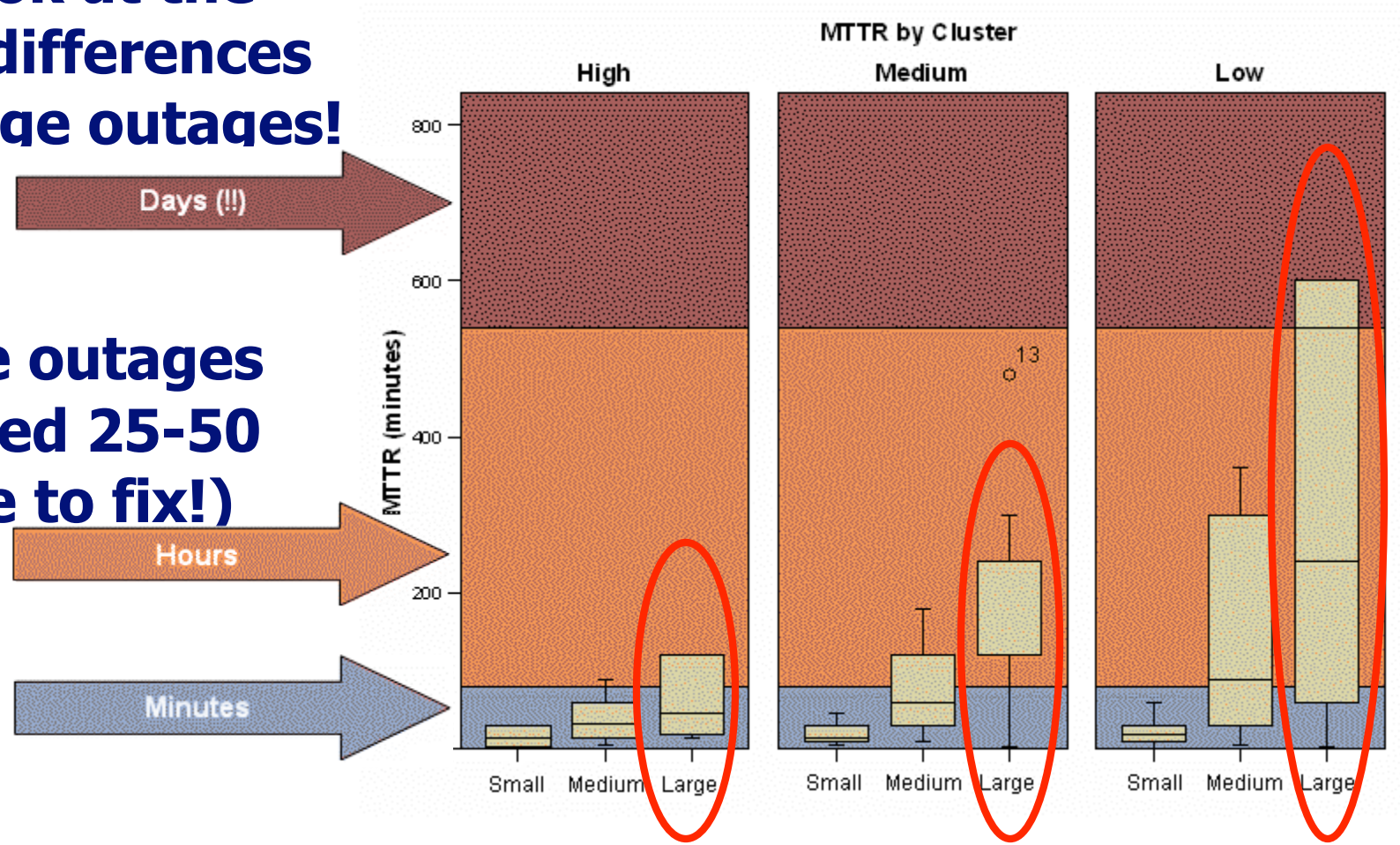


Source: IT Process Institute, May 2006

High Performers Can Bound Maximum MTTR

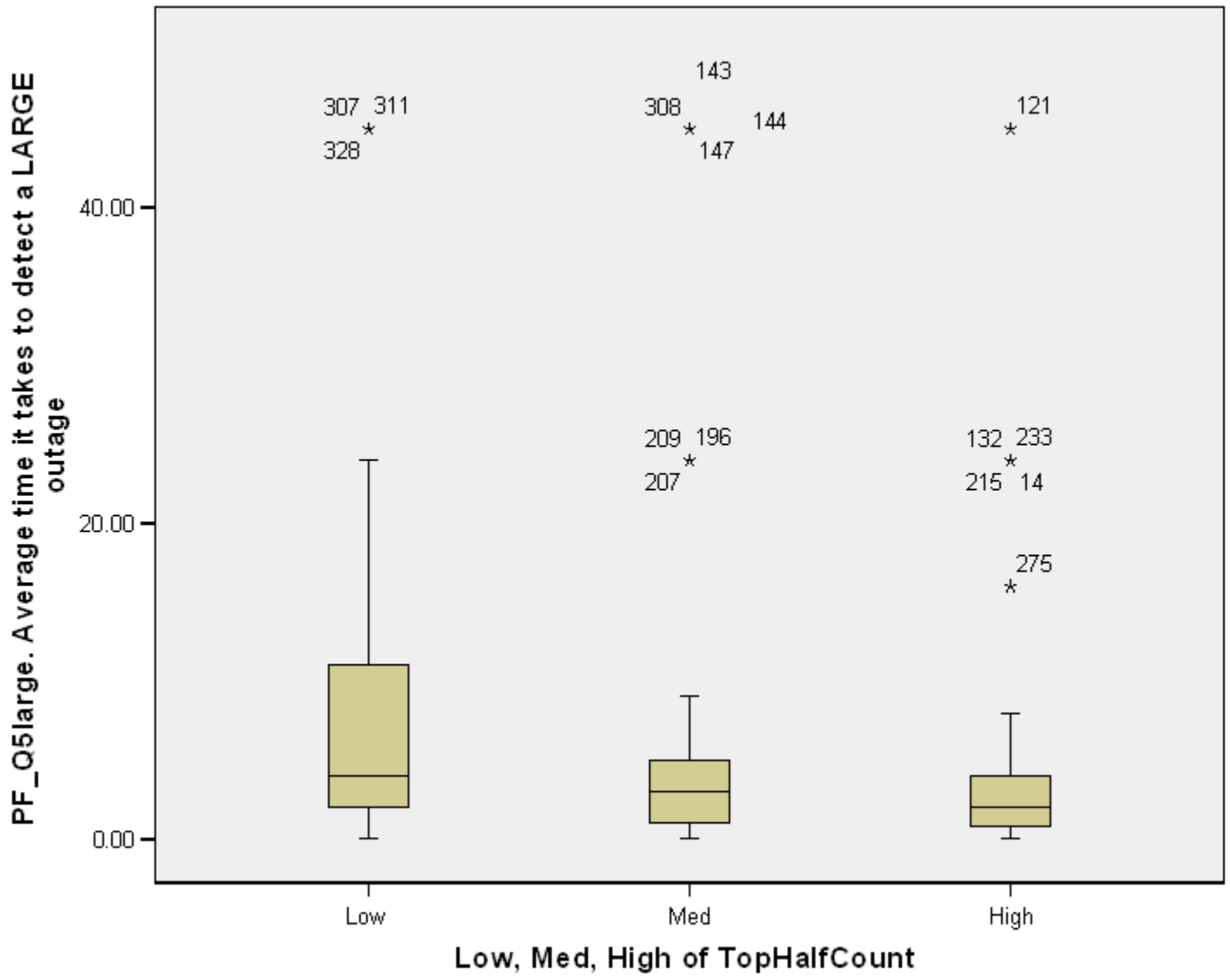
But look at the huge differences for large outages!

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

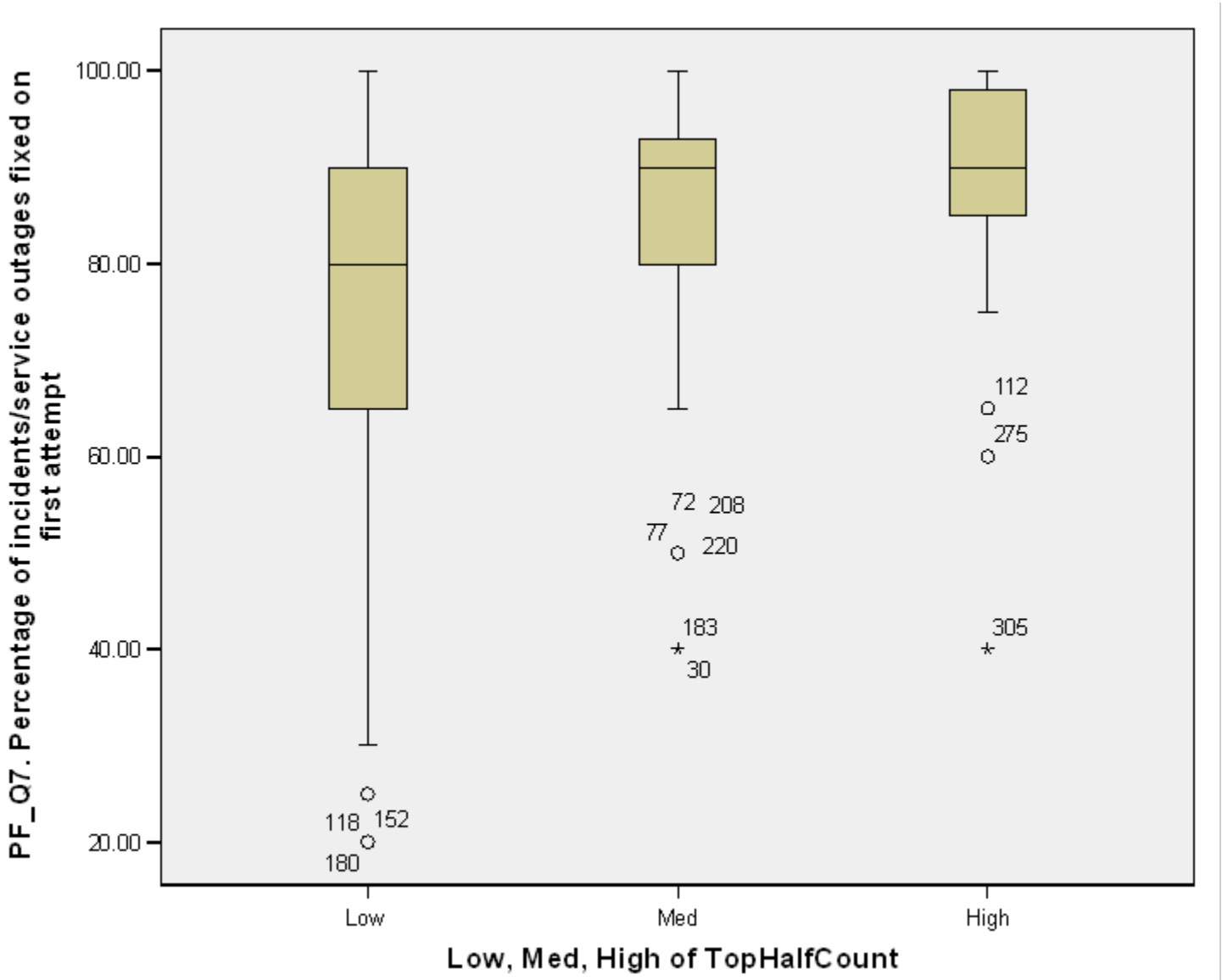


Source: IT Process Institute, May 2006

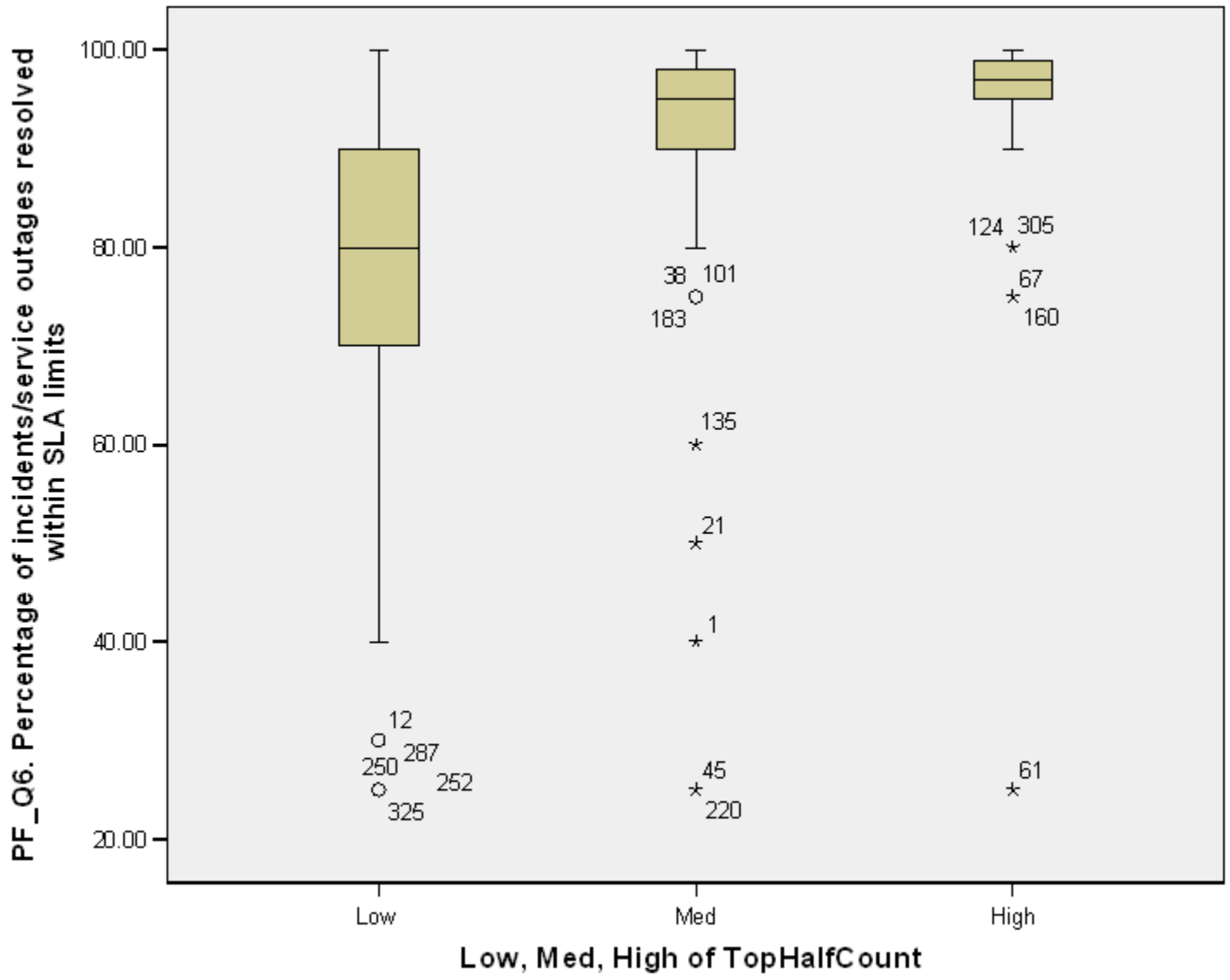
MTTR For Large Outages



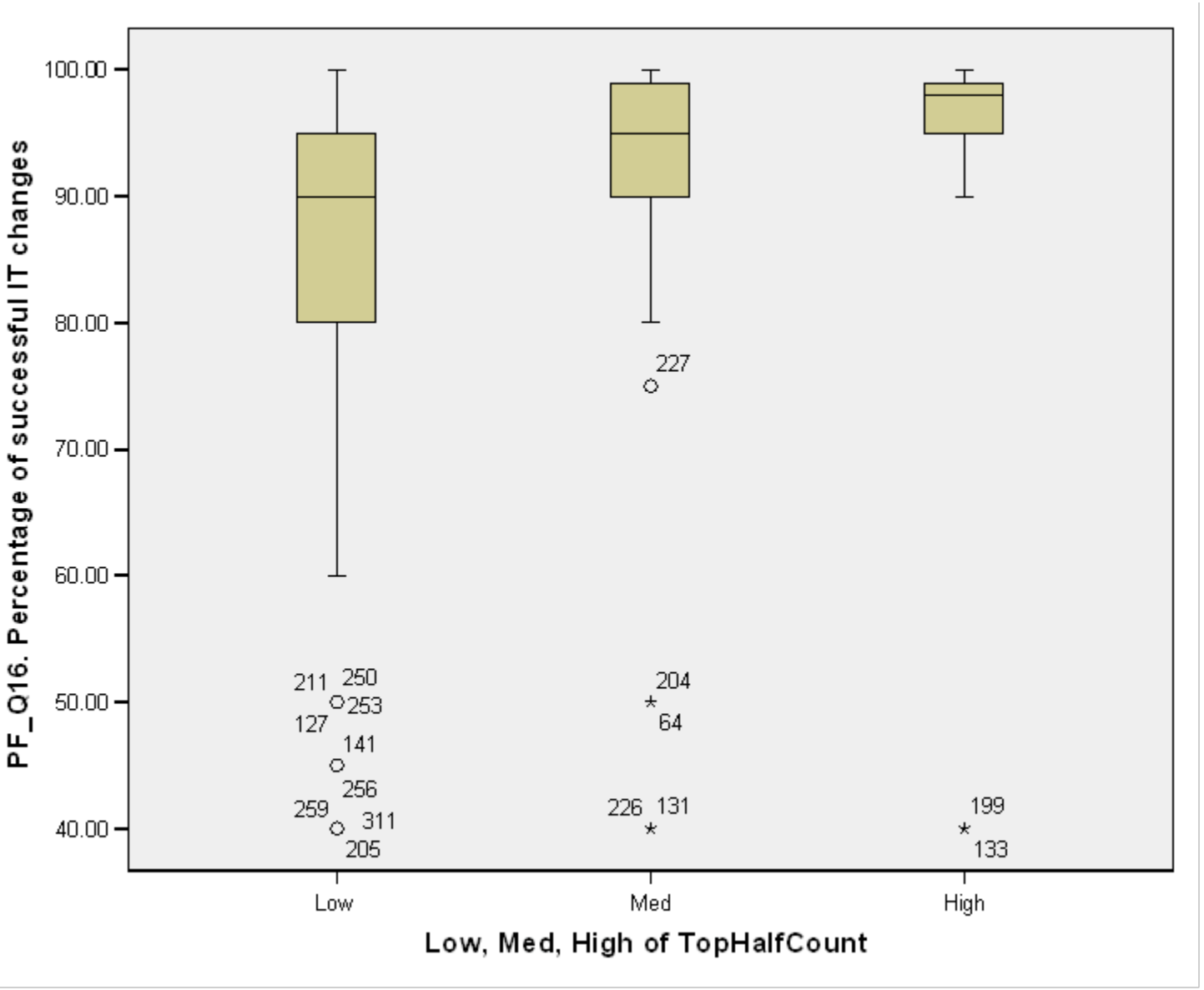
First Fix Rate



Percentage Of Outages Fixed Within SLA Limits



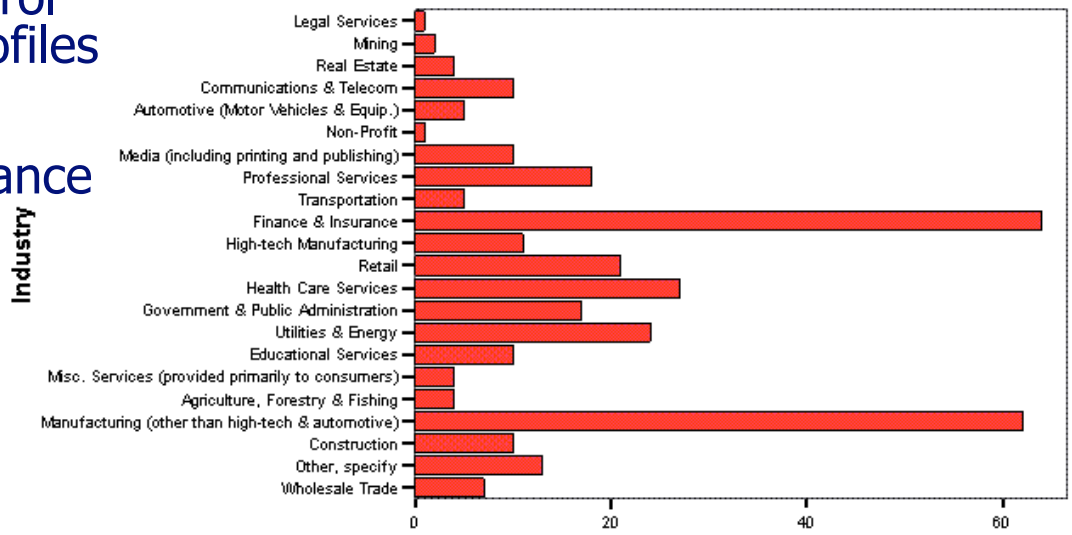
Change Success Rate



2007: Larger Repeat Benchmark With Even More Fascinating Results

- In 2007, the ITPI and the Institute of Internal Auditors repeated the benchmark
- 350 organizations were benchmarked
- Methodology:
  - Regression – no single relationship found
  - Clustering – 5 different clusters with similar control use and performance profiles
- Key Finding:
  - Controls impact performance differently at larger and smaller organizations

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)

2007: Larger Repeat Benchmark With Even More Fascinating Results

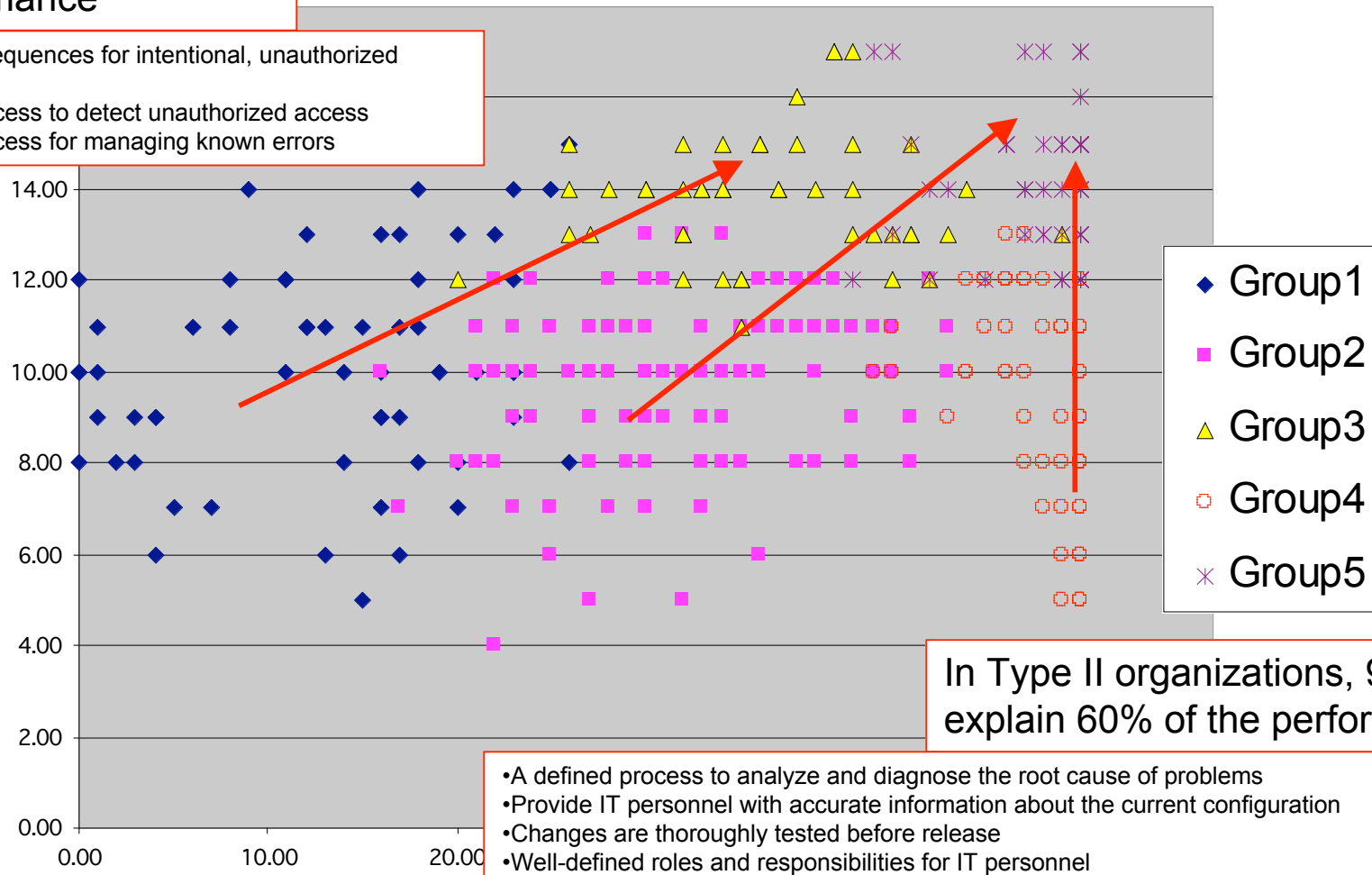
- In the first study, we asked "yes/no" questions for each of the 63 controls
- In the second study, for each control, we used a Likert scale question to determine the nature of the control
  - 0: Not used
  - 1: Documented, but not in use
  - 2: Documented, but only used inconsistently
  - 3: Used consistently, exceptions not detected
  - 4: Used consistently, exceptions detected
  - 5: Used very consistently, exceptions have consequences

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

2007: Overall Performance vs. Control Use

In Type I, 3 foundational controls explain 60% of performance

- Defined consequences for intentional, unauthorized changes
- A defined process to detect unauthorized access
- A defined process for managing known errors



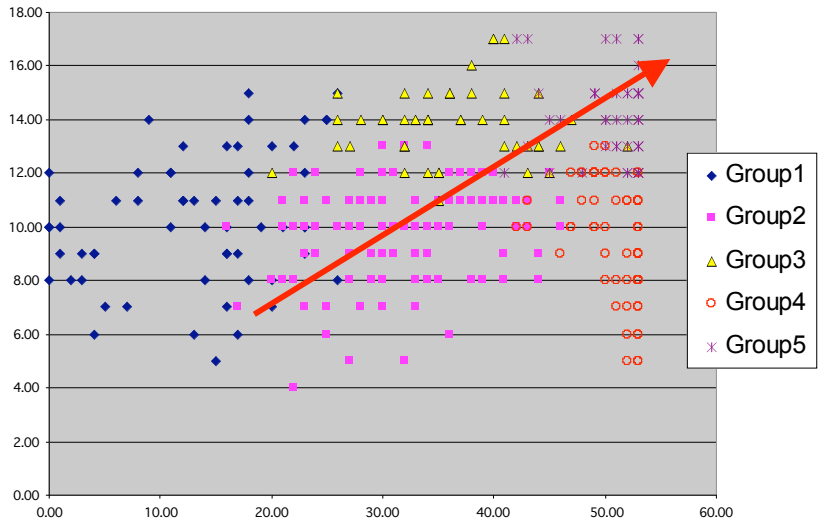
In Type II organizations, 9 controls explain 60% of the performance

- A defined process to analyze and diagnose the root cause of problems
- Provide IT personnel with accurate information about the current configuration
- Changes are thoroughly tested before release
- Well-defined roles and responsibilities for IT personnel
- A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents
- A defined process to identify consequences if service level targets are not met
- A defined process for IT configuration management
- A defined process for testing releases before moving to the production environment
- CMDB describes the relationships and dependencies between configuration items (infrastructure components)

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

2007: Surprise #1: Type 1 Organizations: 3 Foundational Controls

- What do they look like?
  - Smaller, less complex IT organizations
- Three essential foundational controls explain 60% of performance
  - Defined consequences for intentional, unauthorized changes
  - A defined process to detect unauthorized access
  - A defined process for managing known errors

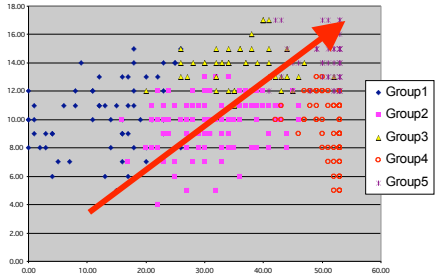


These controls seem familiar…

The controls indicate a **culture of change management** and a **culture of causality!**

2007: Surprise #2: Type 2 Organizations: 3 + 9 Foundational Controls

- What do they look like?
  - Larger, more complex IT organizations
  - More organizational handoffs around change
- Again, nine more foundational controls explain 60% of performance!
  - A defined process to analyze and diagnose the root cause of problems
  - Provide IT personnel with accurate information about the current configuration
  - Changes are thoroughly tested before release
  - Well-defined roles and responsibilities for IT personnel
  - A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents
  - A defined process to identify consequences if service level targets are not met
  - A defined process for IT configuration management
  - A defined process for testing releases before moving to the production environment
  - CMDB describes the relationships and dependencies between configuration items (infrastructure components)



Again, these controls seem familiar –

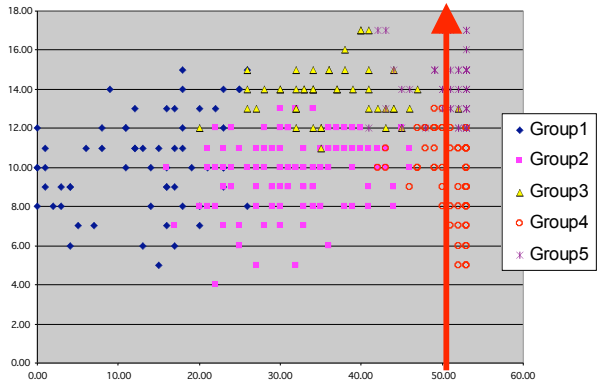
They seem to hint that for complex organizations, enforcing handoffs and accountability is required…

Surprise #3: Control Maturity - How you manage exceptions matters!

Which Type 2f organizations are "Smoking more, but enjoying it less?"

These are the organizations that where the number of foundational controls does not contribute at all to performance!

Why?



Average number essential foundational controls, based on level of use in count

Group 4 = 8.76
Group 5 = 8.40

Group 4 = 7.25
Group 5 = 7.90

Group 4 = 2.65
Group 5 = 4.68

Control Question Scale

0 – not used

1 – documented, but not in use

2: documented, but only used inconsistently

3 – Used consistently, exceptions not detected

4 – used consistently, exceptions detected

5 – used very consistently, exceptions have consequences

These are the organizations that detect process exceptions, but do not **enforce consequences!**

2006: Summary of Key Findings

1. Controls impact smaller and larger organizations differently
2. 3 foundational control predict 45% of performance variation in smaller organizations.
3. 9 foundational controls predict 60% of performance variation in larger organizations.
4. Organizations should monitor and manage process exceptions for foundational controls in order to achieve performance improvement.
5. Performance improvement potential is significant.

2007: Change, Config Release Study

- Build on IT controls study findings

- Objectives
  - Identify specific practices are responsible for performance improvement
  - Determine role of management and process as enablers of performance breakthrough
- Results
  - Study of 340 IT organizations
  - Release and configuration practices impact performance more than change management.
  - Process management and process culture also improve performance
- Deliverables
  - Full research report
  - Executive snapshot white paper
  - Executive interview summary paper
  - Benchmark

Statistical Analysis used to:

- Factor analysis - identify sets of practices commonly implemented together
  - 12 sets of common practice
  - 13 individual practices
- Regression analysis - identify "Key Performance Drivers" that predict top levels of performance
  - 7 sets of common practice predict performance variation
  - 5 sets of common practice do not predict performance variation

2007: Key Practices That Predict Performance

- Release and change processes and exception handling
- Process discipline and culture
- Standardized configurations
- Controlled access to production
- CMDB and change linkage

Closing Thoughts

- Key aha moments
  - It is easy to observe the 4-5x performance difference between high and low performers
  - Detection and recovery security metrics correlate with operations metrics
  - Entity level controls are just as important supervisory controls
  - Something is still missing to create imperative (compliance vs. security vs. operations)

- Limitations
  - We focused on IT general controls: substantiation over scoping
  - We didn't focus on the inputs/outputs of infosec and IT operations
    - Queue time
    - WIP
    - Rework