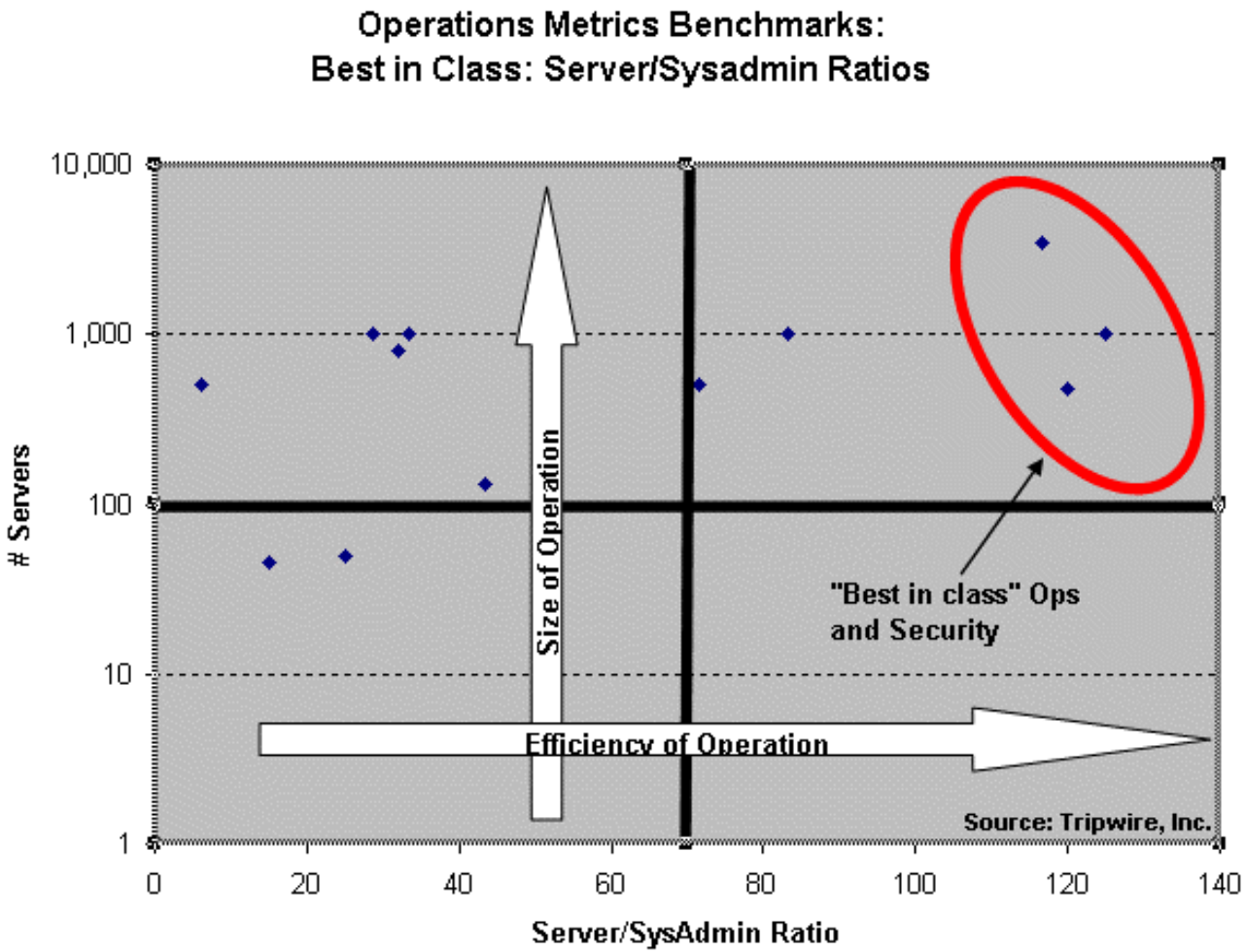
Visible Operations Methodology: Best Practices You Can Actually Use (And Love)

Gene Kim, CTO, Tripwire, Inc.
Kevin Behr, CTO, IP Services, Inc.

HP WORLD 2003
Solutions and Technology Conference & Expo

- Control is possible
- What's good for Security is good for Ops
- What's good for Ops is good for Security

Best In Class Ops and Security

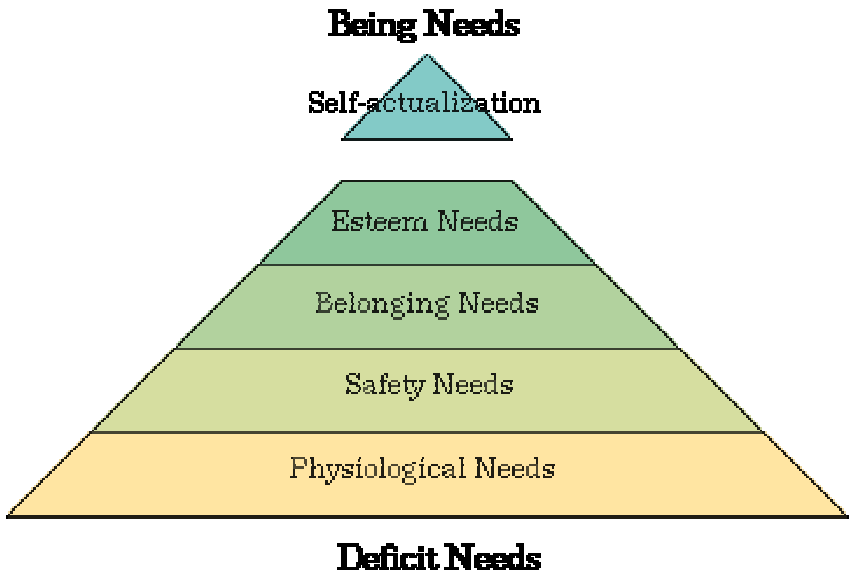


Best in class Ops and Security organizations have:

- Highest server/sysadmin ratios
- Lowest Mean Time To Repair (MTTR)
- Highest Mean Time Between Failures (MTBF)
- Earliest integration of Security into Ops lifecycle

Who is Maslow?

- Psychologist who created “hierarchy of needs” in 1950s
- Needs: Air >> Water >> Food >> Sex >> Happiness
- IT Capabilities: ?? >> ?? >> ??



Agenda

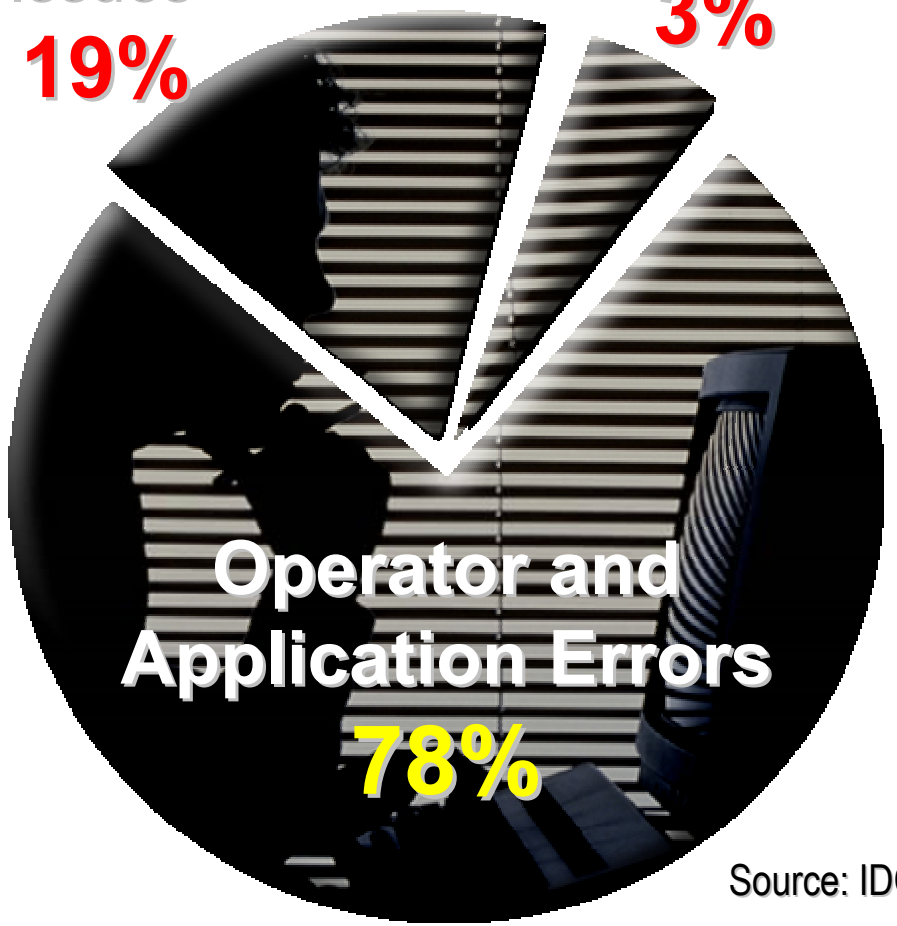
- The Problem
- What We Did About It
- The Resulting Methodology
  - Captured “best in class” operational processes
  - Increase control without reading phonebooks or increasing staff
- Measuring The Results
  - Assessing “actual practice” vs “best practice”
  - The IMCA interview process
- Works In Progress and Future Roadmap
- Call To Action
- Appendix: The Interview Process, Step By Step

The Symptoms

HP WORLD 2003
Solutions and Technology Conference & Expo

Causal Factors of IT Downtime

Percentage of Incidents



Source: IDC, 2001

The Problem: Humans

- IT lacks visibility of changes to servers and network devices that can affect the stability and availability of information services.
- Companies spend millions on change management systems – only to have them circumvented and never know it.
  - No ability to effectively manage undesired change
  - Further hindered by “urgent activities” such as security incident handling and patch management

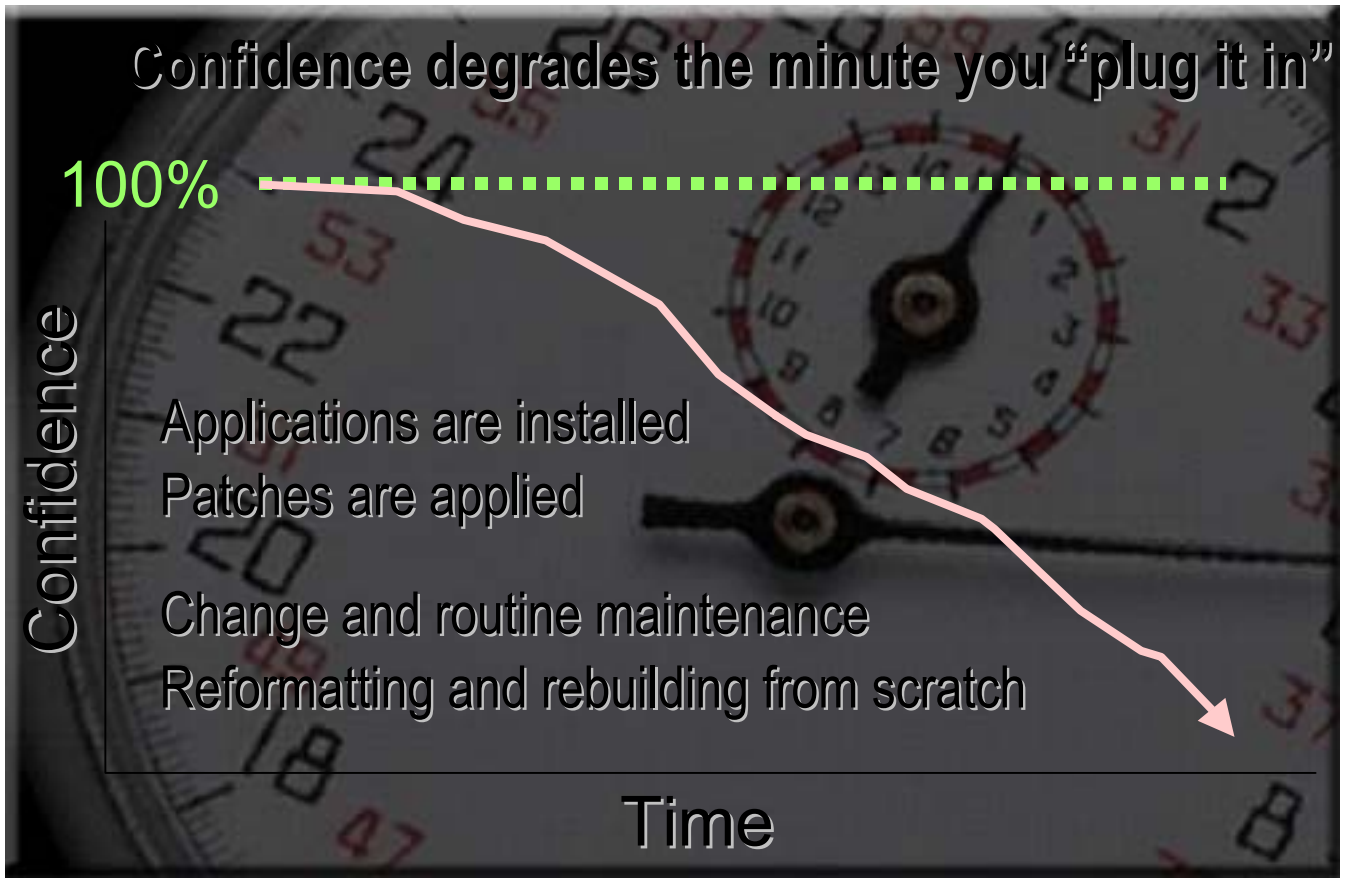
The Problem: Humans

- Many companies have developers maintaining production servers because of downsizing.
- Too often Security and Operations have an adversarial relationship
  - Ops may undo what Security puts in place.
  - Security breaks what Ops provisions trying to minimize risk.
- Documentation is not a traditional IT strength
  - Much of the critical knowledge on how things “really work” lives in a few very busy minds

The Problem: The Way We Work

- Up to 80% of problem resolution is spent determining the exact location and nature of the problem
- Firefighting consumes so much time – there is little or no accurate documentation of existing systems
- Golden builds are not standard practice; no two servers are the same
- Differences between “best and worst” results (Microsoft)
  - 20 x more Reboots
  - 5 x more Blue Screens (Crashes)

The Issue of "Integrity Drift"



A mail server suddenly becomes a DHCP server and a DNS server…

The "Best in Class" Playbook: Visible Ops Methodology

HP WORLD 2003
Solutions and Technology Conference & Expo

What we did about it – Visible*Ops*

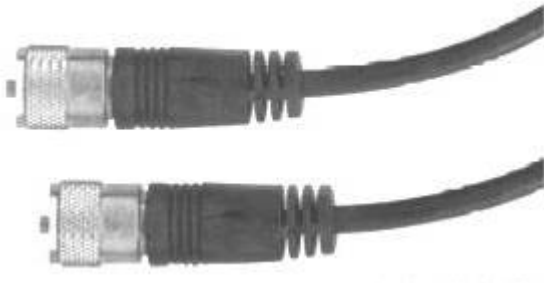
- Gene Kim and Kevin Behr studied many enterprise operations (a major trading company, The largest wireless carrier, a major stock exchange) and we began to note that these organizations had successfully implemented and benefited from preventive and detective control combinations.
- These controls were used to create audit points that made it easy to understand known good states.

Case Study: Major Stock Exchange

- Issues
  - Outages with long remediation times
  - Inconsistent system footprints in 1000+ servers running critical business process
  - Required to contain “configuration drift” during daily Operations

- Solution
  - Surgical integrity scans every 10 minutes for business continuity
  - Audit whether system footprints match “known, good state”
  - Enforce end-of-shift audit process

Case Study: Broadband/Cable Operator



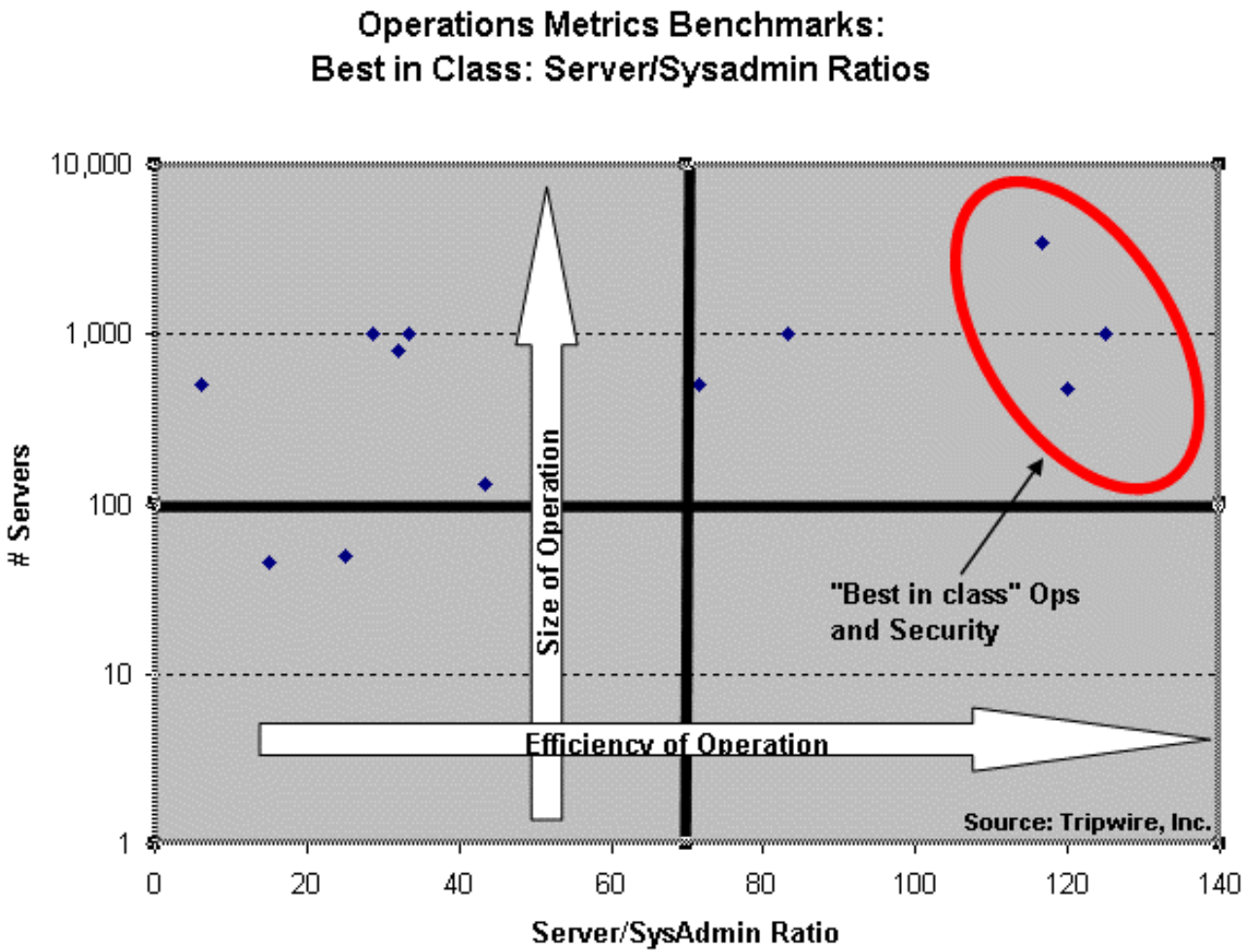
- Issues
  - Operations and Security groups making independent changes without adequate coordination
  - Change control processes were often circumvented
  - Thrash and inappropriate changes impacting service delivery

- Solution
  - Ops and Security groups meet each week in change management meetings to review all changes
  - Change audit reports integrated into Ops EMS, and alerts 2nd level Ops engineers and Security groups

Case Study: Content Distribution Network

- Issues
  - Low server-to-sysadmin ratios, high thrash, high remediation times
  - Developers making changes on production boxes, many undocumented changes, resulting in loss of repeatable builds
- Solution
  - Move to “fusebreaker” methodology: remediation process is almost always “unplug, reprovision new server”
  - Tripwire detects configuration changes prompting remediation process
  - Tripwire ensures that “fuse replacement” always has predictable behavior
  - In this scenario, junior staff can remediate, while senior staff work on process and technology improvements

Best In Class Ops and Security



Best in class Ops and Security organizations have:

- Controls are embedded in the IT Operations and Security processes
- Spending more time in "planned work" instead of "unplanned demand work"
- Effective use of detective controls

The Analysis

HP WORLD 2003
Solutions and Technology Conference & Expo

What we did about it

- We also began to see that if the infrastructure state was understood early on in the problem management cycle the time it took to accurately determine the nature of the problem could drastically be reduced.
- We would be able to stop many inappropriate and costly over-escalations if we could rule out change as early as possible.

What we did about it

- Best in class operations had bounded remediation times for critical infrastructure.
- In order to have valid golden builds to accomplish this the change management process must have more teeth than just the “honor system”.
- These organizations also displayed the earliest integration of security in to the Ops lifecycle

Why Did We Use ITIL?

- All of the best in class Operations organizations built their own methodology, primarily from institutional memory and Darwinistic practices
- Each Ops organization had different names for common practices (e.g., Work Authorization Request, Change Management System, Change Control System)
- We needed a way to normalize these practices, to find which ones led to best in class characteristics!

The ITIL and IMCA

HP WORLD 2003
Solutions and Technology Conference & Expo

What is ITIL?

- Compiled IT best practices, collected from thousands of IT and data center professionals
- Designed to help IT operations increase service levels and decrease cost
  - ComputerWorld 10/7/2002: Proctor & Gamble reports saving $125 million per year on IT cost savings (10-15% of annual IT budget)
  - Boeing, Caterpillar, Shell Oil, IRS,

Who is Using ITIL?

- Widely used in Europe, but gaining acceptance in the U.S.
  - 10,000 companies have adopted ITIL for management practices
  - 40,000 certified professionals (7500 added per year)
- Infrastructure vendors and IT consulting practices moving to ITIL terminology
  - HP OpenView, CA UniCenter, IBM Tivoli, and Remedy
  - HP, IBM, and Microsoft consulting all based on ITIL methdologies

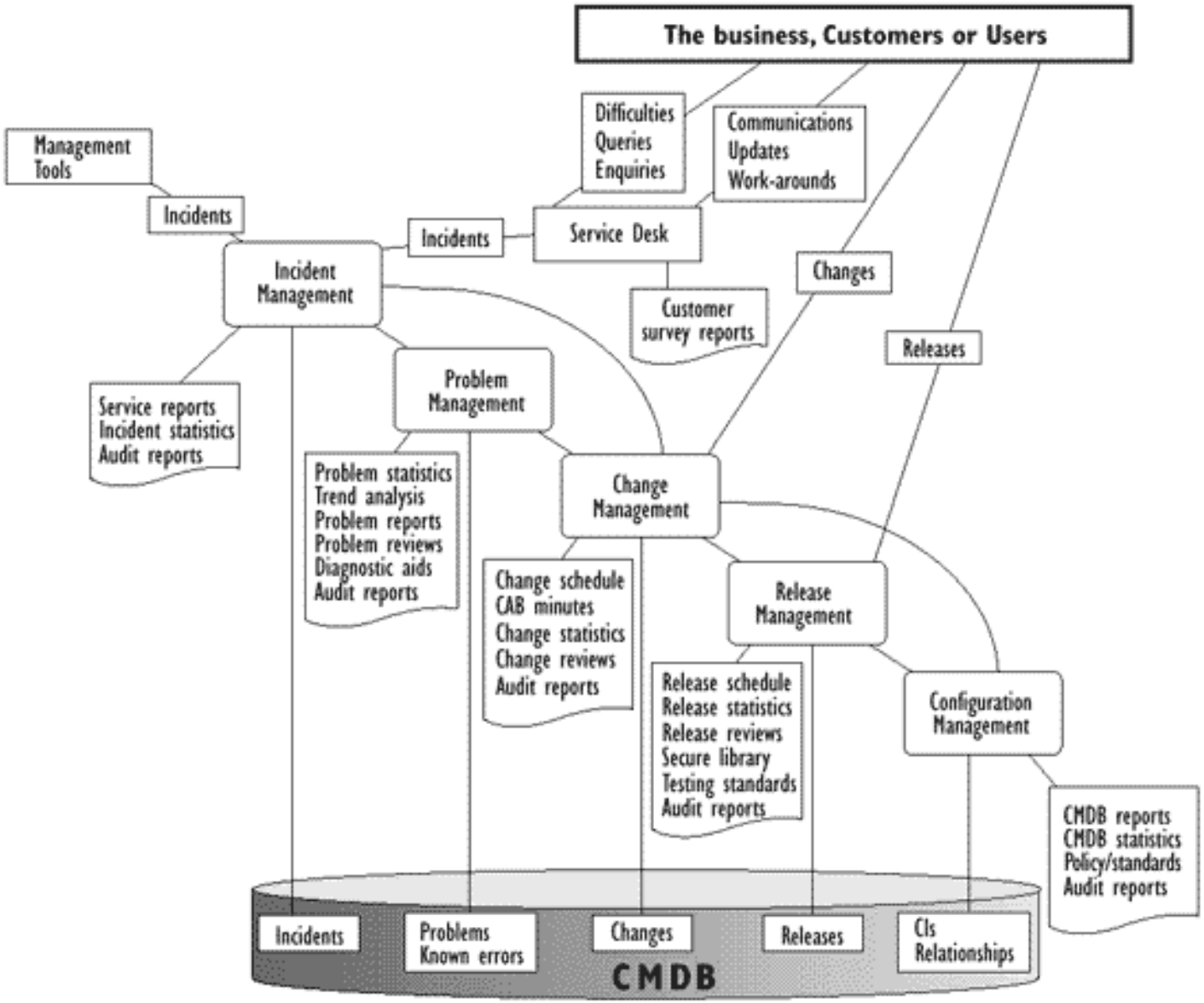
Where did ITIL come from?

- British Office of the Crown Government created ITIL in 1989
  - - Same organization that wrote ISO17799 (BS7799)
- They realized Ops best practices have never been documented, and created ITIL (IT Infrastructure Library) and BS15000 to describe world-class Ops processes

Why ITIL is Scary

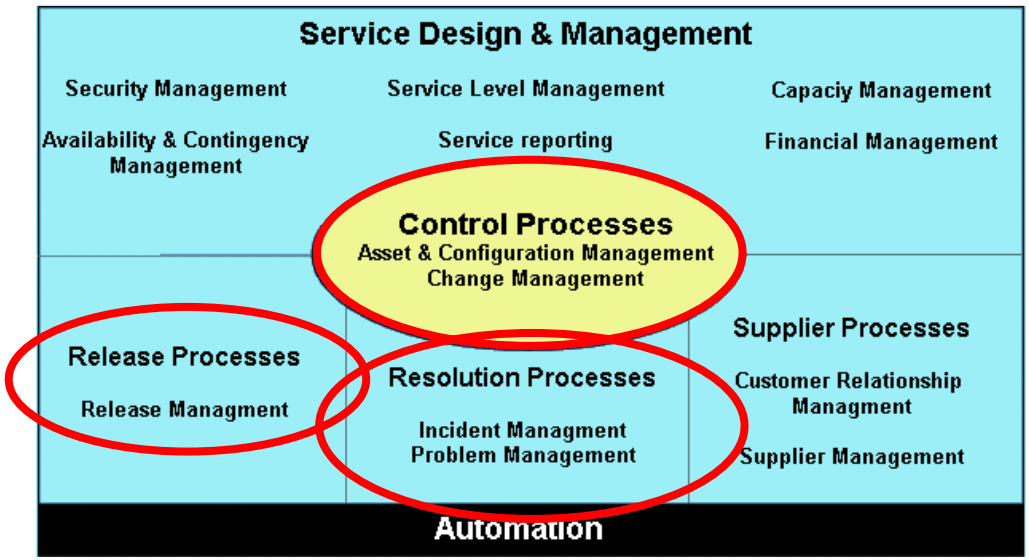
- ITIL is huge
- ITIL is like reading a phone book
- Adopting ITIL is perceived to be like adopting ISO 9000

ITIL Is Comprehensive and Big



IMCA Is Effective

- IMCA assesses assurance of IT operational controls, which hinges on effective change management processes
- Focuses on critical control areas:
  - Release Processes
  - Control Processes
  - Resolution Processes



ITIL Key Processes

- Service Support
  - Change Management: Approval body and process area that controls all change
  - Configuration Management: Librarian function that records all changes and relationships
  - Release Management: Responsible for the rollout of any new software and or hardware
  - Service Desk: The central contact point for all users and service personnel
  - Incident Management: The guardians of tickets and the record keeping around incidents
  - Problem Management: Concerned with resolving unknown errors and turning them into known fixes for inclusion in the CMDB

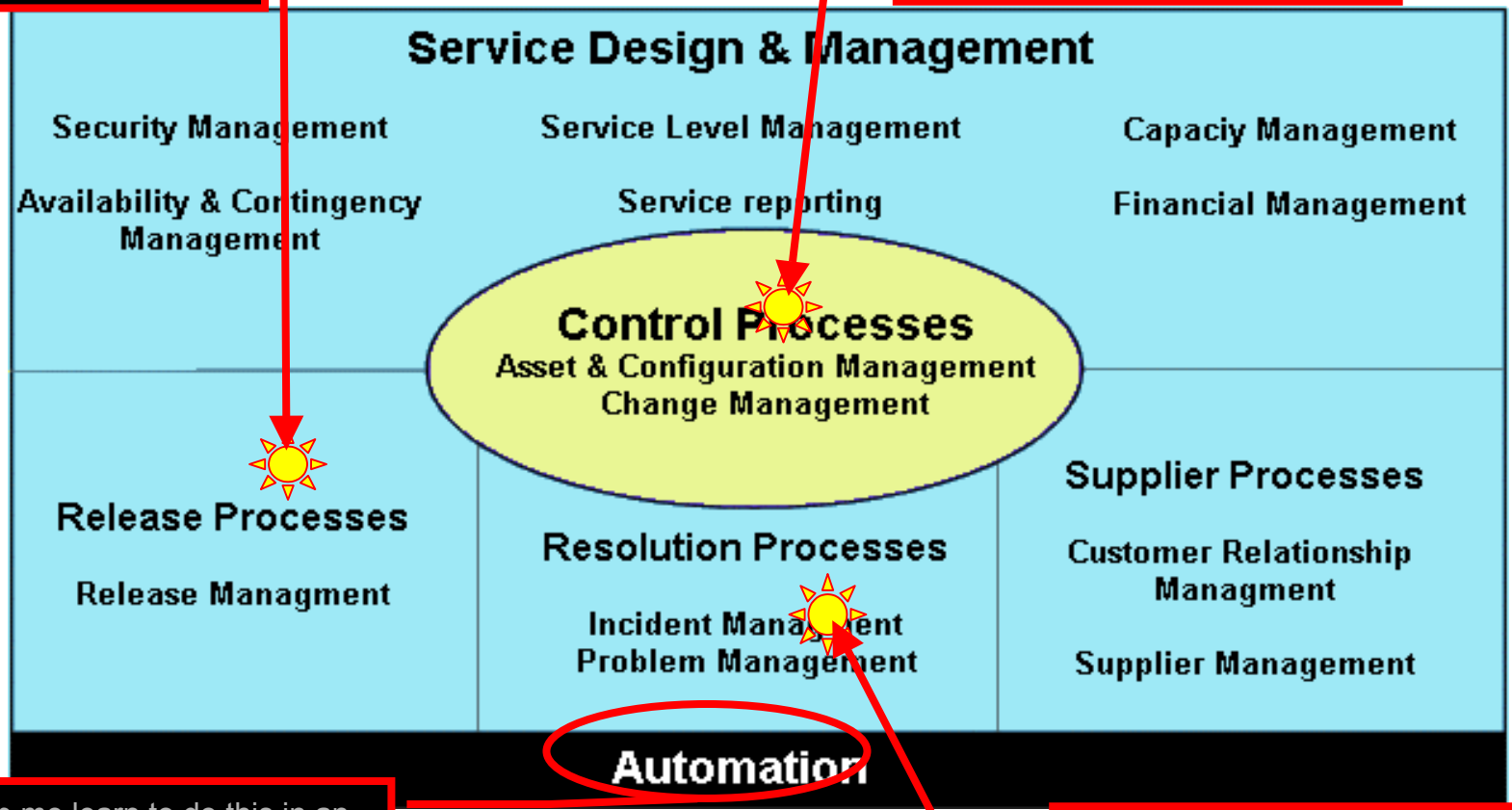
How We Did It

HP WORLD 2003
Solutions and Technology Conference & Expo

Where Is The Leverage?

Ensure that I have predictability around what goes into production

Ensure that I can control changes in my world in the production environment



Help me learn to do this in an automated fashion.

Equip me to deal with problems efficiently and feed the results back into my environment

Process Area Objectives

- Release Management
  - Ensure that provisioned systems match the “known, good build”
  - Promote repeatable builds for all configurations
- Control Processes
  - Ensure that changes can be traced to a valid business reason
  - Create a control point, where Ops, Dev, or Security can so stop a change from occurring
  - Control configuration drift and uncontrolled changes
- Incident Management / Resolution
  - Decrease MTTR (mean time to resolve) outages
  - Increase “culture of causality,” allowing better diagnosis and problem management practices

How we did it – Stabilize the patient

- Attack the 80%. Stop the bleeding caused by: change drive-bys ,integrity drift and changes made during firefighting.
- We used the combination of a preventive control (don't touch that fence it's electric!) and a detective control (why did you touch the fence at 2:11 am on March 3rd?) to get a handle on the state of every piece of critical infrastructure.

How we did it – Catch and Release

- We caught and foot-print audited all critical infrastructure configurations in the wild.
- We created golden builds for these devices.
- We tested and set bounded remediation times for all critical infrastructure.
- We determined audit frequency and methods necessary to support these times .

How we did it – Manage the Change

- Instituted a Change Advisory Board- Stake holders include: Security Lead ,Ops Systems Engineering Lead, VP of Operations , Service Desk Manager, Director of Network Operations, and Internal Audit.
- Made weekly change management meetings mandatory for all CAB members.
- Implemented a Change Transaction Process to make the correct path : Request For Change (RFC)

How we did it – Managing Change

- All RFC are categorized based on a 1-4 severity system. Anything above a 2 goes to the CAB for review and comment.
- Changes can only be administered during maintenance windows and must be approved and scheduled by the CAB.
- Urgent changes trigger an emergency CAB meeting.

How we did it - First Response

- Modified the problem management process to eliminate change as early as possible by identifying the assets directly involved in the ticket and auditing them against their configuration baseline for the last 72 hours. All changes found are attached to the ticket.
- If no changes are found the circle is widened to include changes made to infrastructure supporting the target systems.

Measuring The Results: The IMCA

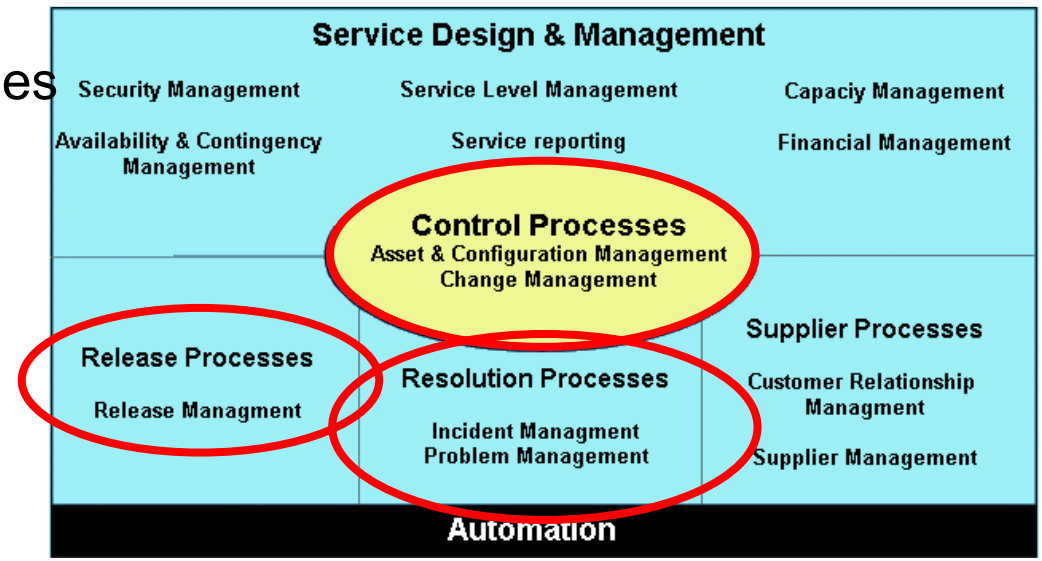
HP WORLD 2003
Solutions and Technology Conference & Expo

IMCA: All Intellectual Property Donated to Non-Profit

- Motivation was a Harvard Business Review article – in a one-hour plant walkthrough, a manufacturing process consultant can estimate quality, supply chain, inventory levels, etc.
- Our goal was to create something similar, using only a one-hour interview
- IMCA is an active research project in progress, now involving Software Engineering Institute, SANS, Institute of Internal Auditors, National Association of Corporate Directors, and more…

Measuring the results - The IMCA

- Based on IT Infrastructure Library (ITIL) / BS 15000 standards and the Visible Ops methodology
- An interview-fueled process with a standardized scoring methodology
- Focuses on high leverage areas:
  - Release Processes
  - Control Processes
  - Resolution Processes



IMCA Measures Controls Assurance

IMCA assesses:

How strong is your change transaction and approval process? Can you map changes to authorized order? Can you assure that systems are in a "known good state?"

Can you capture the "known good state?" Do you have good processes for deployment?

Operational Excellence ?	Overall Operational Excellence: ?			
Control Processes: Overall ?	Change Transaction Processes ?	Change Management Integrity and Accountability ?	Configuration Management Footprint Audits ?	Other Capabilities ?
Problem Management Processes: Overall ?	Problem Management Evidence Chain ?		Rollback Capabilities ?	Other capabilities ?
Release Management Processes: Overall ?	Repeatable Builds ?		Acceptance Process ?	Other capabilities ?
Security ?	Security ?			

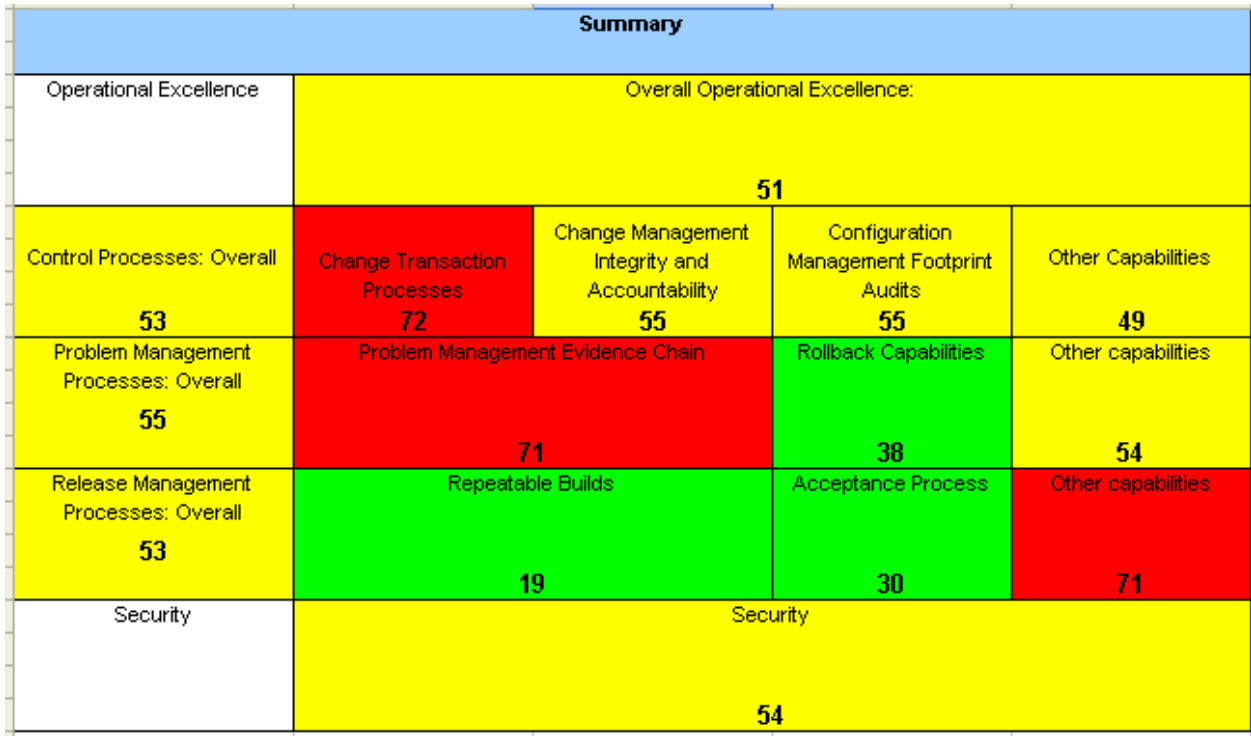
IMCA Measures Controls Assurance

An example of “best in class” operation, with ability to have high controls reliance.

Summary				
Operational Excellence	Overall Operational Excellence: 38			
Control Processes	Change Transaction Processes 42	Change Management Integrity and Accountability 22	Configuration Management Footprint Audits 10	Other Capabilities 40
Problem Management Processes	Problem Management Evidence Chain 35	Rollback Capabilities 58	Other capabilities 15	Other Capabilities 35
Release Management Processes	Repeatable Builds 44	Acceptance Process 38	Other capabilities 45	
Security	Security 38			

IMCA Measures Controls Assurance

An example operation with unacceptable controls reliance.



Summary				
Operational Excellence	Overall Operational Excellence: 51			
Control Processes: Overall 53	Change Transaction Processes 72	Change Management Integrity and Accountability 55	Configuration Management Footprint Audits 55	Other Capabilities 49
Problem Management Processes: Overall 55	Problem Management Evidence Chain 71		Rollback Capabilities 38	Other capabilities 54
Release Management Processes: Overall 53	Repeatable Builds 19		Acceptance Process 30	Other capabilities 71
Security	Security 54			

IMCA Measures Controls Assurance

An example operation with unacceptable controls reliance.

Summary				
Operational Excellence	Overall Operational Excellence: 70			
Control Processes	Change Transaction Processes 89	Change Management Integrity and Accountability 64	Configuration Management Footprint Audits 70	Other Capabilities 69
Problem Management Processes	Problem Management Evidence Chain 83	Rollback Capabilities 78	Other capabilities 72	
Release Management Processes	Repeatable Builds 72	Acceptance Process 75	Other capabilities 72	
Security	Security 64			

IMCA Creates Prescriptive Diagnosis

- IMCA creates a 20 page report, providing Strengths, Risks and Rewards for the three process areas
- For areas identified that undermine controls assurance, IMCA creates prescriptive plan to augment or bootstrap necessary controls

Reliability and Validity of IMCA

- Validity measures
  - Based on IT best practices frameworks of ITIL and BS15000
  - Questions are scored on the integrity of three key ITIL processes
- Reliability measures
  - All answers are subjective, and can vary from day to day
  - All answers do not have any quantitative significance (i.e., arithmetic operations cannot be done on the answers)

Measuring the results- Other Metrics

- Number of changes made in data center
- Number of changes that map to authorized business reason
- Number of times change management system was circumvented
- Percent of outages caused by change
- Number of changes that obsolete repeatable builds
- Ops “clean shift handover” success rate

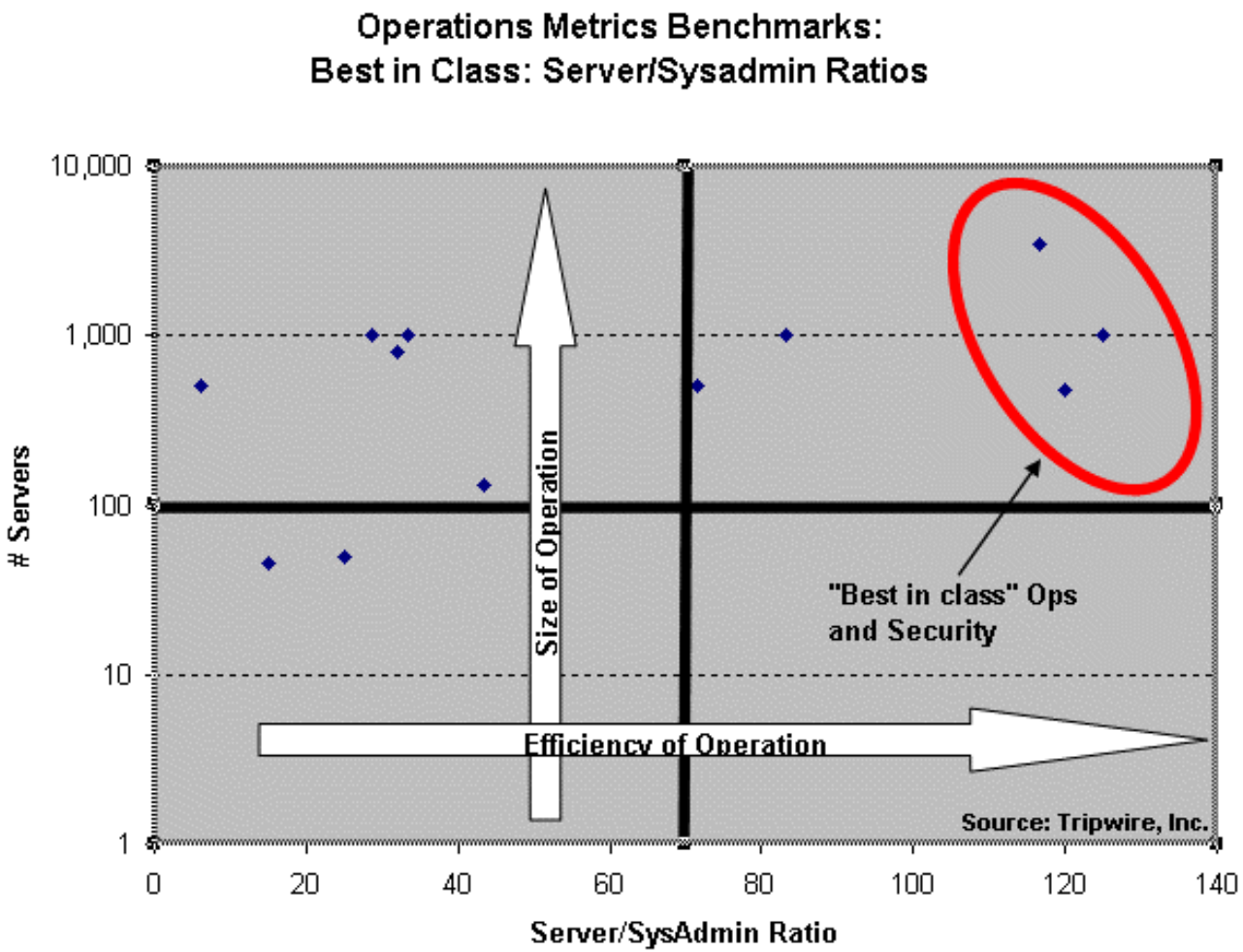
Measuring the results- Other Metrics

- Time to provision known, good build
- Number of fixes/turns to match known, good build
- Percentage of deployed systems that match known, good build
- Percentage of deployed systems that have security sign-off

Measuring the results- Other Metrics

- Outage and issue Mean Time To Repair (MTTR)
- Aggregate outage downtime
- Number of inappropriate escalations
- Increased change success rate
- Increased systemic Mean Time Between Failure
- Smile to frown ration on Ops, Security and Audit staff

Control Is Actually Good For The Business



Best in class Ops and Security organizations have:

- Highest server/sysadmin ratios
- Lowest Mean Time To Repair (MTTR)
- Highest Mean Time Between Failures (MTBF)
- Earliest integration of Security into Ops lifecycle

Bootstrapping Controls Into IT Operations: After The IMCA Assessment

HP WORLD 2003
Solutions and Technology Conference & Expo

The Textbook Example of IMCA Process

- IMCA often uncovers Ops controls reporting issues
- With Ops executive sponsorship, IMCA creates:
  - Collective will to solve the controls issues
  - Buy-in across Ops, Security, Audit, and Management that increased controls will not only remedy audit issue, but will also improve business service levels, relevant reporting, and quality of life
- IMCA is often very effective when combined with a consultative and technical proposal

Example Customer Issues

- Extremely low controls reliance
  - Ineffective change management system (“management by belief” vs. “management by fact”)
  - Inability of Ops executive to prevent cross-organizational boundary incursions (e.g., developers making unauthorized changes)
- Poor service levels
  - High number of protracted outages
  - Ever increasing amount of firefighting

Example Customer: Before Stabilization

Summary				
Operational Excellence	Overall Operational Excellence: 49			
Control Processes: Overall 46	Change Transaction Processes 27	Change Management Integrity and Accountability 50	Configuration Management Footprint Audits 60	Other Capabilities 47
Problem Management Processes: Overall 59	Problem Management Evidence Chain 94		Rollback Capabilities 43	Other capabilities 56
Release Management Processes: Overall 43	Repeatable Builds 47		Acceptance Process 60	Other capabilities 39
Security	Security 41			

Recommendations

- Phase I
  - Stabilize and monitor: Insert detective controls in infrastructure to enforce change management policies:
  - Integrate and correlate: Connect integrity management systems to notification and escalation systems, to allow quick problem management
    - Integrate with Remedy Helpdesk system that drives their change transaction workflow

Recommendations

- Quick implementation of controls and reporting in the change management processes
  - Measure changes made on production infrastructure
  - Ensure that all changes map to an authorized work order by integration with change workflow system
- Creates report on the assurance of change management systems
  - Number of changes that circumvented the change management systems
  - Number of systems in “known good state”
  -

Example Customer: After Stabilization

Summary				
Operational Excellence	Overall Operational Excellence: 39			
Control Processes: Overall 36	Change Transaction Processes 14	Change Management Integrity and Accountability 33	Configuration Management Footprint Audits 30	Other Capabilities 41
Problem Management Processes: Overall 39	Problem Management Evidence Chain 50		Rollback Capabilities 33	Other capabilities 38
Release Management Processes: Overall 41	Repeatable Builds 47		Acceptance Process 60	Other capabilities 35
Security	Security 34			

Recommendations Roadmap

- Note that Phase I fuels all the future phases
- Phase II
  - Augment existing footprint and configuration audits: Ensure post-deployment system integrity to ensure all systems are in a known, good state
    - Capture known, good state in the release management processes (pre-production environment)
  - Augment release management systems: Create harder acceptance processes, and increase scope and automation in repeatable build systems
    - Create additional control points as part of the Ops/R&D acceptance process

Recommendations Roadmap

- Phase III and Beyond
  - Process improvement and metrics generation: Generate metrics to allow continual process improvement

Value to Example Customer

- Enforce change management process integrity
- Decrease firefighting and increase proactive controls
- Avert revenue loss due to unplanned outages
- Decrease Mean Time To Repair by efficient problem management processes
- Create hard organizational change boundaries for accountability and responsibility
- Establish beach head for operational best practices, allowing future process improvement

What You Have Built

HP WORLD 2003
Solutions and Technology Conference & Expo

What you have built - You Can Now:

- Enforce change management process integrity
- Decreased firefighting and increase proactive controls
- Avert revenue loss due to unplanned outages
- Decrease Mean Time To Repair by efficient problem management processes
- Create hard organizational change boundaries for accountability and responsibility
- Establish a beach head for operational best practices, allowing future process improvement

What you have built

- You now can measure and articulate the business benefit of process improvement efforts
- You can target weak areas for quick wins
- Regain the confidence of the business by showing off your new and improving metrics
- Fend off IT Budget Jenga with your CFO and CEO by showing where money needs to be invested and why.

Contact Information

- Gene Kim, CTO, Tripwire, Inc.
  - *genek@tripwire.com*
- Kevin Behr, CTO, IP Services, Inc.
  - *kevin.behr@tcpipservices.com*

Call To Action

- To find out more about IMCA, go to http://www.tripwire.com/imca
- To get an IMCA assessment, email mailto:imca@tripwire.com

Work In Progress and Future Roadmap

HP WORLD 2003
Solutions and Technology Conference & Expo

Works In Progress

- Benchmarking Best In Class Ops and Security
  - Gene and Kevin are working with SEI (home of CMM) to gather best in class organizations for benchmarking activities.
  - Will be discussing mapping their practices against Visible Ops, as well as Six Sigma style variance reduction
- Mapping to Six Sigma
  - Leverage Six Sigma notions of “cost of quality” as percentage of revenue (compare to OpEx?)

Works In Progress

- Mapping to COBIT and ISO17799
  - Organizations desire to map IT Operational processes to ITIL and BS7799
  - Security organizations and auditors desire to map controls into COBIT and ISO17799
  - Working group is tackling the mapping problem
- Mapping to Sarbanes-Oxley as potential Controls Self Assessment
  - Requirements needed to attest the assurance of controls overwhelms internal and external auditors
  - IMCA measures the controls and can be used to provide assurance and reporting on controls

Works In Progress

- Evangelizing in Practitioner Roundtables
- Identifying and collaborating with communities of knowledge
  - SANS, Institute of Internal Audit, National Association of Corporate Directors, ISACA, Palmer Group, CIS
- Identifying repositories of knowledge
  - University of Oregon Decision Sciences Research grant
  - AFCOM, IBM SHARE, itSMF

Call To Action

- Familiarize yourself with ITIL and BS15000 body of knowledge
  - BS15000 diagram is a phenomenal way to view IT Operations
- Anyone interested in working together on some of these projects?
  - IMCA assessments and benchmarking
  - Documenting how to implement security objectives in ITIL framework

Appendix: Overview of the Questions

HP WORLD 2003
Solutions and Technology Conference & Expo

The Interview and Questions: Intent

- Questions are intended to uncover pain and provoke thought
- Create appropriate “tone from the top” to get candid answers and collective problem-solving
- With the right people in the room, questions generate:
  - Nervous laughter
  - Outright hilarity
  - Uncomfortable VPs

Example Questions: General

- Uncover pain
  - Our system administrators spend too much time fire fighting.
  - Our IT department is understaffed to support existing workloads.
  - We have a well-documented change control policy.
  - We have calculated the cost of downtime.
- Uncover new anxieties
  - We have identified and documented the servers and data that are most critical to supporting our business.
  - All changes to production are mirrored in the fail over site.

Example Questions: Problem Resolution

- Uncover pain
  - The longest part of our repair cycle is diagnosing what's wrong.
  - We can quickly detect what changed on systems during problem resolution.
  - We can track who made a specific change.
- Uncover new anxieties
  - During remediation, we can see all authorized work orders pertaining to a target system.
  - We track the change success rate.
  - We have a process that maps all changes to a valid business purpose or authorized work order.

Example Questions: Security

- Uncover pain
  - Security reviews all configurations and change requests before they are deployed into production.
  - We experience "patch and pray" dilemmas, where applying patches have dramatically inconsistent results.
- Uncover new anxieties
  - Security attends all change control meetings.
  - Security has the right to veto any changes made on production systems.
  - We can accurately track the patch level of all of our servers.
  - When our security solutions generate alerts, we often don’t know what the true impact to the target host is.

Example Questions: Release Processes

- Uncover pain
  - We can enforce a standard configuration build across all of our devices.
  - We know precisely how many different configurations we have in our environment.
  - We capture the known good state or "golden build" as part of the release management process.
  - We have confidence that the deployed systems match the golden build.
- Uncover new anxieties
  - We can reliably re-build servers that are in production (bare-metal build).
  - Production and development systems are clearly separated.
  - We ensure that the staging environment matches the pre-production environment before deploying into production.

Example Questions: Control Processes

- Uncover pain
  - We have regularly scheduled change control meetings.
  - When making changes, we schedule them during pre-defined maintenance windows.
  - Before making changes, changes must be authorized via the change management process.
  - We have technology in place to track and enforce the change control policy .
- Uncover new anxieties
  - We have a clearly defined change request process.
  - We can quickly discover unauthorized or undocumented changes.
  - We review change control, release management and problem resolution processes regularly for operational relevance.

Interex, Encompass and HP bring you a powerful new HP World.