



Continually Compliant Data Centers "The 5 Steps Best Practice"

Vick Viren Vaishnavi

ACTIVATE BUSINESS WITH THE POWER OF I.T.™

 **bmcsoftware**

Business Impact of Compliance



Regulatory

Issue:

Pervasive compliance requirements:
SOX 404, SAS-70, GLBA, HIPAA, BASEL II, etc

Impact:

Significant financial and reputational costs for non-compliance

Security

Issue:

Escalating number and level of security threats

Impact:

Increasing risk of security breaches and outages

Operational

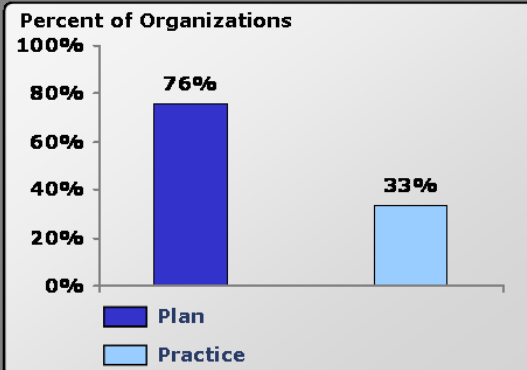
Issue:

Increased demand to conform to industry standards and best practices like ITIL and COBIT

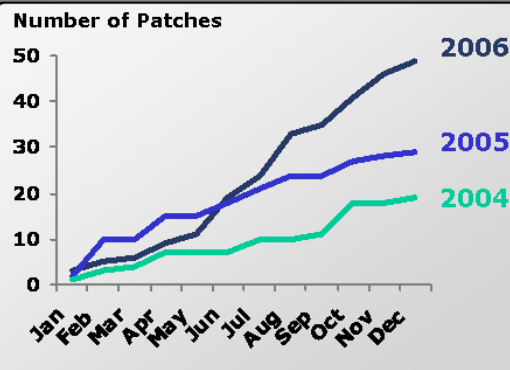
Impact:

Compliance to industry best practices is increasingly difficult and expensive

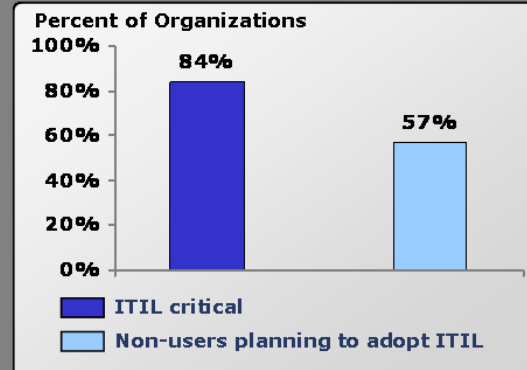
Large Gulf Between Plan and Practice



Critical Vulnerabilities Disclosed by Microsoft



ITIL Critical to IT Processes



Source: Gartner, Microsoft Technet, INS, IT Policy Compliance Group

IT Controls as the Major Cause of Non-Compliance



- Review of transactions
- Staffing Issues (levels/expertise/training)
- Application of GAAP/acctg. Policies
- Merger/predecessor issues
- Financial statement closing process/consol

- Policies/documentation issues
- Controls environment
- Segregation of duties
- Compliance monitoring
- Inventory management
- IT and applications – infrastructure
- IT and applications - security/user access
- IT and applications - change control
- IT and applications - data protection

- Revenue / Billing
- Employee benefit/pension
- Contracts/loan/third-party transactions
- Anti-fraud controls
- Accounts payable
- Accounts receivable
- Property/equipment/leases
- Tax issues
- Accruals/restructuring costs
- International operations/subsidiaries
- Intercompany accounts/reconciliation
- Other

Based on Big 4's experience, deficiencies in IT controls are the most costly and difficult to identify and bring under compliance.

Penalties for Non-Compliance ...



› Choicepoint Case

- 145000 accounts compromised
- \$11.4M in charges => cost of non-compliance
- \$13M => cost of repair
- \$90/customer to repair
- Market cap dropped \$720M

› Card Systems Case

- 40M accounts compromised. Barred by VISA and MC now.

› Penalties via regulations

- Identity Theft Protection Act: \$11K/customer compromised with a cap of \$11M per incident

› Bottom line (F1000 Firm with 500 servers)

- Internal Audit costs around \$150K
- Subscribing to a scan service is \$50K
- Cost of IT Controls is \$200K for every 20 controls

› Summary

- Cost of staying compliant is \$16 per account Vs \$90 per account for repair (not including brand and customer loss)

Source: Gartner Research
Source: Gartner Research



The 5 Steps Best Practice

Step 1: Definition

ACTIVATE BUSINESS WITH THE POWER OF I.T.™

 **bmcsoftware**

1.1: How to Define Data Center Compliance



Security Compliance



- › Are the servers/applications secure in terms of having the necessary security patches in place?
- › Are there any vulnerabilities that exist in the environment that need remediation?
- › Do we have access controls that limit administrative privileges?

Configuration Compliance



- › Are the Servers/Applications configured as per the standards (internal, vendor based, best practice driven)?
- › How can configurations be maintained to adhere to the standards?

Regulatory Compliance



- › Do we have the necessary Controls required by regulatory requirements?
- › How can we demonstrate to the auditors the existence of such controls required to pass the audits?

1.2: Define Key Goals for Compliance



Standardization

How to normalize change definitions across platforms (*BUILD POLICIES*)

How to identify service dependencies for a change (*IDENTIFY RISKS*)



Accountability

What changes were made ? (*AUDIT TRAIL*)

Who made them and were they authorized ? (*SEGREGATION OF DUTIES*)

How can exceptions be detected, documented and fixed ?
(*DRIFT MANAGEMENT*)



Transparency

How to provide visibility to auditors and management ?
(*COMPLIANCE REPORTING*)

Visibility into tasks and processes supporting Compliance
(*ACTIVITY REPORTING*)



Measurability

What is our compliance score over time ?
(*TRENDING, ANALYTICS, SCORE CARDS*)



The 5 Steps Best Practice

Step 2: Implementation

ACTIVATE BUSINESS WITH THE POWER OF I.T.™

 **bmcsoftware**

2.1: Choose and Adopt a Governance Framework



- › COBIT as the control definition framework
- › Accepted worldwide as an IT controls' framework
 - Similar to ITIL, but specific to compliance
- › 100% compliant with ISO17799, ITIL, CMM, BS15000
- › SEC and PCAOB endorses COBIT for SOX compliance
- › Built-in support for IT audit, reduces cost of audit and self-assessment
- › Target Audience
 - Management – Helps them balance risk and control in an fast-changing IT environment
 - Users – Obtain assurance on security and controls of IT services
 - Auditors – Substantiate their opinions and provide evidence of control activity

2.2: Identify Required Controls for Each Initiative



IT CONTROL OBJECTIVES FOR SARBANES-OXLEY

THE ROLE OF IT IN THE
DESIGN AND IMPLEMENTATION
OF INTERNAL CONTROL OVER
FINANCIAL REPORTING
2ND EDITION

SEPTEMBER 2006

12 IT Control Objectives

IT Control Objectives for Sarbanes-Oxley	CobIT	PCAOB IT General Controls			
	Mapping to CobIT 4.0 Processes	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. <u>Acquire and maintain application software.</u>	AI2	✓	✓	✓	✓
2. <u>Acquire and maintain technology infrastructure.</u>	AI3	✓	✓	✓	
3. <u>Enable operations.</u>	AI4	✓	✓	✓	✓
4. <u>Install and accredit solutions and changes.</u>	AI7	✓	✓	✓	✓
5. <u>Manage changes.</u>	AI6		✓		✓
6. <u>Define and manage service levels.</u>	DS1	●	●	✓	✓
7. <u>Manage third-party services.</u>	DS2	●	●	✓	✓
8. <u>Ensure systems security.</u>	DS5			✓	✓
9. <u>Manage the configuration.</u>	DS9			✓	✓
10. <u>Manage problems and incidents.</u>	DS8, DS10			✓	
11. <u>Manage data.</u>	DS11			●	●
12. <u>Manage the physical environment and operations.</u>	DS12, DS13			✓	●

Key IT Controls Mandated



Access Controls

Roles and responsibilities

Record, Review and Analyze Activities

Managing the WHO

Change Controls

Tracking success rate

Monitoring for unauthorized changes

Remediate undesired or unauthorized changes

Managing the HOW

Release Controls

Standardized release process

Automate the build process and distribution (Package, Promote)

Maintain environment consistency during release

Configuration Controls

Formalized CM process (id, record, track)

Automated CM (modify, update, provision)

Granular configuration visibility in real time to the right personnel

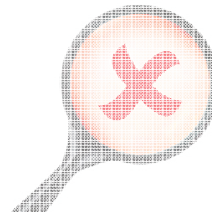
Managing the WHAT

2.3: Choose and Adopt a Compliance Assurance Platform



Prevention

- › How can I add consistency and visibility to my processes in order to appease internal / external audit and IT security?
- › How can I give people access to everything they need to see and do and nothing else?
- › How can I improve the success rate of taking my applications from development to QA to production?



Detection

- › I just built 10 servers exactly the same 3 weeks ago. Why is one now acting funny? What's changed?
- › How can I better manage exceptions to eliminate much of the noise that I receive alerts on?



Correction

- › How can I repair configurations without physically going to the server and/or writing custom program(s)?
- › How can I correct inconsistencies according to set business policies before they cause outages?

3 Key IT Controls Categories to Look For



The 5 Steps Best Practice

Step 3: Measurement

ACTIVATE BUSINESS WITH THE POWER OF I.T.™

 **bmcsoftware**


Measuring the Results



Compliance Exceptions Detail

Template	Rule Group	Rule	Server	Reference	Detail	Date Expired	Date Created	User Created
Windows 2003 Secure Build	Software & Service Config	Symantec AntiVirus Client Enabled	winsql01	Document xyz	Enabling this service causes conflicts with SQL Server 2000. This issue is fixed in SQL 2005. Approved by C. Whitney 06/21/05.	12/31/2006	10/24/05	jtaylor
Windows 2003 Secure Build	Latest Patch Set Installed	Service Pack 1 Installed	winweb2	//Intranet/Policy Exceptions/REF123	Website will crash if SP1 is installed. Approved by J. Matthews. Waiting for release plan to determine how long risk will exist.		10/23/05	jschwartz
Windows 2003 Secure Build	Latest Patch Set Installed	Service Pack 1 Installed	winweb1		Website will crash if SP1 is installed. Approved by J. Matthews. Waiting for release plan to determine how long risk will exist.		10/22/05	jschwartz

Compliance Summary by Rule Group

 Policy = "Windows Security"

Rule Group	Oldest Data Set	Total # Servers	# Servers Audited	# of Failed Servers	Server Compliance	Total # Rules	# of Failed Checks	# of Exceptions	Policy Compliance
Account Policies	08/12/05	200	150	8	95%	3000	56	12	98%
Audit Policies	08/12/05	60	50	30	40%	2500	84	4	97%
Event Log Settings	08/14/05	200	75	10	87%	1500	870	1	42%
Overall	08/12/05	460	275	48	74%	7000	1010	17	79%

> Key Metrics

- Scores by Policy
- MTTAudit
- MTTRemediate
- Exceptions

> Frequency

- Daily
- Weekly
- Monthly
- Quarterly



The 5 Steps Best Practice

Step 4: Enforcement

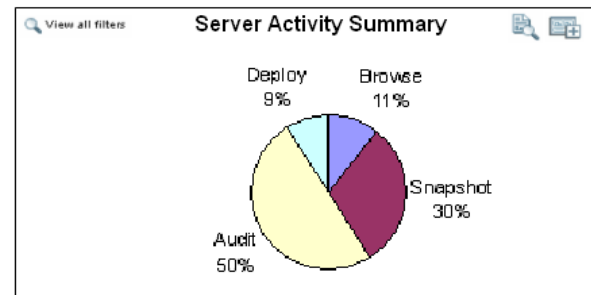
ACTIVATE BUSINESS WITH THE POWER OF I.T.™

 **bmcsoftware**

Drift Detection and Remediation



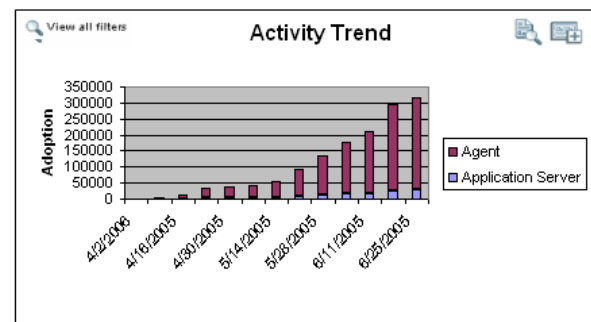
- › Roles – activity tracking
- › Best Practice Policies
- › Audits and Remediation
- › Integrated Processes
- › COBIT references the control review process as a necessary method in a maturity model:
 - ME2 Monitor and evaluate internal control
- › COBIT includes many references to audit trails, such as:
 - AI1.2 Risk Analysis Report
 - AI2.3 Application Control and Auditability



View all filters

Most Active Roles

Role	# of Users	# of Servers	Activity Last 30 Days
RBACAdmin	2	1000	100
UNIX Administrators	4	600	200
Windows Engineers	16	65	457
Overall	22	1665	757



View all filters

Most Active Users

User	# of Roles	# of Servers	Activity Last 30 Days
jtaylor	2	100	200
hkobi	1	60	100
gmoberly	3	6	45
Overall	6	166	345

Desired Process: Policy-Based Compliance and Remediation



Granular, rules-based auditing

Permissions tied to the policy

Bi-directional synchronization



The 5 Steps Best Practice

Step 5: Monitoring

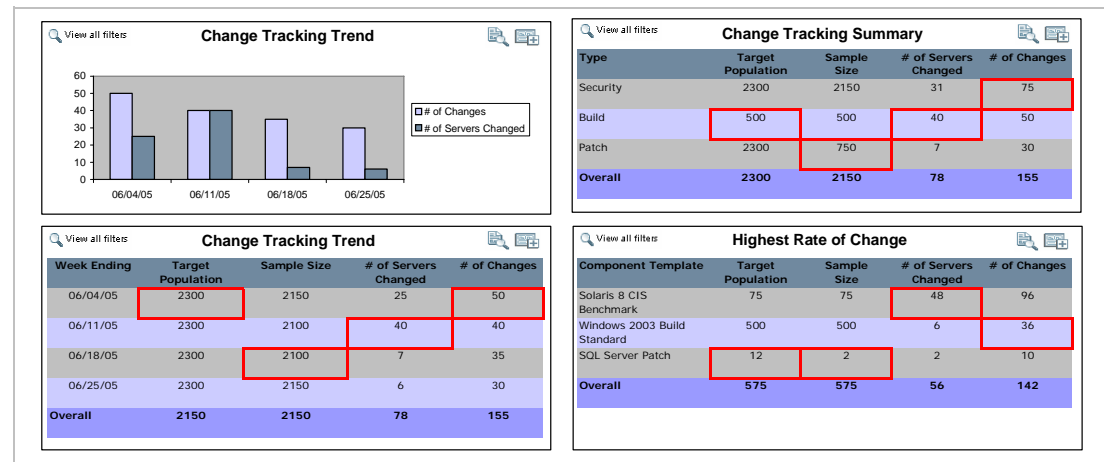
ACTIVATE BUSINESS WITH THE POWER OF I.T.™

 **bmcsoftware**

Reporting and Analytics



- › Controls
- › Activities
- › Scorecards
- › Trends
- › Keeping track of the ongoing changes to the IT environment is key to any compliance regulation
- › A few COBIT references to this issue:
 - AI7.10 System Distribution
 - DS9.1 Configuration Repository and Baseline
 - DS9.3 Configuration Integrity Review





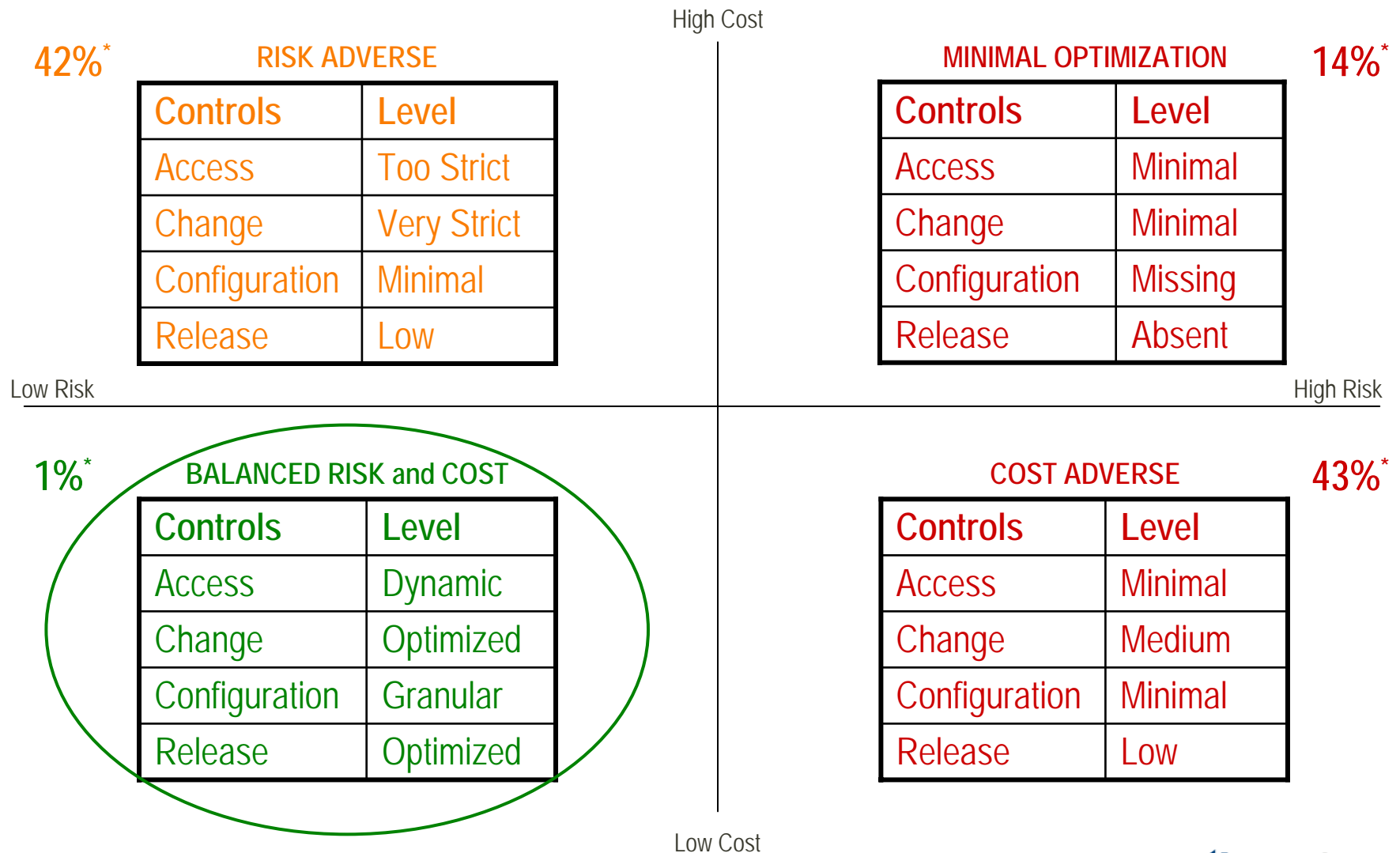
The 5 Steps Best Practice

Closing Thoughts

ACTIVATE BUSINESS WITH THE POWER OF I.T.™

 **bmcsoftware**

Controls Implementation Choices – Risk Vs Cost



* - % of IT Organizations that fit the profile based on Control, IDC Statistics 2005

Recommendations



- › **Invest in an ITGC Framework like COBIT**
 - Endorsed by SEC/PCAOB
 - Auditing Firms Prefer its definition of controls
 - Helps support multiple regulatory requirements
- › **Define, Design and Implement Controls**
 - Access, Change, Configuration, Release
 - Choose your starting “quadrant” and migrate to the magic quadrant
 - Define requirements and candidates for automation
- › **Implement Accountability**
 - Define Required INFORMATION Vs DATA
 - Quality Controls = Low Variability
 - Assign roles within organization against the controls implemented
- › **Process**
 - Standardize using best practice like ITIL
 - Look for cause-effect between a CONTROL and a PROCESS
 - Aim for “low fluctuation” in the process



MART
STEW

Living
2004

Decorating all Spaces

Irresistable
with bread
water

Fun craft id
silver brace

Brought to you by TheDe