

ITVerify

Audit & Control... The Keys to Compliance!

Kenneth Meyers
Verifichi

Synopsis

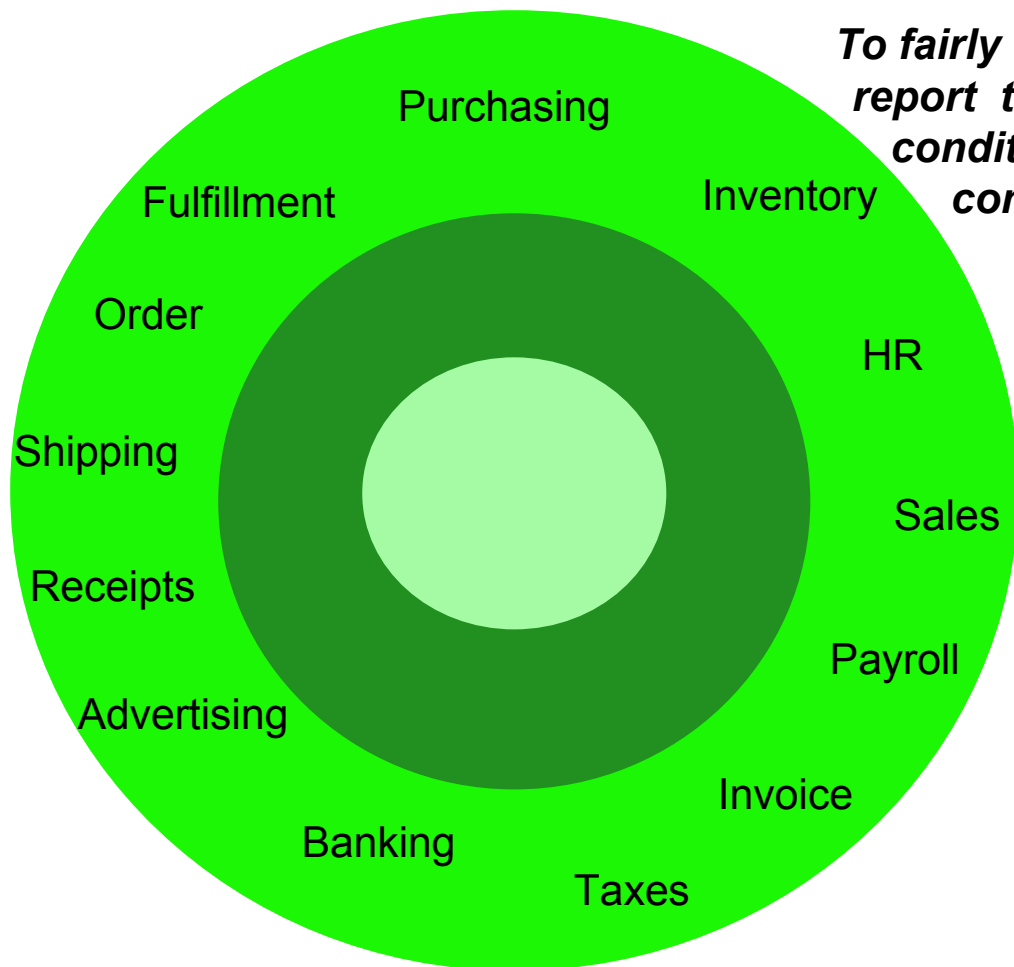
- Overview of Compliance Mandates
 - Financial / Privacy
- Case Studies of IT Compliance
 - Publishing, Financial, MFG, Pharmaceutical
- E-Mail & Messaging

ITVerify *The Compliant Foundation for Audit & Control*

Sarbanes-Oxley

Target:

*To fairly & accurately
report the financial
condition of the
company.*



**Company
Activities**



**Transactions
& Records**



**Income Statement
& Balance Sheet**

21 CFR Part 11

Target:

To implement correct and consistent controls that assure public safety.



**Pharmaceutical
Activities**

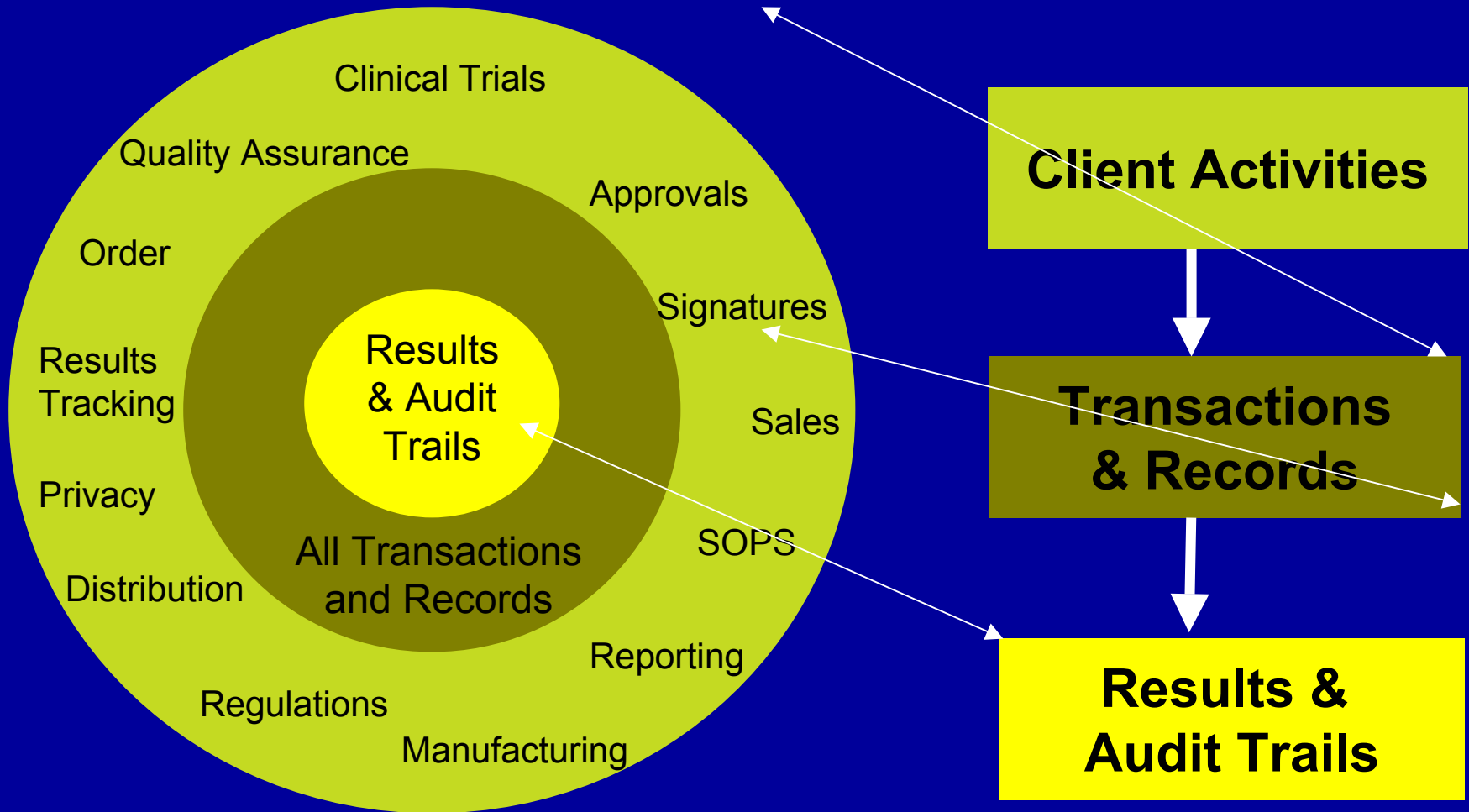


**Transactions
& Records**



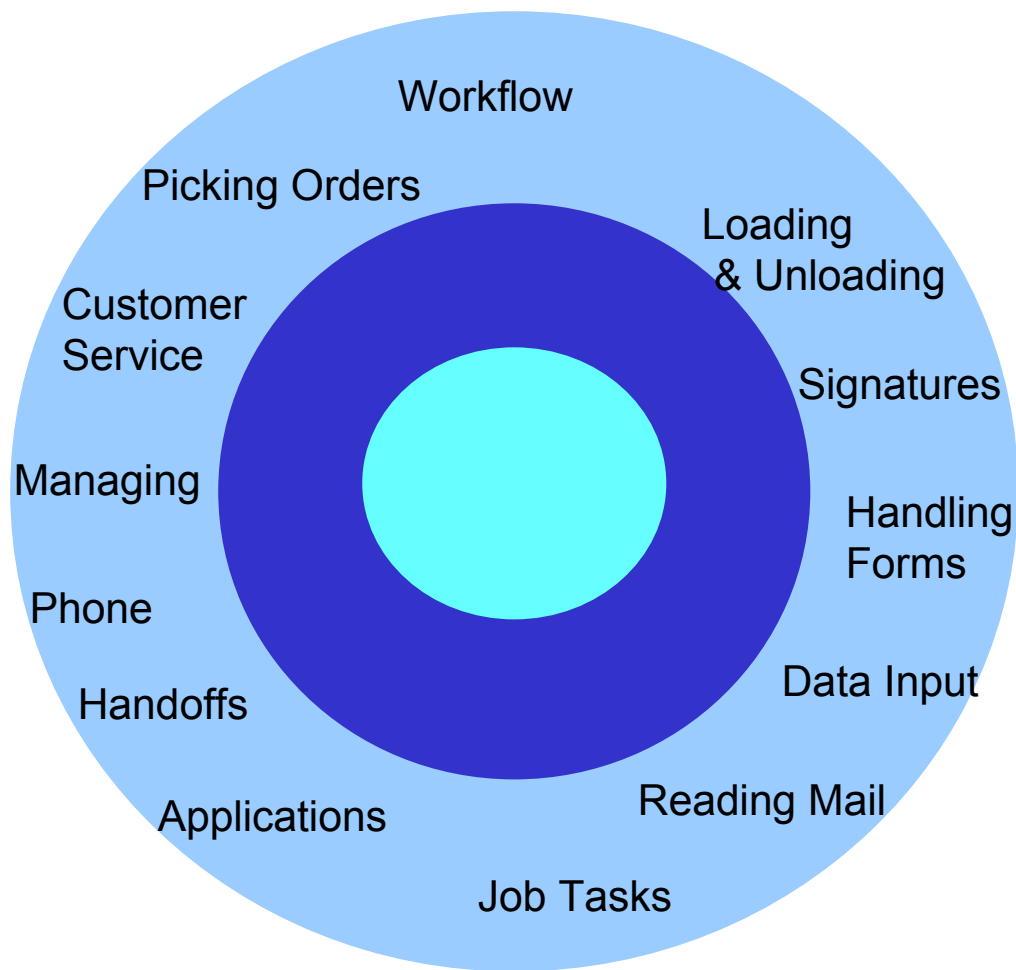
**Results &
Audit Trails**

What Is IT's Role?



IT Compliance

To assure all IT systems that support client Transactions and Records are not compromised.



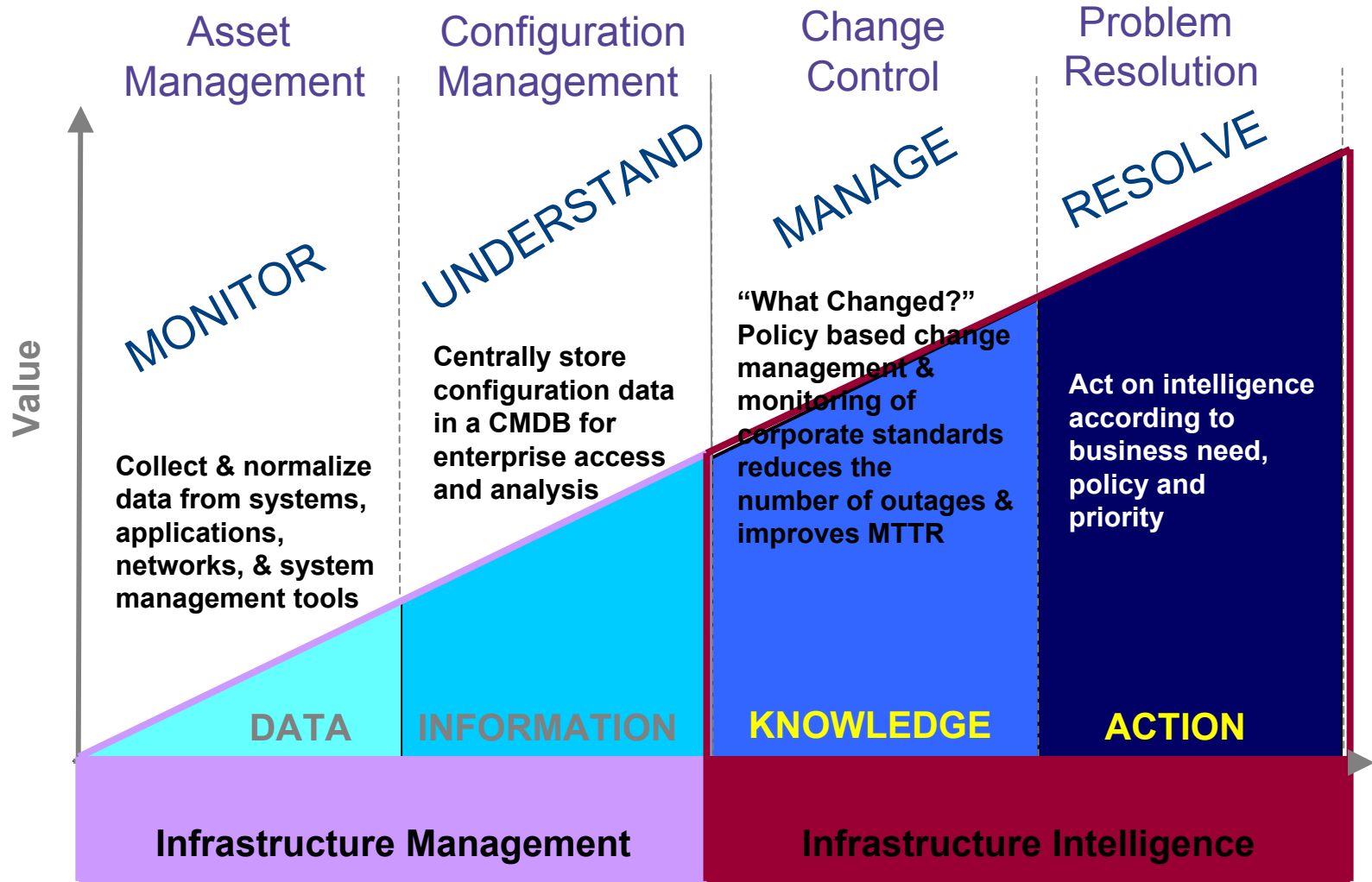
People & Process

Transactions & Records

IT Infrastructure
Servers and Storage

Report Accurate Results

Infrastructure Analysis Maturity Model



Before ITVerify - Data

```
set-root-group [FAIL] root's primary group is not set to 0.
set-root-group [FAIL] Audit Check Total : 1 Error(s)
set-rmmount-nosuid [PASS] Removable HSPFS filesystems are mounted 'nosuid'.
set-rmmount-nosuid [PASS] Removable UFS filesystems are mounted 'nosuid'.
set-rmmount-nosuid [PASS] Audit Check Total : 0 Error(s)
set-sys-suspend-restrictions [FAIL] PERMS is not set to '-' in /etc/default/sys-suspend.
set-sys-suspend-restrictions [FAIL] Audit Check Total : 1 Error(s)
set-system-umask [NOTE] Default file creation mask (CMASK) is set to 022.
set-system-umask [PASS] System file creation mask is set to 022.
set-system-umask [PASS] Audit Check Total : 0 Error(s)
set-tmpfs-limit [FAIL] tmpfs size is not defined in 512m.
set-tmpfs-limit [FAIL] Audit Check Total : 1 Error(s)
set-user-password-reqs [FAIL] Password Aging MINWEEKS is not set to 1.
set-user-password-reqs [FAIL] Password Aging MAXWEEKS is not set to 8.
set-user-password-reqs [FAIL] Password Aging WARNWEEKS is not set in /etc/default/passwd.
set-user-password-reqs [FAIL] Password Policy PASSLENGTH is not set to 8.
set-user-password-reqs [FAIL] Audit Check Total : 4 Error(s)
set-u [PASS] System file creation mask is set to 022.
set-u [PASS] Audit Check Total : 0 Error(s)
set-u [FAIL] tmpfs size is not defined in 512m.
set-u [FAIL] Audit Check Total : 1 Error(s)
set-u [FAIL] Password Aging MINWEEKS is not set to 1.
set-u [FAIL] Password Aging MAXWEEKS is not set to 8.
set-u [FAIL] Password Aging WARNWEEKS is not set in /etc/default/passwd.
update-at-deny [PASS] user daemon is listed in /etc/cron.d/at.deny
update-at-deny [PASS] User bin is listed in /etc/cron.d/at.deny.
update-at-deny [FAIL] User sys is not listed in /etc/cron.d/at.deny.
update-at-deny [FAIL] User adm is not listed in /etc/cron.d/at.deny
```

After ITVerify - Information

ITV ITVerify Console

Node Compare Search

Nodes BaseLine

- BaseLine
 - ITVerify
 - Other
 - Standards
 - Application
 - Security
 - UnixBaseline
 - WinTelBaseline

Nodes Node Group

- PRODUCTION
- PROVISIONING
- SALES
- SUN
- SUPPORT
- UnixLarge
- UnixMid
- UnixSmall
- Wintel

Attribute State

- Global
- Local
- Metric

Only Show Differences

Compare

Reset

Category	Attribute/Group	Security	ATSUN14	ATSUN12	ATSUN08
solarisSecurity	solaris.security.update-cron-deny	PASS	PASS	PASS	PASS
solarisSecurity	solaris.security.update-cron-deny.note	checksum:1236016	checksum:1236016	checksum:1236016	checksum
solarisSecurity	solaris.security.update-at-deny.note	checksum:1236016	checksum:2849971	checksum:1542265	checksum
solarisSecurity	solaris.security.update-at-deny	PASS	FAIL	FAIL	FAIL
solarisSecurity	solaris.security.set-user-password-reqs	PASS	PASS	PASS	PASS
solarisSecurity	solaris.security.set-user-umask	PASS	PASS	PASS	PASS
solarisSecurity	solaris.security.set-system-umask	PASS	PASS	PASS	PASS
solarisSecurity	solaris.security.set-system-umask.note	checksum:4283896	checksum:4284551	checksum:4286189	checksum
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS
solarisSecurity	solaris	S	PASS	PASS	PASS

ITV Checksum Compare

Legend

- Yellow background: "+" Line found only in right hand side attribute result
- Green background: "-" Line found only in left hand side attribute result

NOTE

- + Default file creation mask (CMASK) is set to 077.
- Default file creation mask (CMASK) is set to 022.

What is ITVerify?

A Specialized Tool that Combines

- ▶▶ A DataWarehouse with a...
- ▶▶ Powerful Telemetry Engine and...
- ▶▶ GUI interface that will enable the generation of accurate compliance reports!

Providing Real-Time, Non-Invasive, Attestable IT Infrastructure Compliance Information to....

- ▶ Identify, Monitor, Record and Report on.....
 - Assets, Configurations, Changes, Utilization, Performance of
 - Servers, Attached Storage, Network Components, Applications, Licenses
- ▶ Alert
 - Deviations from Standard (Golden Master)
 - Material Breaches (DR Incompatibility)

- ▶ Input
 - Device/Database
- ▶ Output
 - ODBC (use existing report writer)
 - Ported to any existing Management System/Reporting Tool
- ▶ GUI Interface
 - Real-Time Interactive Query Capability

ITVerify

Client Defined Attributes

- Asset (HW, SW, Application)
- Asset Location
- Utilization
- Performance
- License

Servers/Storage

Network Components

Applications

Licenses

ITVerify Solution Suite

Via

Excel File

Port to "Other"

**Infrastructure Explorer
ITVerify GUI**

EMC Centera

Via ODBC or API
PDF via FTP or E-Mail

**Real Time
Attestable Compliance
Reporting**

Capacity = 1,000 Nodes

Helps Speed Root Cause Analysis

How? By Answering.....

- What changed?
- Which one of these is not like the other?

Helps Manage Configuration Drift

How? By Capturing.....

- Configuration data
- Snapshot data of proven baselines
 - Monitor variations
 - Collect, log, alert, and forward changes

IT's Roles & Responsibilities

1. Compliance Evaluation for Sarbanes-Oxley and COBIT.
- 2. Compliance Evaluation For All Systems.**
3. Security Assessments for System Permissions Given To Users (Entitlement Report).
- 4. Security Assessments for Modifications to Critical System Files.**
5. Security Assessments for Users and Groups with Elevated Rights to the Database.

ITVerify Supports Compliance

ITVerify Architecture

Access Violation

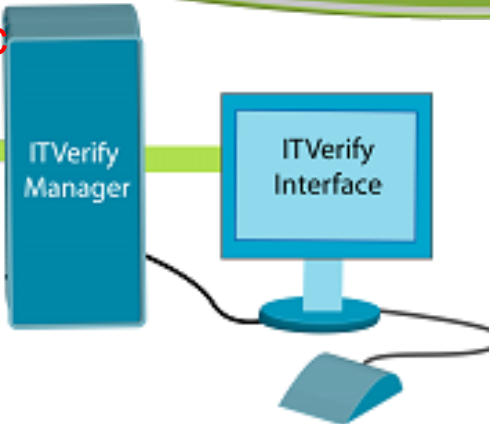
Backups Failed



Unauthorized Change

Missing Disk

DR Site Out of Sync



Infrastructure Explorer
(GUI)

- Security
- Application Changes
- Data Management
- Operations
- Assets

ITVerify Architecture

Access Violation

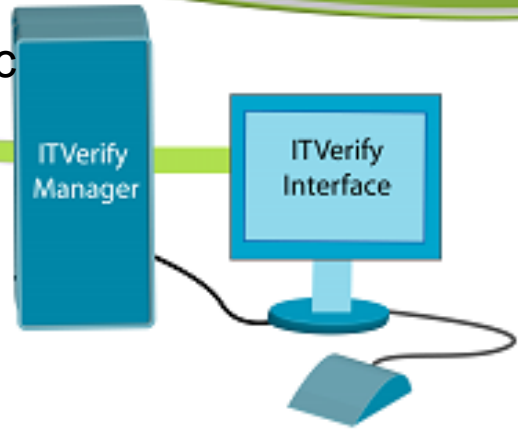
Backups Failed



Unauthorized Change

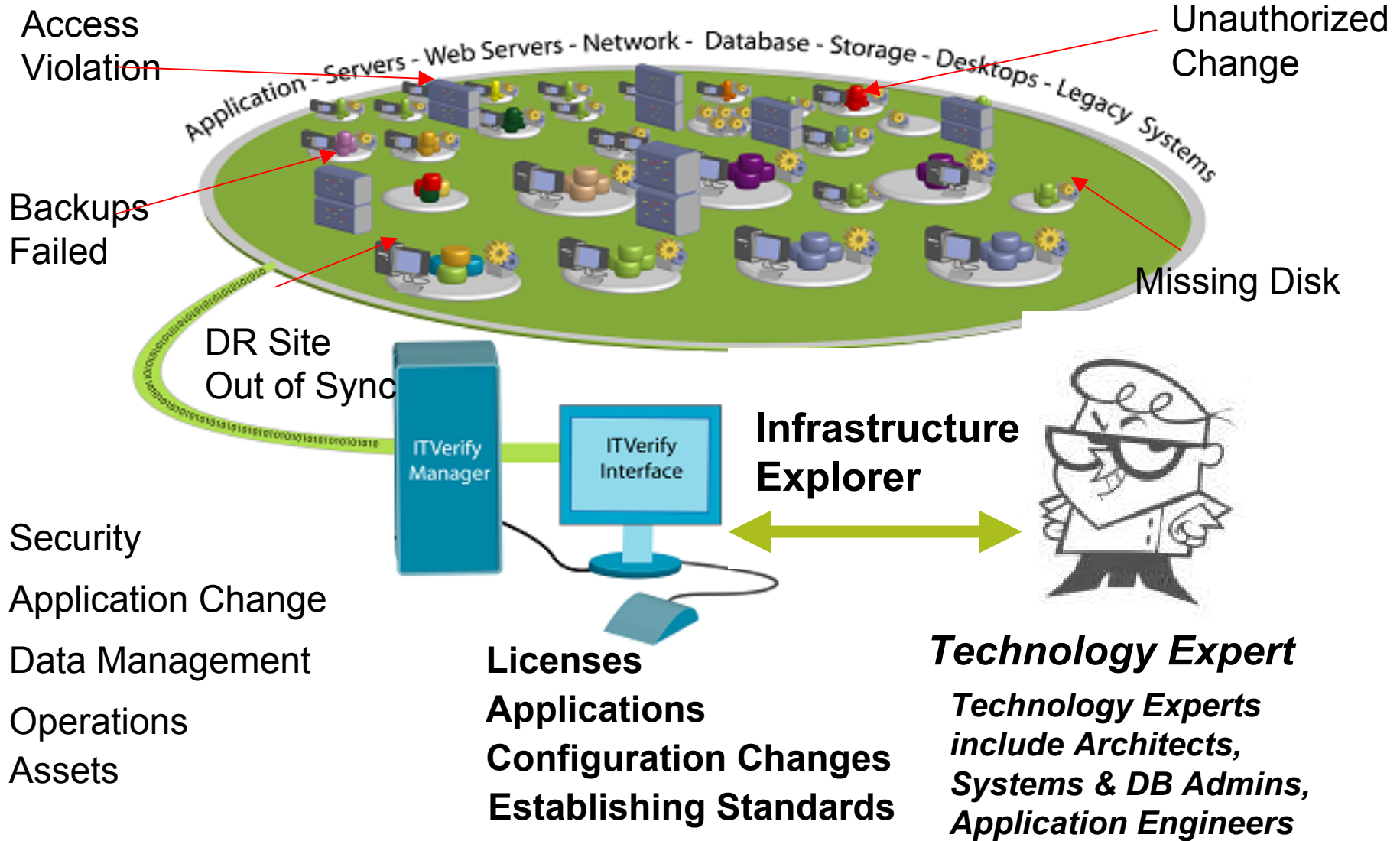
Missing Disk

DR Site Out of Sync



- Security
- Application Change
- Data Management
- Operations
- Assets

ITVerify Architecture



ITVerify Architecture

Access Violation

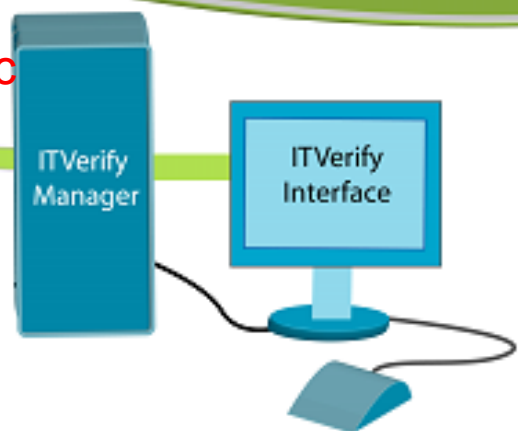
Backups Failed



Unauthorized Change

Missing Disk

DR Site Out of Sync



- Security
- Application Change
- Data Management
- Operations
- Assets

BARNES & NOBLE.com
www.bn.com

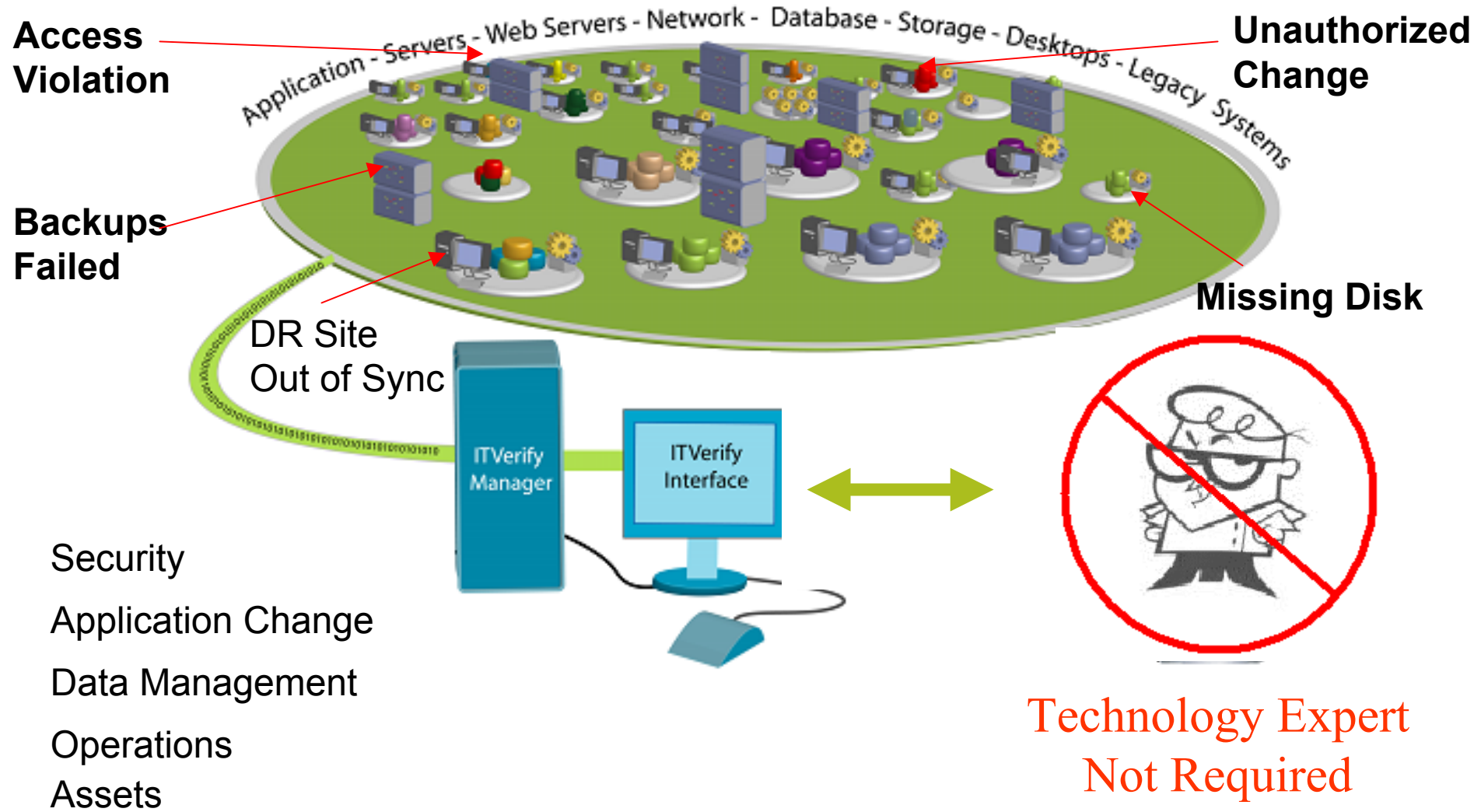
Executive Compliance Summary for SOX
Security Assessments for Modifications to Critical System Files

Summary

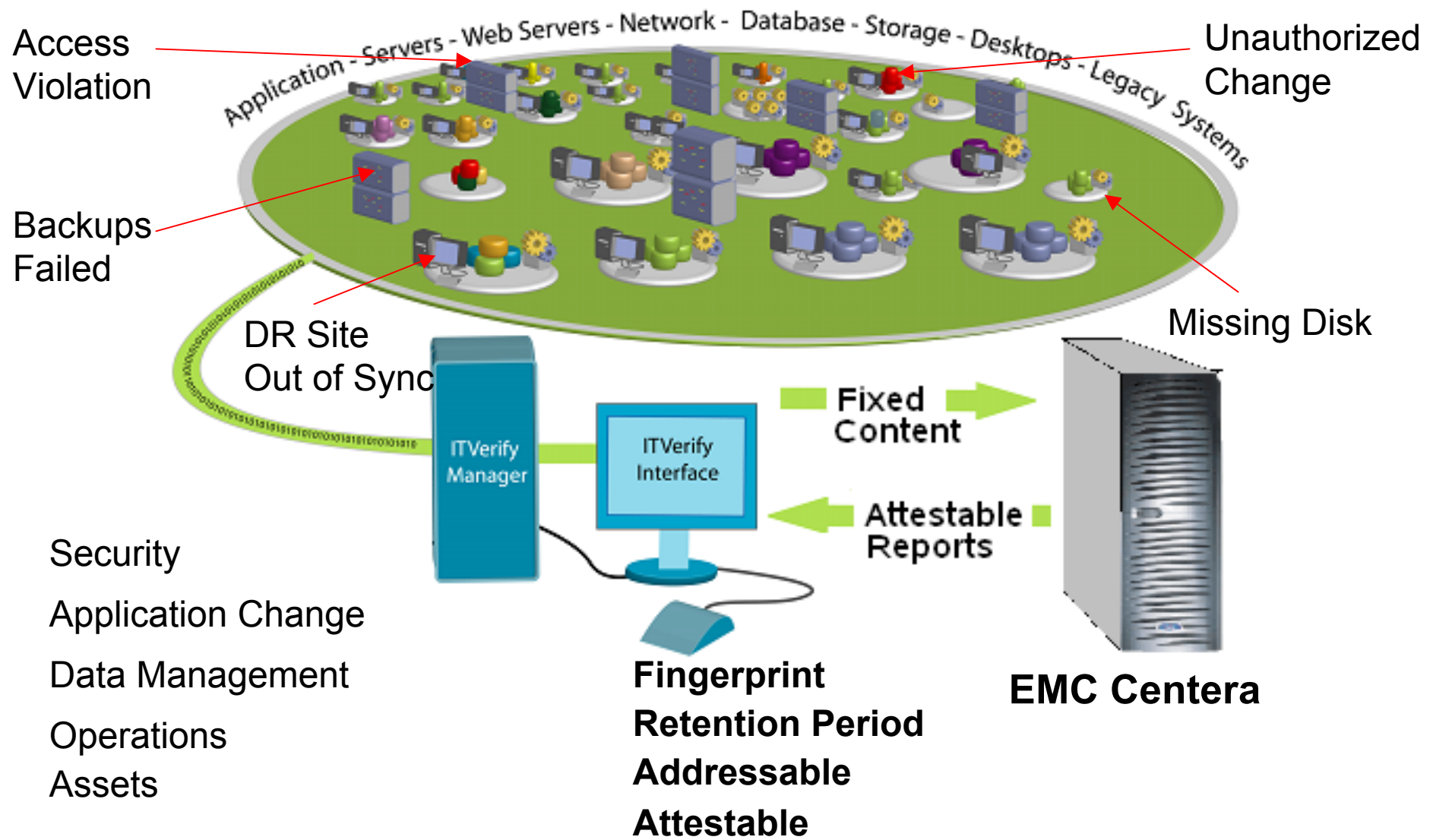
Overview

NodeGroup	# Nodes	Compliant	Non-Compliant
SOX_West	2.0	1.0	2.0

ITVerify Architecture

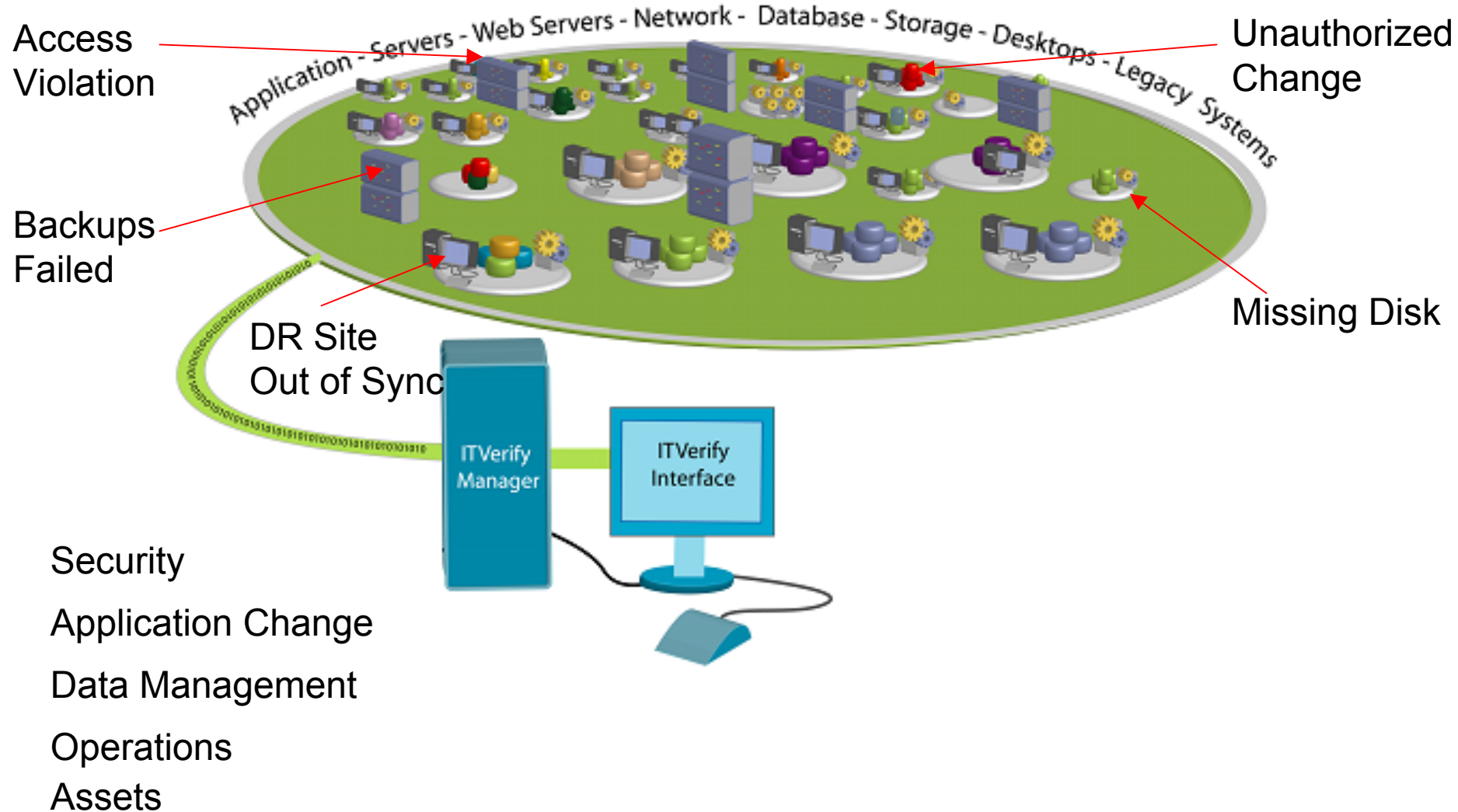


ITVerify Complements ILM*

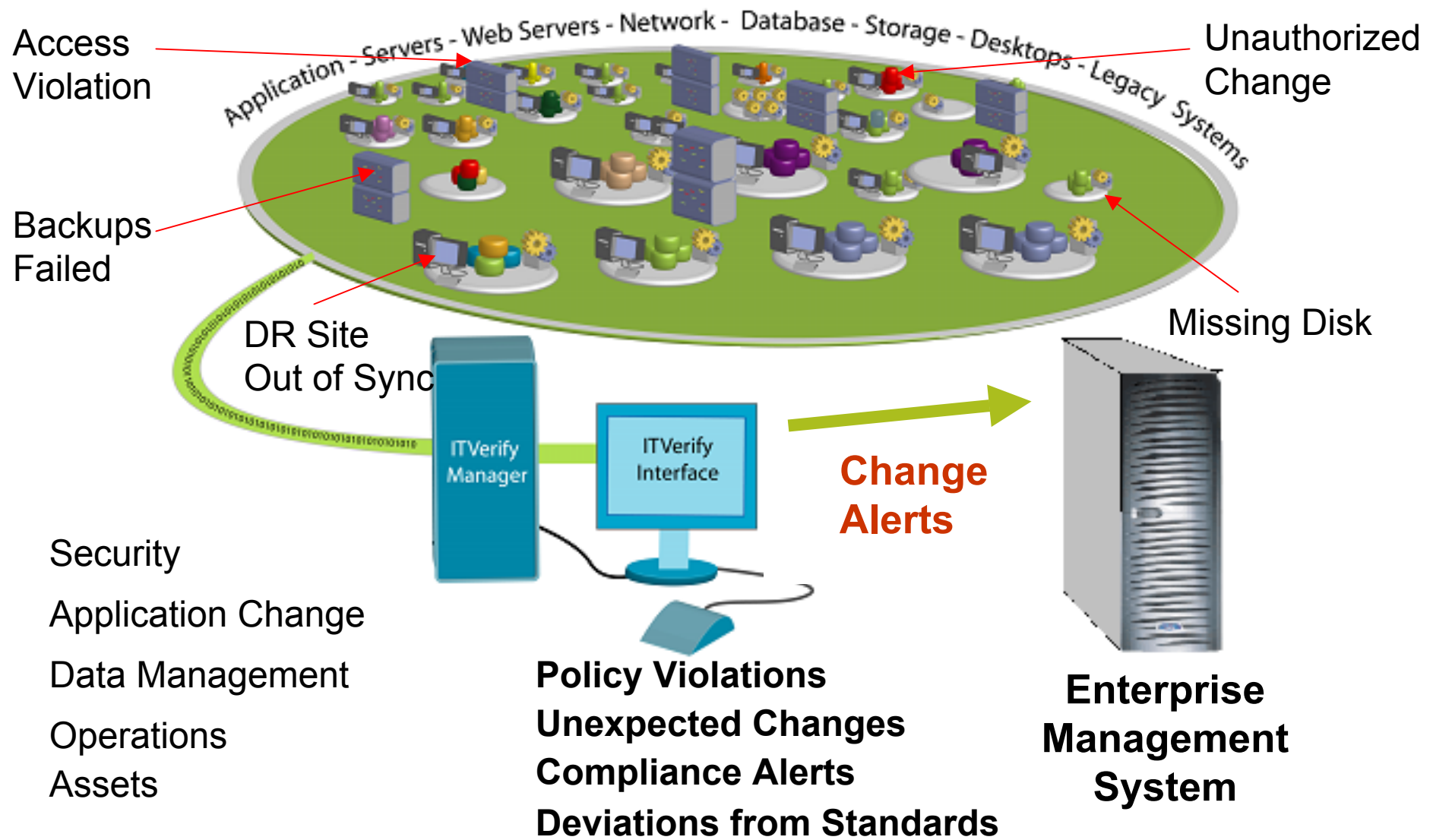


*ILM = Information Lifecycle Management

ITVerify Complements ILM



ITVerify Complements Existing IT Operations



ITVerify Requirements

- O/S Server:
 - Solaris / Linux
 - Minimum:
 - 1 GHz CPU
 - 1 Gig of Memory
 - 500 MB of Disk (Software)
 - Additional 250 MB of Disk Space per Node.
 - Built-in / Mountable CD or DVD drive
- ITVerify Support Capacity:
 - Up to 1,000 nodes
- Initial configuration and load:
 - Up to 200 Data Elements for customization of fields:
 - Dependent upon specific Data Center Architectures
 - 3 minutes/node for initial auto discovery
 - **In less than one week,** ITVerify will meet your desired coverage and intent for asset metrics, configuration, and change control monitoring and auditing.

Final scope and functionality based on customer defined parameters

Concise Reporting

ReportBrowser
Report Actions Window Help

West

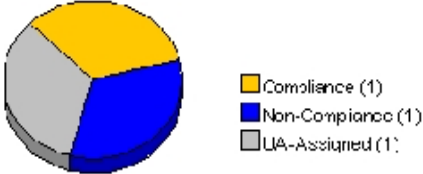
- Executive_Compliance_Summary
 - East
 - Node Group
 - Baseline
 - West
 - Node Group
 - Baseline
 - Corporate
 - Node Group
 - Baseline

BARNES & NOBLE.com
www.bn.com

Executive Compliance Summary for SOX

Security Assessments for Modifications to Critical System Files

Summary



■ Compliance (1)
■ Non-Compliance (1)
■ UA-Assigned (1)

Overview

NodeGroup	# Nodes	Compliant	Non-Compliant
SOX_West	3.0	1.0	2.0

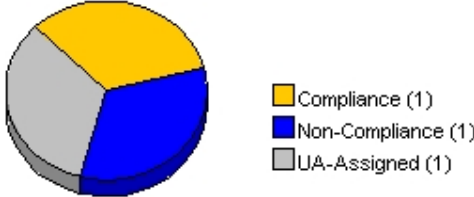
Executive Reports

BARNES & NOBLE.com
www.bn.com

Executive Compliance Summary for SOX

Security Assessments for Modifications to Critical System Files

Summary



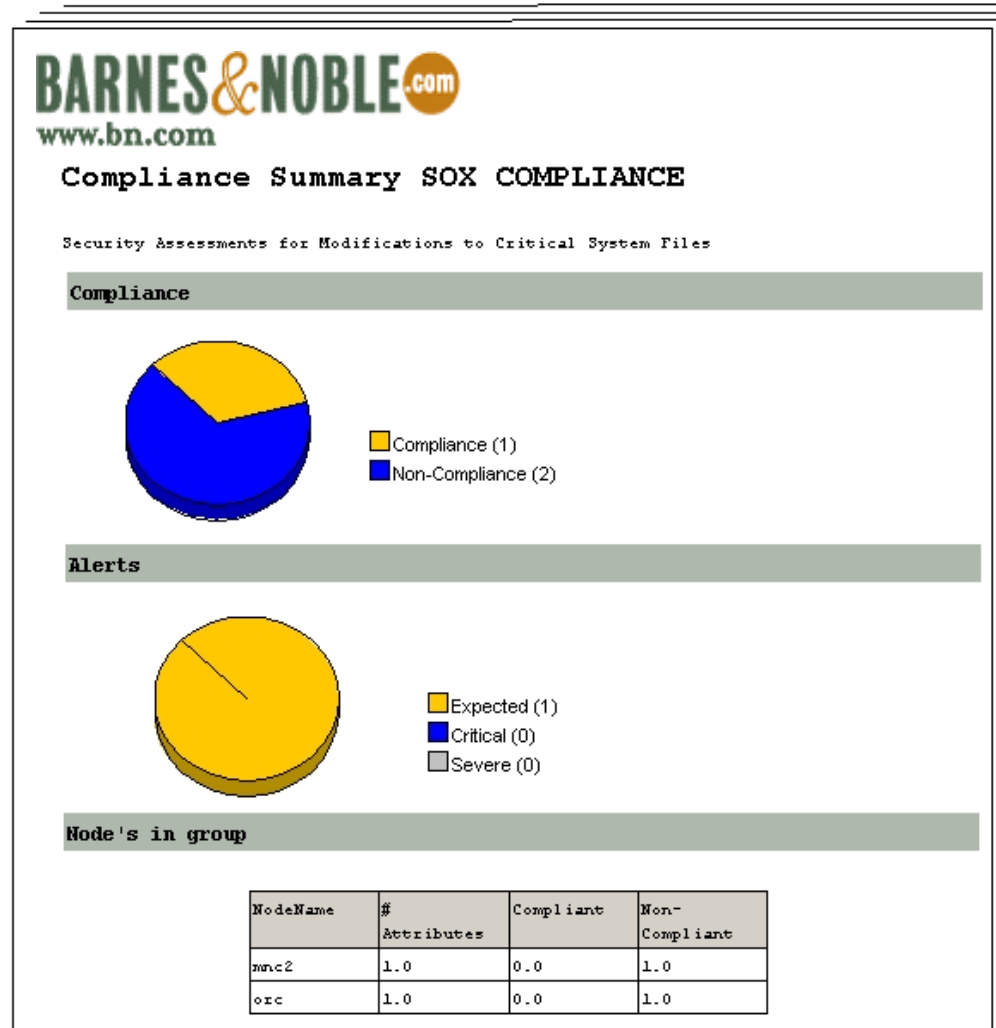
A 3D pie chart illustrating the compliance status of the system. The chart is divided into three segments: a yellow segment representing 'Compliance (1)', a blue segment representing 'Non-Compliance (1)', and a grey segment representing 'UA-Assigned (1)'. A legend to the right of the chart provides the key for each segment.

Category	Count
Compliance	1
Non-Compliance	1
UA-Assigned	1

Overview

NodeGroup	# Nodes	Compliant	Non-Compliant
SOX_West	3.0	1.0	2.0

Management Reports



Operational Reports



Detailed Compliance Report

SOX_COMPLIANCE_NO4 vs kraken for attribute securityassessment.4

L.No.	Type	SOX_COMPLIANCE_NO4	kraken
0		/etc/inet/hosts Type: File Perm: 444 Owner: root Group: sys Size: 999	/etc/inet/hosts Type: File Perm: 777 Owner: root Group: sys Size: 953
1		/etc/vfstab Type: File Perm: 644 Owner: root Group: other Size: 871	/etc/vfstab Type: File Perm: 644 Owner: root Group: other Size: 1302
2		/etc/shadow Type: File Perm: 400 Owner: root Group: sys Size: 4222	/etc/shadow Type: File Perm: 400 Owner: root Group: sys Size: 23626
3		/etc/passwd Type: File Perm: 444 Owner: root Group: sys Size: 7434	/etc/passwd Type: File Perm: 444 Owner: root Group: sys Size: 40894
4		/etc/inet/services Type: File Perm: 444 Owner: root Group: sys Size: 3941	/etc/inet/services Type: File Perm: 644 Owner: root Group: sys Size: 4025
5		/etc/nsswitch.conf Type: File Perm: 644 Owner: root Group: other Size: 1416	/etc/nsswitch.conf Type: File Perm: 644 Owner: root Group: other Size: 1458
7		/etc/hosts.equiv Type: File Perm: 644 Owner: root Group: other Size: 318	/etc/hosts.equiv Type: File Perm: 644 Owner: root Group: other Size: 92

ITVerify Value

“Providing Real-Time, Attestable IT Infrastructure Compliance Information”

- Identifies, Monitors and Records:
 - Assets & Locations
 - Configurations (patch levels)
 - Utilization & Performance
 - Changes from Baseline
- Notifies:
 - Changes from mandated standard (Golden Master)
 - Customer designated “material breaches:”
 - Ex. hard drive loss, disaster recovery site incompatibilities
- Output:
 - Compliance Reports
 - Can be ported to existing management systems
 - Provided in Excel or Crystal, or any ODBC based report
- Infrastructure Explorer provides real time interactive query capability

Solution

Partnership

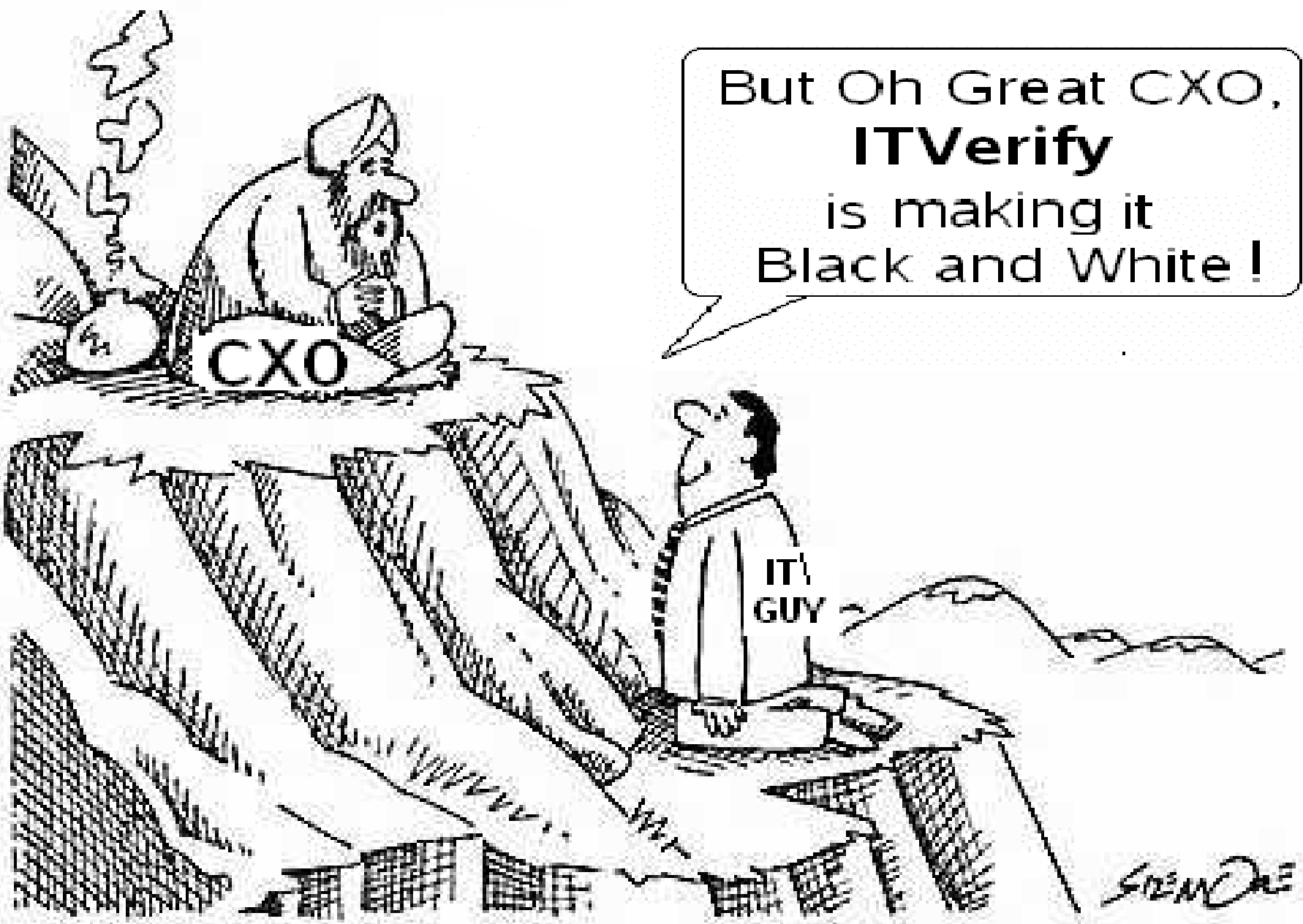
- Verifichi
 - Compliance Monitoring Software & Services
- EMC Storage & System Management
 - E-Mail & Messaging
- G Force Technologies Consulting
- Unisys Services

Next Steps

- Complete “Compliance Readiness Assessment Survey”
 - Provide the guidelines needed to understand the areas that need to be addressed
- Determine when you would like to review the document with our team
 - Allocate between 2 days
- Based upon the results, our team will provide recommendations and suggestions.

ITVerify

- Simplify the Capture of Information
- Manage Information More Effectively
- Reduce Cost of Managing Infrastructure
- Ensure Information is Attestable
 - Help Executives Stay out of Jail!



But Oh Great CXO,
ITVerify
is making it
Black and White!

"You're in luck. Business ethics is a gray area."