Virtualize More While Improving Your Risk Posture – The 4 "Must Haves" of Virtualization Security

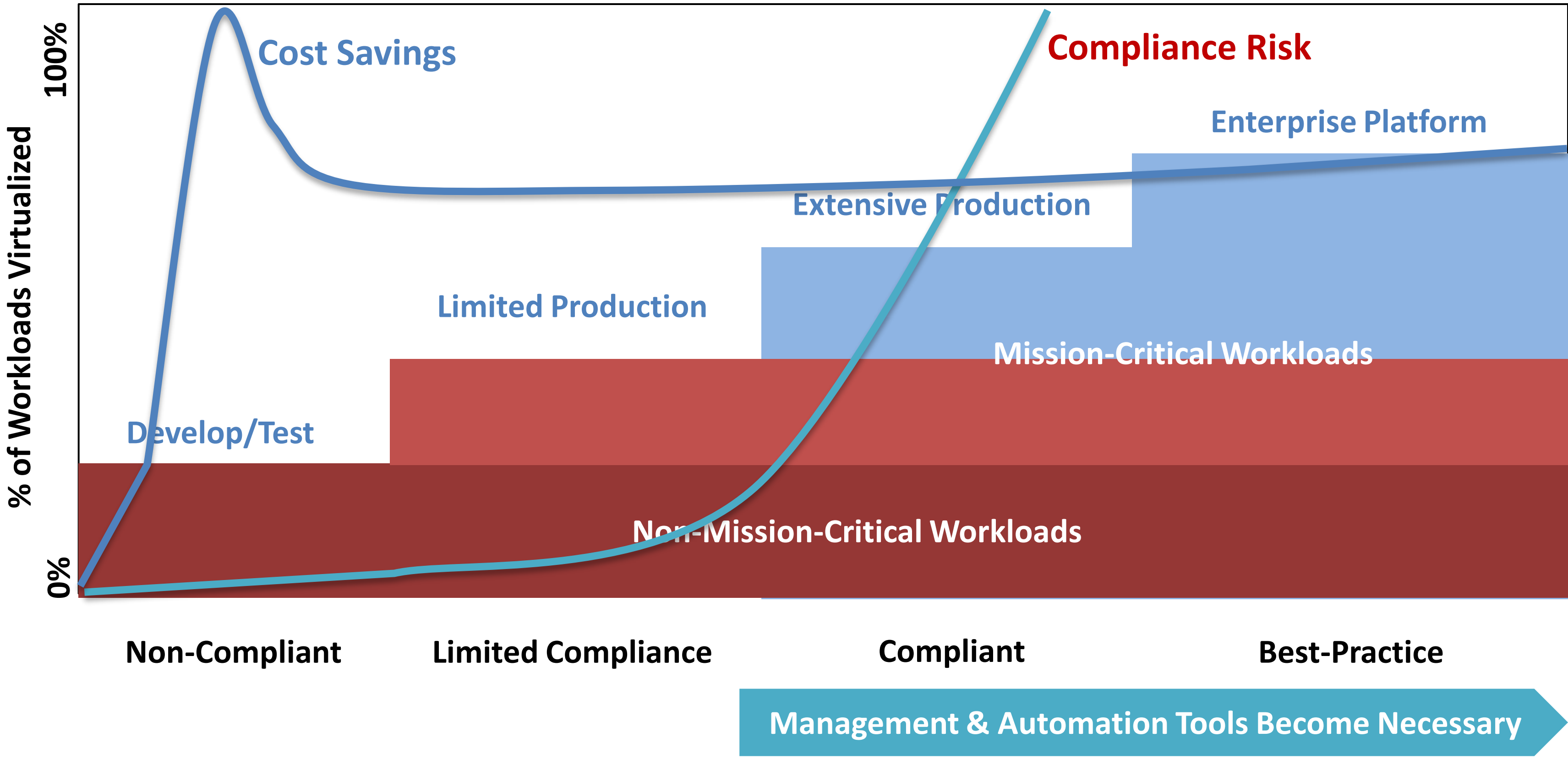
Hemma Prafullchandra, CTO/SVP Products, HyTrust
George Gerchow, Director, Center for Policy & Compliance, VMware
Rishi Bhargava, Sr Director, Product Management, McAfee
Rick Norman, Director, Professional Services, Coalfire Systems

Professional Techniques – T21

Agenda

- Security and Compliance Challenges
  - Alignment of broader objectives
- The “4 Must Haves”
  - Access Control and Account Management
  - Network and Endpoint Security
  - Configuration Management and Hardening
  - SIEM and Log Management
- Key Takeaways & Resources

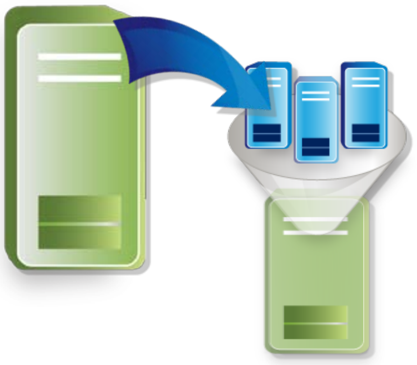
Organizations are rapidly adopting virtualization



How Best to Align Broader Objectives?

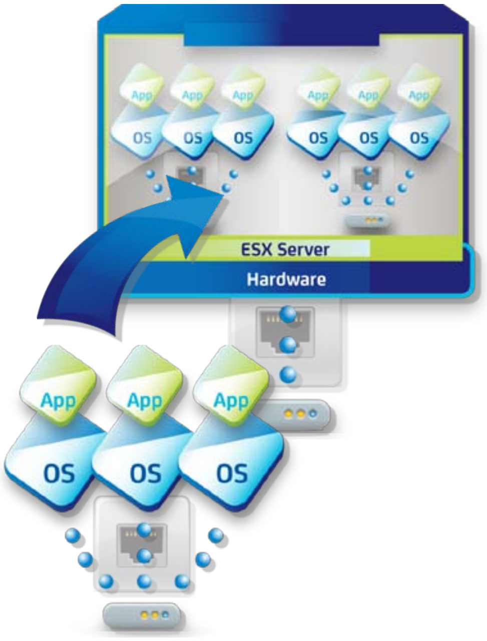
	CFO	CIO	Implications for CSO
Cost	Cost transparency Forecast accuracy	Do more with the same/less budget Resource planning	Limited or no budget (Need very compelling event, or to tightly align to revenue generation)
Agility	Investment analysis	Modernize legacy IT Select the right cloud strategy	Accountable for security solution that matches agility of virtualization
Risk	Mitigate potential corporate risk Adhere to security and Compliance	Gain control over IT workload leakage to Manage data and application security	Accountable for security of virtual assets that Do Not exist yet.

Virtualization platform effects on security



Abstraction and Consolidation

- ⬆ Capital and Operational Cost Savings
- ⬇ New infrastructure layer to be secured and subject to compliance
- ⬇ Greater impact of attack or misconfiguration



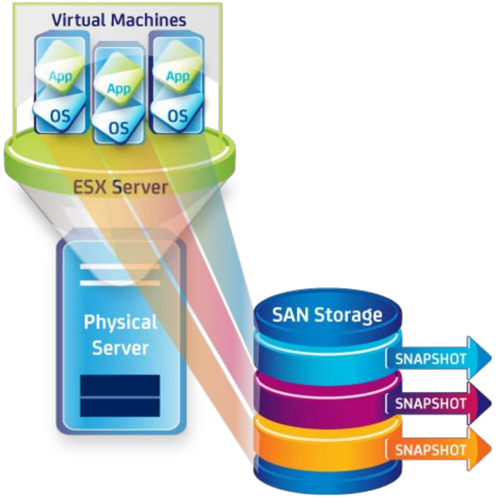
Collapse of Switches and Servers into One Device

- ⬆ Flexibility
- ⬆ Cost-savings
- ⬇ Lack of visibility and control for virtual network and storage
- ⬇ No separation of church and state (network, security, storage administration)

Faster Deployment in Shared Environment

- ⬆ IT responsiveness
- ⬇ Inconsistencies in configuration
- ⬇ Physical change processes ineffective
- ⬇ Inadequate tenant segmentation

Virtualization containers effects on security



Fuzzy Time Boundaries

- ⬆ Great availability / recovery mechanism
- ⬇ Security and audit events can be lost
- ⬇ Changes in time are not visible from inside the virtual server

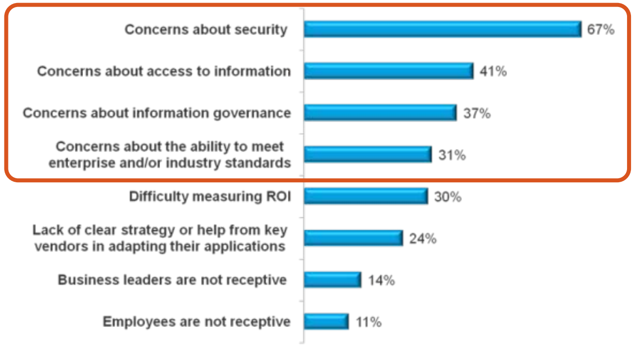
VM Mobility

- ⬆ Improved Service Levels
- ⬇ Identity divorced from physical location
- ⬇ Policies may not follow virtual machine

VM Encapsulation

- ⬆ Ease DR
- ⬆ Hardware Independence
- ⬇ Outdated offline systems
- ⬇ Unauthorized copy
- ⬇ Reconfiguring virtual hardware and console access are over the network operations

Security and compliance challenges for Cloud



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

PCI Security Standards Council™

Shionogi & Co:
$3.2B pharmaceutical company
Laid off IT admin:

- Logged in remotely to vSphere from local McDonald's WIFI
- Deleted 88 virtual production servers
- Took down email, order entry, payroll, BlackBerry, & other services
- Caused $800K damage

CIO security concerns for cloud

Top CIO challenges to implementing a cloud computing strategy:

1. Security
2. Access to information
3. Information Governance
4. Ability to meet enterprise standards

Source: 2010 IDG Enterprise Cloud-based Computing Research, November 2010

Compliance standards

Virtualization/Cloud

- Increases impact of any compromise
- Creates a more complex environment—additional layers require additional controls
- Creates a new attack surface that must be hardened
- Impacts roles and responsibilities

Access control and management

- **87%** of companies have experienced a data breach

  — IT Compliance Institute

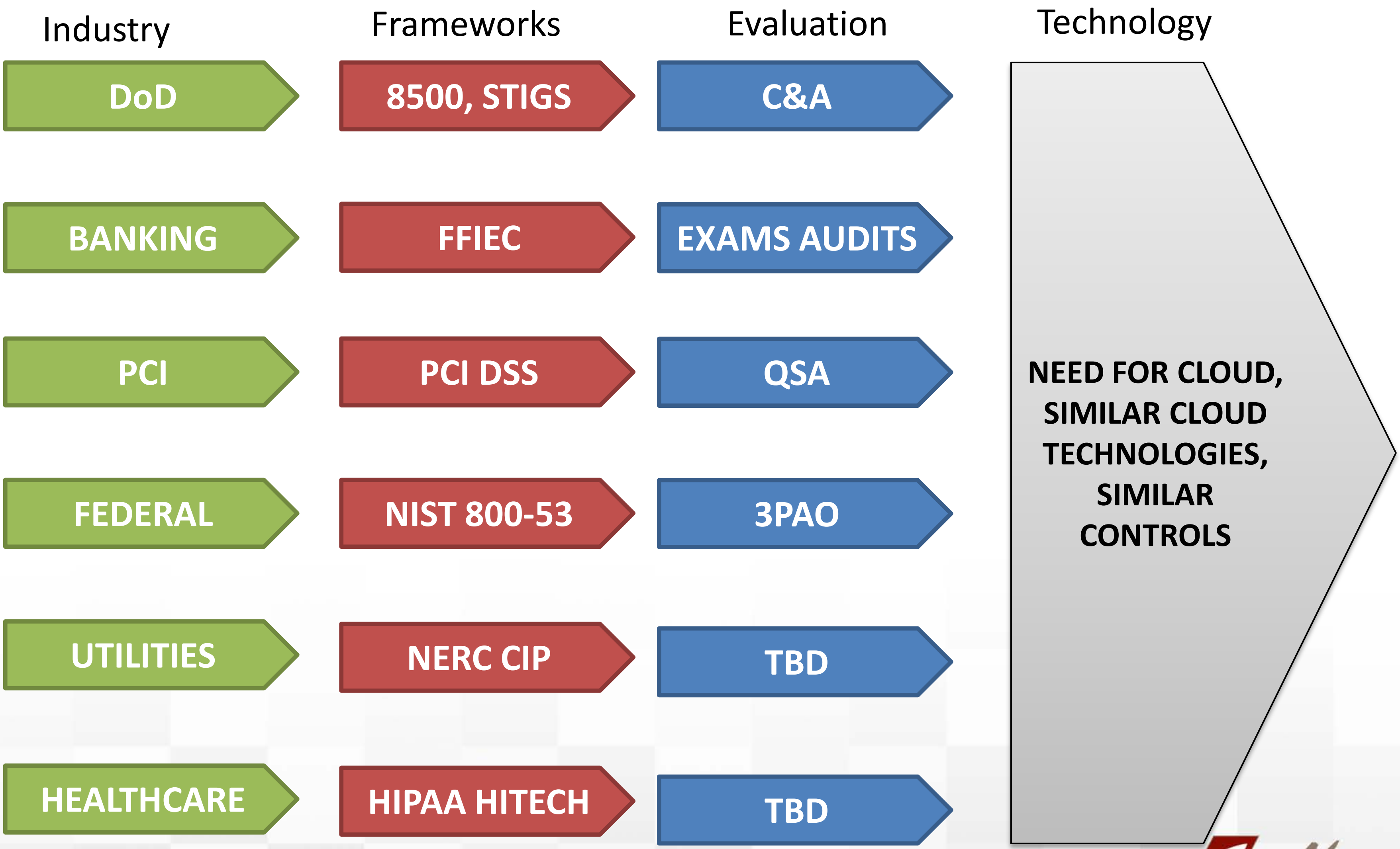
- **74%** lost customers as a result of the breach

  — IT Compliance Institute

- **48%** of all breaches involved privileged user misuse

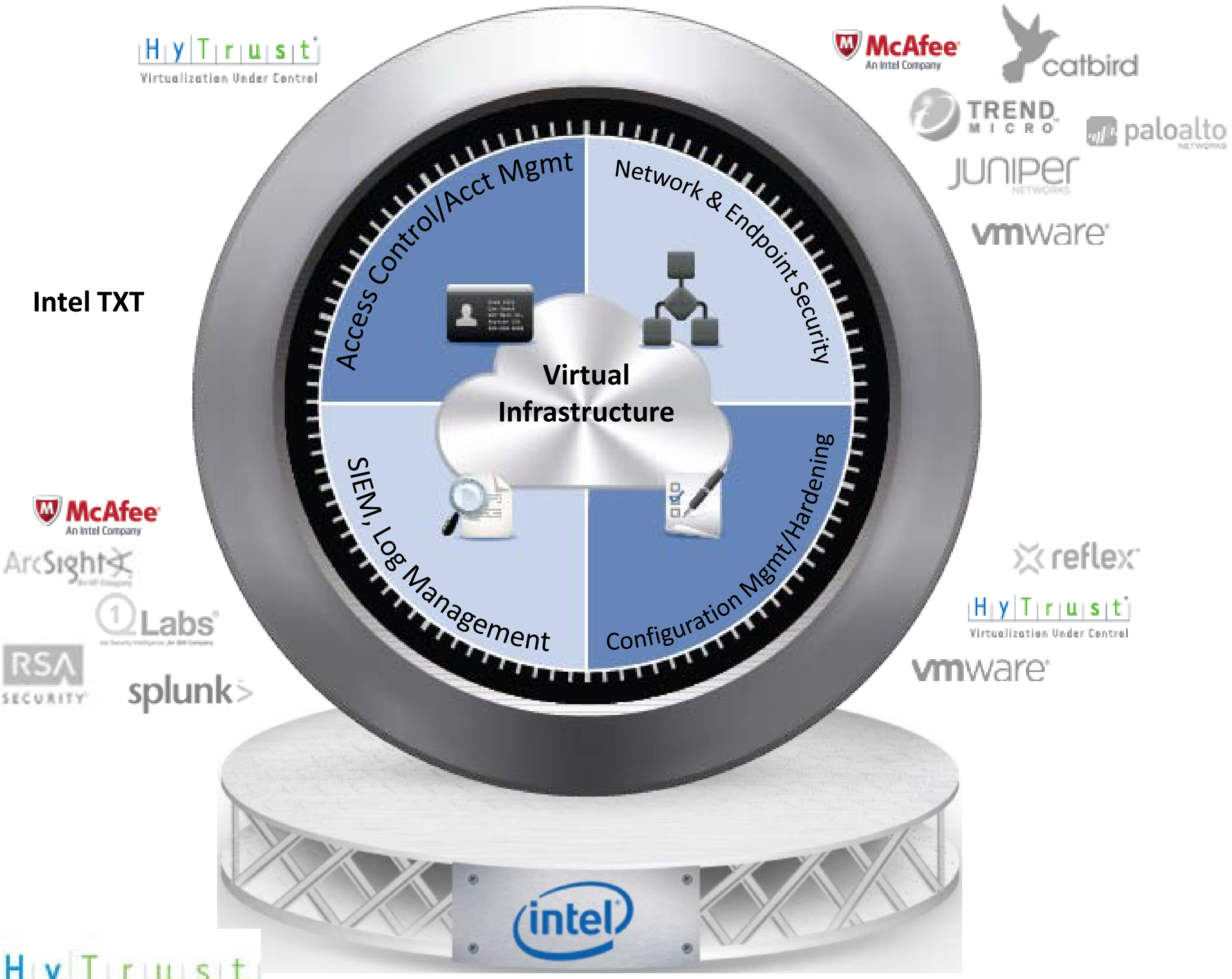
  — Verizon report, 2010

Different Industries have similar challenges.



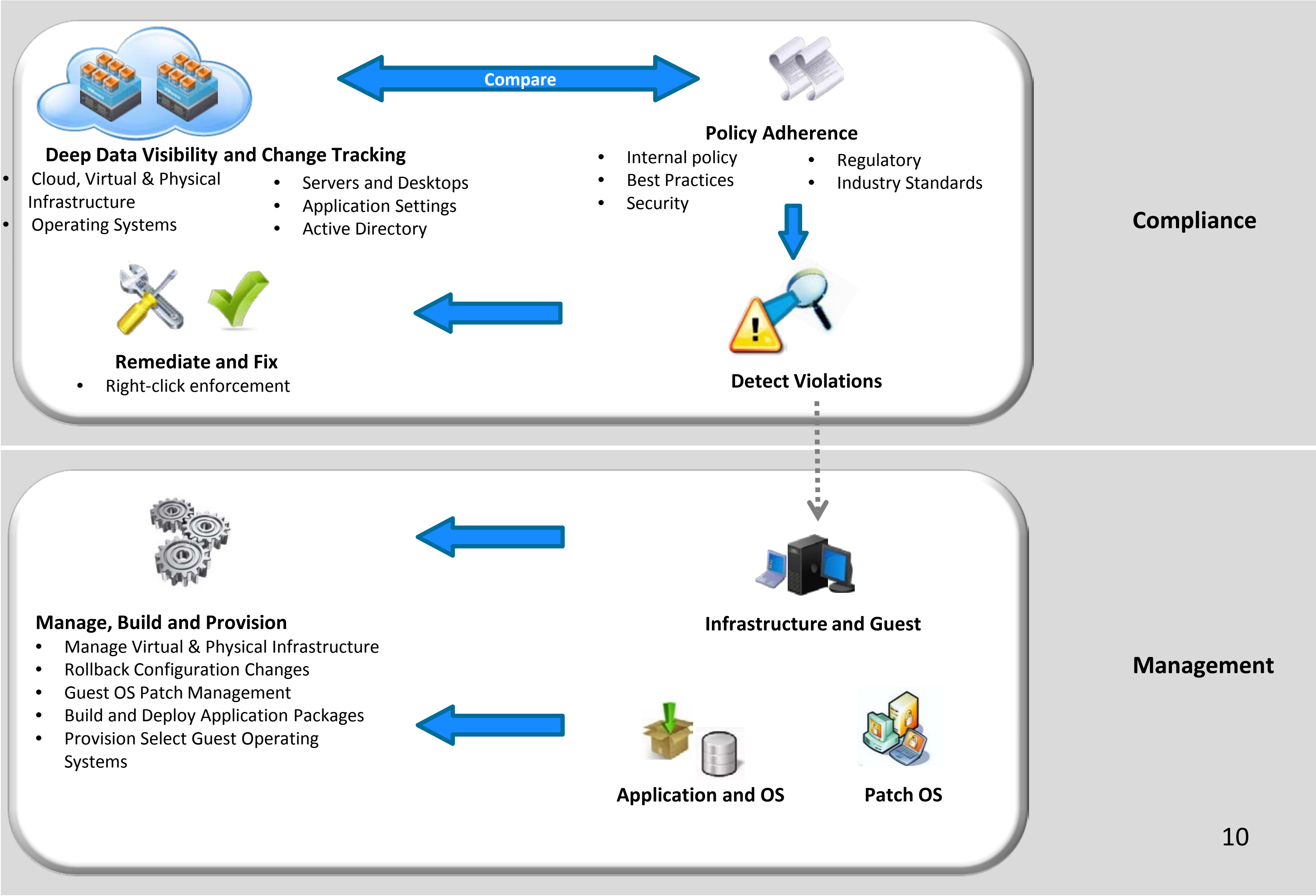
Industry	Frameworks	Evaluation	Technology
DoD	8500, STIGS	C&A	NEED FOR CLOUD, SIMILAR CLOUD TECHNOLOGIES, SIMILAR CONTROLS
BANKING	FFIEC	EXAMS AUDITS	
PCI	PCI DSS	QSA	
FEDERAL	NIST 800-53	3PAO	
UTILITIES	NERC CIP	TBD	
HEALTHCARE	HIPAA HITECH	TBD	

4 “Must Haves”



Intel TXT

Virtual and Physical Configuration Management



Deep Data Visibility and Change Tracking

- Cloud, Virtual & Physical Infrastructure
- Operating Systems
- Servers and Desktops
- Application Settings
- Active Directory

Policy Adherence

- Internal policy
- Best Practices
- Security
- Regulatory
- Industry Standards

Remediate and Fix

- Right-click enforcement

Detect Violations

Compliance

Manage, Build and Provision

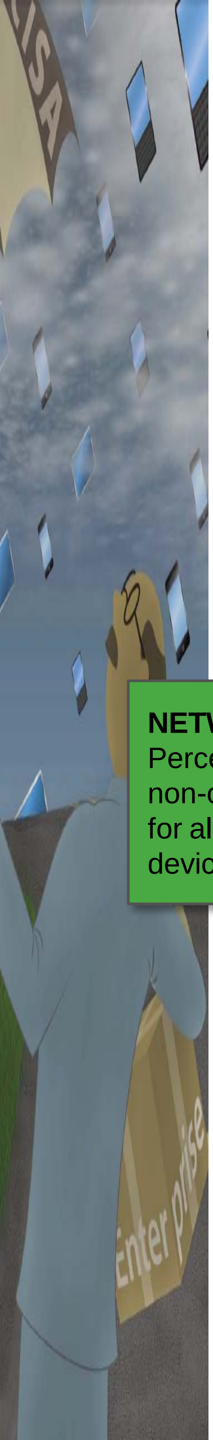
- Manage Virtual & Physical Infrastructure
- Rollback Configuration Changes
- Guest OS Patch Management
- Build and Deploy Application Packages
- Provision Select Guest Operating Systems

Infrastructure and Guest

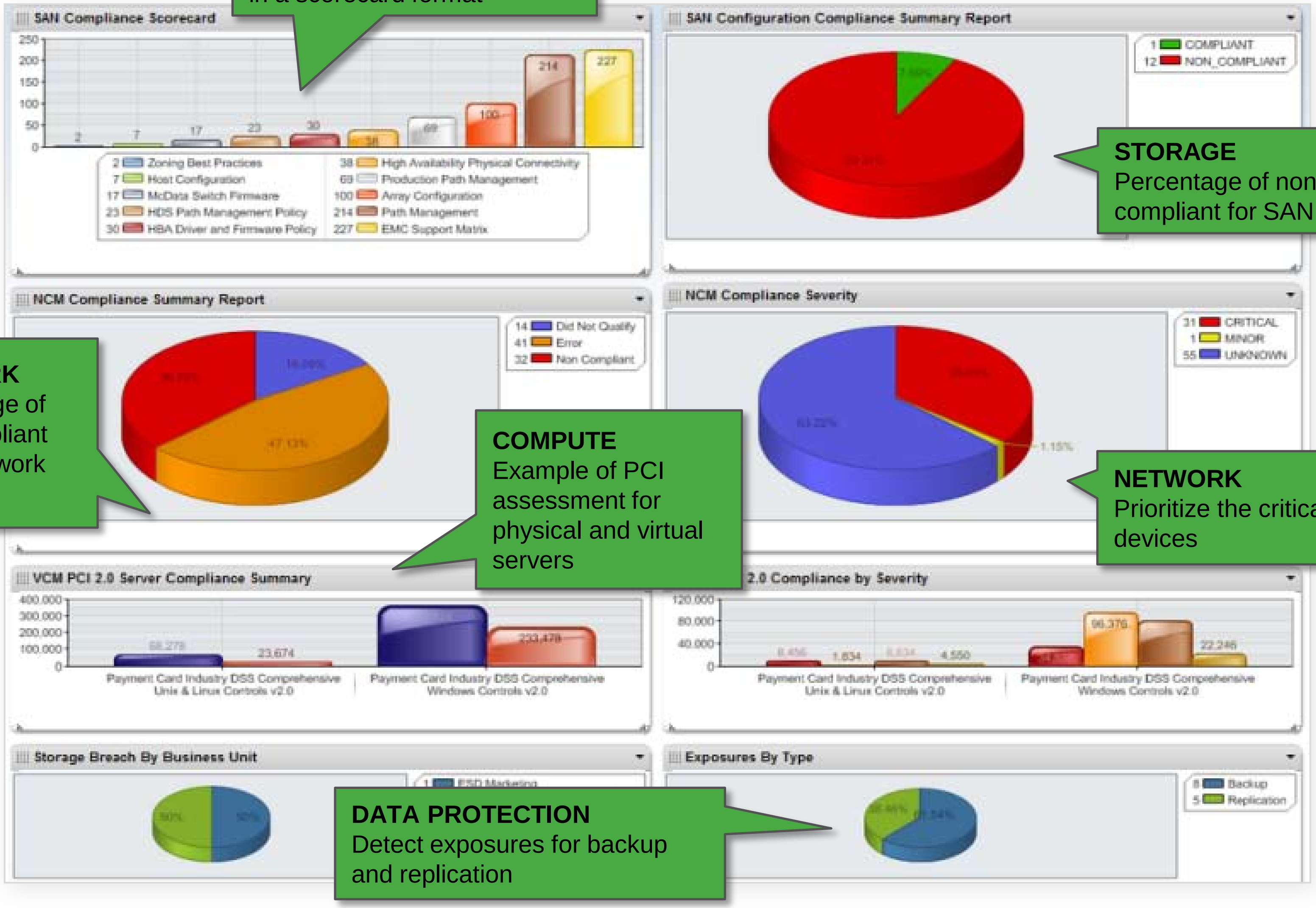
Application and OS

Patch OS

Management



eGRC Ecosystem Ex - VMware + EMC + RSA


SAN Compliance Scorecard
250
200
150
100
50
0
2
7
17
23
30
38
69
100
214
227
2 Zoning Best Practices
7 Host Configuration
17 McData Switch Firmware
23 HDS Path Management Policy
30 HBA Driver and Firmware Policy
38 High Availability Physical Connectivity
69 Production Path Management
100 Array Configuration
214 Path Management
227 EMC Support Matrix
SAN Configuration Compliance Summary Report
1 COMPLIANT
12 NON_COMPLIANT
NCM Compliance Summary Report
16.09%
47.13%
14 Did Not Qualify
41 Error
32 Non Compliant
NCM Compliance Severity
63.22%
1.15%
31 CRITICAL
1 MINOR
55 UNKNOWN
VCM PCI 2.0 Server Compliance Summary
400,000
300,000
200,000
100,000
0
68,279
23,674
233,478
Payment Card Industry DSS Comprehensive Unix & Linux Controls v2.0
Payment Card Industry DSS Comprehensive Windows Controls v2.0
2.0 Compliance by Severity
120,000
80,000
40,000
0
8,456
1,834
8,834
4,550
96,376
22,246
Payment Card Industry DSS Comprehensive Unix & Linux Controls v2.0
Payment Card Industry DSS Comprehensive Windows Controls v2.0
Storage Breach By Business Unit
50%
50%
1 ESD Marketing
Exposures By Type
8 Backup
5 Replication

STORAGE
Enable category of breaches in a scorecard format

STORAGE
Percentage of non-compliant for SAN storag

NETWORK
Percentage of non-compliant for all network devices

COMPUTE
Example of PCI assessment for physical and virtual servers

NETWORK
Prioritize the critical devices

DATA PROTECTION
Detect exposures for backup and replication

PCI Solution Components

Endpoint Protection

- Comprehensive Endpoint Solution
- Blacklisting and Whitelisting
- Virtualization Optimizations (vShield API Integration)

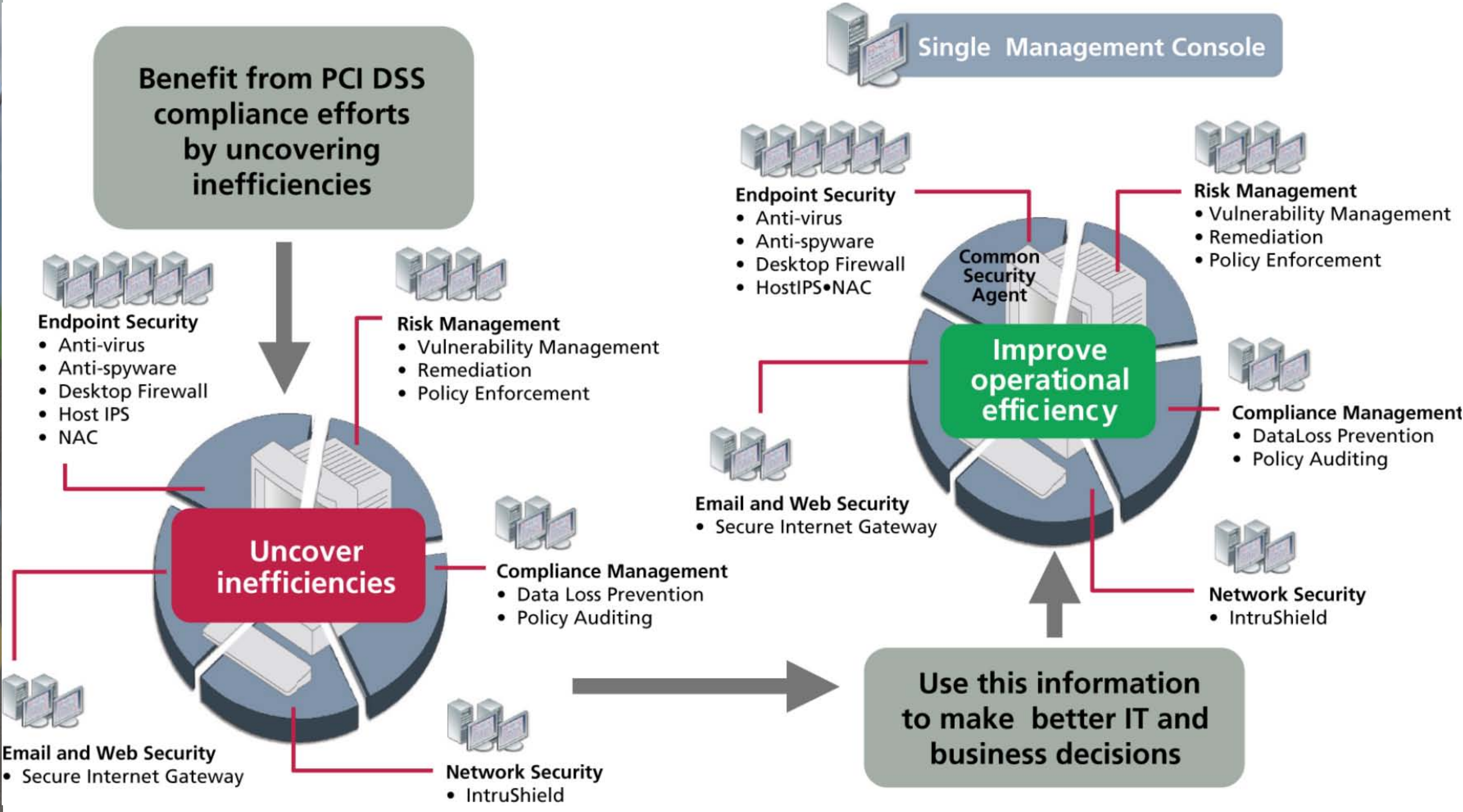
Network Security

- Complete Network Security
- Integration with vShield API

Security Management

- Unified Security Management
- SIEM integration with Virtual infrastructure

McAfee Compliance Solution & Process



Benefit from PCI DSS compliance efforts by uncovering inefficiencies

Endpoint Security
- Anti-virus
- Anti-spyware
- Desktop Firewall
- Host IPS
- NAC

Risk Management
- Vulnerability Management
- Remediation
- Policy Enforcement

Uncover inefficiencies

Compliance Management
- Data Loss Prevention
- Policy Auditing

Email and Web Security
- Secure Internet Gateway

Network Security
- IntruShield

Single Management Console

Endpoint Security
- Anti-virus
- Anti-spyware
- Desktop Firewall
- HostIPS•NAC

Common Security Agent

Risk Management
- Vulnerability Management
- Remediation
- Policy Enforcement

Improve operational efficiency

Compliance Management
- DataLoss Prevention
- Policy Auditing

Email and Web Security
- Secure Internet Gateway

Network Security
- IntruShield

Use this information to make better IT and business decisions

Key Takeaways

- Understand security and compliance implications of virtualizing your datacenter
- Review and update existing processes and technologies
  - An ecosystem of technologies will be required to address even the minimum MUST HAVES
  - Look to vendors that are working together

Resources

- ISACA Virtualization Checklist - http://www.isaca.org/Knowledge-Center/Research/Documents/Virtualization-Security-Checklist-26Oct2010-Research.pdf
- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Virtualization-Benefits-and-Challenges.aspx
- Coalfire Systems:
- HyTrust: http://www.hytrust.com/resources/main
- McAfee:
- VMWare: http://www.vmware.com/

Appendix

COBIT

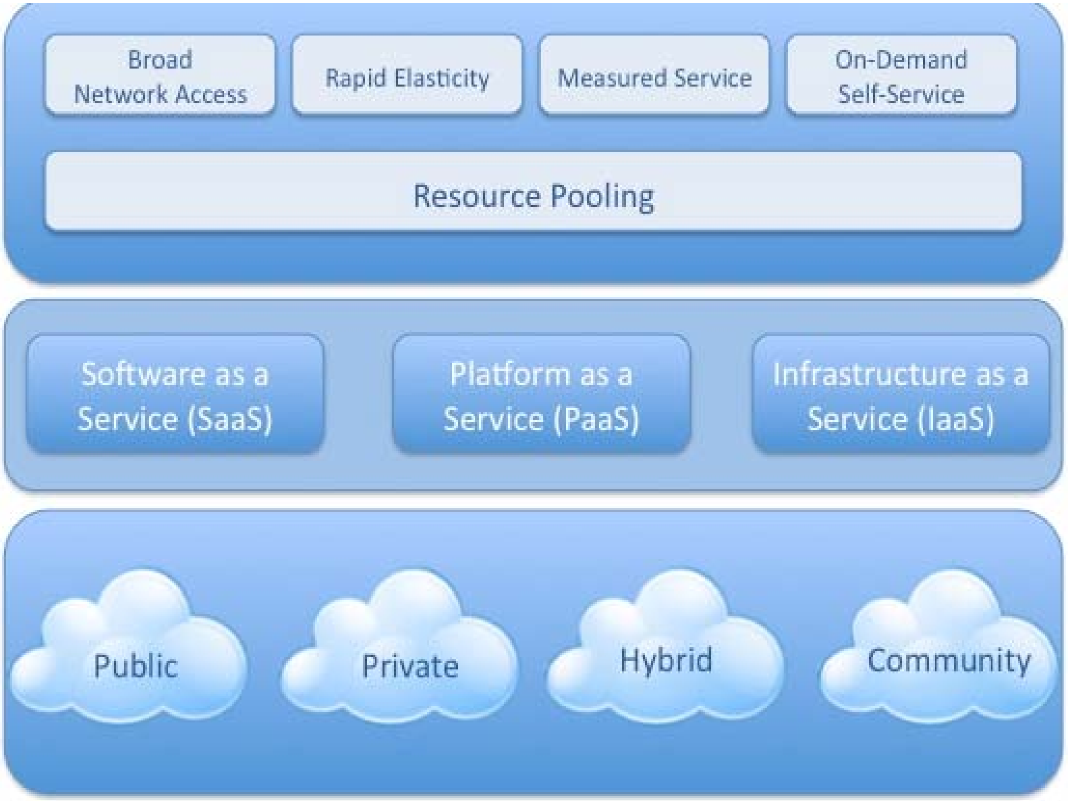
ISACA Checklist Mapping To	CObIT Control Objective(s)
1. Securing the virtualization platform a. Platform and installation requirements	
1.a.1 Limit physical access to the host: only authorized administrative personnel should have physical access to the host system to prevent unauthorized changes.	PO4.9, DS12.3
1.a.2 Verify integrity of files prior to installation: verify the hash values of system files, as provided by the vendor, prior to installation to ensure integrity.	PO2.4, AI3.2
1.a.3 Load and enable only required operating system components and services: no unnecessary operating systems components (e.g., drivers) should be loaded, and no unnecessary services should be enabled (e.g., printing services, file sharing services).	AI3.2
1.a.4 BIOS, bootloader passwords: passwords should be used for BIOS and bootloaders (e.g., GRUB) for both hosts and guests.	DS5.3

Source: ISACA Virtualization-Security-Checklist-26Oct2010-Research.pdf

Planning an IT Assessment/Audit

The cloud is defined, but….

how can it be assessed?



How do you determine that something is a cloud?
What is the accepted methodology to measure rapid elasticity?

How do you assess a stand alone service?
Can you assess a service without the underlying supporting technology?

How is the accreditation boundary/scope affected?

What assessment can you re-use?

What is “Compliance in the Cloud?”

COBIT ISO-27002 CSA cloud security alliance FedRAMP PCI Security Standards Council SHARED ASSESSMENTS

Compliance is built from standards . Today there are several emerging standards attempting to solve the question “what are reasonable controls ?”

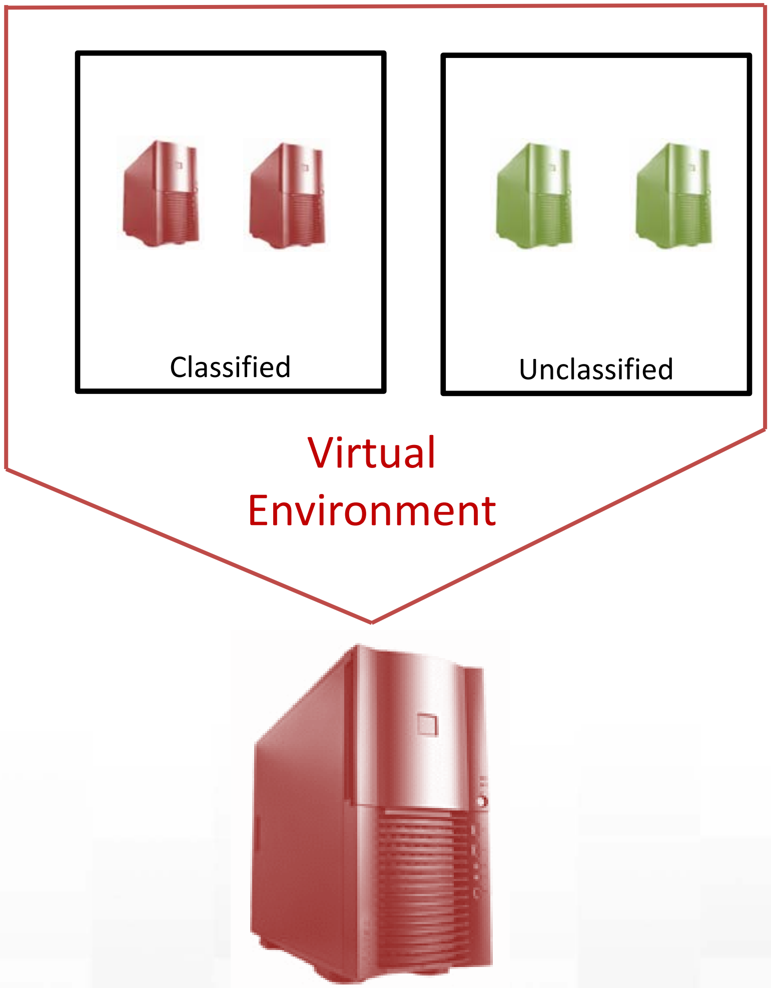
Big Issues

1. What is “the Cloud?”
2. What are the appropriate controls for the cloud?
3. What is the scope/boundary of the assessment?
4. What are the appropriate tests?
5. What are the required skillsets?
6. Snapshots, sprawl, authentication.

Other Issues

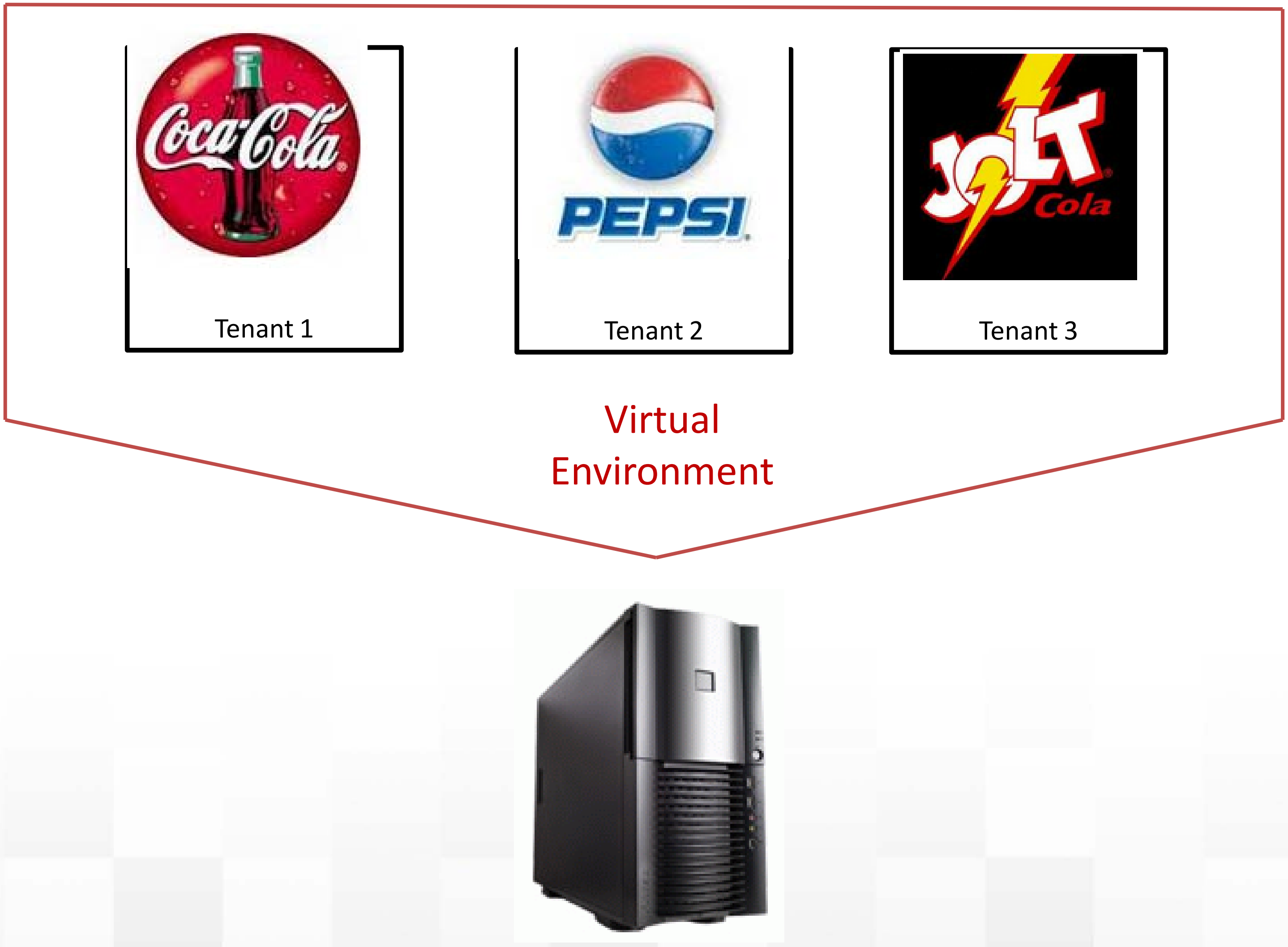
1. What tools are required?
2. What education is required?
3. How much testing can be leveraged from other audits/assessments?
4. How do different approaches affect scope (encryptions, access control, authentication)?
5. What does the report look like?
6. How often should it be conducted?
7. How does it integrate with continuous monitoring?
8. What’s the appropriate sample size for a dynamic environment?

Segmentation – “Mixed Mode”



“Mixed-mode” refers to a virtualization configuration where different security profiles are running on the same hypervisor.

Segmentation - Multi-Tenancy



Tenant 1

Tenant 2

Tenant 3

Virtual Environment

Multi-Tenant