HIMSS® 11

ANNUAL CONFERENCE & EXHIBITION

SECURING HEALTH INFORMATION IN THE CLOUD

Feisal Nanji, Executive Director, Techumen

feisal@techumen.com

Techumen

Conflict of Interest Disclosure

Feisal Nanji, MPP, CISSP

Has no real or apparent
conflicts of interest to report.

LEARNING OBJECTIVES

- Describe the advantages of Cloud computing for Health Providers
- Identify the major concerns of securing health information in the cloud
- Recognize the key steps to overcoming health information security and privacy issues in the cloud
- Define a suitable audit and compliance process to ensure security and privacy in the cloud

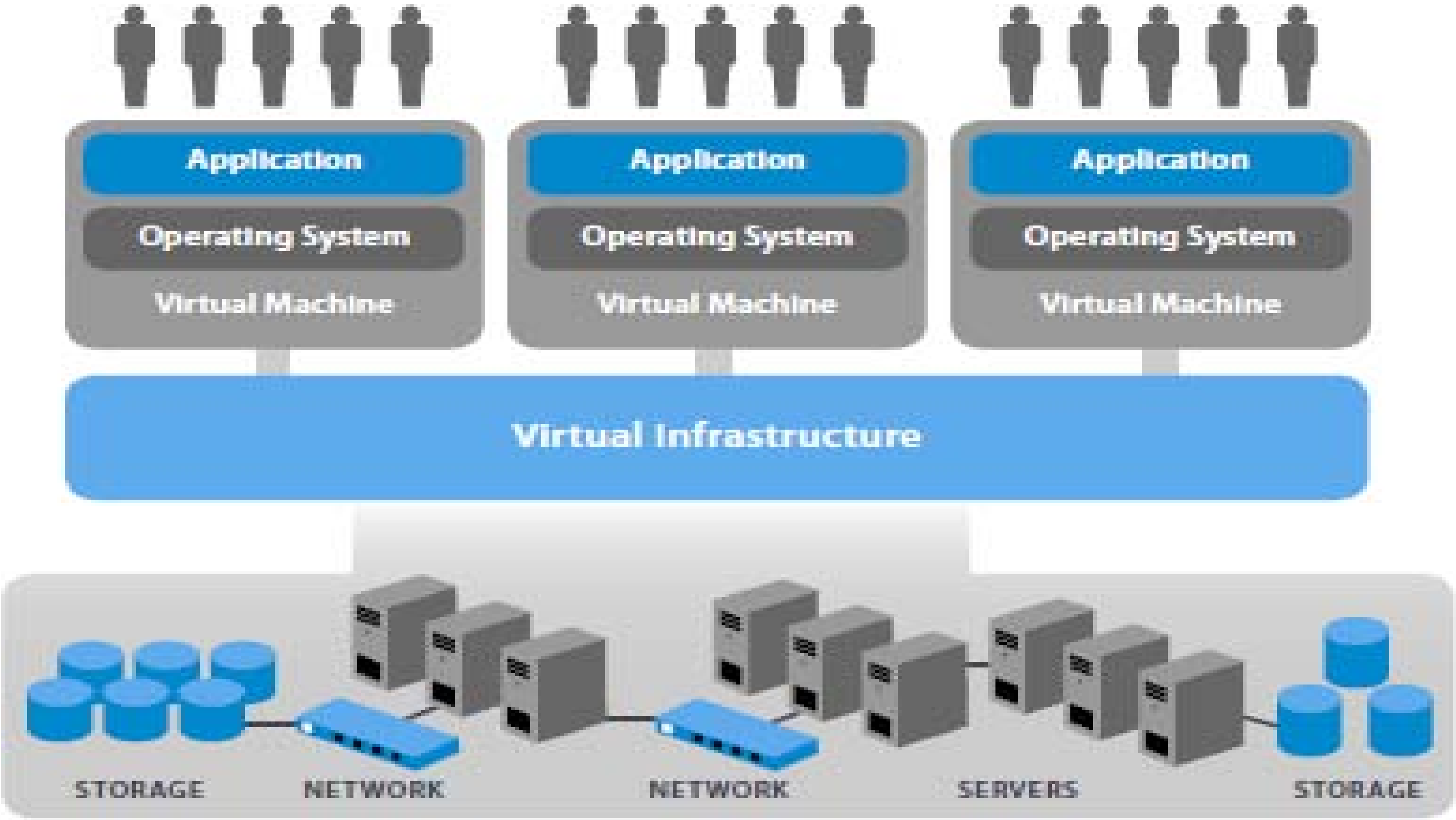
On Cloud Nine
9

WHAT SHOULD YOU TAKE AWAY?

1. Level set – Core technology for cloud computing
2. Cloud computing -- variants
3. What are the key compliance / security concerns of the cloud?
4. How should we manage security in the cloud?

CORE TECHNOLOGY

- Fast networks
- Web enabled eco-system
- The “Virtual Machine”


Application
Operating System
Virtual Machine
Application
Operating System
Virtual Machine
Application
Operating System
Virtual Machine
Virtual Infrastructure
STORAGE
NETWORK
NETWORK
SERVERS
STORAGE

VIRTUALIZATION CONCERNS…

- Increases complexity
- Strains infrastructure
- Can cause large-scale failure
- Requires special maintenance

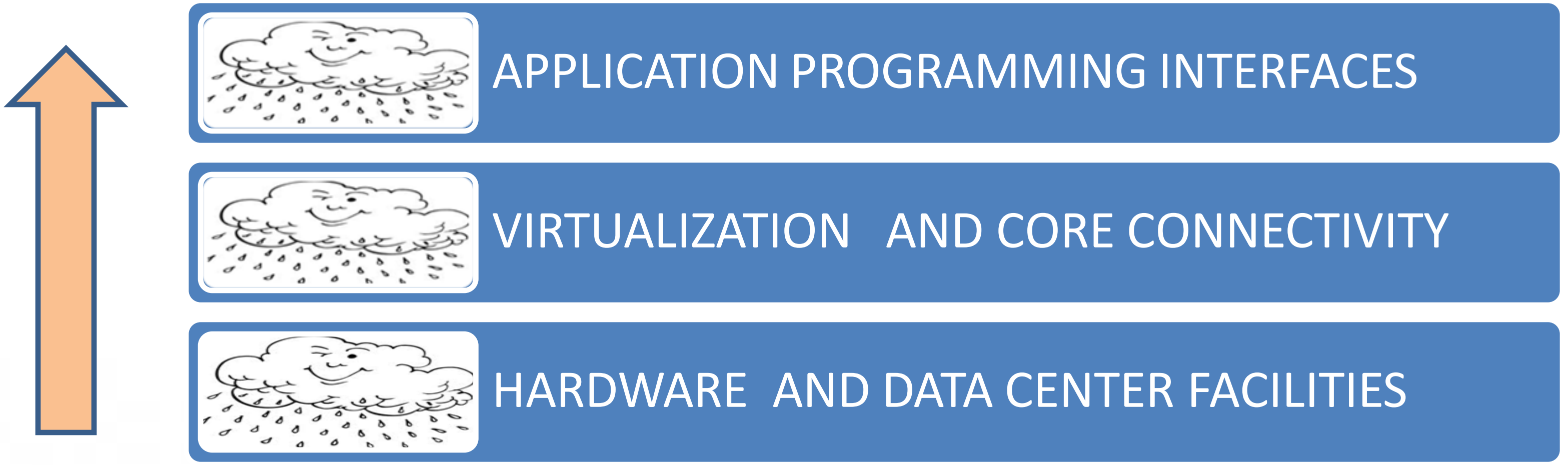
THIS ALLOWS……

- Computing capability on demand
- Resource pooling – storage, CPU
- Rapid deployment and scaling of IT services
- Easy measurement of what’s been used

LEADING TO CLOUD VARIANTS….

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

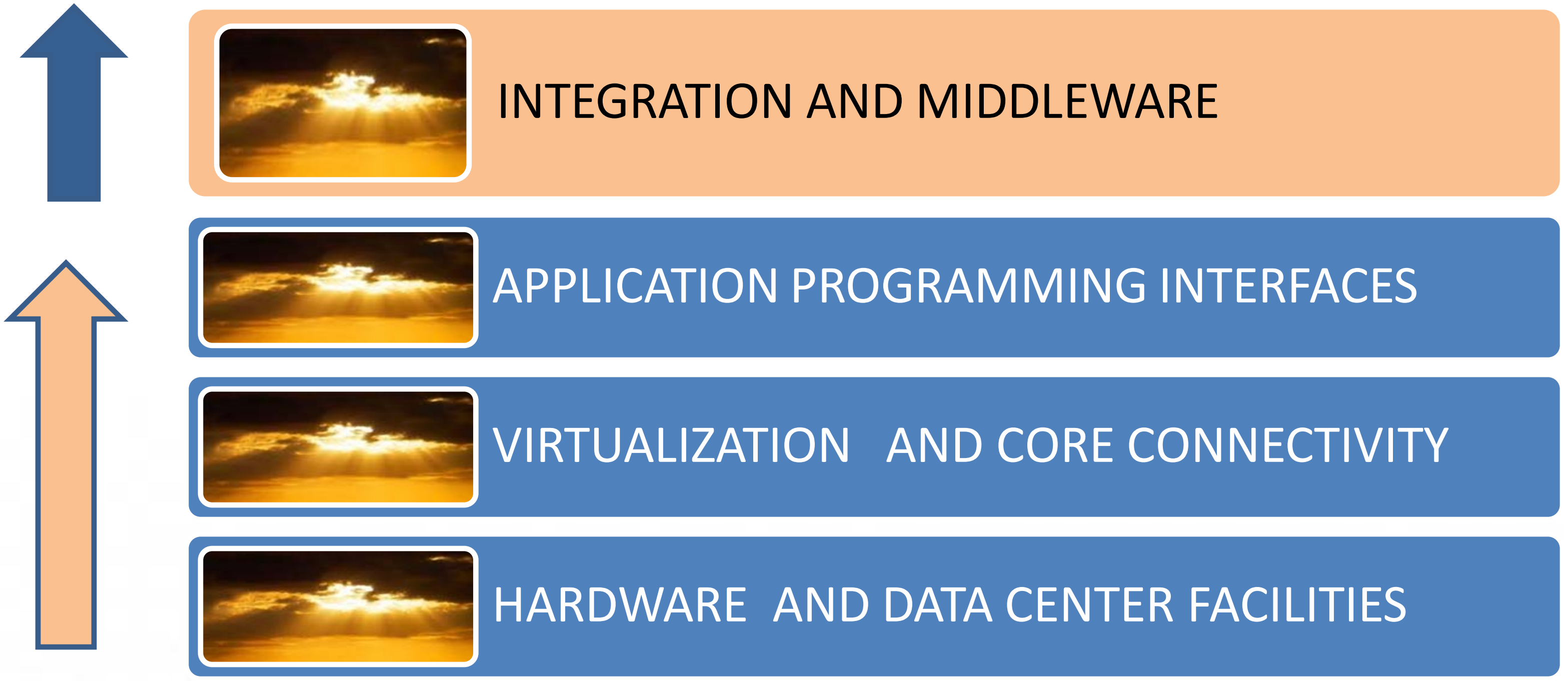
Infrastructure as a Service (IaaS)


APPLICATION PROGRAMMING INTERFACES

VIRTUALIZATION AND CORE CONNECTIVITY

HARDWARE AND DATA CENTER FACILITIES

Platform as a Service (PaaS)



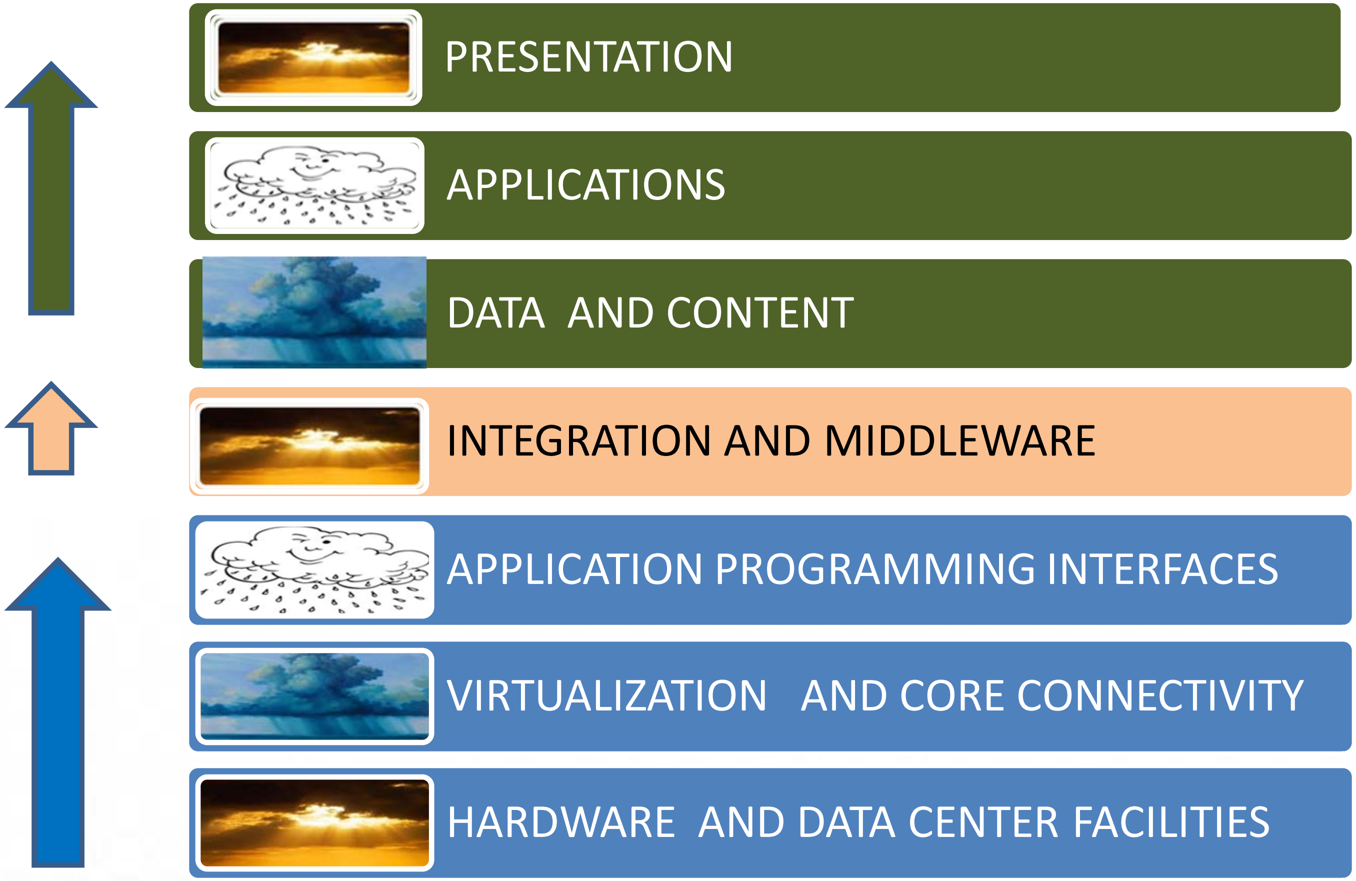
INTEGRATION AND MIDDLEWARE

APPLICATION PROGRAMMING INTERFACES

VIRTUALIZATION   AND CORE CONNECTIVITY

HARDWARE AND DATA CENTER FACILITIES

Software as a Service (SaaS)



PRESENTATION

APPLICATIONS

DATA AND CONTENT

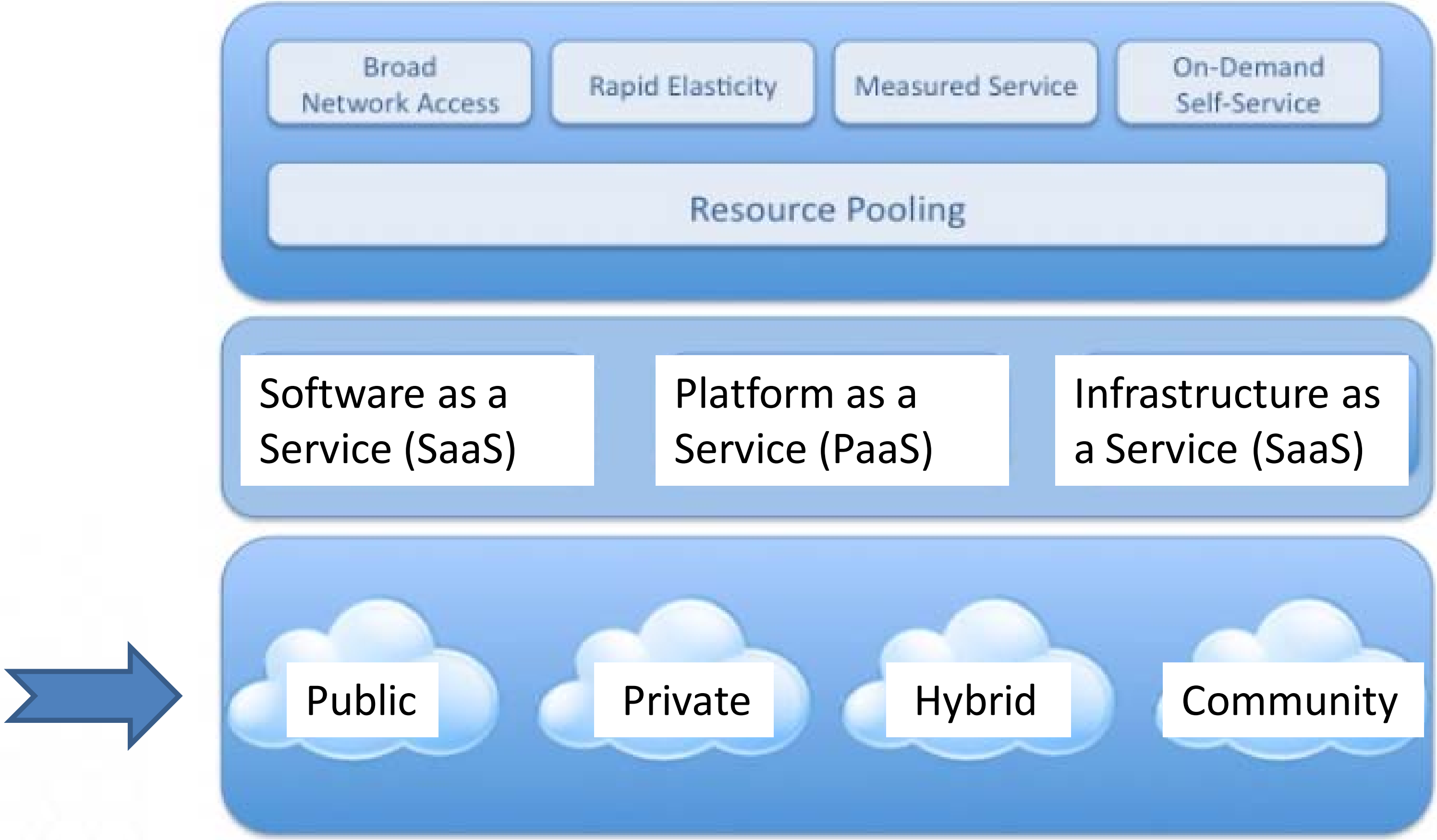
INTEGRATION AND MIDDLEWARE

APPLICATION PROGRAMMING INTERFACES

VIRTUALIZATION AND CORE CONNECTIVITY

HARDWARE AND DATA CENTER FACILITIES

CLOUD: A SUMMARY



Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Resource Pooling

Essential Characteristics

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (SaaS)

Service Models

Public

Private

Hybrid

Community

Deployment Models

CLOUD – HELPING HEALTH CARE….

- Providers, EMR vendors, Health Plans, Government, HIE etc.
- Cheaper and faster
- Better compliance (security)???

TRADITIONAL DATA CENTER SECURITY APPROACHES…

- Physical configuration management governs deployment and control implementation --- standards for specification, configuration, and operation
- Physical control as the ultimate breakwater for logical access control to platforms and applications
- Enterprise policies and organization for separation of duties and control
- Patch testing and patch management … physical-platform- by-physical-platform
- Data and applications are wherever the machine is and networks are between machines

BUT AS "PHYSICAL" VISIBILITY IS LOST….

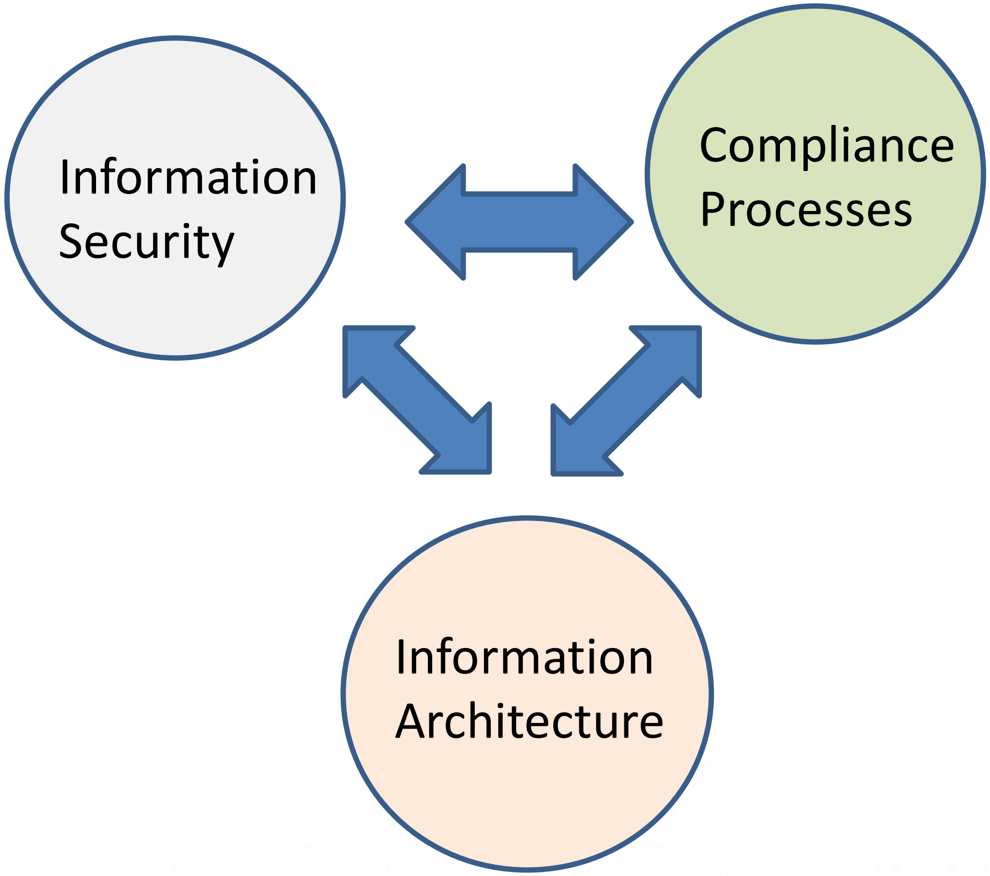
- Where is the data?
- Who can see the data?
- Who has seen the data?
- Has data been tampered?
- Where is processing performed?
- How is processing configured?
- Does backup happen? How? Where?

AND COMPLIANCE -- IS NOT JUST SECURITY

1	HIPAA Security
2	Medical Fraud
3	e- Prescribing
4	Mental and behavioral health
5	Health Information Exchange
6	Health Quality reporting
7	Policy, Procedure Mgt.
8	Medical Research
9	Payment Card Industry (PCI)
10	FTC Red Flags Rule

HEALTH CARE COMPLIANCE AND THE CLOUD

TYPES OF AUDITS	PERFORMED BY	AUGMENTED BY
↓	↓	↓
Systems Reviews	Dept of Health and Human Services(CMS)	Audit tools and legal framework
Transaction Reviews	Independent Review Organizations	Internal audit processes
Policy and Procedure Reviews	States	**Information technology**
Risk Assessments	Federal Trade Commission	
	Payment Card Industry (PCI)	
	Customers / Business Associates	
	Internal Audit	
	Food and Drug Adminstration (FDA)	


Information Security

Compliance Processes

Information Architecture

Requires an interconnected strategy

ARE YOU CLOUD READY?

- Have you standardized most commonly repeated operating procedures?
- Have you fully automated deployment and management?
- Can you provide self-service access for users?
- Are your business units ready to share the same infrastructure?

MAJOR CLOUD COMPLIANCE ISSUES INCLUDE:

- Data ownership and control
  - Trust ,consequences and chain of custody
  - Access and authentication
- Facilities and service provision
  - e.g. shared data centers / resources
- Administration
  - Policies, transparency, auditing

KEY CLOUD SECURITY CONCERNS

- Virtualization software (e.g., hypervisor) risk exposure
- Inability to determine location of data or processing
- Mobility among VM's **contradicts** control principles; boundaries become unreliable and blurred
- Limited visibility into host O/S's and virtual network (to find vulnerabilities and assess/report configuration, patching)

LEAD TO VERY GRANULAR ISSUES:

- Security policies need to shift "up the stack" to match logical attributes

- Network Access control and Intrusion Prevention

- Root kit Detection

- Inter VM traffic analysis

KEY CONSIDERATIONS

- Move away from physical attributes for meeting compliance

- Application, Identity and Content awareness

CORE RECOMMENDATIONS

- Think of information security as a set of adaptive services integrated with **compliance** requirements and **Information Architecture/Design**
- Get security vendors to deliver their security controls in a virtualized form
- Express security policy across physical, virtualized and private cloud-computing environments
- Maintain separation of duties between security policy enforcement and IT operations

On Cloud Nine
9

Feisal Nanji, Executive Director
feisal@techumen.com