



The Security Division of EMC

The Security Division of EMC



# Getting to the Bottom of Compliance in the Cloud

Steve Schlarman

eGRC Solutions Manager



**Steve Schlarman**

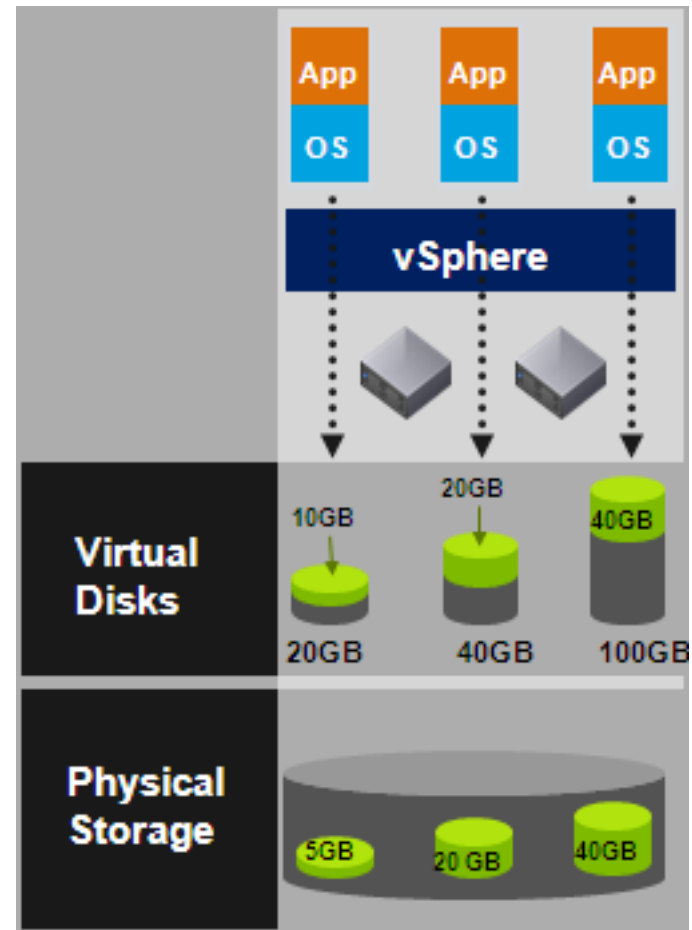
eGRC Solution Manager

RSA, The Security Division of EMC

[steve.schlarman@archer.com](mailto:steve.schlarman@archer.com)

# What Is Virtualization?

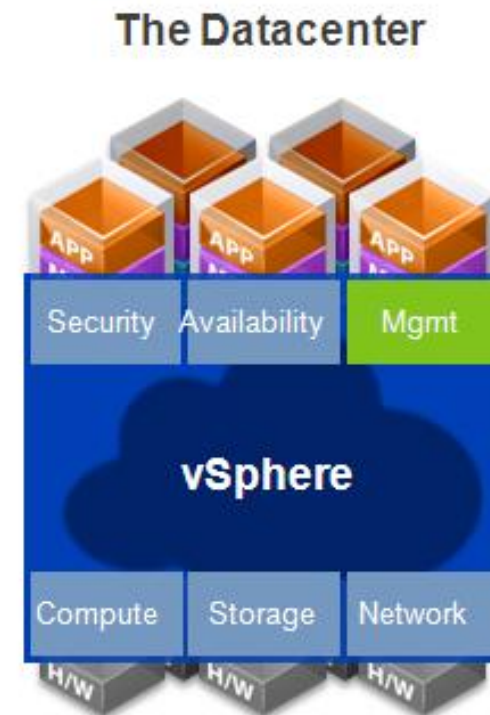
- ▶ Adds a layer of software on top of a server's hardware known as a "hypervisor"
- ▶ Creates a single resource pool from many separate servers
- ▶ Allocates hardware resources dynamically and transparently, between different servers and their clients
- ▶ Safely runs several operating systems and applications at the same time on a single server



- ▶ VMware customers typically save 50-70% on overall IT costs when virtualizing their data centers
- ▶ 51 million virtual servers are expected to run by 2012



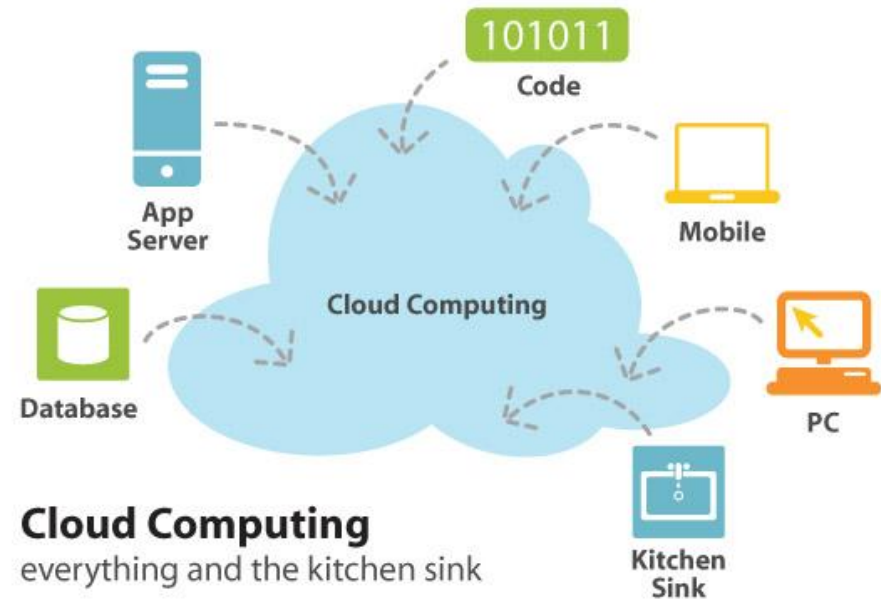
- ▶ On demand access computing resources as needed
- ▶ Applications pull resources from a virtual pool instead of being tied to a single server and storage array
- ▶ In a cloud environment, the virtual data center is moved off-site and is shared by a number of different organizations.
- ▶ This allows for even greater scalability and cost savings



# What is Cloud Computing?

Cloud Computing as defined by the National Institute of Standards and technology:

*A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”*

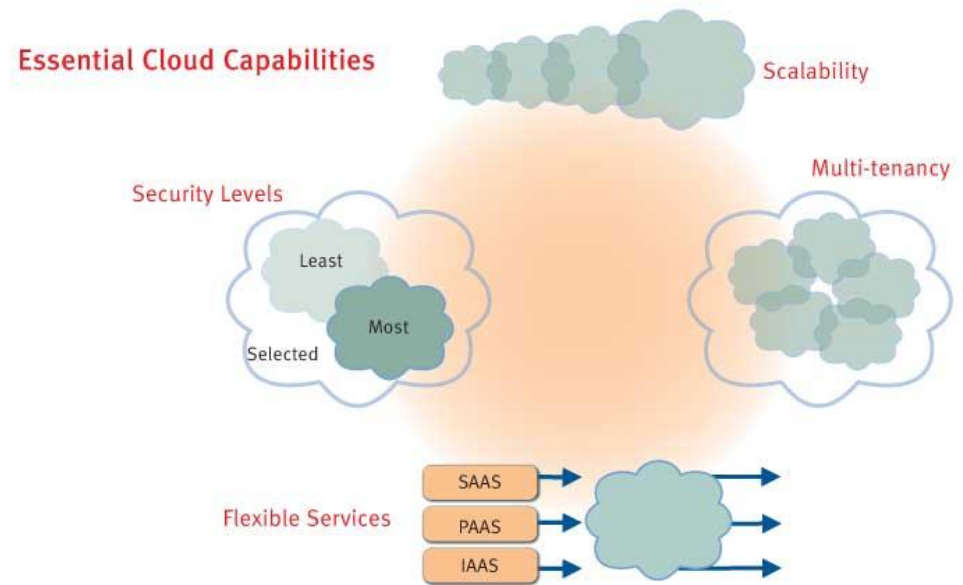


- 1. On-demand self-service:**  
Computing capabilities are automatically provisioned
- 2. Broad Network Access:**  
All computing available over the network
- 3. Resource Pooling:**  
Resources dynamically assigned based on demand
- 4. Rapid Elasticity:**  
Rapid provisioning, scaling out or in on demand
- 5. Measured Services:**  
Users only pay for the resources that they use



# What Does the Cloud Offer?

- ▶ Massively scalable and flexible through a huge pool of shared resources.
- ▶ Computing power and applications in a centralized location to which users connect over a network.
- ▶ Location is only centralized in a logical sense. The computing infrastructure can be spread around the globe.



## Definitions



A number of different on-demand services are made available to users in an external cloud environment.

## Examples



Consumers/businesses subscribe to whole or parts of an application that is hosted on a platform managed by a service provider

**Software as a Service (SaaS)**

Salesforce.com  
Hotmail  
Mozy by Decho

Consumers/businesses deploy their own applications on cloud infrastructure managed by the service provider

**Platform as a Service (PaaS)**

Google App Engine  
Force.com

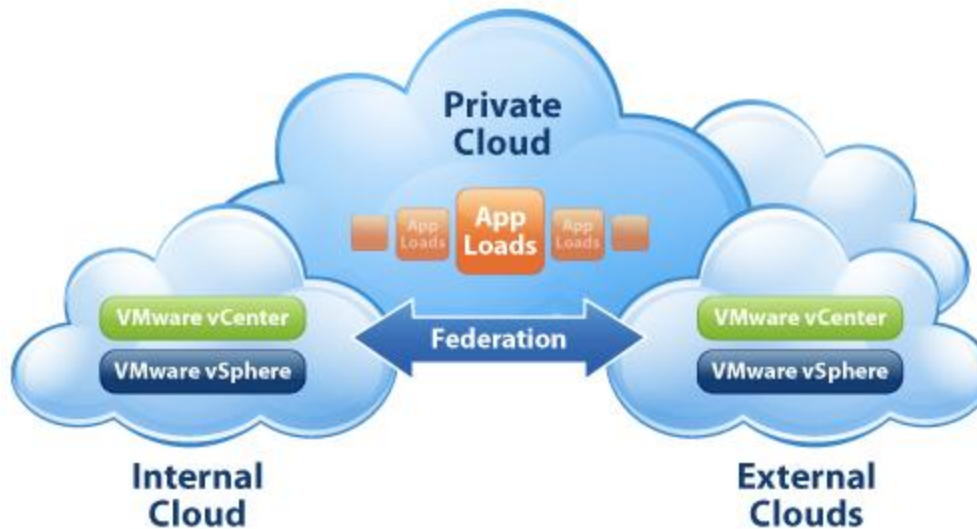
Consumers/businesses subscribe to processing, networks, or storage services for use with operating systems and applications of their choice

**Infrastructure as a Service (IaaS)**

Amazon EC2 (computing)  
EMC Atmos (storage)

The private cloud offers the scalability of the public cloud with the security and control of a internal cloud by utilizing both.

Organizations often host mission critical applications and sensitive data on internal clouds, while moving less important apps/data to an external cloud.



‘Cloud Computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.’

- Cloud Security Alliance, 2009



# Cloud Service Models (NIST SPI Model)

## Cloud Service Model

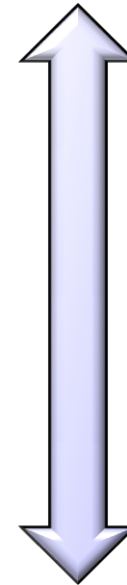
Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service  
(IaaS)

## Security Management

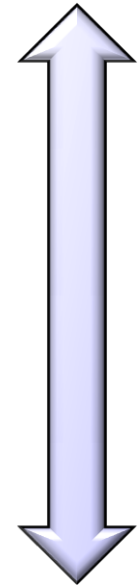
Provider



Provider &  
Customer

## Compliance Implications

Contractual



Collaboration

# Controls Environments of SPI Models

## Software as a Service (SaaS)

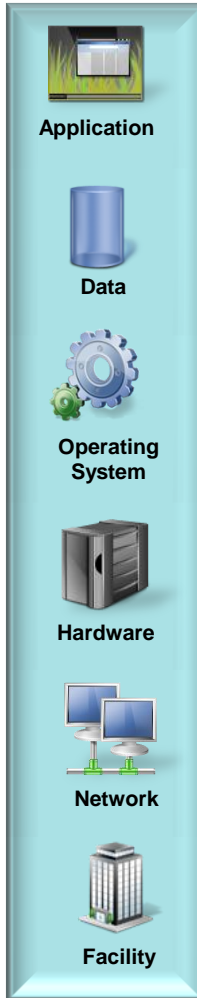
### Controls Environment

Customer:

- Application usage and user provisioning.

Provider:

- Application, development, management and security
- Database management and security
- Operating system configuration
- Hardware management
- Network management
- Facilities management



## Platform as a Service (PaaS)

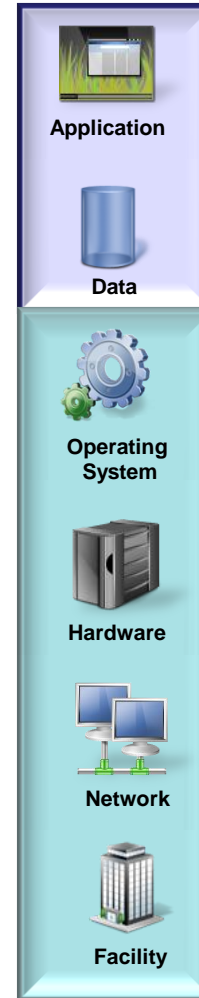
### Controls Environment

Customer:

- Application usage and user provisioning.
- Application development, deployment and security
- Database management and security

Provider:

- Operating system configuration and provisioning
- Hardware management
- Network management
- Facilities management



## Infrastructure as a Service (IaaS)

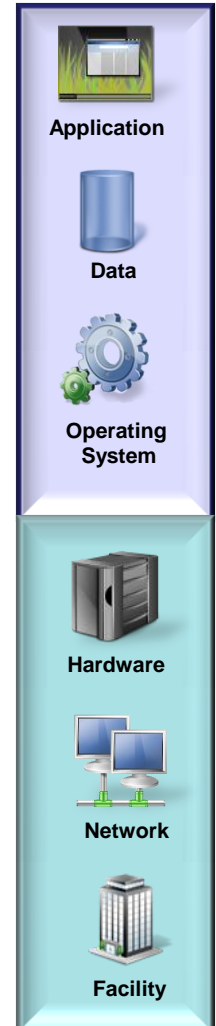
### Controls Environment

Customer:

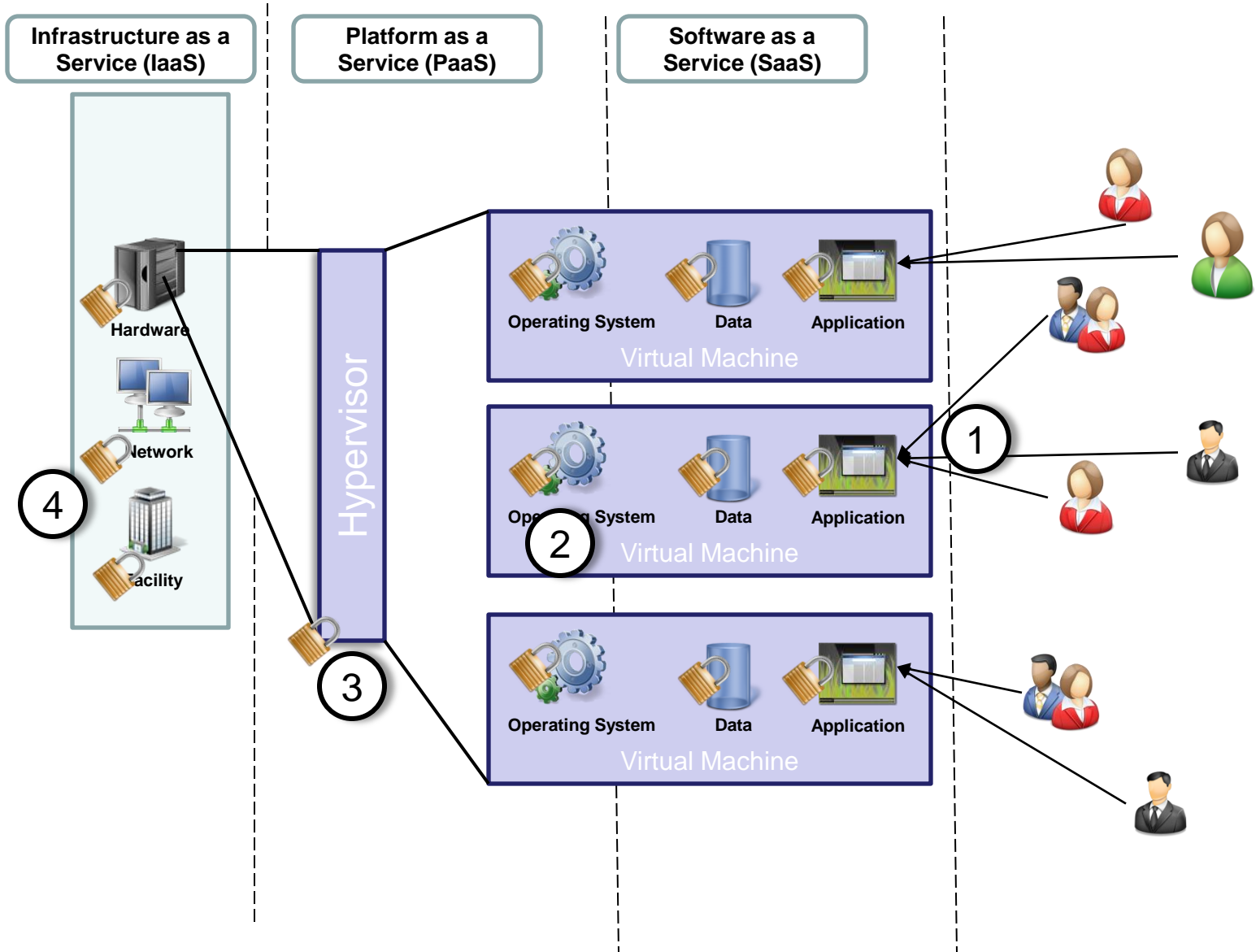
- Application usage and user provisioning.
- Application security
- Database security
- Operating system configuration

Provider:

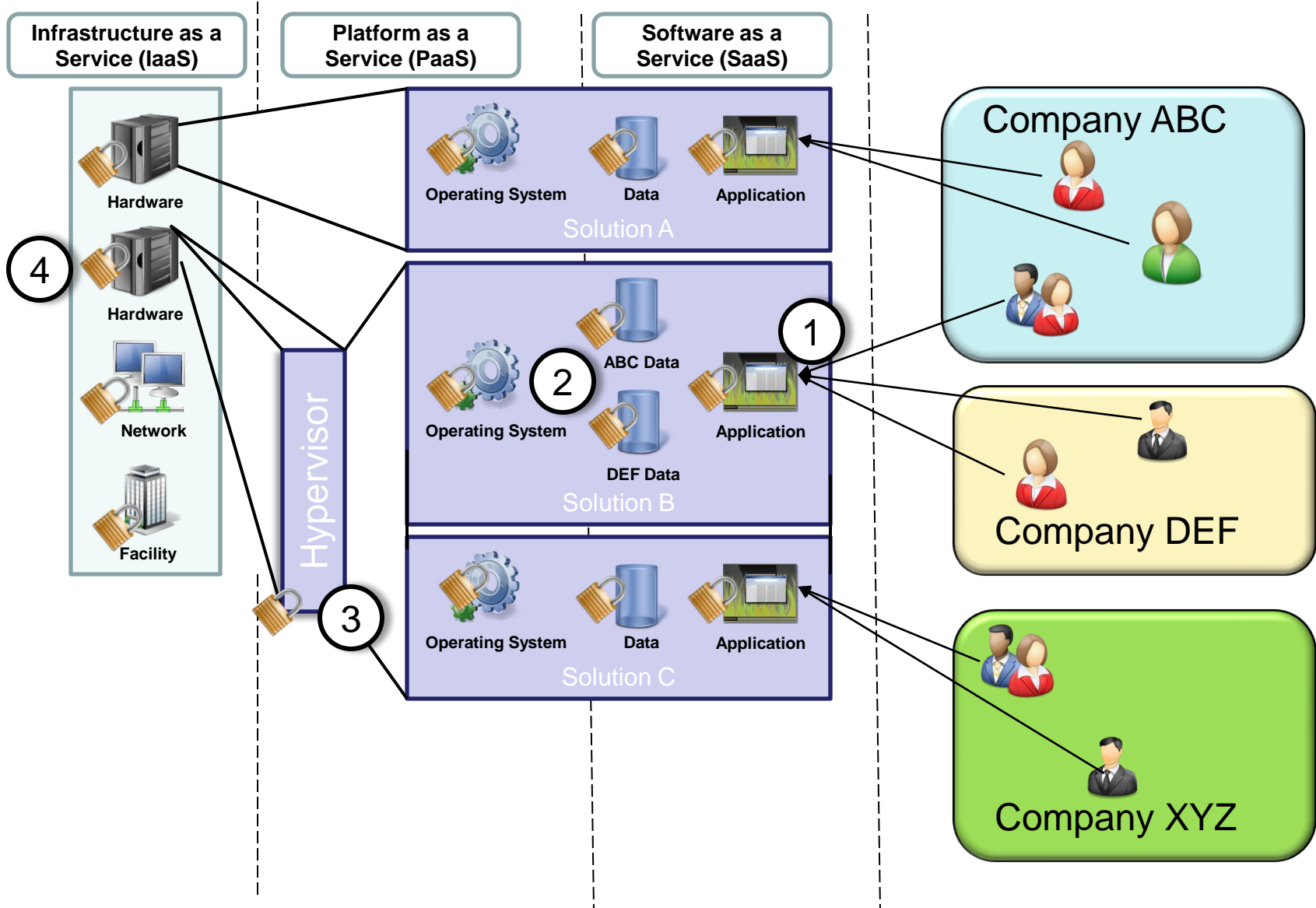
- Hardware provisioning and management
- Network management
- Facilities management



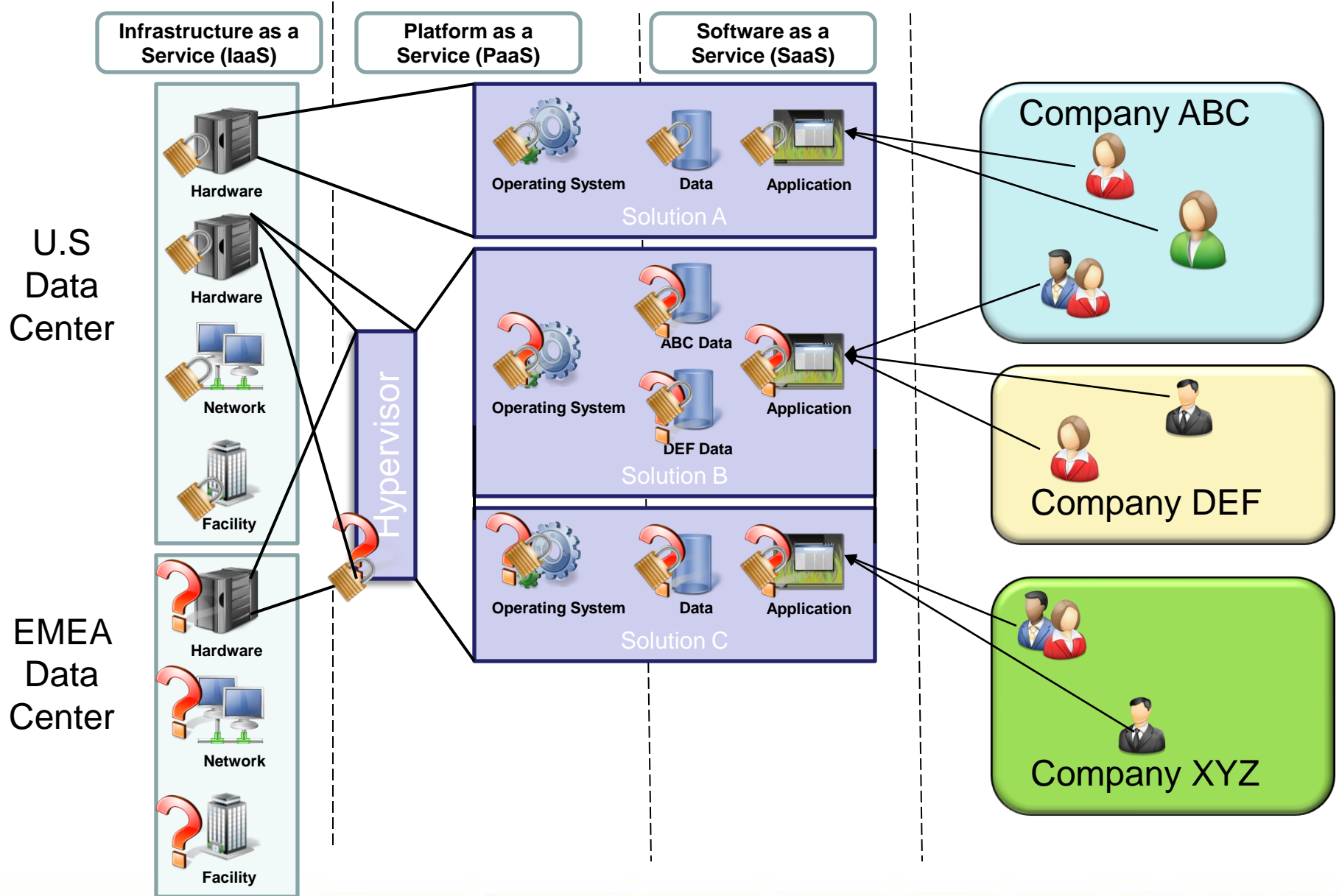
# Virtualization and Controls



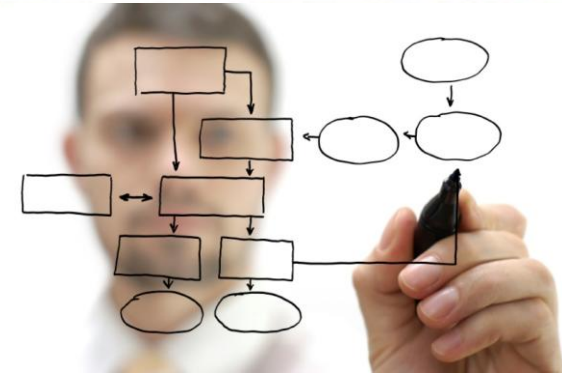
# Multi-Tenancy and Controls



# Elasticity and Jurisdictions



- ▶ Risk Management
  - Legal and contractual coverage
  - Assessing risk
  - Dealing with multi-tenancy, elasticity
- ▶ Establishing Controls requirements
  - Determining control requirements for multiple information types
  - Breach/Disclosure considerations
  - Regulatory and privacy issues
- ▶ Compliance Measurement
  - Measurement of providers controls vs. internal and external control requirements
- ▶ Information Lifecycle Management
  - Collection, retention and destruction of information
- ▶ Business Process transitions
  - Moving services, information and processes from internal to external (and potentially back or to other providers)



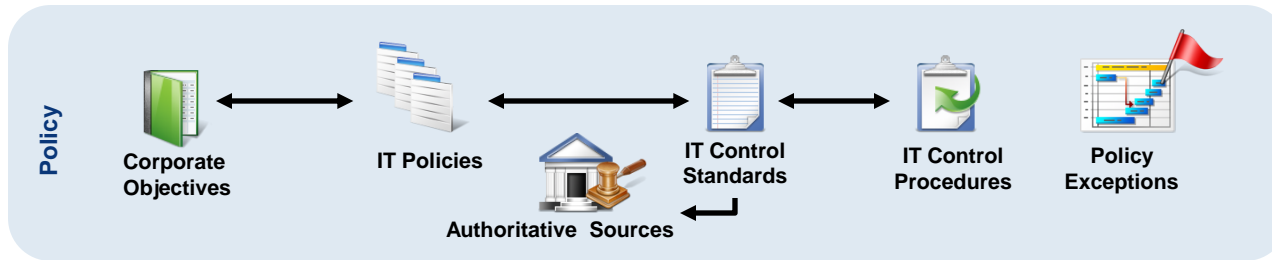
- ▶ Traditional Security infrastructure
- ▶ Business Continuity
- ▶ Disaster Recovery Operations
- ▶ Incident Management
  - Coordination and escalation with external provider
- ▶ Access and Identity
  - Nuts and bolts of connecting internal user stores with external provider
  - Access to internal information by external provider
- ▶ Encryption Management (if applicable)
  - Key management and scalable encryption requirements
- ▶ Technical infrastructure
  - Virtualization, connectivity, bandwidth, performance, etc.



# Thinking about IT GRC for the Cloud



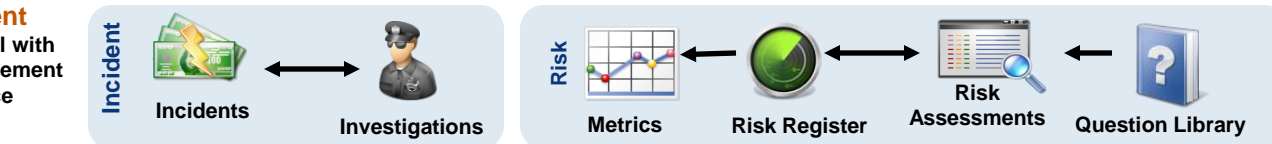
The Security Division of EMC



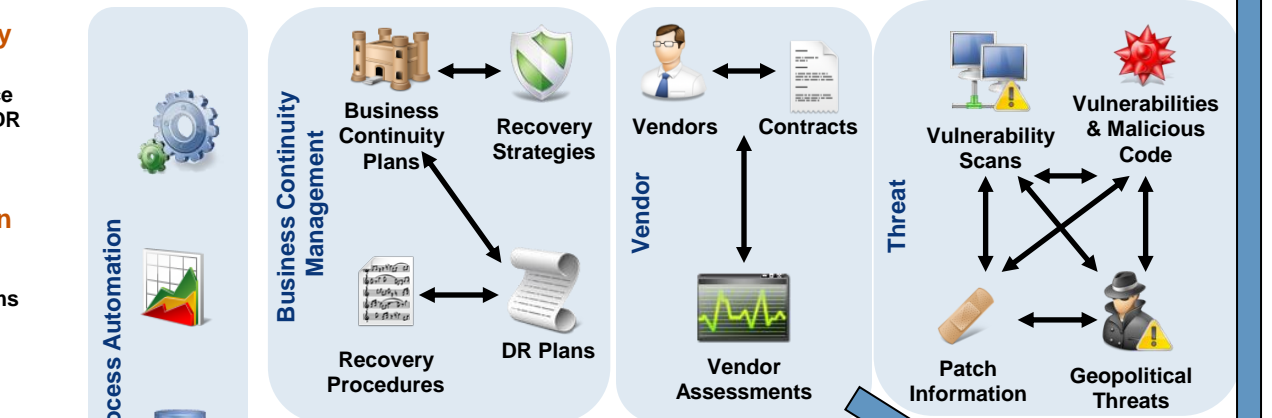
**Policy Management**  
Addressing Cloud issues via polices, standards and procedures, e.g. contracting services, outsourcing, deployment models, etc.



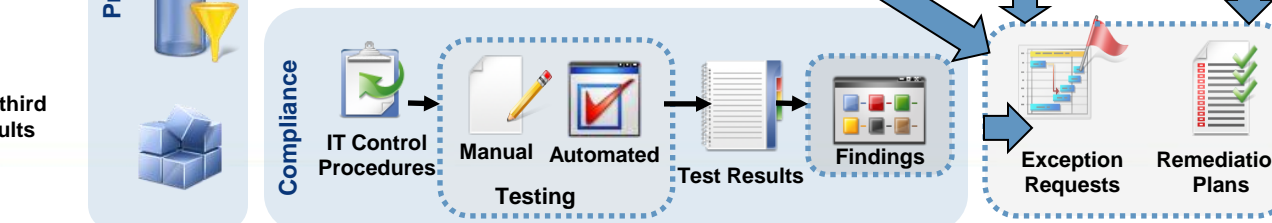
**Enterprise Management**  
Becoming aware of virtual assets and “cloud” components, e.g. identifying external vs. internal applications



**Risk Management**  
Develop risk assessments/approaches for outsourcing and cloud “opportunities”



**Threat Management**  
Determine how to share threat information with providers or identify threats to cloud resources



**Vendor Management**  
Manage...Manage...Manage

Centralize, manage and report on exceptions and remediation efforts across all IT GRC activities.

**Incident Management**  
Build capabilities to deal with external incident management participants, e.g. Service provider

**Business Continuity Management**  
Factor in external service providers into BCP and DR plans

**Process Automation**  
Determine how external service provider data needs to be used in terms of GRC

**Compliance Management**  
Implement strategy to measure compliance of third parties and factor in results to internal compliance reporting

- ▶ Are you ready for cloud services?
  - Risk Assessments
  - Legal/contractual understanding
  - Compliance restrictions
  - History of outsourcing
- ▶ Once you are using cloud services:
  - Traditional security issues (application, access, physical security, etc.)
  - Business continuity
  - Data Management (lifecycle management from collection to destruction)
  - Encryption
  - Identity management
  - Virtualization, data co-mingling, technical implications





The Security Division of EMC

The Security Division of EMC



**Questions**

# Thank You

## Steve Schlarman eGRC Solutions Manager [steve.schlarman@archer.com](mailto:steve.schlarman@archer.com)

