Managing Risk and Reward In Moving to the Cloud

August 27, 2013

Jim Cowing, CISSP
Managing Director

Coalfire
IT Audit and Compliance
www.coalfire.com

Show of Hands

How many attendees are already working with CSPs ?
How many are considering Cloud or think they may w/in 24 mos.

Goalfire

Agenda

- Introduction
- Cloud Background and Trends
- Cloud Security and Privacy Issues
- Information Security Issues
- Cloud Service Models and Deployments
- Selecting Your Model
- Cloud Governance Domains
- Top 5 Cloud Risk & Compliance Issues

About Coalfire

IT Governance Risk and Compliance

- Leading independent provider of IT Governance, Risk and Compliance (IT-GRC) solutions
- Focused expertise in Healthcare (HIPAA), Retail (PCI), Banking (GLBA), Utilities (NERC) and Cloud (FedRAMP)
- Full suite of IT GRC solutions: compliance audit, risk and vulnerability assessment, application security, penetration testing and forensic analysis
- Served over 1,500 clients to date, including Oracle, Epic, IBM, Ford, Nordstrom, Echostar, Microsoft, Intuit, Overstock, Savvis
- Over 150 employees and contractors across [9] offices: Denver, Seattle, New York, Atlanta, Los Angeles, San Francisco, Boston, Dallas and Washington, DC.

The Inevitability (?) of Cloud Computing

- **U.S. Government - FedRAMP**
  - (Former) Federal CIO Vivek Kundra planned to consolidate/eliminate 800 data centers by 2015
  - Shift to "Cloud First" policy wherein each agency will identify three "must move" services within three months and move one of these services to the cloud within 12 month and the remaining two within 18 months.
- **Improved Economics**
  - Typical in-house IT infrastructure operates at ~30% of capacity
  - The City of Los Angeles' email migration from Gmail is expected to produce $6M annual savings in software license costs and $500M save in hardware retirement costs.
- **IBM**
  - Has trained 20,000 sales representatives worldwide to promote their Cloud based services
  - Is on track for a projected $15B in revenue by 2015

Facebook, Gmail, Salesforce, LinkedIn Hotmail, Box, etc. All Cloud based…

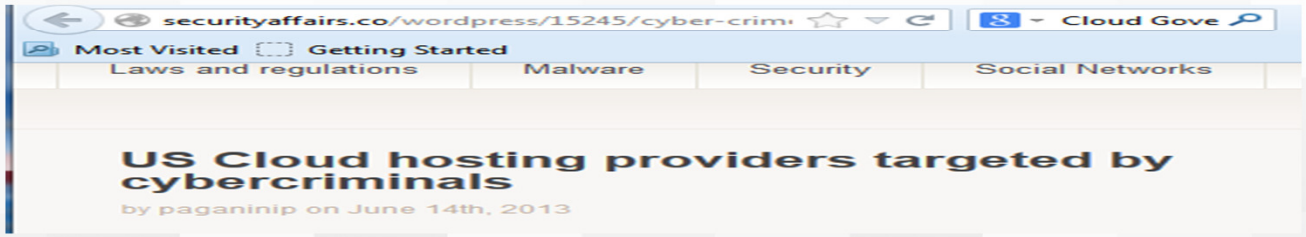
The majority of us already participate in cloud computing on a daily basis!

The 'Bright Side'….

- Cloud Service Providers (CSPs) typically offer **better (stronger) security and controls** than is present at most SMB data centers
- The inherent resiliency of the Cloud provides a **higher degree of redundancy and business continuity** support than is typical
- The **'Utility' (email, Collaboration, etc.) functions** provided by Cloud services are more cost effectively provided on a large scale basis
- Cloud hosting providers -
  - Are likely to have **one or more types of control reports** that have been independently tested by a third party (SSAE 16, ISAE 3402, etc.)
  - Typically will align their controls environment with accepted regulatory requirements (PCI, HIPAA, GLBA, FISMA, etc.) and control frameworks (NIST 800, ISO 27000, COBIT, etc.)

The 'Dark Side'…

- Cloud host providers are being chosen with increasing frequency as Targets of CyberCrime - ***Ideal Platforms*** for attacks.
- CSPs are **harnessed to facilitate malicious activities**.
- Cloud facilities have become an increasing part of the 'malware supply chain'
- Botnet **'command and control'** nodes were discovered in the cloud as early as 2009
- Spammers '**purchase' Cloud services for use in phishing campaigns** that are a key mechanism in the distribution of malware
- Cloud-based massively parallel processing facilities have been used for distributed 'brute force' cracking of encryption keys



What is “Cloud Computing?”

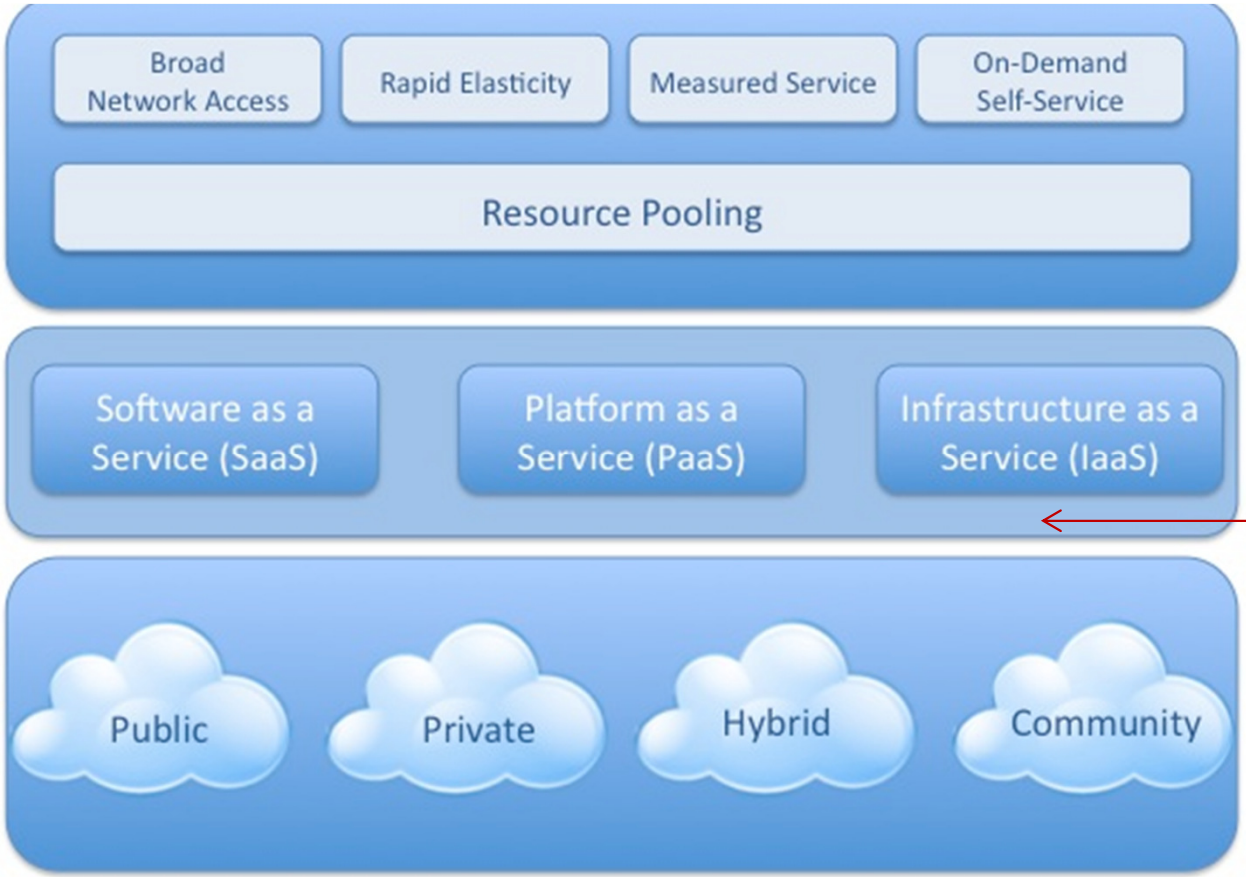
Cloud computing is a **means “for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”**

*– **The NIST definition** of Cloud Computing*

Essential Characteristics

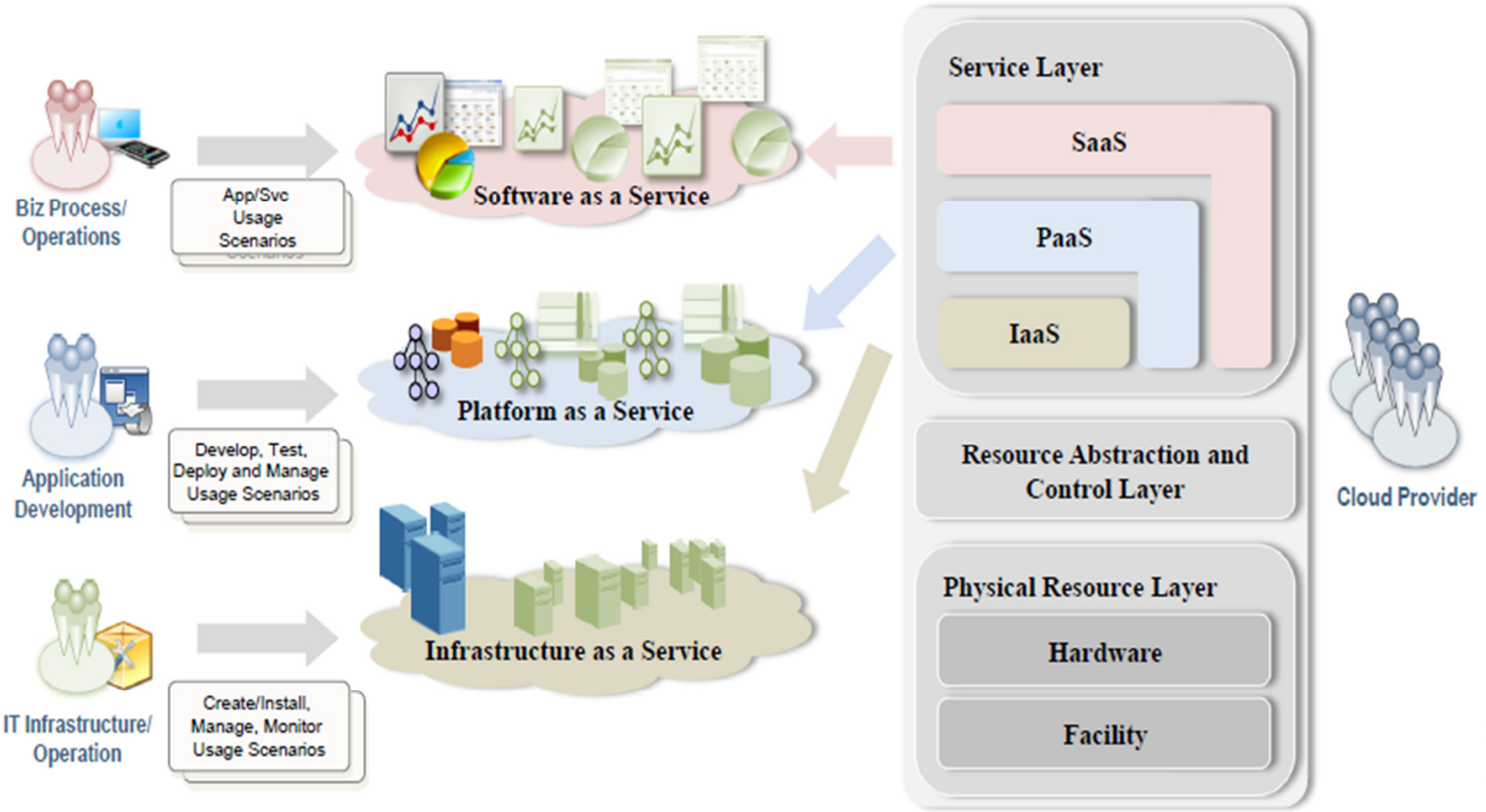
Service Models

Deployment Models



Security and Compliance as a Service

Cloud Service Layers



Service Models: SaaS, PaaS, and IaaS

- **Cloud Software as a Service (SaaS)**
  - **BaseCamp** – project collaboration
  - **Salesforce** – CRM
  - **Qualys** – Security testing on Demand

http://basecamphq.

- **Cloud Platform as a Service (PaaS)**
  - **Force.com** – Salesforce Apps Platform
  - **Google Apps**

http://www.salesforce.com/platform/

- **Cloud Infrastructure as a Service (IaaS) or Hardware as a Service (HaaS)**
  - **Amazon EC2** - Compute
  - **Rackspace CloudFiles** – Storage
  - **Cloud Foundry** – Services Management

Cloud Service Models

- **Cloud Software as a Service (SaaS)**
  - Consumer uses provider's applications running on a cloud infrastructure
  - Applications accessible to client through thin client (HTTP) web interface
  - Consumer ***does not manage or control underlying cloud*** infrastructure or application capabilities (except limited user- specific application configuration settings)
- **Cloud Platform as a Service (PaaS)**
  - Consumer deploys onto cloud infrastructure ***consumer-created or acquired applications*** created using programming languages and tools supported by the provider
  - Consumer does not manage or control the underlying cloud infrastructure, but has control over deployed applications and possibly application hosting environment configurations
- **Cloud Infrastructure as a Service (IaaS) or Hardware as a Service (HaaS)**
  - Consumer can provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications
  - Consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Security and Privacy Issues

Governance

- How are cloud services contracted?
- How are cloud vendors managed?

Compliance

- Location of data/information assets
- Law & Regulations
  - Federal Information Security Management Act (FISMA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Gramm Leach Bliley Act (GLBA)
  - FFIEC IT Examination
  - Federal Rules of Civil Procedure (FRCP)

Electronic Discovery

- Production of tangible and intangible assets
- Comingling of data and information systems/assets

Cloud Security and Privacy Issues

Trust

- Insider access – control of privileged access to data
- Data ownership
- Composite services – reliance on second, third and fourth parties in a cloud delivery model
- Visibility – lack of transparency in operations
- Risk Management – assessment and effective management of risk when the system components are outside the direct control of the subscriber

Information Security Issues

- **Data security -** Confidentiality, Integrity, Availability, Authenticity, Authorization, Authentication, and Non-Repudiation.
- **Location of the data -** There must be assurance that the data, including all of its copies and backups, is stored only in geographic locations permitted by contract, SLA, and/or regulation. For instance, use of "compliant storage" as mandated by the European Union for storing electronic health records can be an added challenge to the data owner and cloud service provider.
- **Data persistence -** Data must be effectively and completely removed to be deemed 'destroyed.' Therefore, techniques for completely and effectively locating data in the cloud, erasing/destroying data, and assuring the data has been completely removed or rendered unrecoverable must be available and used when required.
- **Commingling data with other cloud customers -** Data – especially classified / sensitive data must not be commingled with other customer data without compensating controls while in use, storage, or transit. Mixing or commingling the data will be a challenge when concerns are raised about data security and geo-location.

Information Security Issues

- **Data availability, backup and recovery schemes (for restoration) -** Data must be available and data backup and recovery schemes for the cloud must be in place and effective in order to prevent data loss, unwanted data overwrite, and destruction. Don't assume cloud-based data is backed up and recoverable.

- **Data discovery (eDiscovery) -** As the legal system continues to focus on electronic discovery, cloud service providers and data owners will need to focus on discovering data and assuring legal and regulatory authorities that all data requested has been retrieved. In a cloud environment that question is extremely difficult to answer and will require administrative, technical and legal controls when required.

- **Data aggregation and inference -** With data in the cloud, there are added concerns of data aggregation and inference that could result in breaching the confidentiality of sensitive and confidential information. Hence practices must be in play to assure the data owner and data stakeholders that the data is still protected from subtle "breach" when data is commingled and/or aggregated, thus revealing protected information (e.g., medical records containing names and medical information mixed with anonymous data but containing the same "crossover field").

Deciding what to move to the Cloud

- Information Assets
  - Applications
  - Data

In a cloud-based model, data and applications are not necessarily co-located

  - Functions – Typically an organization unit (i.e. Human Resources)
  - Processes – Can span multiple organizational units or organizations (i.e. Payroll)

- Evaluate the Assets
  - Confidentiality
  - Integrity
  - Availability

SSAE 16

ISAE 3402

ISO 2700x

NIST

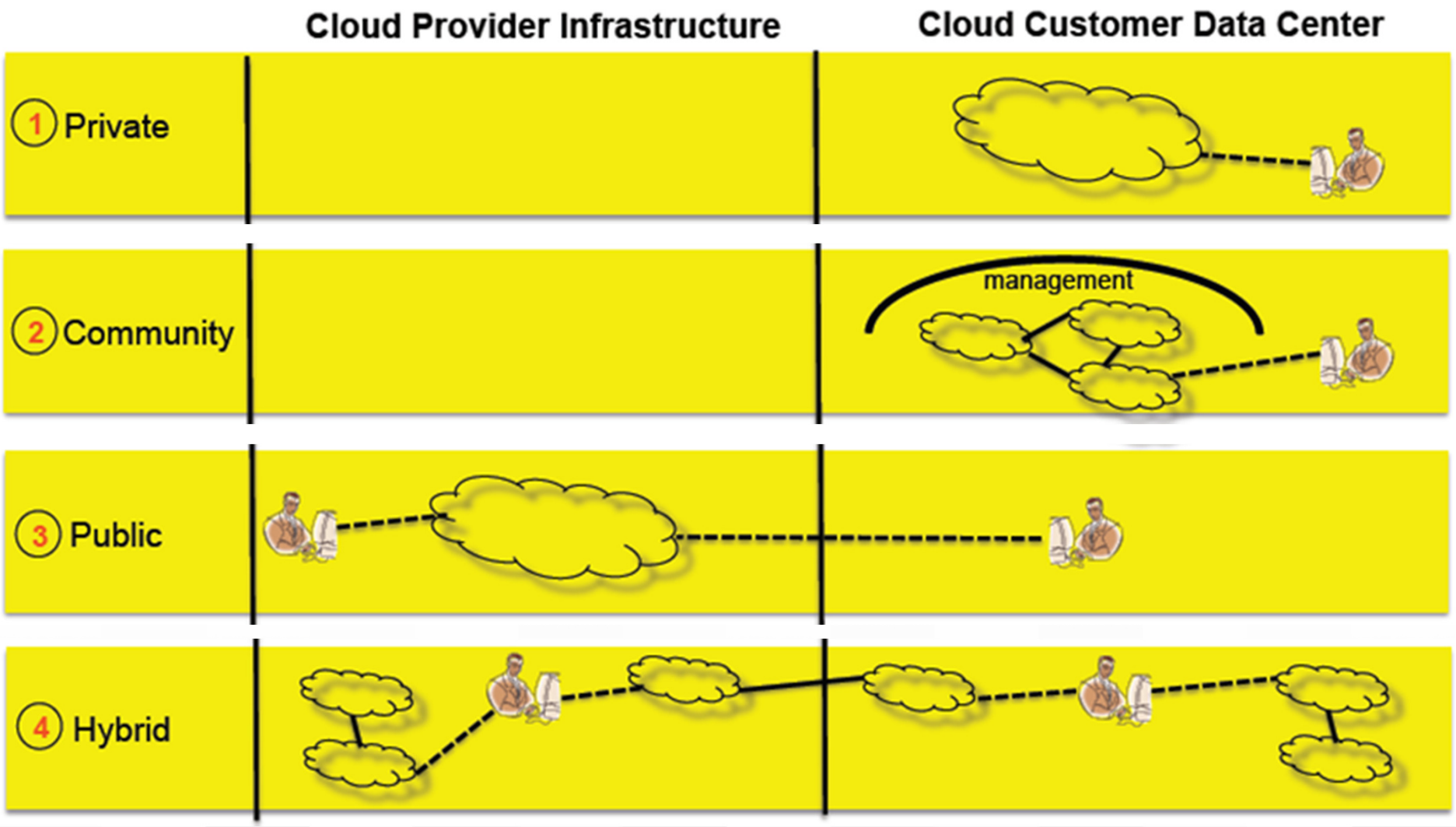
Use accepted standards for Asset Classification and Valuation

Selecting your Deployment models

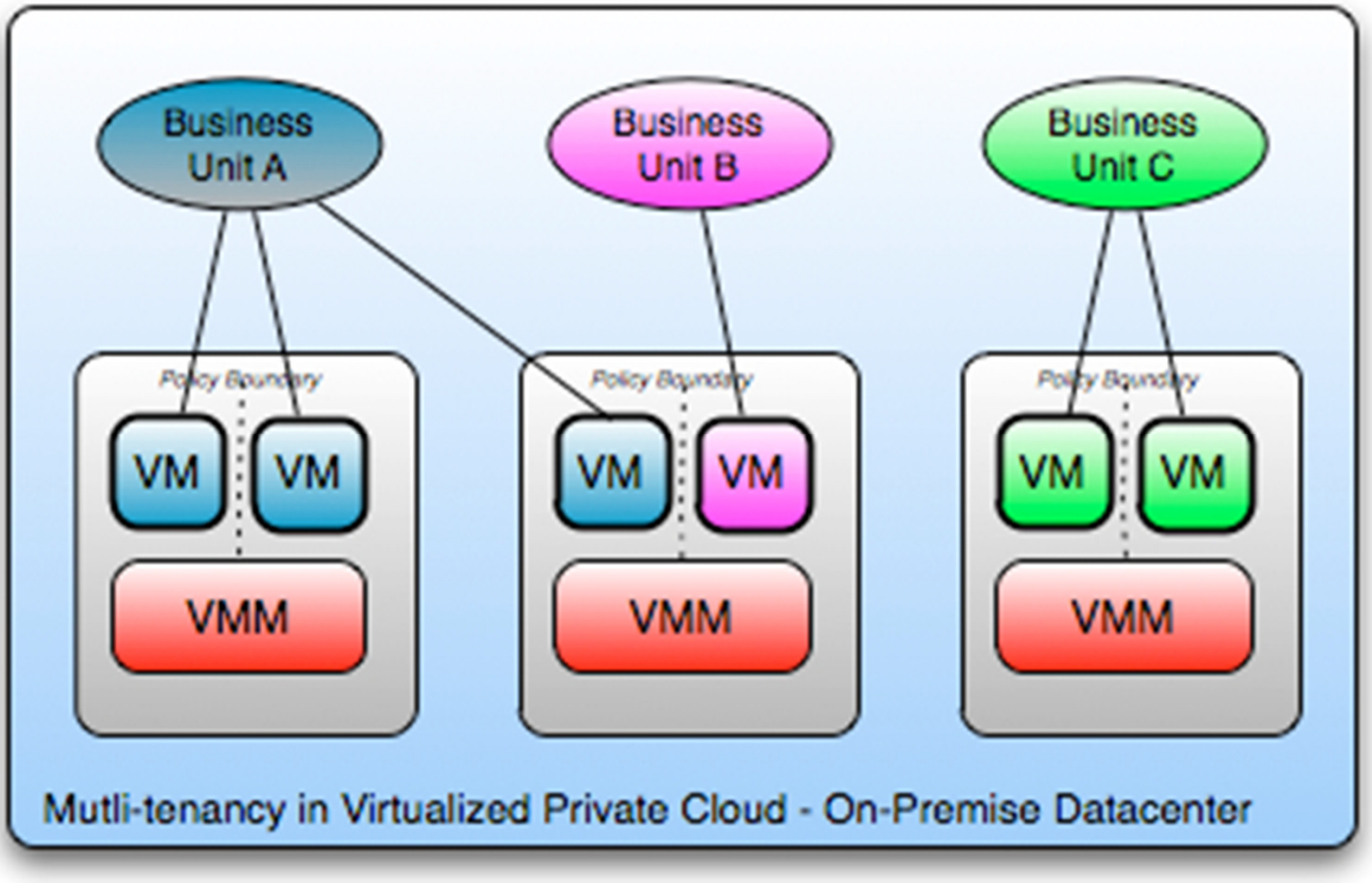
- **Public**
- **Private; internal/on-premises**
- **Private; external** (including dedicated or shared infrastructure)
- **Community**; taking into account the hosting location, potential service provider, and identification of other community members
- **Hybrid**; to effectively evaluate a potential hybrid deployment, you must have in mind at least a rough architecture of where components, functions, and data will reside

Source: CSA Guide v3 (2009)

Know your Deployment Model



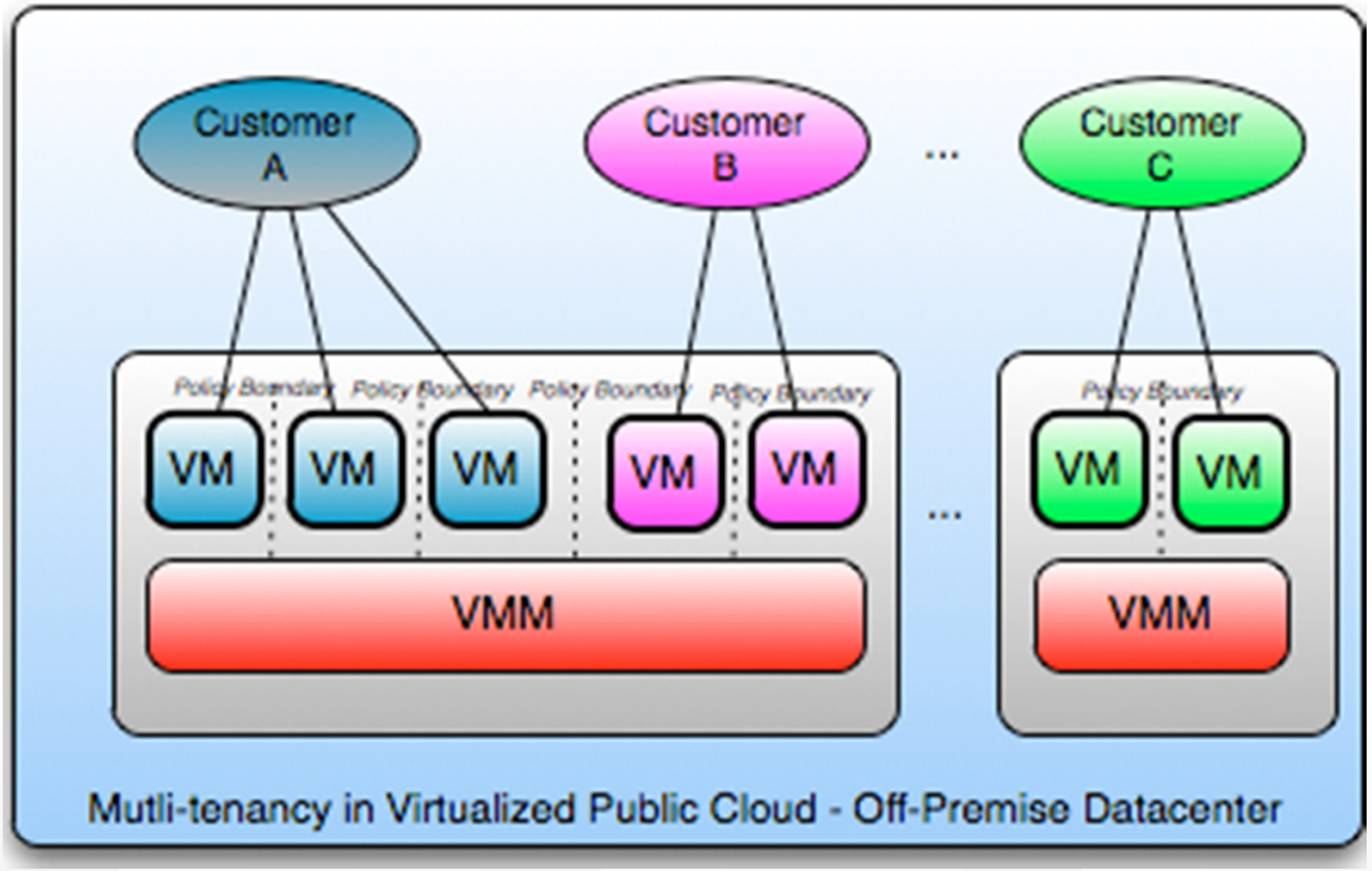
Why does it matter?



Multi-tenancy in its simplest form implies **use of same resources** or application by multiple consumers that may belong to same organization or different organization. The impact of multi-tenancy is visibility of **residual data or trace of operations by other user or tenant**.

Source: Cloud Service Alliance (CSA) Guide v3.0 (2009)

Multi-Tenancy May Matter



Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies.

Source: CSA Guide v3 (2009)

Questions to ask…

- How would we be harmed if
  - the **asset became public and widely distributed**?
  - an **employee of our cloud provider accessed the asset**?
  - the **process or function were manipulated** by an outsider?
  - the process or function **failed to provide expected results**?
  - the **information/data were unexpectedly changed**?
  - the asset were **unavailable for a period of time**?

Source: CSA Guide v3 (2009)

Cloud Governance Domains

- **Governance and Enterprise Risk Management**
  The ability of an organization to govern and measure enterprise risk introduced by Cloud Computing.
- **Legal and Electronic Discovery**
  Potential legal issues when using Cloud Computing.
- **Compliance and Audit**
  Maintaining and proving compliance when using Cloud Computing.
- **Information Lifecycle Management**
  Managing data that is placed in the cloud.
- **Portability and Interoperability**
  The ability to move data/services from one provider to another, or bring it entirely back in-house.
- **Traditional Security, Business Continuity and Disaster Recovery**
  How Cloud Computing affects the operational processes and procedures currently use to implement security, business continuity, and disaster recovery.

Cloud Governance Domains

- **Data Center Operations**
  How to evaluate a provider's data center architecture and operations.
- **Incident Response, Notification and Remediation**
  Proper and adequate incident detection, response, notification, and remediation.
- **Application Security**
  Securing application software that is running on or being developed in the cloud.
- **Encryption and Key Management**
  Identifying proper encryption usage and scalable key management.
- **Identity and Access Management**
  Managing identities and leveraging directory services to provide access control.
- **Virtualization**
  The use of virtualization technology in Cloud Computing.

Key Takeaways

- **Methods for assessing and managing risk in the Cloud are evolving**
- **Cloud computing changes the risk profile of an organization**
  - You need to determine the 'new effect' of the change +/-
  - What impact will moving to a Cloud environment have on regulatory compliance for my organization?
- **Questions to ask;**
  - What exactly is covered in the service level agreement (SLA) from the cloud provider?
  - What type of third party risk/controls assessment is offered by the Cloud provider? (SSAE-16 SOC?, BITS?, ISO 27000?, etc)
  - Do we have a vendor risk management program to assess and manage the 3rd party risk associated with a Cloud vendor?

Top 5 Cloud Risk and Compliance Issues

1. **Scope of Environment**
2. **Risk Management and Governance**
3. **Policies and Procedures**
4. **New Data Controls**
   - Access Controls
   - Logging and Alerting
   - Data Protection (encryption and disposal)
5. **Vendor Management**

1. Scope and Environment

- Where is the data? (US or Int'l?)
- Who owns the data?
- How sensitive is the data and who has responsibility for securing the data and maintaining compliance?
- Do you really need to collect and store as much data today as required in legacy systems? *(Is one central copy enough?)*
- Who are the users and where are they located? (physically and logically)
- How do you know when changes occur?

2. Risk Management and Governance

Update your Risk Assessment

- Each critical application allowing access must be documented to include a data flow
- Each function and application must be assessed for threats and vulnerabilities
- Understand the Risks (server and client side)
- Select justified controls … right level
  - What is the right cloud environment? Segmentation?
  - Server side versus user side controls?
- Conduct periodic testing and and monitoring
- Communicate changes in risk profile
- Train users to comply with policies

3. Policy Development

- Restate data ownership and user duty to protect sensitive data
- Obtain consent to participate in Incident Response and investigation
- Enforce configuration and security policies or other configuration policy management to protect corporate data
- Require that user access credentials be entered prior to accessing enterprise applications and data … *probably 2 factor*

4. New Data Controls

in a multi-tenant environment

- Access Controls
- Continuous Monitoring
- Data Encryption (P2PE for PCI)

5. Vendor Management

- Contracts and agreements
  - Who owns data?
  - Who owns users?
  - What type of service provided (public or private)?
  - Where is data stored and how does an organization respond to e-Discovery?
  - What security reports are provided and when?
- Oversight (SAS70 was not adequate … Is SSAE16 /FedRAMP better?)
- Authority to conduct independent audits
- Obligation to participate in security investigations and incident response

Traditional IT audits and compliance reports may cover less 60% of the environment containing sensitive data

Goalfire

References

- Cloud Security Alliance; https://cloudsecurityalliance.org/
- NIST SP800-144; Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP800-145; The NIST Definition of Cloud Computing
- Cloud Security Alliance, December 2009; Security Guidance for Critical Areas of Focus in Cloud Computing v2.1
- RAND Corporation, November 2010; The Cloud: Understanding the Security, Privacy and Trust Challenges (TR-933-EC)

Goalfire

QUESTIONS

Jim Cowing, CISSP, QSA, CISM
Managing Director - Coalfire

E: Jim.Cowing@coalfire.com

T: (650) 595-9700 ext 7410 – O
(650) 346-8959 – M

3 Twin Dolphin Drive, Suite 150
Redwood City, CA 94065

www.coalfire.com