Cloud Computing: What needs to Be Validated and Qualified

- Ivan Soto

Learning Objectives

- At the end of this session we will have covered:
  - Technical Overview of the Cloud
  - Risk Factors
  - Cloud Security & Data Integrity
  - Applying a Risk Based Approach to Qualification & Validation

What is the Cloud?

What is the Cloud? NIST Definition

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be **rapidly provisioned** and **released** with minimal management effort or service provider interaction

- This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**

Three Service Models

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure

- *Cloud Platform as a Service (PaaS)*. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider

- *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software

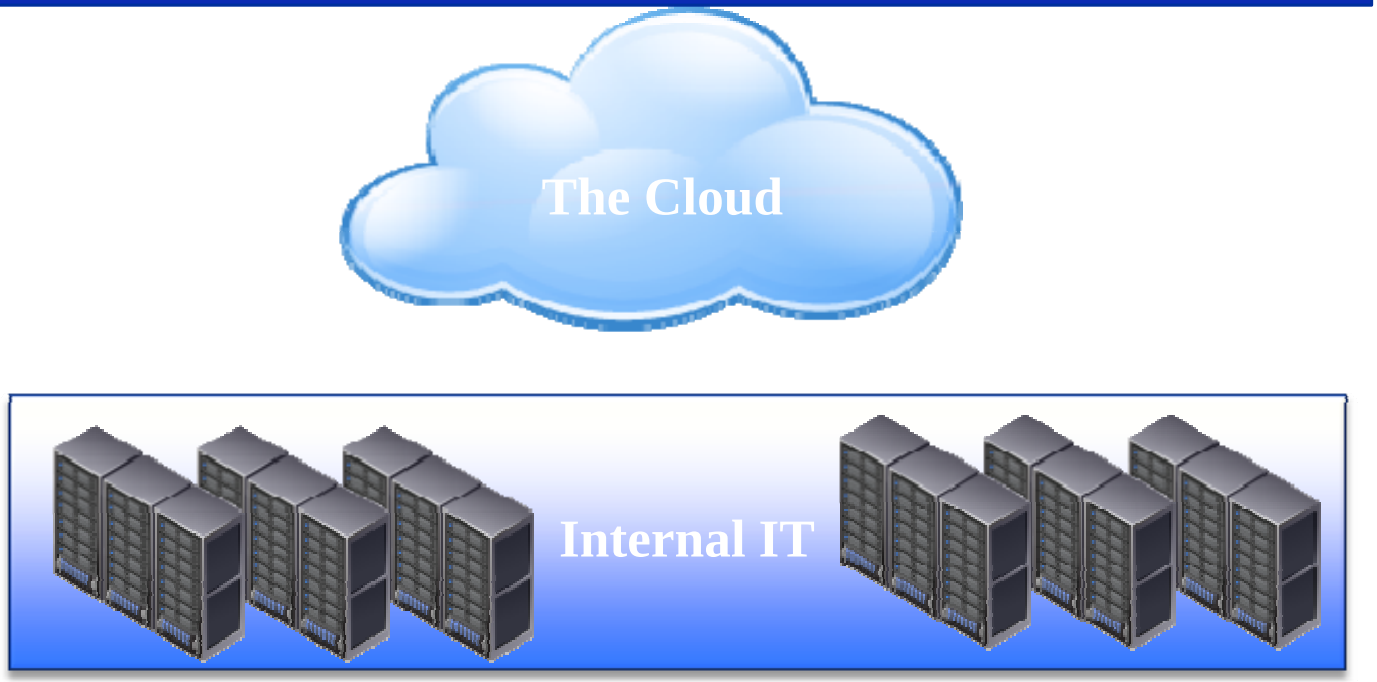
Four Deployment Models

- *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise
- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns
- *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services
- *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

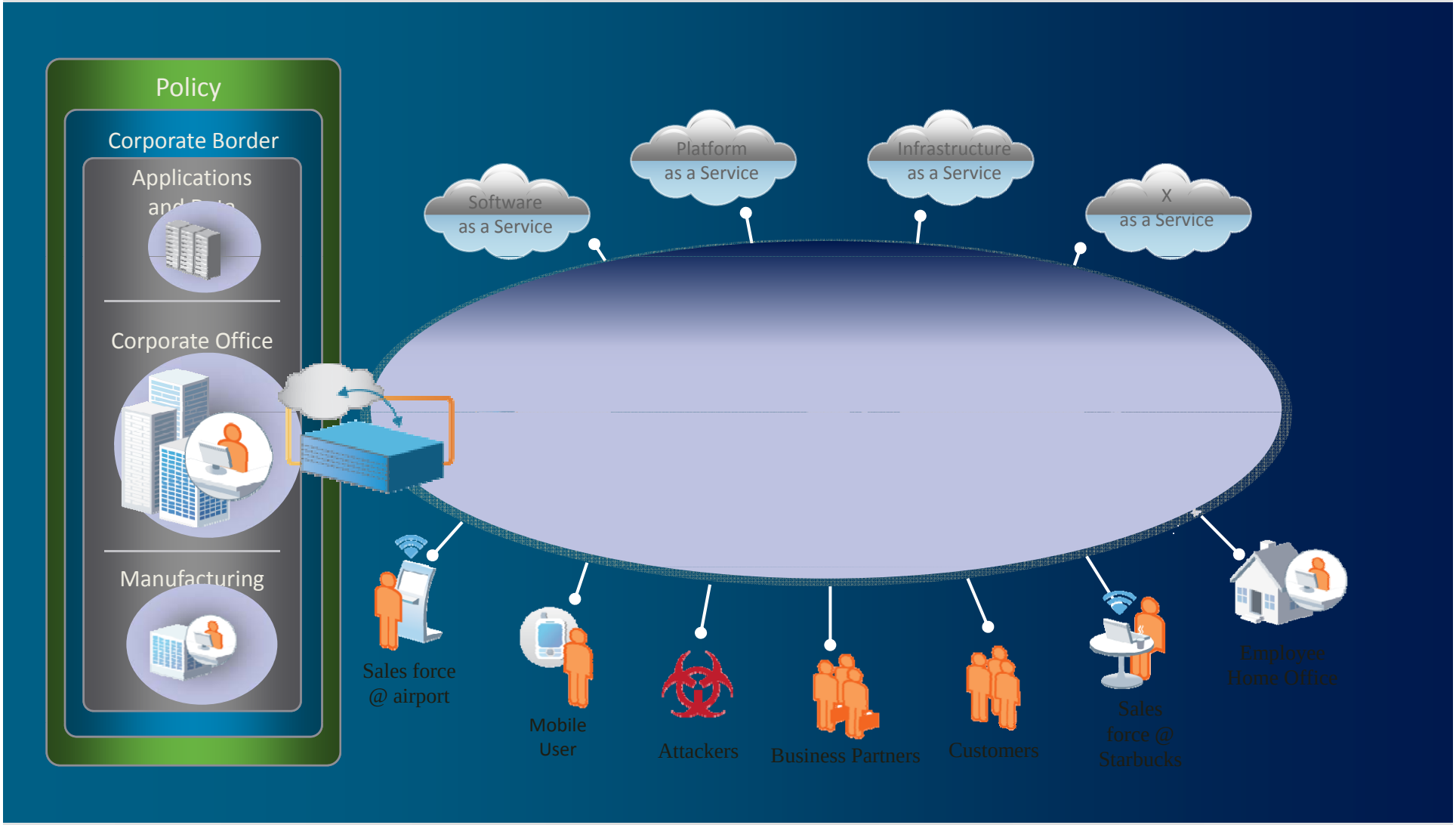
Security and Compliance

Virtualization forms the foundation for building private clouds. Security must change to support both.

--Gartner, 2010



Compliance Challenge – Security, Data Integrity, Visibility & Control



Cloud Data & Security Management Challenge

- Audit/Reporting/Alerting
- Secure Mobile Devices
- Data Security at Rest
- Data Security in Transit
- Strong Authentication
- Personal-business-regulated Data Co-mingled
- Regulated company data – Non regulated company data Co-mingled
- Data segregation

Risk in the Cloud

- Access Control Policy
- Electronic Record Policy
- Acceptable Use Policy
- Threat Protection Policy
- Record Retention Policy

Trust & Reliability in a cloud environment centers on four core concepts:

Security –Issues around data integrity and resource access control, encryption and incident detection

Control – The ability of the enterprise to directly manage how and where data and software is deployed, used and destroyed

Service-Level Management – The definition, contracting and enforcement of service level agreements between a variety of parties

Compliance – Conformance with required regulatory, legal and general industry requirements (such as Part 11, Annex 11, HIPAA and Sarbanes-Oxley)

Cloud Security Issues

- Abuse and Nefarious Use

  Password and Key cracking, Launching dynamic attack points, Hosting malicious data, Botnet command and control, and Building rainbow tables.

- Insecure Interfaces and APIs

  Used for provisioning, management, orchestration, and monitoring.

  Security/availability dependent on security of APIs.

  Weak APIs expose data to variety of security issues.

- Malicious Insiders

  Combo of IT Services, cloud customers, competitors + lack of transparency of security process and procedure practices of Cloud provider.

- Shared Technology Issues

  CPUs, disk partitions, other shared components not designed for strong compartmentalization.

Cloud Security Issues (cont)

- Data Loss or Leakage

  Risk can be amplified due to architectural/operational characteristics of cloud services,, inconsistent crypto use, residual data issues, data center reliability, and disaster recovery

- Account or Service Hijacking

  Credentials/passwords reuse, Eavesdrop on connection, Redirect users illegitimate site then launch attack based on your reputation

- Unknown Risk Profile

  What are details of security procedures? Compliance details? configuration hardening, patching, audit/logging?

  How are logs stored? What info will vendor disclose in security incident? Service Level Agreement!

Risk Mitigation Considerations

- Identification and Assessment of Cloud Component
- Implementation of Controls
- Security & Data Security

Identification & Assessment

- Identification and Assessment of Cloud Components
  - What components define the configured cloud?
  - Where are they?
  - How many applications running?
  - How many users?
  - All GMP or not?
  - Hardware and Applications under Change Management?
  - How changes are communicated and under control?
  - How is data integrity and security provided in the cloud?

Implementation of Controls

- **Change Management**
- Configuration Management
- **Security Management**
- Server Management
- Client Management
- Network Management
- Problem Management
- Help Desk
- Backup, Restore, and Archiving
- Disaster Recovery
- **Performance Monitoring & Reporting**
- Supplier Management
- **Periodic Review**
- System Retirement

Cloud Security & Data Integrity

- Privileged user access. – Who has access to your data?
- Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider
- Data location – where in the world is the cloud
- Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," *Gartner "Cloud-computing Security Risks"*
- Backup & Recovery. – Make sure that your cloud is recoverable

Applying a Risk Based Approach to Qualification and Validation

Supplier Assessment

- Goal – Determine suppliers ability to meet clients expectations related to controls needed to ensure security, data integrity, compliance with client procedures and regulatory expectations
- Off-site audit should be consider as the first step to assess cloud computing suppliers
- Off-site audit should be used to determine if the supplier merits further consideration
- On-site audit may be performed after the supplier is deemed capable to meet client expectations
- The scope of the audit should be based on the type of service that will be provided to the customer

Service Level Considerations

- Availability and performance
- Change management
- Quality of service
- Security
- Business continuity / Backup and Recovery
- Personnel Qualification

Service Level Considerations (Cont.)

- Testing
- Incident management
- Defining documentation and information ownership/responsibilities
- Performance monitoring expectations
- Incident reporting
- Alert & escalation procedures
- Which processes and procedures will be used?

Hardware Qualification?

- Goal should be to leverage vendor hardware testing
- Lite application IQ to verify hardware is adequate to host application
- Infrastructure security verification
- Effort should be based on the results of the supplier assessment and audit

Validating Applications in the Cloud

- Risk based approach based on the risk level of the application
- User Requirements Specification
- IQ – simple verification that hardware requirements are met
- OQ – verify critical high risk system functions
  - Security & Data Integrity
  - Audit trails
  - Electronic Signatures
  - High & Medium Risk Requirements
- PQ – verify workflow & business process requirements

Change Management

- Consider the following
  - Visibility to infrastructure changes
  - Adequate notification
  - Ability to assess changes (depends on the service model)
  - Approval of changes prior to release (depends on the service model)
  - Testing
  - Change impact assessments (technical, GxP, process)

Periodic Review and Assessment

- Critical if Cloud is outside your organization
- Consider measuring SLA adherence during periodic review
- Consider performance requirements
- Incident and problem management review

Summary

- Cloud Technical Overview
- Security & Data Integrity
- Change Management
- Risk Based Validation Approach
- Periodic Review and Assessment