weaver

Assurance • Tax • Advisory

One Cloud, Two Clouds, Ten Clouds...

Auditing In A Multi-Cloud World

Presenter

Eric Peeters

Senior Manager – Governance, Risk, Compliance
CISA, CCAK, CCSK, ISO 27001 Lead Auditor
Weaver & Tidwell LLP
eric.peeters@weaver.com

Public / Private / Hybrid Clouds

- Private Cloud: Cloud services built on top of an infrastructure contr
  a single organization, not available to the public
- Public Cloud: Cloud services sold to the public
- Hybrid Cloud: Leveraging public and private clouds
  - Speed of execution: Live data processing in a private cloud, data archival in a public cloud
  - Enhanced data control: Data stored in a private cloud, transferred to a public cloud for processing only

Cloud Delivery Model

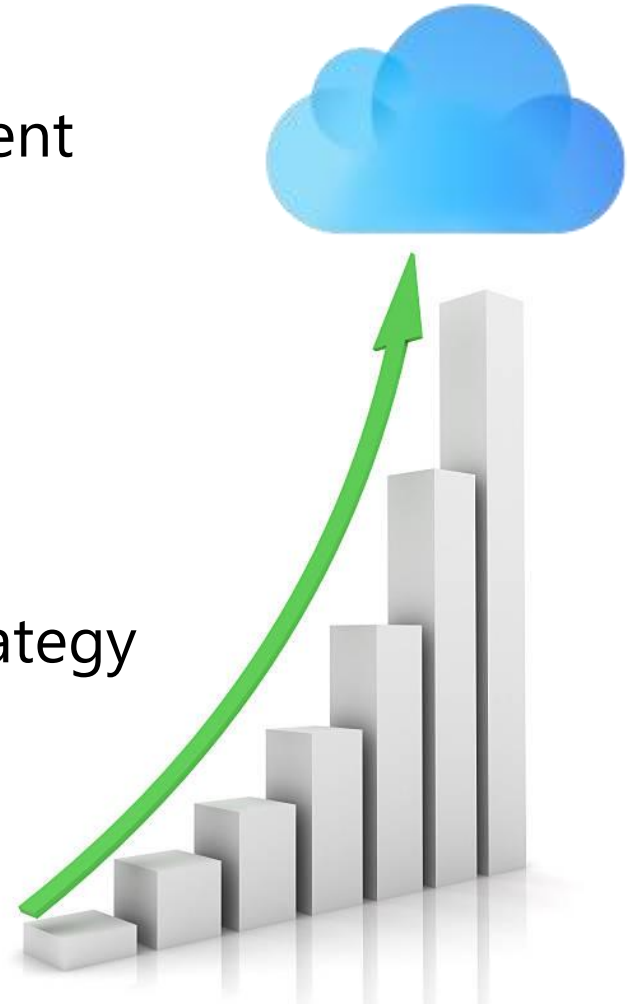
- Infrastructure-as-a-Service (IaaS): Virtual data center
- Platform-as-a-Service (PaaS): Software development and deployment platform
- Function-as-a-Service (FaaS): Code execution platform
- Software-as-a-Service (SaaS): Virtual application managed by a vendor

Cloud migrations often start as IaaS – duplicating existing physical infrastructure

Solutions available across multiple models – database as IaaS, PaaS, SaaS

The Cloud Is Still Growing

- 44% of small businesses use at least one cloud environment
- 94% of enterprises are in the cloud
- 98% of financial services firms of all sizes are in the cloud
- By 2025, 85% of organizations will adopt a cloud-first strategy

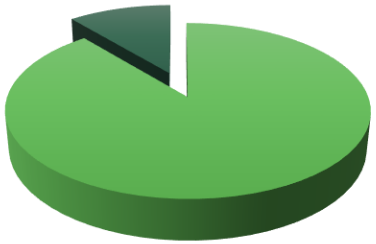


Sources: CSA, Edge Delta, Gartner, RightScale

Clouds Are Specializing

Reliance on hyperscalers is decreasing

SaaS and PaaS providers are multiplying



89% of cloud users are multi-cloud

Sources: CSA, Edge Delta, Gartner, RightScale

Multi-Cloud By Strategy

- Best of Breed
- Business Continuity
- Compliance Requirements
- Cost Efficiency
- Cyber Risk Mitigation
- Vendor Lock-In Avoidance

Or By Happenstance

- COVID
- Decentralized IT Management
- Insufficient Policy Enforcement
- Mergers and Acquisitions
- Self-Sustaining Business Units
- Vendor Selection

Or Both…

The best multi-cloud strategies are ignored if insufficiently communicated and enforced

Common Multi-Cloud Examples

- Authentication in Azure AD + cloud computing services in AWS
- Personnel functions: Payroll, HR, Learning Management System
- Data functions: acquisition, storage, processing, reporting, archival
- Business support functions: help desk, service delivery, asset management
- Resilience: primary operations in one cloud, backup/DR in another cloud
- Legal and contractual data localization requirements

Multi-Cloud as Audit Risk

- Comprehensive cloud inventory is a frequent challenge
- Ubiquitous, easy-to-deploy cloud solutions make tracking difficult
- Especially prevalent when multi-cloud by happenstance
- By strategy too, especially with independent business units
- Cloud transparent to end users
- *What clouds are we in* vs *What's in our clouds*

Challenging Cloud Governance

- Relevance of on-premise policies to a cloud environment
- Lack of clarity over responsibilities of vendors, end-users, technology function
- Complex integration options reduce single-stream approach to governance
- Lack of integration requires cloud-by-cloud governance management
- Key risk area: logical access

Data Ownership and Management

- Data stores separated from tools acquiring and processing data
- Multiple data stores with different capabilities for one application
- Multiple applications with different capabilities for one data store
- Data ownership and responsibility varies by service delivery model
- Data classification tools not standardized across multiple clouds
- Key risk area: data backup and recovery

Performance Monitoring

- Typically extensive monitoring capabilities
- Limited negotiation opportunities over enforcement and damages
- Performance metrics not defined or not enforceable
- Lack of clarity over responsibility to monitor performance between vendor and client, and between teams at the client
- Annual SOC 2 review insufficient for most use cases
- Key risk area: service delivery reliability


Do You Know
What You
Have?

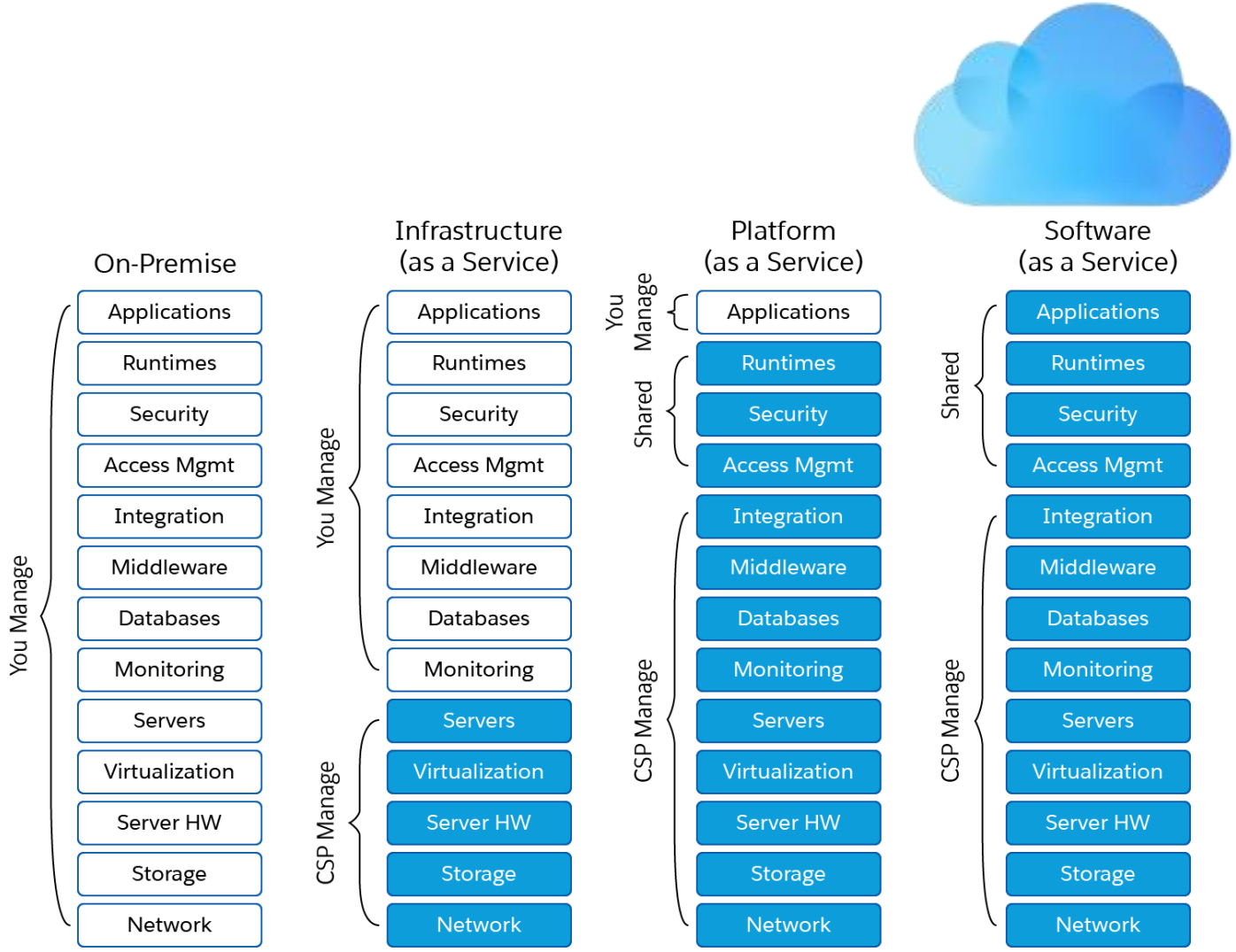
Cloud Governance

- Coverage over all public and private clouds
- All cloud service delivery models
- All data stores and supporting infrastructure

  - Approval for cloud acquisition and migration
  - Defined vendor management responsibilities
  - Maintenance of comprehensive cloud inventory
  - Annual vendor review

Multi-Cloud Shared Responsibility Model

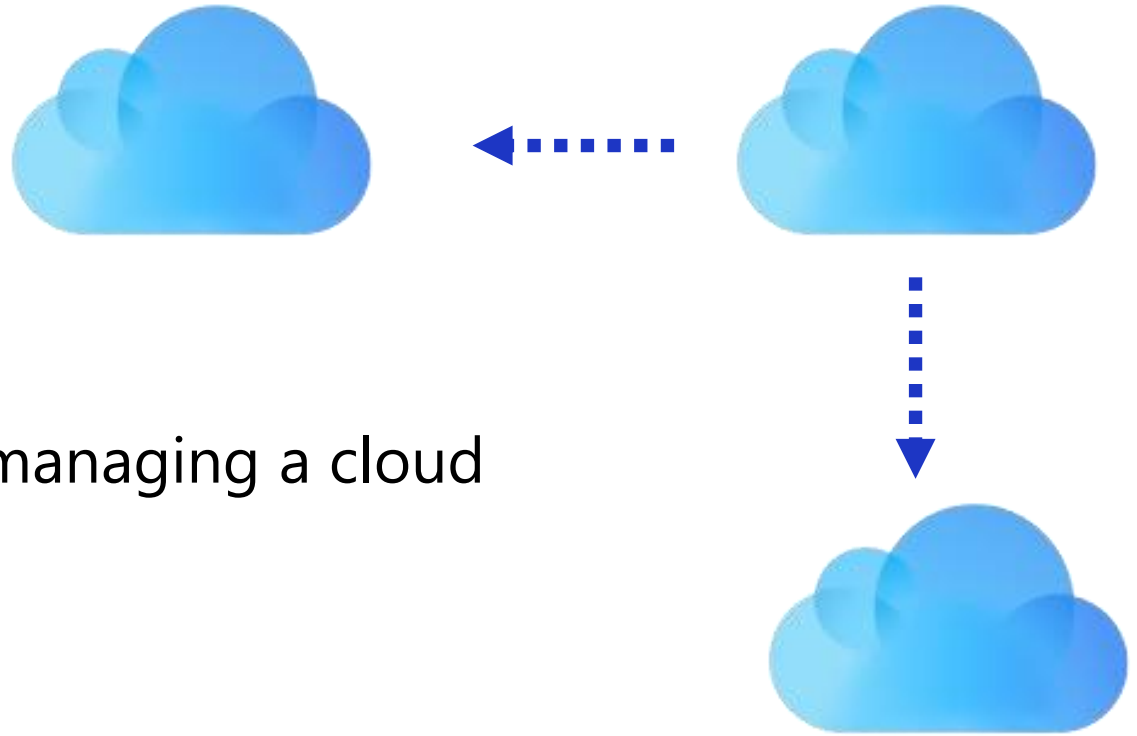
The Shared Responsibility Model is an effective way to depict internal responsibilities over multi-cloud environments



Source: Salesforce

Multi-Parties Shared Responsibility

- When the cloud cannot be fully managed centrally
  - IT/InfoSec teams
  - Business/owner/user teams
  - Service provider team
- To share and define roles over managing a cloud inventory
  - IT/InfoSec teams
  - Business/owner/user teams
  - Procurement/planning/acquisition teams
- To define security responsibilities and assign accountability for each



Dream State Inventory

- All public clouds
- All cloud-based services
- All data stores and supporting infrastructure

  - Criticality of asset and data
  - Authentication method
  - Asset owner and data owner
  - Processes to maintain, review, update, enforce


Next Steps

Audit Plan

1. Cloud inventory completeness and accuracy
2. Cloud governance and shared responsibility
3. Logical access management for non-integrated clouds
4. Cloud assets disaster recovery
5. Cloud configuration management

6. Repeat

Adapt the plan based on where you anticipate the largest impact in a short period of time

weaver

Assurance • Tax • Advisory

Eric Peeters

Senior Manager

Governance, Risk, Compliance

eric.peeters@weaver.com