CIO Magazine: 90% of Business's using Cloud Technology at Some Level

- IT & Records Managers Unaware
- Services
  - Payroll, Taxes, Accounting, HR Recruiting
- Storage
  - Backups, Sharing Information
  - OneDrive, Google, Dropbox

What is "The Cloud" NIST Definition

- Style of Computing Services
  - Shared Pool of Network Resources (servers, storage, applications, services)
  - On Demand – Self Service
  - Elastic
  - Scalable with Little Management or Intervention Needed
  - Metered

Cloud Service Models

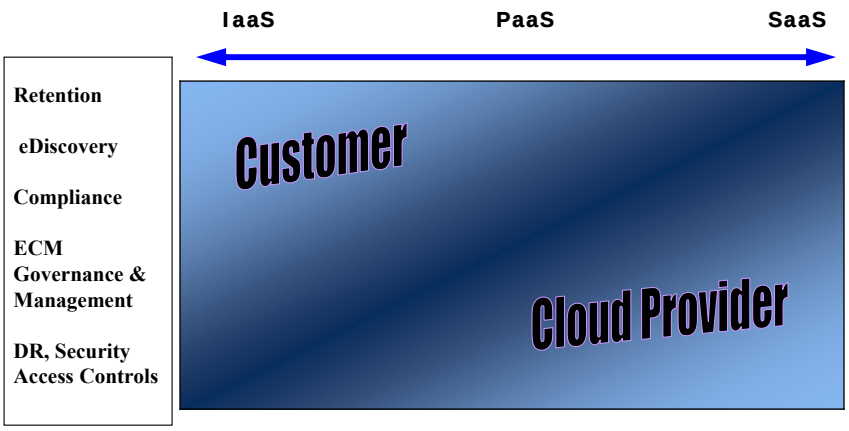
- IaaS
  - On Demand Network and Server Space
  - Customer Deploys and Controls
    - Systems, Databases, Software, Data
- PaaS
  - Operating System Specific Network, Server Space and Development Tools
  - Customer Builds / Deploys Compatible Applications and Controls Databases, Software, Data Storage
- SaaS
  - Lease Software / Possible Data Storage

Outsourcing IT & Data Storage

- Real CSP
  - Own Cloud or Using Another CSP's Data Center
  - 3rd Party CSP Vendors
- Data Center Locations
  - Data Residency
  - Cross Jurisdictional Regulations

- CSP Reputation, Longevity
- Outages
- Security
- Access
- Data Ownership

Shared Responsibility



Public Cloud

- Features
  - Multi–Tenant
  - On Demand
- Benefit - Cost
- Issues
  - Compliance Standards
    - PCI, HIPAA, HITech, Industry
  - Security
    - Segmentation

Private Clouds

- Features
  - On Premise or Off
- Benefit – No Other Tenants
- Issue
  - Cost Reduction?

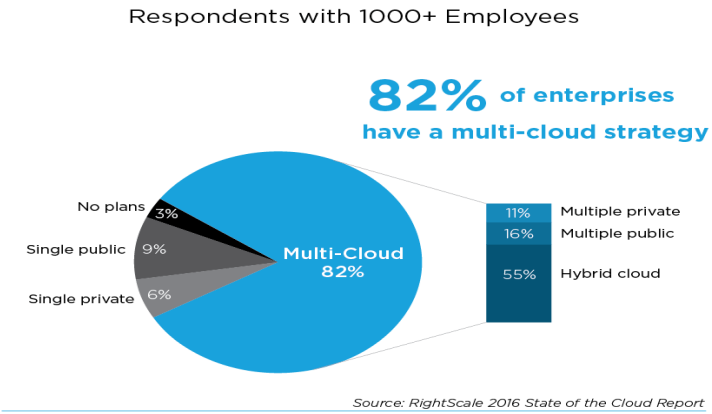
Community Clouds

- Features
  - Like Minded Tenants
  - Address Specific Compliance Concerns
- Benefit
  - Tailored to Meet Community Requirements
    - Financial Services, PCI, HIPAA, HiTech, Government
- Issue
  - Security Segmentation of Customer Data

Hybrid Clouds

- Multi – Cloud Environment
  - Public, Private, Community, In-house IT
  - IaaS, PaaS, SaaS
- Benefits
  - Data & Risk Distribution
  - Risk / Information Appropriate Deployment
- Issues
  - Tracking Deployments, Information Across Clouds
  - Documenting Compliance
  - eDiscovery

Enterprise Adoption



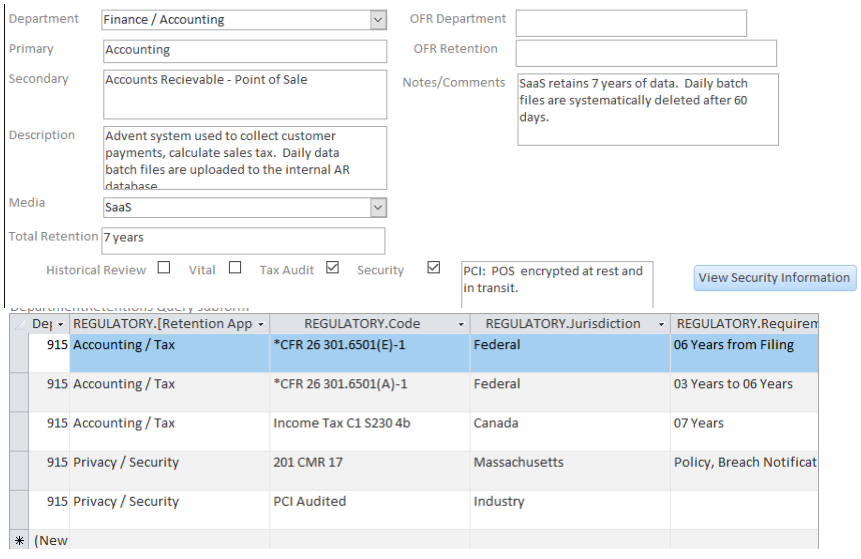
Challenges - Tracking

- Information Storage
- Hybrid Multi-Cloud Deployments
- Compliance

Add to Department Retention Schedules

- Media
  - In-House Server Drives
  - SaaS, PaaS, SaaS
- Compliance Requirements
  - Privacy, Security
  - Industry
- Link to IT Tracking
  - Security
  - Vendor Compliance Attestations

Record Series Example with Compliance



Department: Finance / Accounting
Primary: Accounting
Secondary: Accounts Recievable - Point of Sale
Description: Advent system used to collect customer payments, calculate sales tax. Daily data batch files are uploaded to the internal AR database
Media: SaaS
Total Retention: 7 years
Historical Review ☐ Vital ☐ Tax Audit ☑ Security ☑
OFR Department:
OFR Retention:
Notes/Comments: SaaS retains 7 years of data. Daily batch files are systematically deleted after 60 days.
PCI: POS encrypted at rest and in transit.
View Security Information

Dep	REGULATORY.[Retention App	REGULATORY.Code	REGULATORY.Jurisdiction	REGULATORY.Requiren
915	Accounting / Tax	*CFR 26 301.6501(E)-1	Federal	06 Years from Filing
915	Accounting / Tax	*CFR 26 301.6501(A)-1	Federal	03 Years to 06 Years
915	Accounting / Tax	Income Tax C1 S230 4b	Canada	07 Years
915	Privacy / Security	201 CMR 17	Massachusetts	Policy, Breach Notificat
915	Privacy / Security	PCI Audited	Industry	
(New				

Example IT Security Tracking

System Name	POS System	Truncated	
System	POS Payment Processing	Encrypted	X
Primary User Group	Finance	Cloud Provider	AWS: Advant System
IT Owner	John Burk	Cloud Type	Private / Community
Business Owner	Tanya Clarke	Certification	PCI: 2016, SOC2:2015
Outside Point of Contact	Greg Roster (Advant)	Comments	Advant vendor SOC2 & PCI audited and certified. Information encrypted at rest and in transit. Advant retains 7 years of data.
Access Restrictions	Limited to AR User Role		
Sensitive Information	Credit Card / Bank Card		

Example Contract Record Series

Department	Legal / Contract Management	OFR Department	
Primary	Contracts	OFR Retention	
Secondary	Master Service Agreements	Notes/Comments	
Description	Includes signed agreements, ammendments, significant correspondence, vendor insurance certificates.		
Media	Office 365 & Paper		
Total Retention	Termination + 7 years		

Historical Review ☐ Vital ☐ Tax Audit ☐ Security ☑

PII: Vendor Tax ID numbers included in the last page of every contract.

View Security Information

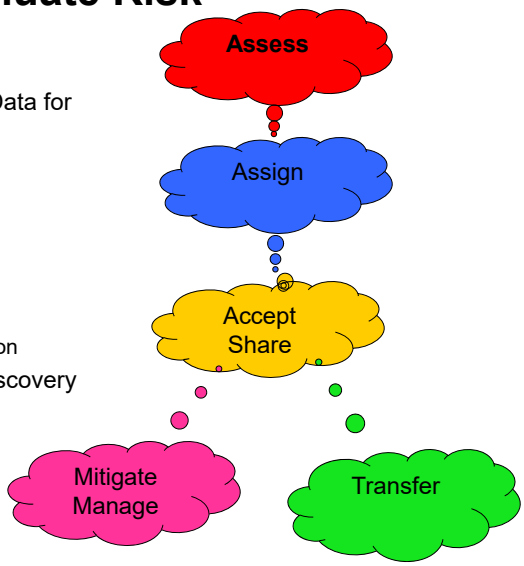
Dep	REGULATORY.[Retention App	REGULATORY.Code	REGULATORY.Jurisdiction	REGULATORY.Requir
916	Legal / Contracts	AKS 09.10.120	Alaska	06 Years
916	Legal / Contracts	MIN 541.05	Minnesota	06 years
916	Legal / Contracts	NY 213	New York	06 years
916	Legal / Contracts	ORS 12.080	Oregon	06 Years
916	Legal / Contracts	RCW 14.16.040	Washington	06 Years

Loss of Control

- Access Rights Management
  - Internal - BYOD
  - CSP & CSP Vendor Access to Data
- Interface with Existing Systems
  - ECM, eDiscovery
- Litigation / eDiscovery
  - Cost to Isolate and Segregate Data
  - Access to Meta Data
- Ability to Change Cloud Providers
  - Transferable Format

Evaluate Risk

- What Would Happen If:
  - Accessed by Cloud Provider
  - Lost Access to Software or Data for a Period of Time
- Is it:
  - Litigation Prone
  - Heavily Regulated / Audited
  - Sensitive: IP, PII, PHI, PCI
- What Can Be Done to:
  - Protect: Encryption / Tokenization
  - Document Compliance / eDiscovery
  - Assess and Validate CSP
    - 3rd Party Audits
    - Attestations: ISO, SOC, FedRamp



SLA Areas

- CSP Provider / Vendors
  - Cloud – Owned or Leased
  - Reputation
  - 3rd Party Vendors
- CSP Security Compliance Assessment Measures
  - SOC 1, SOC 2, ISO, FedRamp, PCI, HITech
  - Ongoing Verification / Audit Measures
- Responsibilities, Rights, Required Notifications
  - Governance, Audit, and Compliance Controls and Reporting
  - Data Ownership
  - Data Location
  - Access Rights Management
  - Breach Notification
  - Litigation, Subpoena, Discovery
  - Retention: Verification of Destruction
  - Legal Rights Options, Remedies
- Contract End – Data Transfer

What We Can Do

- Data Mapping / Tracking
  - Department Retention Schedules
  - Integrate Compliance Requirements
  - Integrate with IT Security
- Work with IT / Legal on Assessment of Data to Be Deployed
  - Compliance / Audit Requirements
  - Integration
    - Retention, Destruction
    - ECM, eDiscovery, Public Disclosure, Compliance, Governance

Questions

Denise Simons
dsimons@haystackassociates.com