Selecting a Cloud Service Provider (CSP)

Steven C. Markey, MSIS, PMP, CISSP, CIPP, CISM, CISA, STS-EV, CCSK, CompTIA Cloud Essentials

Principal, nControl, LLC
Adjunct Professor
President, Cloud Security Alliance – Delaware Valley Chapter (CSA-DelVal)
Selecting a CSP

• Presentation Overview
  – Cloud Overview
  – Selection Considerations, Criteria & Tools
  – Case Studies
Selecting a CSP

• Cloud Overview
  – Why should you care about the “cloud”? 
80% of Fortune companies 1000 will pay to use cloud computing services and 30% will pay for infrastructure.

Gartner

At this moment, the 5 major search engines together have 2,000,000 computers

Microsoft data centre in Chicago: 610,000 servers

33% of IT business will be in Cloud Computing

Gartner

Market: 42 billion: IDC
95 billion: Merrill Lynch

Source: Open Group
Selecting a CSP

• What is Cloud Computing?
  – Re-branded IT Business Model
    • Application Service Provider (ASP)
    • IT Outsourcing (ITO)
  – Confusion
    • Hosting
    • Virtualization
    • Service Provider
Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Resource Pooling

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models:
- Public
- Private
- Hybrid
- Community
Selecting a CSP

• Selection Considerations, Criteria & Tools
  – Risky Business
  – Security Guidance
  – Privacy & Data Protection Rules
  – Service Provider / Consumer Process Alignment
  – Portability / Interoperability
  – Contractual / Legal Agreements
  – Industry Tools & Tricks
Selecting a CSP

• Partly Cloudy with a chance of risk!
  – The Cloud is perceived as risky business.
    • Lack of Control
    • Regulatory Compliance
    • Hacks, outages, disasters....oh my!

Source: Youtube
Selecting a CSP

- Security Guidance
  - Existing Certifications / Attestations
    - SAS 70 Type II / SSAE 16 / ISAE 3402
    - ISO 27001 / 2
    - ISO 27036
    - BITS Shared Assessments
    - PCI DSS
    - HIPAA / HITECH
  - Guidance Specifically for the Cloud
    - Cloud Security Alliance (CSA) Guide v3.0
    - CSA Security, Trust & Assurance Registry (STAR)
    - ENISA Cloud Computing Risk Assessment
    - NIST SP 800-144 Guidelines Security / Privacy for a Public Cloud
Selecting a CSP

• Privacy & Data Protection Rules
  – Jurisdictions*
    • Regional: EU DPA
    • National: PIPEDA, GLBA, HIPAA / HITECH, COPPA, Safe Harbor
    • Statutory: Bavarian, CA SB 1386 / 24, MA 201 CMR 17, NV SB 227
  – Data Flow & Jurisdictional Adherence
    • Backups
    • CSP Big Data: Traditional, Sensory (e.g. Logs, Metadata) & Social
    • Business / Organizational Ecosystem
  – Contract Clauses
    • European Model Contract Clauses
    • PCI DSS
  – Privacy Best Practices
    • Generally Accepted Privacy Principles (GAPP)

* Not all inclusive.
Selecting a CSP

• Svc Provider / Consumer Process Alignment
  – Change / Configuration Management
    • Process, process & some more process.
    • Automated configuration management?
    • Maturity Model
  – Vendor Loading / Off-loading
    • Provisioning / De-provisioning
  – Disaster Recovery
    • Business / Organizational Ecosystem
    • Maturity Model
Selecting a CSP

• Svc Provider / Consumer Process Alignment
  – Incident Response
    • Computer Security Incident Response Team (CSIRT)
      – Digital Forensics
    • Legal Hold / Litigation Response / e-Discovery
      – Electronic Discovery Reference Model (EDRM)
      – Federal Rules of Civil Procedure (FRCP) 30(b)(6)
  – Records and Information Management (RIM)
    • Generally Accepted Recordkeeping Principles (GARP®)
    • Information Governance Reference Model (IGRM)
    • Information Lifecycle Management (ILM)
    • MIKE2.0
Selecting a CSP

- Portability / Interoperability
  - Software
  - Data
  - Third Parties
Selecting a CSP

- Contractual / Legal Agreements
  - Service Level Agreements (SLA)
    - Uptime
    - Data Ownership
      - Escrow Data
      - Include Sensory Data, Metadata
    - Exit Clause
    - Testing
      - Disaster Recovery
      - Incident Response
      - Legal Hold / Litigation Response / e-Discovery
    - Right to Audit
      - Vendor & Vendor’s Vendors
      - Privacy Impact Assessments (PIA)
    - Additional Clauses
      - European Model Contract Clauses
Selecting a CSP

Introducing Core CloudInspect™ Security Testing for Amazon Web Services (AWS)

Do you know if your cloud deployment is secure?
We do.

Learn more >

Ready to test the security of your AWS cloud deployment?

- It’s Fast: begin testing in minutes
- It’s Easy: no security experience required
- It’s Affordable: $20 per machine instance or web application tested (introductory price)

Test your cloud
Selecting a CSP

- Industry Tools & Tricks
  - Cloud Strategic Roadmap
  - Matrices & Software
  - Cloud Brokers
Selecting a CSP

• Industry Tools & Tricks
  – Cloud (Consumer) Strategic Roadmap
    • Business Model Alignment
      – Centralized / Decentralized
      – Industry Vertical
      – Ecosystem Awareness (Customers, Partners, Vendors)
  • Project Portfolio Management (PPM)
    – Assimilate Cloud Projects
      » Involves many stakeholders (business, PMO, IT, etc.).
  • Phased Implementation Approach
    – Private → Hybrid → Public
    – Basic → Advanced Services
Selecting a CSP

• Industry Tools & Tricks
  – Cloud (Provider) Strategic Roadmap
    • Business Model / Product Line Scalability
      – e-Discovery, Authentication, Encryption, Scanning
        » Organic
        » Merger & Acquisition
    • Longevity / Sustainability
    • Industry / Jurisdiction Focus
    • Ecosystem Awareness
    • Technology / Enterprise Architecture (TOGAF, SABSA, ITIL)
Selecting a CSP

• Industry Tools & Tricks
  – Matrices & Software
    • Matrices
      – Audit / Compliance Focused
        » CSA Consensus Assessments Initiative Questionnaire
        » CSA Cloud Controls Matrix
        » BITS Enterprise Cloud Self-Assessment
    • Software
      – VMware Cloud Readiness Self-Assessment (CRSA)
      – Bit Titan MigrationWiz
      – Gravitant cloudWiz
Cloud Readiness Self-Assessment

Before you begin or continue further on your cloud computing journey, it's important to know how ready your organization is in adopting cloud, in the following categories:

- Strategy – Aligning business needs with IT capability.
- Process – Streamlining and automating processes to achieve business agility.
- Architecture – Establishing an enterprise architecture for this new IT infrastructure.
- Technology – Designing and deploying your technology infrastructure from virtualization to cloud.
- People and Governance – Creating the roles and skills necessary to ensure company-wide adoption, and the accountability framework and policies for stakeholder collaboration.

By answering a series of questions within each category, you will get an assessment of your current cloud maturity. Upon completion, you will receive a customized report with detailed next steps that embody VMware best practices to help you be successful in your cloud deployment. See a sample report.

Start Assessment
Mailbox Connector

A mailbox connector defines how your email flows between two locations (where your email currently resides and where you would like your email to reside). Once a connector is created, you can associate one or more mailboxes to that connector. These mailboxes will be connected between the two locations using the mechanism that you have specified.
Capacity planning is a vital component of cloud computing adoption that involves understanding necessary resource requirements in order to meet the anticipated needs of customers and users.

Companies who are able to predict their computing needs can reserve capacity and plan for their predicted usage based on their IT budgets. Other models allow organizations to utilize an on-demand, pay-per-use model which may be more economical.
Step 2: Compare Vendors

Once a cloudWiz user has filled out their current resource utilization and projected demand, they can then **compare vendors, side-by-side.** Our **inbuilt standardized vendor catalog** allows cloud users to compare prices from multiple providers in an expedia-like interface and then **optimize for the best vendor** based on individual goals and constraints such as cost, QoS and best match.
As a cloudWiz user compares vendors across cost, QoS and other constraints, they can also determine ROI Benefits to analyze the effects of selecting a particular provider.
Selecting a CSP

- Industry Tools & Tricks
  - Cloud Brokers
    - RightScale
    - CloudFloor
    - Skydera
    - enStratus
AWS US-East EC2 Instance -changeme-

Unable to save sidebar preferences

- SSH Console
- Bundle
- Terminate
- Reboot

**Info**

- **State:** operational
- **Public DNS name:** ec2-204-236-226-149.compute-1.amazonaws.com
- **Private DNS name:** ip-10-46-114-248.ec2.internal
- **IP address:** 204.236.226.149
- **Private IP address:** 10.46.114.248
- **Current Elastic IP:** -none-
- **Frozen Repositories:** -none-
- **Tag(s):** [Edit Tags]

**EC2 Info**

- **AWS id:** i-1b436d7a
- **SSH key:** sj
- **Security group(s):** -none- \[Required before launching this server.\]
Case Study: Choosing a PaaS CSP

- **Background**
  - Mid-sized Capital Management Firm
  - FINRA Regulated
  - Outsourced IT with hardware onsite.

- **Drivers**
  - Cost
  - Compliance

- **Technologies**
  - Microsoft Exchange / Office 365 Exchange Online
  - Onsite Symantec Enterprise Vault
Cloud Computing

- Case Study: Choosing a PaaS CSP
  - Limitations
    - Budget
    - Skill-sets
    - Resources
    - Monitoring
  - Risks
    - System / Software Interoperability
    - Availability
    - Vendor Management: Contractual / SLA Omissions
    - Scope Creep
    - Data Ownership
Cloud Computing

• Case Study: Choosing a PaaS CSP
  – Lessons Learned
    – Better Safe Than Sorry – Follow GLBA Safeguards
    – Many Moving (Technical) Parts
    – Use Existing Vendors
    – e-Discovery Helped
      – Onsite Journaling
  – Next Steps
    – Testing BCP / DR, Incident Response
    – System Architecture Upgrades
Cloud Computing

• Case Study: Choosing an IaaS CSP
  
  – Background
    – Venture capital funded pharmacy service provider.
    – Small HIPAA / HITECH Business Associate
    – Level 4 PCI Service Provider
  
  – Drivers
    – Cost Savings
    – Core Competency Focus
  
  – Technologies
    – Open-source solutions at a co-location facility.
    – Leverages third party / upstream system providers.
Cloud Computing

• Case Study: Choosing an IaaS CSP
  – Limitations
    – Buying / Negotiating Power
    – HIPAA / HITECH / PCI Requirements
    – Third Party Systems
  – Risks
    – Jurisdiction
    – Availability
    – Cloud / Third Party Ecosystem Reliance
Cloud Computing

• Case Study: Choosing an IaaS CSP
  – Lessons Learned
    – Bigger is not better.
    – Standardize Technology
    – Ask for the documentation from attestations.
    – Sticker Shock
  – Next Steps
    – Work with the CSP
      – Conduct a PIA.
      – Test incident response plans.
Cloud Computing

• Presentation Take Aways
  – There Are No Silver Bullets
  – Think Cloud Strategy & Business Ecosystem
  – You Are Not Alone
    – Leverage CSA, BITS & NIST’s Research
    – Leverage Industry Tools, Tips & Tricks
  – Compare Apples to Apples
    – Technology
    – Pricing
    – SLAs
Cloud Computing

References

- CSA CAIQ: https://cloudsecurityalliance.org/research/cai/
- CSA CCM: https://cloudsecurityalliance.org/research/ccm/
- CSA STAR: https://cloudsecurityalliance.org/star/
- CSA Guide: https://cloudsecurityalliance.org/research/security-guidance/
- Core CloudInspect: https://www.corecloudinspect.com/microsite/index.html
- ARMA GARP: http://www arma.org/GARP/
- IGRM: http://www.edrm.net/projects/igrm
- EDRM: http://www.edrm.net/
- MIKE2.0: http://mike2.openmethodology.org/
- VMware CRSA: http://getcloudready.vmware.com/crsa/
- Gravitant cloudWiz: http://www.gravitant.com/cloudwiz-home.html
- RightScale: http://www.rightscale.com/
- CloudFloor: http://www.cloudfloor.com/
- Skydera: http://www.skydera.com/
- enStratus: http://enstratus.com/
Cloud Computing

• Personal References
  – e-Discovery 2.0: In the Cloud: https://s3.amazonaws.com/nControl-Docs/CSA11_Session-SMarkey.ppt
• Questions?
• Contact
  – Email: steve@ncontrol-llc.com
  – Twitter: @markes1, @casdelval2011
  – LI: http://www.linkedin.com/in/smarkey