

➤ Information Security Decisions



Cloud Compliance: Pulling Back the Curtain on Provider Controls

Diana Kelley
diana@securitycurve.com
@securitycurve

Agenda (40 minutes/20 slides/5 Q&A)

- Security is a Roadblock?
 - What we Love about Cloud
 - And What we Don't
 - Ongoing Work: CSA, FedRAMP, PCI VirtSec
 - What you Can Do for your Organization
-

Security is a Roadblock?



© Copyright Richard Webb and licensed for reuse under Creative Commons License.

Security is a Roadblock?

*Total Cloud Market will Reach **61 Billion USD** by the end of
2012*

SaaS will be **33 Billion** of that

- Source: “*10 Cloud Predictions for 2012*”, by Holger Kisker, Forrester Research,
http://blogs.forrester.com/holger_kisker/11-12-13-10_cloud_predictions_for_2012

Defining the Cloud

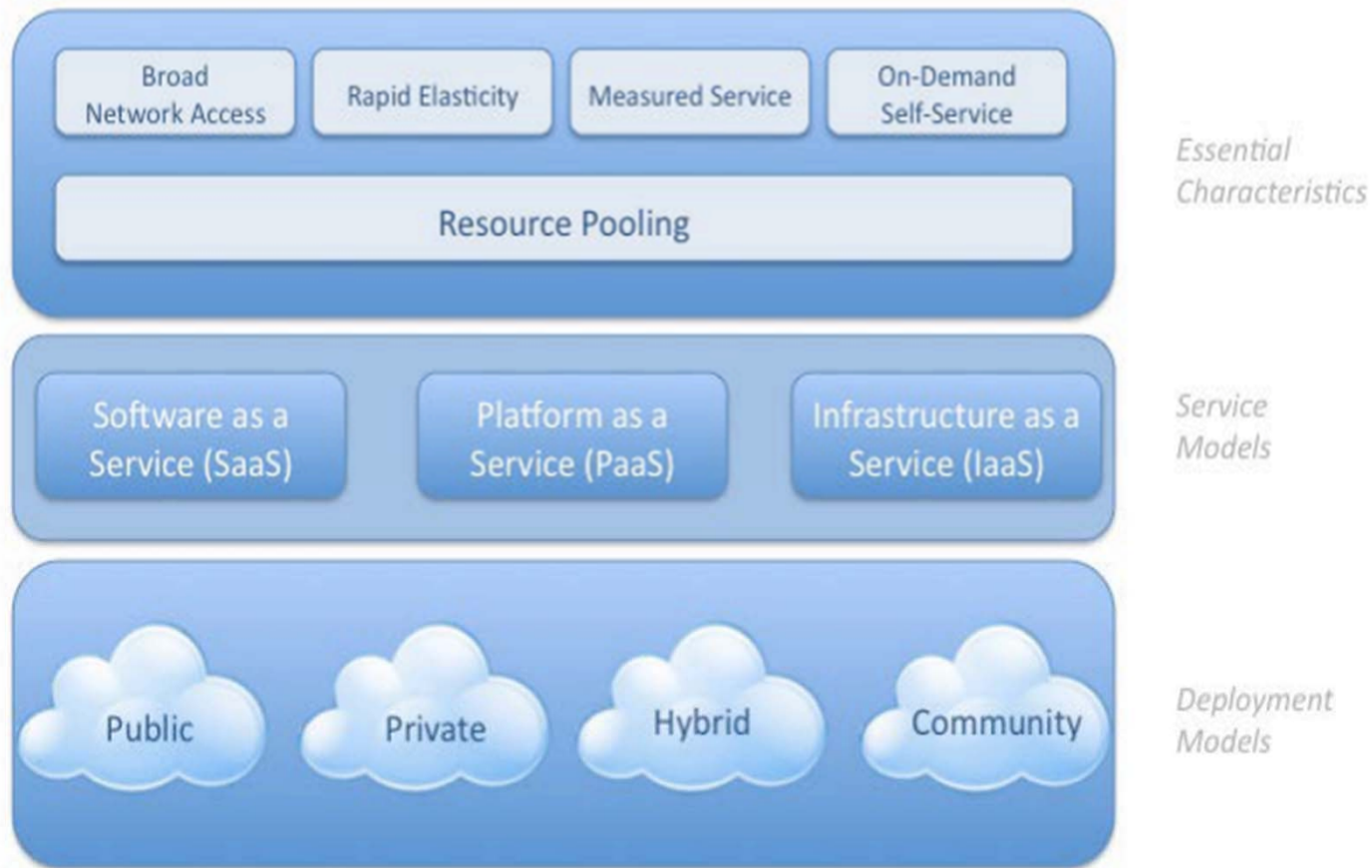


Figure 1—NIST Visual Model of Cloud Computing Definition²

Image Source: <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>

Original data: The NIST Definition of Cloud Computing, <http://csrc.nist.gov/publications/nistpubs/800->

145/SP800-145.pdf

What We Love About Cloud

- Economies of scale
 - More efficient resource allocation
- Elasticity
 - Resources as needed
 - When needed
- Ease of Use
 - Low barrier to entry

US Public IT Cloud Services by Industry Sector: More Details on the Opportunity, “**from 2009 to 2014, U.S. public IT cloud services revenue will grow 21.6%, from \$11.1 billion to \$29.5 billion.**”

IDC Report

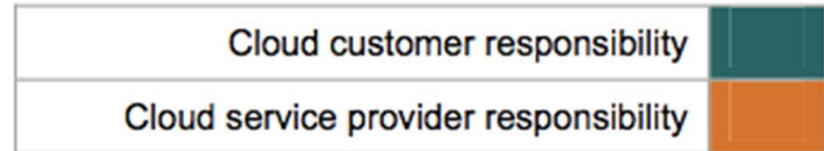
What We Love About Cloud

- Reduced Overhead
 - Headcount
 - Provider handles installation and manages administrators
 - Externalization
 - Compliance reporting
 - Resource management
- Increased Reliability
 - Configured for HA
 - *Service Level Agreements*
 - For 24/7 5 9s uptime



Another View – Responsibility

Example of how scope and responsibility may differ* by type of cloud service:



<u>Area of Responsibility</u>	<u>Type of Cloud Service</u>		
	IAAS	PAAS	SAAS
Data	Customer	Customer	Customer
Software, user applications	Customer	Customer	Provider
Operating systems, databases	Customer	Provider	Provider
Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)	Customer	Provider	Provider
Computer and network hardware (processor, memory, storage, cabling, etc.)	Provider	Provider	Provider
Data center (physical facility)	Provider	Provider	Provider

Cloud Benefits the Flip-Side

“It's *beyond my control*”

- Vicomte de Valmont

- Some examples
 - Vetting of administrative staff
 - Cost control of utilities
 - Upgrades and patching
 - Economies of scale



Control and Accountability

- Who is responsible for the data?
 - Amazon's web services contract: "we strive to keep your content secure, but cannot guarantee that we will be successful at doing so, **given the nature of the internet**". . .
 - ... "you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content. We strongly encourage you, where available and appropriate, to **use encryption technology to protect Your Content from unauthorized access** and to routinely archive Your Content. We will **have no liability to you for any unauthorized access or use**, corruption, deletion, destruction or loss of any of Your Content.

Amazon Web Services™ Customer Agreement, Updated September 25, 2008, Section 7.2. Security, <http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html>

Who's Got Your Data?

- Data stored in public cloud data centers
 - Many located all over the world
 - Bringing in location jurisdiction considerations
 - Level of control varies
 - By model – IaaS, PaaS, SaaS
 - By provider and specific SLA
 - Virtualization commonly means shared hardware
 - And often shared operating systems and apps
-

Data and Transferability Issues

- Who Owns the Data?
 - It was yours
 - But now the SaaS has it
- Who is Responsible if it is lost?
- Can it be moved?
 - To another provider?
 - Back on-prem?
- What about transparency?
 - Right to audit
 - Access to log files
 - Data recovery



Protecting Data in the Cloud

- Security controls are usually most effective when layered
 - But in the cloud the customer doesn't always have access to all those layers
 - Cloud Security Alliance
 - *“a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.”*
 - Publishes the **Security Guidance for Critical areas of Focus in Cloud Computing**
-

Protecting Data in the Cloud

Domain 11 of the Security Guidance for Critical Areas of Focus in Cloud Computing

- ***“ For unstructured files that must be protected when stored or shared in the cloud use data-centric encryption, or encryption embedded into the file format whenever practical to apply protection directly to files ”***

<https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>



CSA Security Guidance – Domains At a Glance

Domain 1: Cloud Computing Architectural Framework

Domain 2: Governance and Enterprise Risk Management

Domain 3: Legal Issues: Contracts and Electronic Discovery

Domain 4: Compliance and Audit

Domain 5: Information Management and Data Security

Domain 6: Interoperability and Portability

Domain 7: Traditional Security, Business Continuity, and Disaster

Domain 7: Traditional Security, Business Continuity, and Disaster

Domain 8: Data Center Operations

Domain 9: Incident Response

Domain 10: Application Security

Domain 11: Encryption and Key Management

Domain 12: Identity, Entitlement, and Access Management

Domain 13: Virtualization

Domain 14: Security as a Service

<https://cloudsecurityalliance.org/guidance/csaguide.v3.pdf>

CSA Cloud Controls Matrix

- Guide from the CSA
 - Normalized guide for prospective cloud customers
 - Helps assess provider against the 13 domains of the CSA guidance
 - Using 11 Control Areas
 - Also maps scope applicability against commonly used frameworks including
 - BITS Shared Assessments
 - CoBiT
 - HIPAA/HITECH
 - ISO27001-2005
 - NIST SP800-53 R3
 - PCI DSS 2.0
 - FedRAMP

<https://cloudsecurityalliance.org/research/initiatives/ccm/>

CSA Cloud Controls Matrix

Control Specification	Control Notes	Architectural Relevance					
		Phys	Network	Compute	Storage	App	Dat
<p>ndent reviews and assessments shall be ned at least annually, or at planned is, to ensure the organization is compliant olicies, procedures, standards and ible regulatory requirements (i.e., /external audits, certifications, vulnerability etration testing)</p>		X	X	X	X	X	X
<p>arty service providers shall demonstrate ance with information security and ntiality, service definitions and delivery level ents included in third party contracts. Third ports, records and services shall undergo nd review, at planned intervals, to govern intain compliance with the service delivery ents.</p>		X	X	X	X	X	X

..... Screenshot taken from: CSA Cloud Controls Matrix v1.2

CSA Cloud Controls Matrix – Control Areas

Compliance

Data
Governance

Facility
Security

Human
Resources

Information
Security

Legal

Operations
Management

Risk
Management

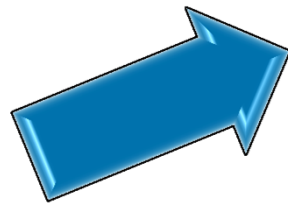
Release
Management

Resiliency

Security
Architecture

CSA Cloud Controls Matrix – Control Areas

Cloud
Security
Alliance
Guidance



Compliance

- CO-01 Audit Planning
- CO-02 Independent Audits
- CO-03 Third Party Audits
- CO-04 Contact/Authority Maintenance
- CO-05 Information System Regulatory Mapping
- CO-06 Intellectual Property

FedRAMP

- Federal Risk and Authorization Management Program

- “...a standardized approach to assessment, authorization, and continuous monitoring for cloud products and services.”



FedRAMP Security Controls Baseline Version 1.0					
Control Number and Name	Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance	
	Low	Moderate			
1.1. Access Control (AC)					
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AC-2	Account Management	AC-2	AC-2	AC-2]. [Assignment: organization-defined frequency] Parameter: [at least annually]	
			AC-2 (1)		
			AC-2 (2)	AC-2 (2) [Assignment: organization-defined time period for each type of account (temporary and emergency)] Parameter: [no more than ninety days for temporary and emergency account types]	
			AC-2 (3)	AC-2 (3) [Assignment: organization-defined time period] Parameter: [ninety days for user accounts]	AC-2 (3) Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB.
			AC-2 (4)		
			AC-2 (7)		

FedRAMP – Security Controls Baseline



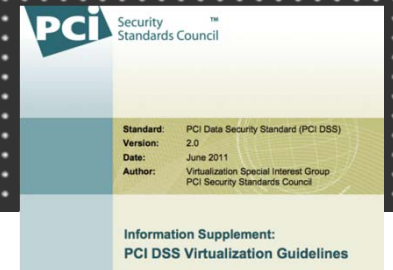
PCI Guidance - In Process

- Special Interest Group established for Cloud
 - Began work in January 2012
 - Est. for publication, late 2012
- Objectives –
 - Explore architectures and models
 - Identifying risks and security
 - Clarify how PCI DSS requirements can be applied to cloud
 - Provide guidance for cloud customers and cloud providers

Source:

https://www.pcisecuritystandards.org/get_involved/special_interest_groups.php

PCI Guidance - Available Now



- Information Supplement: PCI DSS Virtualization Guidelines
 - *“The cloud provider should clearly identify which PCI DSS requirements, system components, and services are covered by the cloud provider’s PCI DSS compliance program.”*
- Recommendations
 - Get everything in writing and validate compliance and control information from provider
 - Hosted entities are ultimately responsible for data in the cloud and must ensure CC protection for areas where the provider can not

What You Can Do for Your Organization

- SLAs
 - Get it in writing
 - Policies
 - Security relies on technical policies
 - Who can/can't access a service
 - Or specific data
 - Transparency
 - Right to Audit
 - Ongoing, continuous monitoring - log access
 - Standard Operating Procedures
 - Incident response
 - Reporting
 - Escalation
 - Mitigation activity
-

What You Can Do for Your Organization

- Educate executives/champions
 - Start with a reality check
 - Is the service really cheaper?
 - Complete a thorough cost/benefit analysis
 - Will the service be able to grow with the enterprise/SMB?
- Current Administrators
 - Responsibilities for working with provider
 - Liaison responsibilities
 - On-going management




Summary

- Benefits of cloud are real
 - And here to stay
 - But cloud brings with it a loss of data control
 - To secure our cloud environments will take a lot of work
 - And planning
 - Keep up to date with work from CSA, FedRAMP (and PCI SSC)
 - Implement Policies and Education
 - Don't depend just on the provider's policies
 - Users need to understand how to use new service
-

Resources

- Security Guidance for Critical Areas of Focus in Cloud Computing v3.0, Cloud Security Alliance, <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>
- Cloud Security Alliance Cloud Controls Matrix, <https://cloudsecurityalliance.org/research/initiatives/ccm/>
- Information Supplement: PCI DSS Virtualization Guidelines, <https://www.pcisecuritystandards.org>
- FedRAMP, <http://www.gsa.gov/portal/category/102371>
- The NIST Definition of Cloud Computing, NIST SP800-145, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- DRAFT Guidelines on Security and Privacy in Public Cloud Computing, NIST SP800-144, http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf



Diana Kelley
diana@securitycurve.com
@securitycurve



Featured Member of the
TechTarget Editorial
Speaker Bureau

