Lessons from FedRAMP

IT Security Controls in the Shared Computing Model

Ken E. Stavinoha, Ph.D
ITGRC Solutions Architect

17 May 2013

FedRAMP Overview

Impact of Cloud Computing

Cloud computing and virtualization have changed the concept of traditional network perimeter and security boundaries as well as how consumers procure IT services and the ways that providers offer them.

CLOUD COMPUTING	IMPACT
• Introduces operational as well as architectural changes into a more dynamic IT environment	• CSP must address operational risk in addition to secure configurations/architectures
	• CSP must prove virtual boundaries adequately protect data
• Has outpaced laws, regulations, and many standards leaving customers at a disadvantage	• More emphasis on proactive IT governance rather than reactive standards compliance
	• Shared responsibility for security and compliance

Requires Holistic Serves Solutions Beyond Implementation

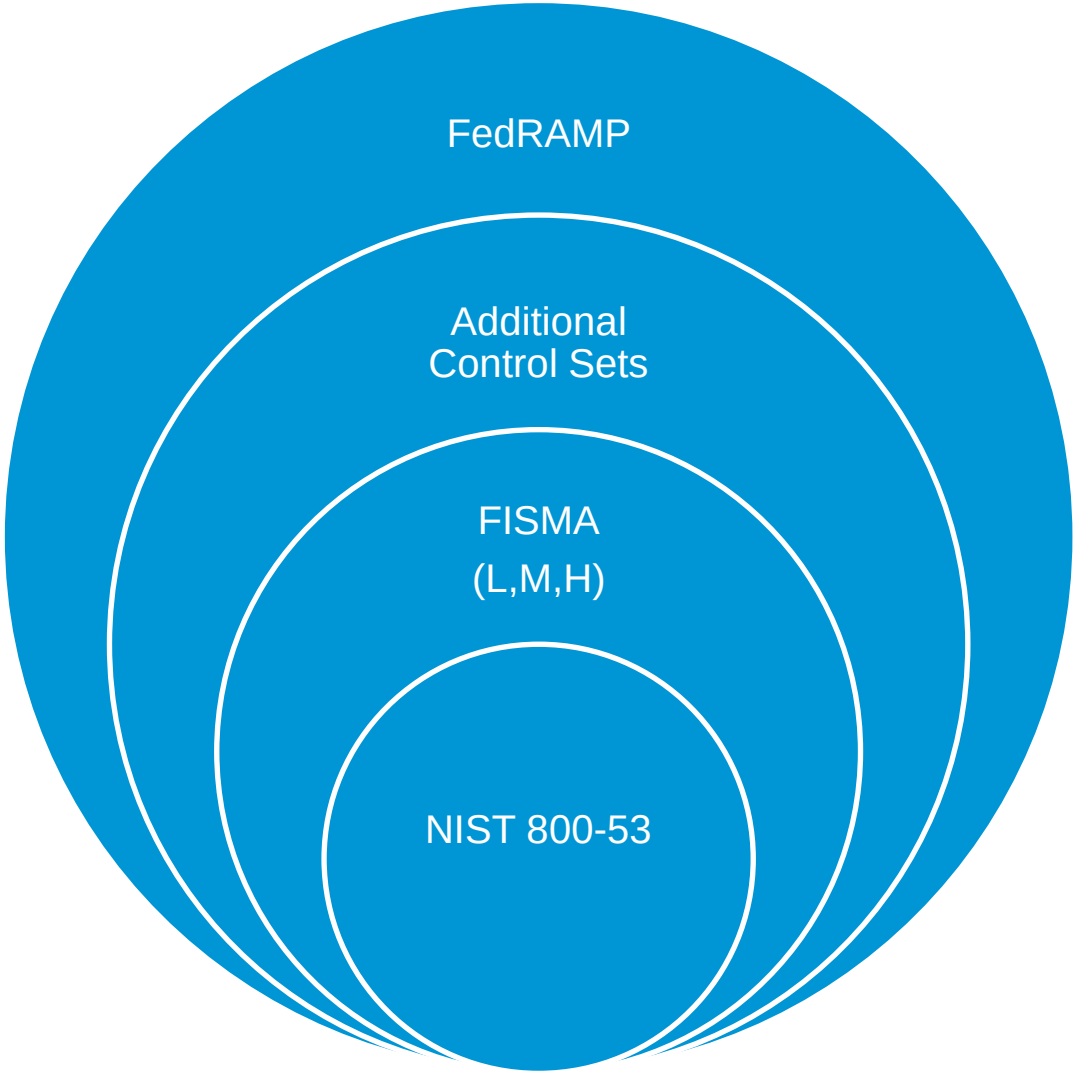
FISMA

- What is it?
  - Federal Information Security Management Act (FISMA)
  - United States **legislation** (not an agency program)
  - Defines a comprehensive **framework** to protect government information, operations and assets against natural or man-made threats
- What's it's purpose?
  - Assigns responsibilities to various agencies to ensure the security of data
  - Requires annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels
- Who manages it?
  - Individual agencies
- NOTE: Federal agencies are required to adhere to FISMA, but many state/local governments and higher educational institutions follow FISMA guidance and recommendations

FedRAMP

- What is it?
  - Federal Risk and Authorization Management Program (FedRAMP)
  - A **government-wide program** leveraging a “do once, use many times” framework (not legislation)
  - Provides a standardized approach to security assessment, authorization, and continuous monitoring for **cloud products and services**
- What’s it’s purpose?
  - Ensure that *cloud based services* have adequate information security;
  - Eliminate duplication of effort and reduce risk management costs; and
  - Enable rapid and cost-effective procurement of information systems/services for Federal agencies.” (CIO.gov)
- Who manages it?
  - GSA oversees
  - Accredited 3PAO’s validate proposed offers before GSA approves

Not FISMA -vs- FedRAMP, its FISMA & FedRAMP



NIST 800-53

- What is it?

  Provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

  Applies to all components of an information system that process, store, or transmit federal information

- What's it's purpose?

  Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations;

  Providing a stable, yet flexible catalog of security controls to meet current information protection needs and the demands of future protection needs based on changing threats, requirements, and technologies;

  Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems;*

  Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and

  Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

- Who manages it?

  Department of Commerce

  National Institute of Standards & Technology

NIST 800-53 Control Baselines

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5)	AC-6 (1) (2) (3) (5)
AC-7	Unsuccessful Login Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
AC-12	**Withdrawn**	---	---	---	---
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14	AC-14
AC-15	**Withdrawn**				

Additional Control Sets for FedRAMP

- Using NIST 800-53 defined baselines for low and moderate impact systems, FedRAMP selected additional controls and enhancements to address the unique risks of cloud computing environments, including but not limited to: multi-tenancy, visibility, control/responsibility, shared resource pooling, and trust.

FedRAMP Security Controls Baseline
Version 1.0

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AU-10	Non-Repudiation	Not Selected	**AU-10**		
			AU-10 (5)	AU-10 (5) [*Selection: FIPS-validated; NSA-approved*] Parameter: See additional requirements and guidance.	AU-10 (5) Requirement: The service provider implements FIPS-140-2 validated cryptography (e.g., DOD PKI Class 3 or 4 tokens) for service offerings that include Software-as-a-Service (SaaS) with email.
AU-11	Audit Record Retention	AU-11	AU-11	AU-11 [Assignment: organization-defined time period consistent with records retention policy] Parameter: [at least ninety days]	AU-11 Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

Federal INFOSEC Compliance Landscape

- Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Freedom of Information Act as Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Rehabilitation Act of 1973 [Section 508 Amendment]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

Lesson One:
Know Your History

Key Control Areas in Play

- Access Controls
- Asset Classification and Owner(s)
- Monitoring & Logging
- Patching & Updates
- Incident Response
- Security Baselines & Configurations
- System Boundaries
- Policy & Procedure

FedRAMP CIS Worksheet

FedRAMP Control Implementation Summary (CIS)												
Control ID	Implementation Status					Control Origination						
	In Place	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Service Provider Corporate and Service Provider System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Provisional Authorization
AC-1												
AC-2												
AC-2 (1)												
AC-2 (2)												
AC-2 (3)												
AC-2 (4)												
AC-2 (7)												
AC-3												
AC-3 (3)												
AC-4												
AC-5												
AC-6												
AC-6 (1)												
AC-6 (2)												
AC-7												
AC-8												
AC-10												
AC-11												
AC-11 (1)												
AC-14												
AC-14 (1)												
AC-16												
AC-17												

Lesson Two: Plan for Change

Cloud Services Scope and Control

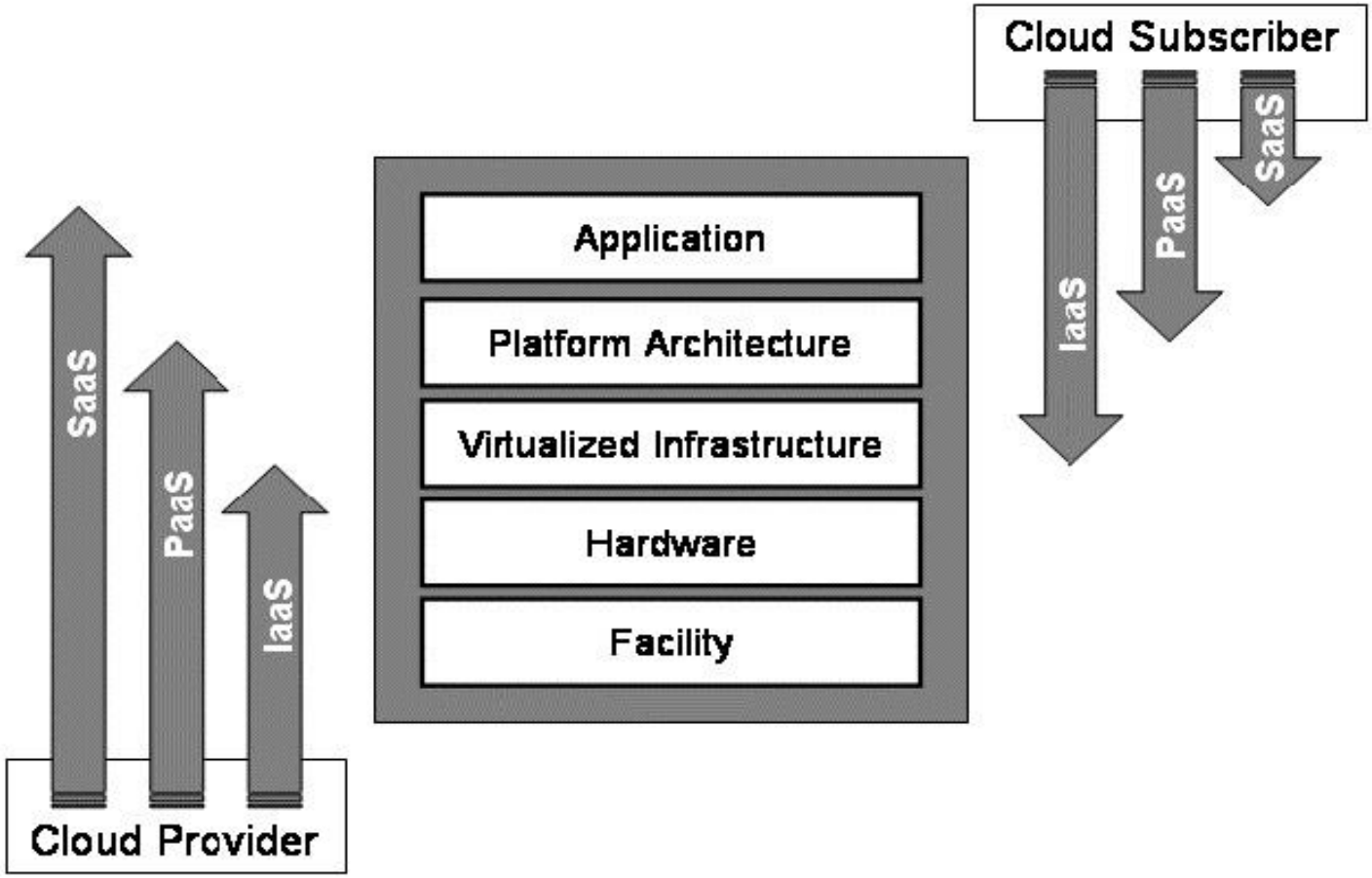


Figure 1: Differences in Scope and Control among Cloud Service Models

Source: NIST SP800-144

Controls Responsibility Matrix

FedRAMP Control Implementation Summary (CIS) Pre Cloud						
Control ID	Control Origination					
	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Service Provider Corporate and Service Provider System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)
ACCESS CONTROL				X		
ASSET CLASS/OWN				X		
MONITORING/LOGGING				X		
PATCHING/UPDATES				X		
INCIDENT RESPONSE				X		
SECURITY BASELINE				X		
SYSTEM BOUNDARY				X		
POLICY/PROCEDURE				X		

Lesson Three: Prepare to Negotiate – Sample Language for Contracts/SLAs

Data Jurisdiction

- No FedRAMP controls govern data location; providers may describe boundaries that include foreign data centers. Agencies with specific data location requirements must include contractual requirements identifying where data-at-rest (primary and replicated storage) shall be stored.
- **Sample Template Language for Technical Requirements:**
- *The vendor shall identify all data centers that the data at rest or data backup will reside. All data centers will be guaranteed to reside within [defined boundary / country / jurisdiction].*
- *The vendor shall provide a Wide Area Network (WAN), with a minimum of [#] data center facilities at [#] different geographic locations with at least [#] Internet Exchange Point (IXP) for each price offering. The vendor shall provide Internet bandwidth at the minimum of [#] GB.*

Encryption

- The FedRAMP security control baseline includes IA-7, SC-8(1), SC-9(1), SC-13, and SC-13(1) all of which require cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. If agency requirements stipulate FIPS 140-2 validated cryptography be used from the agency to the cloud service provider, that should be specified.
- **Sample Template Language for Technical Requirements:**
- *All deliverables shall be labeled [appropriate label such as "Controlled Unclassified Information" (CUI) or other agency selected designation per document sensitivity]. External transmission/dissemination of [labeled deliverables] to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with [standard, such as FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."]*

Non Repudiation

- **AU-10(5): Non-Repudiation**
- The organizational parameter requires that cloud service providers implement FIPS 140-2 validated cryptography for digital signatures. If the agency has a requirement for integration with specific digital signature technologies, that should be included within the contract requirements.
- **Sample Template Language for Technical Requirements:**
- *The vendor shall provide a system that implements [encryption standard] that provides for origin authentication, data integrity, and signer non-repudiation*.

Audit Record Retention

- Agencies should consider the length of time they require Cloud Service Providers to retain audit records as part of their contracts with the CSP. The FedRAMP requirement is that the service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.
- **Sample Template Language for Technical Requirements:**
- *The vendor shall support a system in accordance with the requirement for Federal agencies to manage 19 their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including **but not** 20 **limited to** capabilities such as those identified in:*
- *DoD STD-5015.2 V3 (ref. b), Electronic Records Management Software Applications Design 22 Criteria Standard, 23*
- *NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving 24 applications to store e-mail (ref. c), 25*
- *NARA Bulletin 2010-05 September 08, 2010, Guidance on Managing Records in Cloud 26 Computing Environments (ref 8).*

Multi-Factor Authentication

- **Identification and Authentication (Organizational Users) Multi-Factor Authentication**
- Cloud Service Providers pursuing a FedRAMP authorization will have to provide a mechanism for Government consuming end-users to utilize two-factor authentication. However, Agencies requiring a specific method of authentication, or integration with an existing agency system (such as a SAML 2.0 authentication to the agency's Identity Provider) must specify this requirement in their contract.
- **Sample Template Language for Technical Requirements:**
- *The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.*
- *The vendor shall support dual factor authentication including [specific method of authentication].*

Incident Reporting Timeframes

- FedRAMP parameters set compliance for Incident Reporting at the levels stipulated in NIST SP 800-61; and the JAB will require an Incident Reporting plan that complies with those requirements. Agency contracts should stipulate any specific incident reporting requirements including who and how to notify the agency.
- **Sample Template Language for Technical Requirements**:
- *Cloud Service Providers are required to report all computer security incidents to the United States Computer Emergency Readiness Team (US-CERT) in accordance with US-CERT "Incident Categories and Reporting Timeframes" in , Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to US-CERT within 1 hour of detection regardless of the incident category reporting timeframe.*

Personnel Screening

- FedRAMP parameters set compliance for Incident Reporting at.
- **Sample Template Language for Technical Requirements:**
- *The vendor shall provide support personnel maintaining a NACI clearance or greater in accordance with OMB memorandum M-05-24, Section C.*
- *Vendor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel supporting the system. Vendor shall comply with [agency directive on personnel screening]. [Agency] separates the risk levels for personnel working on Federal computer systems into [#] categories: [category descriptions]. In accordance with [agency directive on personnel screening], the cost of meeting all security requirements and maintaining assessment and authorization shall be [method of meeting cost]. Those vendor personnel (hereafter known as "Applicant") determined to be in a [category of risk] will require a [level of clearance] investigation. [repeat for each category of risk]*

Lesson Four:
Implement Continuous Monitoring

Continuous Monitoring Defined

- Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions.
- Continuous does not mean instantaneous. According to NIST SP 800-137, the term “continuous” means “that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.”

Continuous Monitoring Metrics

Administration Priority Area	Section	Performance Metric	Minimal Level for 2013	Target Level for 2013
Continuous[2] Monitoring – Assets	2.2	% of assets in 2.1, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	80%	95%
Continuous Monitoring – Configurations	3.1.3	% of the applicable hardware assets (per question 2.1), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and provide visibility at the organization's enterprise level.		
Continuous Monitoring – Vulnerabilities	4.2	% of hardware assets identified in section 2.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.		
Identity Management HSPD-12	5.2.5, 5.4.5, 10.2.5	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	50%	75%
Boundary Protection CNCI[3] #1	7.2	% of external network traffic passing through a Trusted Internet Connection (TIC[4]).	80%	95%
Boundary Protection CNCI #1 & #2	7.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	95%	100%

Near Term Goals for CM

- The Federal CMWG has recommended that **asset management** is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices and software (both authorized/managed and unauthorized/unmanaged) before they can manage the devices/software for configuration and vulnerabilities.
- A key goal of hardware asset management is to **identify and remove unmanaged hardware assets/components** before they are exploited and used to attack other assets. An underlying assumption is that if they are unmanaged, then they are probably vulnerable and will be exploited if not removed or "authorized" in near-real-time (less than 72 hours).
- Another goal is to **define the universe of assets** to which other controls need to be applied. These other controls include software asset management, boundary protection (network and physical), vulnerability management, and configuration management. These other areas of monitoring assess how well the hardware assets are managed.

Recap:

1. Know your history
2. Plan for change
3. Prepare to negotiate
4. Implement CM

Thank you.