Contemporary Challenges for Cloud Service Providers Seeking FedRAMP Compliance

July 2017

Jeff Roth, CISSP-ISSEP, CISA, CGEIT, QSA

Regional Director

NCC Group

Agenda

- FedRAMP - Foundations/Frameworks
- Cloud Service Providers (CSPs) drive to participate in FedRAMP and Challenges
- New to the Party – What you do not know will hurt you
- Key challenges to FedRAMP Ready
  - Administrative
  - Operational
  - Technical
- Smoothing out the Bumpy Road
- Summary
- Questions

Introduction

With the recent fifth anniversary of The Federal Risk and Authorization Management Program (FedRAMP) we are seeing greater and greater participation and end user acceptance of Cloud Service Providers (CSP) and delivery of innovation within IaaS, PaaS, SaaS and related products and services to government clients.

Although FedRAMP is a well thought out and structured framework, CSPs with commercial focus invariably face challenges when seeking FedRAMP authorization - resulting in significant losses in time, money, and reputation if not prepared.

This presentation will address the key practices essential to successful FedRAMP ready outcomes.

FedRAMP - Foundations/Frameworks

FedRAMP - Foundations/Frameworks

FedRAMP authorizes cloud systems in a three step process:

- **Security Assessment:** Uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations.
- **Leveraging and Authorization:** Federal agencies view security authorization packages in the FedRAMP repository and leverage the security authorization packages to grant a security authorization at their own agency.
- **Ongoing Assessment & Authorization:** Once an authorization is granted, **ongoing assessment and authorization activities** must be completed to maintain the security authorization.

FedRAMP - Foundations/Frameworks

- Types of FedRAMP Packages
  - **Joint Authorization Board P-ATO** - When the JAB grants the P-ATO, the JAB will provide a recommendation to all Federal Agencies about whether a cloud service has a recommended acceptable risk posture for Federal Government use at the designated data impact levels.
  - **FedRAMP Agency ATO** - CSPs may work directly with an Agency to obtain a FedRAMP Agency ATO. CSPs will work directly with the Federal Agency security office and present all documentation to the Authorizing Official (AO) or equivalent for an authorization.

FedRAMP - Foundations/Frameworks

- Types of FedRAMP Packages
  - **FedRAMP Ready (CSP Supplied Package) -** CSPs may supply a security package to the FedRAMP Secure Repository for prospective Agency use.
    - CSP decides to work independently instead of through the JAB or through a Federal Agency.
    - Will not have an authorization at the completion, but will have a FedRAMP-compliant package available for leveraging.
    - CSPs must contract with an accredited 3PAO to independently verify and validate the security implementations and the security assessment package.

FedRAMP - Foundations/Frameworks

- Types of FedRAMP Packages
  - **FedRAMP Accelerated-**
    - *Phase 1* – FedRAMP Readiness Assessment - FedRAMP PMO will assess a system's operational security capabilities first as opposed to having CSPs undergo a lengthy documentation process first. This Readiness Assessment testing will be executed by an **accredited 3PAO**, and the PMO will review all submitted reports within one week.
    - *Phase 2* – CSP Security Package Development - CSP must develop **a complete security package** for review including the SSP, SAP, SAR, and Plan of Action and Milestones (POA&M).
    - *Phase 3* – JAB Authorization Review Process - JAB Technical Representative (TR) teams at DoD, DHS, and GSA will conduct a thorough review of a CSP's security package. **Turn around for a P-ATO is 6 months.**

FedRAMP - Foundations/Frameworks

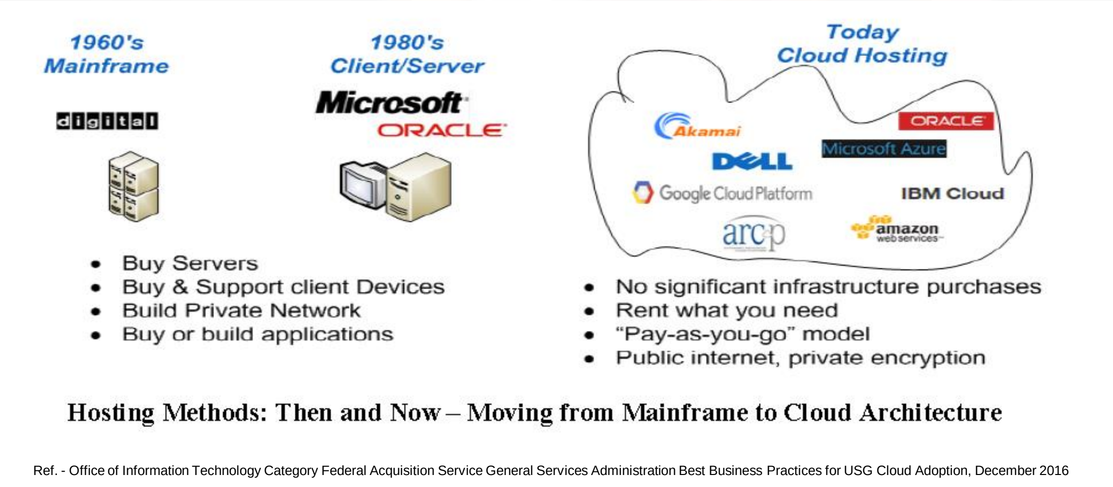
- Types of FedRAMP Packages
  - **FedRAMP Tailored (Under Draft Review)-**
    - Low Impact Solutions only (SaaS)
    - Much smaller number of control requirements
    - Must be able to answer “Yes” to the following:
      - Does the service operate in the cloud?
      - Is the cloud service fully operational (e.g. not under development)?
      - Is the cloud service a Software application (SaaS), rather than Infrastructure (IaaS) or a Platform (PaaS)?
      - Can the cloud service provide services without requiring the collection of personally identifiable information (PII)?
      - Is the cloud service low-security-impact, according to the FIPS 199 definition?
      - Is the cloud service hosted within an existing FedRAMP authorized infrastructure, where pre-existing controls and validations can be inherited?

CSP’s drive to participate in FedRAMP

CSP’s drive to participate in FedRAMP

The federal government spends more than $80 billion dollars on IT annually, with more than $2 billion of that amount spent on acquiring cloud-based services. This amount is expected to rise in coming fiscal years, according to OMB.[1]

This is not the first of migrations within USG IT



- Buy Servers
- Buy & Support client Devices
- Build Private Network
- Buy or build applications

- No significant infrastructure purchases
- Rent what you need
- “Pay-as-you-go” model
- Public internet, private encryption

Hosting Methods: Then and Now – Moving from Mainframe to Cloud Architecture

Ref. - Office of Information Technology Category Federal Acquisition Service General Services Administration Best Business Practices for USG Cloud Adoption, December 2016

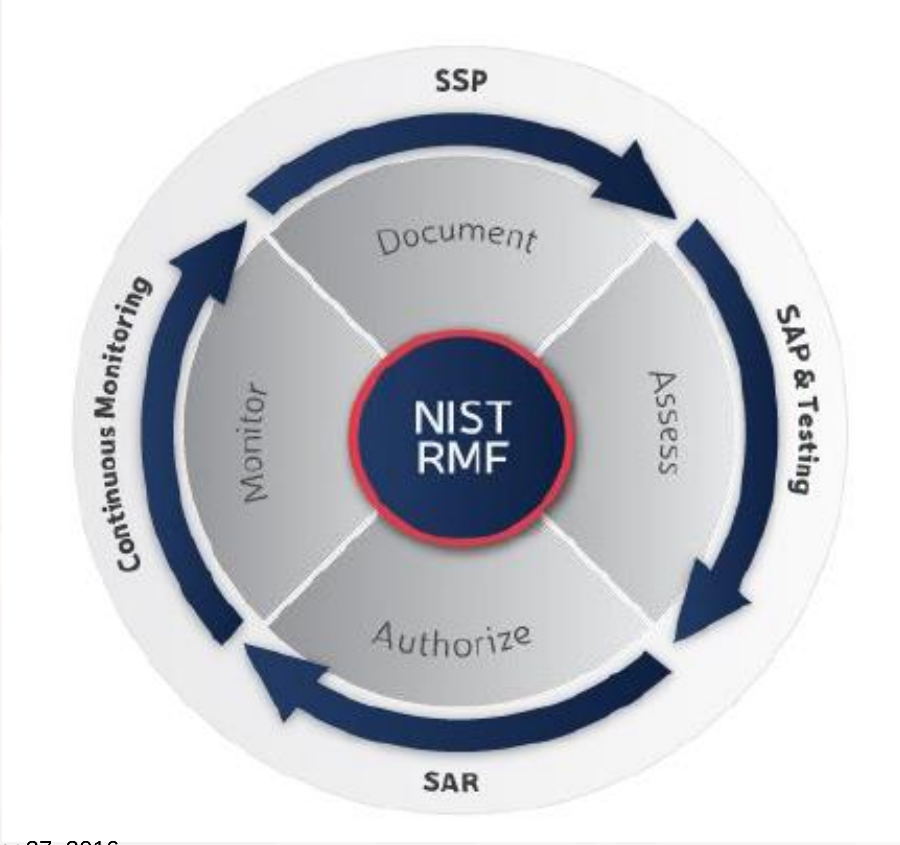
[1] GAO Report to Congressional Requesters CLOUD COMPUTING Agencies Need to Incorporate Key Practices to Ensure Effective Performance

FedRAMP - Challenges

FedRAMP - Challenges

While the FedRAMP Security Assessment Framework is well established and based on solid security practices, CSP and USG understanding of responsibilities and service levels still can be a challenge.

"The greatest challenge is not getting a contract in place, but what you find out is where those boundaries cross of who's now responsible because you're in a different infrastructure set-up, and what the cloud provider's going to do versus the contract staff, versus the application support staff versus the infrastructure staff,"[2]



[2] 5 years into the 'cloud-first policy' CIOs still struggling, Kenneth Corbin, Freelance Writer, CIO| Apr 27, 2016

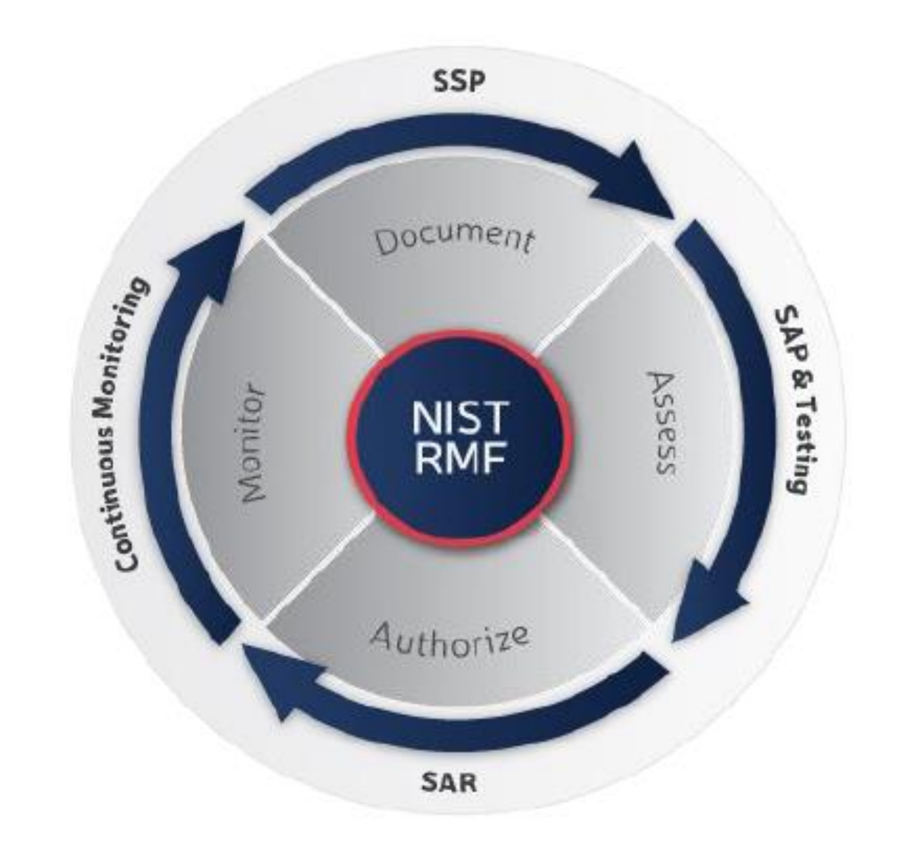
FedRAMP - Challenges

Realization that all things are best suited for the Cloud – but how do we decide?

- "Do not move things to the cloud unless we can engineer them for the cloud…

- …There are ways of designing software for the cloud that really take advantage of what the cloud offers and make things perform well…

- …At the Food and Drug Administration set up a "cloud advisory board" that helps determine which applications belong in the cloud and aids in managing that transition."[2]



[2] 5 years into the 'cloud-first policy' CIOs still struggling, Kenneth Corbin, Freelance Writer, CIO| Apr 27, 2016

New to the Party – What you do not know will hurt you

New to the Party – What you do not know will hurt you

CSPs are now seeing the opportunities in providing IaaS, PaaS and most especially SaaS surrounding big data analytics and managed services.

While many of these CSPs may meet ISO 27001or have Payment Card Industry Data Security Standards (PCI-DSS) Attestation of Compliance (AoC) and/or Report on Controls at a Service Organization (SOC 2, Type 1 / 2 or SOC 3):

- Not all the ISO27001 Annex A controls map to meet FedRAMP control requirements.
- PCI DSS assessment can be rigorous, however, these controls also do not completely meet FedRAMP control, continuous monitoring or reporting requirements.
- SOC Trust Services selection and mapping do not directly correlate to meeting FedRAMP control requirements.

New to the Party – What you do not know will hurt you

- Examples from ISO 27001 Annex A to FedRAMP (via SP 800-53 rev 4 App H)

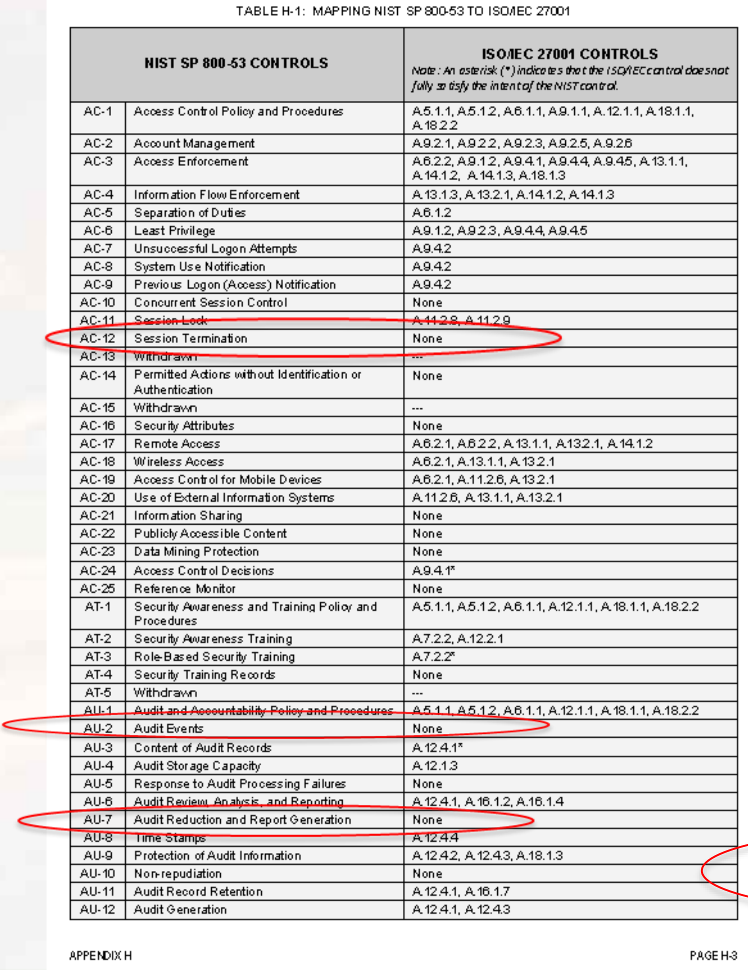
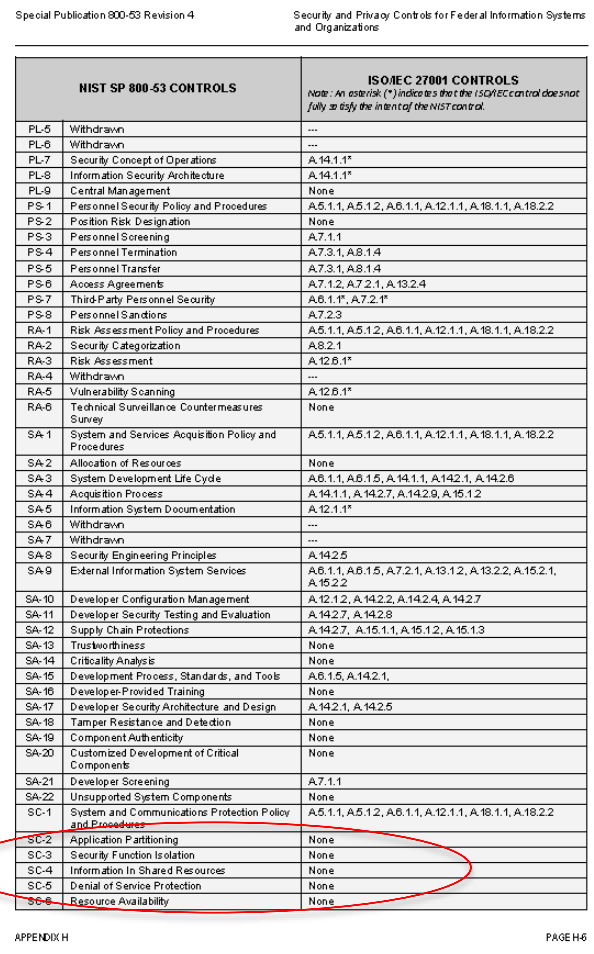


TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	Account Management	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	Access Enforcement	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	Information Flow Enforcement	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	Separation of Duties	A.6.1.2
AC-6	Least Privilege	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	Unsuccessful Logon Attempts	A.9.4.2
AC-8	System Use Notification	A.9.4.2
AC-9	Previous Logon (Access) Notification	A.9.4.2
AC-10	Concurrent Session Control	None
AC-11	Session Lock	A.11.2.8, A.11.2.9
AC-12	Session Termination	None
AC-13	Withdrawn	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	Withdrawn	---
AC-16	Security Attributes	None
AC-17	Remote Access	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	Wireless Access	A.6.2.1, A.13.1.1, A.13.2.1
AC-19	Access Control for Mobile Devices	A.6.2.1, A.11.2.6, A.13.2.1
AC-20	Use of External Information Systems	A.11.2.6, A.13.1.1, A.13.2.1
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.9.4.1*
AC-25	Reference Monitor	None
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT-2	Security Awareness Training	A.7.2.2, A.12.2.1
AT-3	Role-Based Security Training	A.7.2.2*
AT-4	Security Training Records	None
AT-5	Withdrawn	---
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU-2	Audit Events	None
AU-3	Content of Audit Records	A.12.4.1*
AU-4	Audit Storage Capacity	A.12.1.3
AU-5	Response to Audit Processing Failures	None
AU-6	Audit Review, Analysis, and Reporting	A.12.4.1, A.16.1.2, A.16.1.4
AU-7	Audit Reduction and Report Generation	None
AU-8	Time Stamps	A.12.4.4
AU-9	Protection of Audit Information	A.12.4.2, A.12.4.3, A.18.1.3
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.12.4.1, A.16.1.7
AU-12	Audit Generation	A.12.4.1, A.12.4.3

APPENDIX H PAGE H-3



Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
PL-5	Withdrawn	---
PL-6	Withdrawn	---
PL-7	Security Concept of Operations	A.14.1.1*
PL-8	Information Security Architecture	A.14.1.1*
PL-9	Central Management	None
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PS-2	Position Risk Designation	None
PS-3	Personnel Screening	A.7.1.1
PS-4	Personnel Termination	A.7.3.1, A.8.1.4
PS-5	Personnel Transfer	A.7.3.1, A.8.1.4
PS-6	Access Agreements	A.7.1.2, A.7.2.1, A.13.2.4
PS-7	Third-Party Personnel Security	A.6.1.1*, A.7.2.1*
PS-8	Personnel Sanctions	A.7.2.3
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
RA-2	Security Categorization	A.8.2.1
RA-3	Risk Assessment	A.12.6.1*
RA-4	Withdrawn	---
RA-5	Vulnerability Scanning	A.12.6.1*
RA-6	Technical Surveillance Countermeasures Survey	None
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6
SA-4	Acquisition Process	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
SA-5	Information System Documentation	A.12.1.1*
SA-6	Withdrawn	---
SA-7	Withdrawn	---
SA-8	Security Engineering Principles	A.14.2.5
SA-9	External Information System Services	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2
SA-10	Developer Configuration Management	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7
SA-11	Developer Security Testing and Evaluation	A.14.2.7, A.14.2.8
SA-12	Supply Chain Protections	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3
SA-13	Trustworthiness	None
SA-14	Criticality Analysis	None
SA-15	Development Process, Standards, and Tools	A.6.1.5, A.14.2.1,
SA-16	Developer-Provided Training	None
SA-17	Developer Security Architecture and Design	A.14.2.1, A.14.2.5
SA-18	Tamper Resistance and Detection	None
SA-19	Component Authenticity	None
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.7.1.1
SA-22	Unsupported System Components	None
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SC-2	Application Partitioning	None
SC-3	Security Function Isolation	None
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	None
SC-6	Resource Availability	None

APPENDIX H PAGE H-6

New to the Party – What you do not know will hurt you

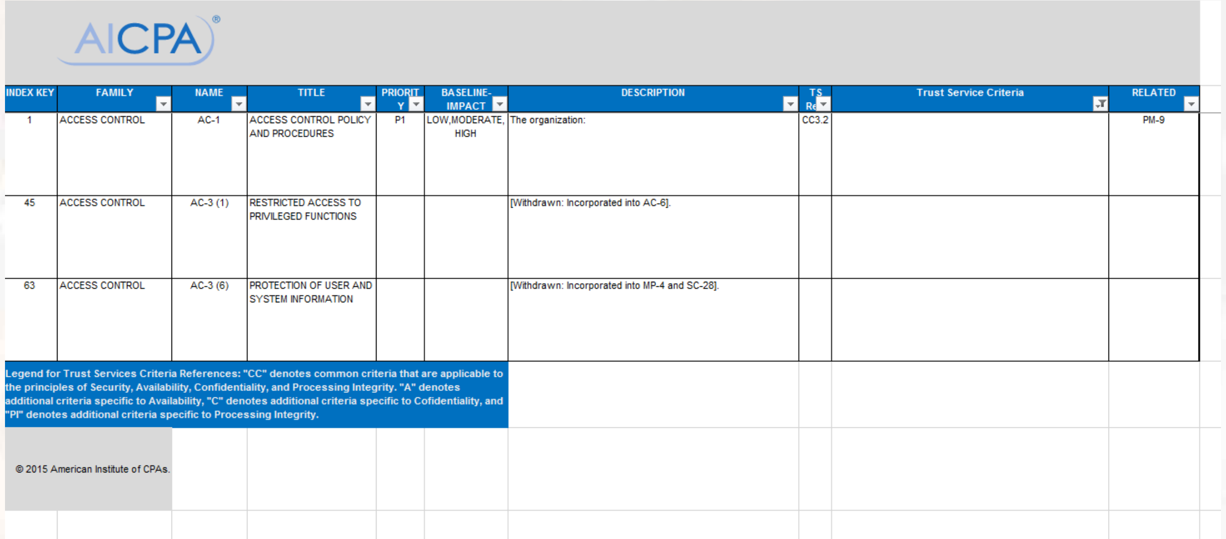
PCI DSS does not address the below listed examples:

- Inventory requirements are not as detailed
- Risk management processes are quarterly and semi-annual basis minimum standard
- Password length
- Required use of PIV/CAC products
- MFA multifactor authentication for network access to non-privileged accounts

New to the Party – What you do not know will hurt you

SOC Trust Services do not address the below listed examples:

- Access Control Policies related to AC-1
- Would require implementation of all Trust Services which is rarely the case
- Still need to be tailored to FedRAMP reporting and CONMON requirements



AICPA®

INDEX KEY	FAMILY	NAME	TITLE	PRIORIT Y	BASELINE-IMPACT	DESCRIPTION	TS Re	Trust Service Criteria	RELATED
1	ACCESS CONTROL	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	LOW,MODERATE, HIGH	The organization:	CC3.2		PM-9
45	ACCESS CONTROL	AC-3 (1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS			[Withdrawn: Incorporated into AC-6].			
63	ACCESS CONTROL	AC-3 (6)	PROTECTION OF USER AND SYSTEM INFORMATION			[Withdrawn: Incorporated into MP-4 and SC-28].			

Legend for Trust Services Criteria References: "CC" denotes common criteria that are applicable to the principles of Security, Availability, Confidentiality, and Processing Integrity. "A" denotes additional criteria specific to Availability, "C" denotes additional criteria specific to Cofidentiality, and "PI" denotes additional criteria specific to Processing Integrity.

© 2015 American Institute of CPAs.

New to the Party – What you do not know will hurt you

FedRAMP.gov Tips and Cues clearly identifies the critical knowledge and preparation that CSPs need to address; however many CSPs forget the following:

- Review and understand the FedRAMP SAF process
- Download the following templates from FedRAM.gov to get a true understanding of the level of effort, rigor and capabilities required:
  - System Security Plan
  - Test Cases
  - Security Assessment Plan
  - Security Assessment Report
  - Plan of Actions and Milestones
  - Continuous Monitoring Plan

Key Challenges to FedRAMP Ready

Key challenges to FedRAMP Ready

Administrative challenges:

- Development and/or updating existing policies and procedures to address and implement FedRAMP controls, processes and reporting requirements. Examples are -
  - All applicable NIST SP 800-53 rev 4 XX-1 controls (to include overlays if applicable)
  - Training (role based)
  - Incident Response and Continuity Plans
  - Risk Management Program, Plans and Processes

Key challenges to FedRAMP Ready

Technical and Operational challenges:

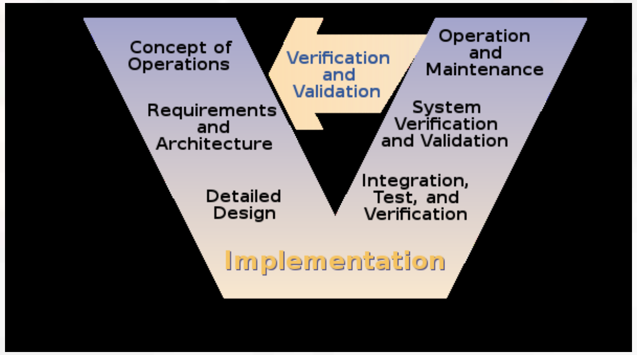
- Definition of the system and authorization boundary to include:

Clearly defines services wholly within the boundary.	Depicts all major components or groups within the boundary.	Identifies all interconnected systems.
Depicts all major software/virtual components (or groups of) within the boundary.	Is validated against the inventory.	All shared corporate services, with explicit rationale of any that are not within the boundary, such as a corporate Security Operations Center (SOC) or corporate security awareness training.
All other external services with explicit rationale of any that are not within the boundary that includes all leveraged services.	All systems related to, but excluded from the boundary.	Clearly identify anywhere Federal data is to be processed, stored, or transmitted.
Clearly delineate how data comes into and out of the system boundary.	Clearly identify data flows for privileged, non-privileged and customers access.	Depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed

- The needed rigor for vulnerability scans and penetration testing (at least 95% of the system inventory is also new).
- Automation of controls for High Impact systems

Smoothing out the Bumpy Road

- Using solid System Engineering and System Security Engineering practice will provide a clear roadmap to obtaining desired FedRAMP system authorizations.
  - Concept of operations (CONOPS) and Secure CONOPS
  - Clearly defined Requirements and Architecture
  - System Design
  - Testing
  - Documentation and configuration control through all above phases


Concept of Operations
Requirements and Architecture
Detailed Design
Implementation
Integration, Test, and Verification
System Verification and Validation
Operation and Maintenance
Verification and Validation

Smoothing out the Bumpy Road

Smoothing out the Bumpy Road

- Concept of operations (CONOPS) and Secure CONOPS
  - You know your Cloud Solution better than any outsider. How do you see this being adapted for use by the USG or its contractors? Let's look at SaaS as an example with a few general questions.
    - What CSP will you use as your IaaS and PaaS? Do they hold a current FedRAMP ATO? If not how will you be able to validate and verify their controls?
    - What type of data do you see being processed? What is the impact level of these data?
    - How many USG customers will be using this SaaS offering (Multi-tenant verses single tenant)?

Smoothing out the Bumpy Road

- Clearly defined Requirements and Architecture

  - Security Requirements (examples to be considered)
    - What is the impact level of the data and applicable regulations?
    - Based on the CONOPS and Operational Threat Analysis, what are the real-world threats and risks?
    - Based on the user base, what type of access is required and are the processes performed by these users?

  - Architecting
    - Based on impact level and regulatory considerations, where and how will USG data be stored, processed and transmitted?
    - Does the architecture support all defined requirements? Are there alternative implementations that can meet these requirements?

Smoothing out the Bumpy Road

- Design considerations need to go beyond just functionally meeting the requirements:
  - Do security mechanisms have needed robustness and utility to meet USG requirements?
  - Does the design foster consistency in deployment of services (repeatable and reliable – Gauge R&R) through well defined and configuration controlled images and role based provisioning mechanisms.

Smoothing out the Bumpy Road

- Testing needs to thoroughly address defined requirements and align with targeted USG customer base data and business operational needs.

  - For technical and operational controls – Do we clearly define specific tests that enable your solution to provide reliable artifacts needed not only during the initial FedRAMP authorization effort, but feed future annual assessment and CONMON activities

  - Do we enable feedback from test results and any gaps noted to update Administrative controls (Plans, Policies, Procedures, Standards, etc.)

Smoothing out the Bumpy Road

- Documentation and configuration control through all phases ensures the following:

    - Consistency in administrative, operational and technical control design, development, integration, testing and on-going operations.

    - Solid foundation for the SSP and CONMON.

    - CSP’s capabilities to streamline required FedRAMP processes and support multi-tenant requirements.

Smoothing out the Bumpy Road

Regardless of which FedRAMP approach being pursued CSPs need to also look at the body of knowledge, guidance and tip and cues on the FedRAMP.gov site.

- The best starting point is to download the appropriate FedRAMP documentation:
  - Review the Readiness Assessment Report with your internal team to identify areas of understanding, gaps and areas requiring greater clarification
  - Review the following to help establish level of complexity and effort, technology and skills needed.
    - FedRAMP Initial Authorization Package Checklist
    - Test Cases
    - SSP
    - SAP
    - SAR
    - CONMON

Summary

- CSPs can realize significant business opportunities through successful FedRAMP authorization

- While existing commercial/non-federal security frameworks and accreditation/attestations are useful starting points, there will be administrative, operational and technical gaps to address

- Application of sound system and system security engineering practices

- Being fully informed as to the nature, requirements and on-going commitment to FedRAMP will better enable CSPs to successfully pursue and achieve the desired FedRAMP system authorization.

Questions?

Thank You

Jeff Roth
jeff.roth@nccgroup.trust
321-795-0391