FEDRAMP TIPS & CUES COMPILATION

2015 - 2017

January 2018

FedRAMP

Hello Everyone!

The FedRAMP PMO began publishing our weekly “Tips and Cues” as a way to address common concerns and issues being raised by Federal Agencies, Cloud Service Providers (CSPs), and Third Party Assessment Organizations (3PAOs).

We have received a lot of positive feedback about these posts. In order to make them even more accessible to our readers, we’ve compiled every tip we’ve published into a single document.

We hope you find this compilation helpful. If you’d like to sign up to receive our weekly Tips and Cues, please use this link.

Thanks and all the best,

Matt Goodrich

FedRAMP Director

TABLE OF CONTENTS

KEY

Cloud Service Provider (CSP) Tip

Federal Agency Tip

Their Party Assessment Organization (3PAO) Tip

I. CONTINUOUS MONITORING

TIP: CSPs must address every vulnerability they submit as part of their continuous monitoring data. There are a few different options for managing those vulnerabilities.

1. Remediate the finding within the required timeframe. This should be the default approach to vulnerability management.
2. As part of the Deviation Request process:
   a. Implement mitigations and request a risk adjustment, if appropriate.
   b. Seek approval for any False Positive (FP) findings. Be sure to provide evidence that proves the finding was an FP. An FP would not be appropriate in instances where the system setting is not active and, therefore, not vulnerable, but if it were active, the vulnerability would exist. This type of finding should be submitted as a Risk Adjustment with layers of mitigations that prevent exposure if the system setting is activated.
   c. Seek approval as an Operational Requirement (OR). OR requests should be infrequent since it means the vulnerability remains in production until it is eventually remediated. High findings must be mitigated and Risk Adjusted to at least Moderate for acceptance as an OR.
3. Justify the finding as a Vendor Dependency and check in with the vendor every 30 days. In this case, the vulnerability will not be considered late. The CSP should seek vendor components that are FedRAMP compliant when possible to avoid any Vendor Dependencies. In this case, the vulnerability will not be considered late.

TIP: Select your monthly continuous monitoring scan and Plan of Action & Milestones (POA&M) delivery date wisely.

Consider vendor patch release schedules and your typical duration between the release of a vendor patch and its application within your environment. Plan your scans as soon as possible after patches are typically applied each month. If your monthly scans are out-of-sync with your patch cycle, the number of vulnerabilities reported can be artificially inflated.

For example, if you have Microsoft-based hosts and a two-week patch cycle, running scans just one week after "patch Tuesday" will report all of the newly released patches as new vulnerabilities on those hosts and inflate your vulnerability count. Scanning shortly after your patch cycle gives your admins time to remediate all of those new vulnerabilities. Therefore, only the exceptions – if any – are reported.

Q: The effort and/or costs are too great to remediate a vulnerability within the required time period. Is it acceptable to submit a risk adjustment in this situation?

A: Generally, level of effort and/or cost of implementing a remediation are not acceptable justifications for leaving a system that is authorized for processing federal data in a vulnerable state. During the initial assessment of the system, the CSP is assessed to determine its ability to perform continuous monitoring successfully, which includes timely remediation of vulnerabilities. This also includes an assessment of the CSP's equipment acquisition and life-cycle management plan to ensure vendor products can be maintained and/or replaced to stay on top of security. This means the CSP should be aware of equipment end-of-life/end-of-support.

In the rare event that timely remediations need to be postponed, it is incumbent upon the CSP to employ mitigations that reduce the risk of the vulnerability. This risk mitigation and adjustment should be described in detail in the Deviation Request, and a plan for ultimate remediation and compliance should be included.

Q: How are "false positive" scan results managed?

A: A False Positive (FP) scan result is noted when an identified vulnerability does not actually exist on the system. For instance, a vulnerability scanner might identify a weakness for a component that is not installed or fail to recognize a recent system update. As long as evidence is offered to support the non-existence of the component and/or the existence of the system update install, this is now noted as a "FP". For the Security Assessment Report (SAR), the FPs are noted in a False Positive Report for the Infrastructure, Databases, Web Applications, and "Other" miscellaneous (automated and manual) tool results. The FPs are recorded on the "Open" Plan of Actions and Milestones (POA&M) tab of the POA&M workbook until the Security Assessment Package is signed off and accepted by the Joint Authorization Board (JAB). Once the package is accepted, these FPs are validated and verified through the Provisional Authorization to Operate process, and moved to the "Closed" POA&M tab.

From that point forward, all FPs identified through the Continuous Monitoring process are recorded as Deviation Requests embedded with all supporting evidence, and noted on the Open POA&M tab. Once the Deviation Request is accepted by the JAB Technical Review Reviewers, the FP can be moved to the Closed POA&M tab.

Q: What are the Continuous Monitoring (ConMon) roles and responsibilities associated with the FedRAMP Program Management Office (PMO) for a FedRAMP Agency Authorization? Is there a FedRAMP PMO ISSO assigned to each FedRAMP Agency Authorization?

A: ConMon is a critical component in understanding evolving risks associated with an IT system. CSPs are required to follow stringent ConMon requirements and provide Agencies with the information they need on a periodic basis, to ensure their data remains secure to include, but not limited to: monthly Plan of Action and Milestones (POA&M), monthly database, operating system, and web application raw scan files, ad-hoc (as appropriate) incident response notifications, major system change requests, and annual assessments. These deliverables are required, regardless of authorization type (JAB or Agency) and are located within the FedRAMP Secure Repository on OMB MAX.

Each Agency should review these materials, regularly, to ensure their ATO remains valid and the risk remains acceptable. The FedRAMP PMO does not have a dedicated ISSO that supports each Agency Authorization; but, provides the structure and access to each CSPs' ConMon materials in OMB MAX. As always, if any Agency has questions regarding specific ConMon vulnerabilities or is unable to obtain the information they need pertaining to ConMon for any given CSP, the FedRAMP PMO is here to help.

Q: What scanning depth does FedRAMP require?

A: FedRAMP requires full-range authenticated scans with all plugins enabled. This requirement pertains to all network, operating system, database, and web application scans, using the type-specific scanning toolset, which must be conducted at least monthly. Each scan must include all components within the system boundary and as agreed within the most current Security Assessment Plan. Detailed requirements are provided in the FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide and the Continuous Monitoring Strategy Guide, both located in the "Documents" section of www.fedramp.gov.

CSPs and 3PAOs should plan for, and configure, scans that meet FedRAMP requirements from the outset. Doing so helps to avoid the need to rescan and resubmit results, which can lead to schedule delays and additional costs.

Q: Why does FedRAMP require authenticated scans, and how do they differ from unauthenticated scans?

A: Unauthenticated scans provide a perimeter view of the system, typically including open network ports, services, operating systems, and data leaks. In contrast, authenticated scans utilize credentials to detect internal vulnerabilities that could provide an intruder that penetrated the perimeter with privileged access to the system. Scanning monthly with authentication is a FedRAMP requirement because it identifies and prompts the cloud service provider to fix these internal targets.

Q: What is the relationship between continuous monitoring and continuous diagnostics & mitigation (CDM) and ongoing authorization?

A: The FedRAMP and CDM monitoring requirements are both based on NIST Special Publication 800-137 guidance for implementing an Information Security Continuous Monitoring program. The CDM program has initially focused on providing tools to Federal Agencies to ensure that they can fulfill vulnerability management, malware detection, asset management, and configuration management program responsibilities and aggregate data from those tools into a central console or dashboard to facilitate a more robust awareness of one's risk posture. Agencies would also provide aggregate output from this dashboard to DHS to facilitate a government-wide view of vulnerabilities and associated risks. FedRAMP security controls also require that these elements (vulnerability management, malware detection, asset management, and configuration management) be in place at the CSP to support visibility into the operational status of a system, much like the CDM program. However, FedRAMP does not prescribe the exact tools and dashboards nor does it require real-time or near real-time uploading of all tool output to FedRAMP.

There is no planned integration of CDM and FedRAMP continuous monitoring at this time as CDM is focused on government assets and not external providers. FedRAMP is interested in evolving its continuous monitoring program to facilitate a shift from a compliance-based to a more risk-based approach and is preparing to solicit feedback from Agencies and industry.

2. CONTROLS

Q: What is an example of a commonly overlooked or insufficiently answered control?

A: FedRAMP documentation writers tend to overlook "Implementing Configuration Settings (CM-6)." This is a significant control because it is (1) required and (2) because writers typically use it as an umbrella to map failures.

When writing this control, be sure to follow these steps:

1. Include in your answer all system components that must be configured within the system boundary.
2. Explain where the system configuration documentation is located.
3. Identify all the system components that are to be configured.
4. Identify, for each component, who is responsible for configuring the component.
5. Identify how the responsible party configures each component in detail.
6. Identify and address any special FedRAMP requirements included in the configuration process in detail.

7. Explain how configuration setting deviations are identified, documented, and approved.
8. Explain how the organization monitors and controls changes to the configuration settings. Explain how this process is in accordance with organizational policies and procedures.

Q: What are common missed or neglected FedRAMP and/or National Institute of Standards and Technology (NIST) requirements?

A: The PMO is unable to evaluate authorization packages that do not completely respond to FedRAMP and/or National Institute of Standards and Technology (NIST) requirements. Although not a complete listing, the following items highlight some common incomplete requirements:

- Not identifying portals
- Non-compliance with multi-factor authentication
- Tenant separation for multiple customers (government vs. public) does not exist
- High vulnerabilities detected during P-ATO testing
- Authorization boundary is not clearly defined
- Policies and procedures that do not exist, incomplete, or not well defined
- Not having FIPS-140 enabled

Q: How do I indicate "sole," "shared," or "customer" responsibilities when answering the Awareness and Training (AT) controls?

A: When answering Awareness and Training (AT) controls, it is mutually beneficial for both the CSP and the Agency to share that responsibility in providing awareness and training (e.g., Mandatory Security Awareness Training, specific systems level training and guidance). The SSP implementation should be checked as a shared control responsibility between the CSP and the Agency in addition to any boxes.

It is good practice to have Security Awareness Training incorporated and a shared responsibility as opposed to simply responding to the implementation as solely a "corporate" or "customer responsibility."

Q: My system uses various platforms and operating systems, so how do I relate technical control implementation statements?

A: The security control implementation statements for technical controls (AC, AU, IA, SC, etc.) must be developed to include all of the applicable platforms/operating systems (e.g., Windows, Linux, Solaris, VMware) that comprise the cloud service architecture.

It is critical for reviewers (either Joint Authorization Board (JAB) or Agency) to delineate each platform/operating system against the applicable security control requirement to ensure compliance is adequately being met.

Q: When is the FIPS 140 compliant/validated cryptography applicable?

A: For data flows crossing the authorization boundary or anywhere else encryption is required, FIPS 140 compliant/validated cryptography must be employed. FIPS 140 compliant/validated products will have certificate numbers. These certificate numbers will be required to be identified in the SSP as a demonstration of this capability. JAB TRs will not authorize a cloud service that does not have this capability.

Q: If a Software-as-a-Service (SaaS) is built on a previously authorized Infrastructure-as-a-Service (IaaS), does the IaaS's authorization boundary cover the SaaS as well? If it does, is an Authority to Operate (ATO) letter necessary for the SaaS?

A: The IaaS's authorization boundary does not completely cover the SaaS. All pieces of the cloud stack have to be authorized — which means the IaaS has its own authorization boundary (what it is responsible for), and the SaaS has its own authorization boundary. However, your SaaS can inherit some of the security controls from the IaaS, depending on the services used from the IaaS.

Each portion of the cloud stack requires its own ATO letter, so the SaaS will need an ATO separate from the IaaS.

3. FEDERAL AGENCY

Q: How do security controls impact Quality of Service (QoS) of an application or system?

A: Quality of Service (QoS) and security are interrelated. The implementation of security controls must be thoughtfully considered and deployed/implemented so as to NOT adversely impact an application's or system's QoS. This is important because improperly thought-out or excessive security controls can impact QoS. The CSP must plan the "right" amount of security as it pertains to the system performance and financial considerations.

Q: Do the FedRAMP security controls restrict data to reside only within the United States?

A: There are no FedRAMP requirements restricting data to within the United States. There are multiple security controls that detail where data is stored, what the boundary of the system is, and where and how data in transit is protected. We have some providers that are authorized through FedRAMP that are located globally, although a majority of service providers do restrict their data to the United States. It is up to each individual Agency and authorizing official to place restrictions, if needed, on data location.

Q: Can a Federal Agency require CSPs to be FedRAMP authorized in a request for proposal (RFP)?

A: Federal Agencies cannot require CSPs to be FedRAMP authorized as part of their RFP but can state that a CSP needs to be FedRAMP authorized once federal data is placed in the system. For more information on contract clauses, please review the FedRAMP Standard Contractual Clauses.

Q: How does a Federal Agency access JAB approved and Agency Authorized packages in the OMB MAX Secure Repository?

A: To access a CSP's P-ATO and/or Agency ATO security package documentation, Federal Agency employees or contractors must complete a Package Access Request form available at www.FedRAMP.gov and submit the completed form to info@fedramp.gov. The PMO will then review, validate, and grant access within 72 hours if all required fields are populated in the form.

Q: Do Federal Agencies need an Interconnection Security Agreement (ISA) with a CSP?

A: Interconnection Security Agreements (ISAs) are not designed for use between a CSP and an Agency. An Agency ATO memo should be the governing document for Agency and CSP interaction and security requirement communications. CSPs should document security protections in place for Agency access – whether through dedicated connections or publicly routable internet space. This documentation should be included within the standard FedRAMP-required templates, policies, and procedures.

Agencies should follow the documented processes for issuing ATOs included in the FedRAMP guidance and documentation available on FedRAMP.gov.

CSPs should also continue to utilize ISAs for cloud system interconnections that fall within the scope of the cloud boundary. These ISAs will be reviewed as part of the security assessment and testing process by 3PAOs and testing for control CA-3. The FedRAMP Agency or JAB P-ATO process should be the mechanism for validating ISA documentation.

Q: How can an Agency ensure it maintains reasonable investigation capabilities, auditability, and traceability of data within the cloud?

A: Agencies can ensure they maintain reasonable investigation capabilities, auditability, and traceability of data by logging and monitoring the following application events:

- Management of network connections
- Addition or removal of users
- Management of changes to privileges
- Assignment of users to tokens
- Addition or removal of tokens
- Management of system administrative privileges access
- Actions by users with administrative privileges
- Use of data encrypting keys
- Management of key changes
- Creation and removal of system level objects
- Import and export of data, including screen-based reports
- Submission of user-generated content, especially file uploads

Q: Would a cloud service require a FedRAMP authorization if it already has a FISMA ATO? If so, can you reference the specific language in the requirement?

A: While FISMA and FedRAMP authorizations are similar, FedRAMP authorizations involve extra requirements and parameters specified in the FedRAMP templates/baseline requirements documentation, available on fedramp.gov. Agencies that are using a cloud system or services must follow FedRAMP requirements and go through the FedRAMP Authorization process. The driving policy for FedRAMP is a policy memo released by OMB.

The initial cloud system/service authorization package (to include the ATO, for Agency-authorized systems) must be reviewed and approved by the FedRAMP PMO to receive a FedRAMP Authorization.

Q: Who is my FedRAMP approver to sign off on an access request form?

A: Your FedRAMP approver is either your Agency's CISO or DAA. If the form is signed by a DAA, that person must be at a level that has the authority to grant an ATO for a system.

Q: Can an Agency share complete Authorization to Operate (ATO) package materials with another Agency?

A: Yes, Agencies can share complete ATO package material with other Federal Agencies. But it is recommended that Agencies receive this information directly from the FedRAMP PMO, as it ensures documentation is validated against FedRAMP standards.

Q: I received a request from a Federal Agency to review my system's Provisional Authorization to Operate (P-ATO) letter and I am concerned that sharing the letter will violate sensitivity policies. Is it appropriate to share an authorization letter with Agencies?

A: Yes! The Authorization Letter is intended to serve as evidence that the CSP has obtained their FedRAMP P-ATO. The CSP may show or even provide a copy to a requesting Agency. Indeed, the Agency may need a copy for their own ATO package as evidence they selected a CSP with a valid FedRAMP P-ATO.

Q: If an Agency wants to leverage another Agency's FedRAMP authorization, but recognizes the existence of risk that the potential leveraging Agency is unwilling to accept, is there an option to work with the Cloud Service Provider (CSP) to resolve these risks prior to authorization?

A: If an Agency is already using a CSP and has not yet issued an authorization to use that cloud service within their operating environment, the Agency can leverage an existing Agency Authorization as it applies within their operating environment. If a leveraging Agency is unwilling to accept risks associated with the existing Agency authorization, the Agency should work with the providing Agency to determine how to remediate and mitigate the amount of risk associated with the leveraged Agency package so that the risk can be managed to an acceptable level within their own Agency environment. The CSP has the opportunity to remediate vulnerabilities at any time. An Agency can engage with the CSP to resolve issues that the Agency is unwilling to accept.

For more information, please visit the Office of Management and Budget (OMB) A-130 Revised, dated July 28, 2016, Appendix I - 22, (OMB Circular A-130, "Managing Federal Information as a Strategic Resource" (7/28/2016 - 85 pages)) section j. Joint and Leveraged Authorizations on page 59.

Q: If an Agency leverages an Agency authorized security package to meet their FISMA authorization requirements, how does the Continuous Monitoring then come into play?

A: Each Agency is responsible for meeting their organizational responsibilities for FISMA and Continuous Monitoring in monitoring, evaluating, and reporting the risk posture monthly for the Agency information systems.

According to OMB A-130 Appendix I-23, section k. Continuous Monitoring:

> *"Agencies must develop information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and implement ISCM and PCM activities in accordance with applicable statutes, directives, policies, instructions, regulations, standards, and guidelines. Agencies have the flexibility to develop an overarching ISCM and PCM strategy (e.g., at the Agency, bureau, or component level) that addresses all information systems, or continuous monitoring strategies that address each Agency information system individually. The ISCM and PCM strategies must document all available security and privacy controls selected and implemented by Agencies, including the frequency of and degree of rigor associated with the monitoring process. ISCM and PCM strategies, which must be approved by the appropriate Agency Authorizing Official and the Senior Agency Official for Privacy, respectively, must also include all common controls inherited by Agency information systems."*

TIP: While Agency use of accredited 3PAOs is not mandatory, it is recommended. Below is the guidance provided in the FedRAMP Security Assessment Framework.

1.6.8. THIRD-PARTY ASSESSMENT ORGANIZATIONS

> *"3PAOs play a critical role in the FedRAMP security assessment process, as they are the independent assessment organizations that verify cloud providers' security implementations and provide the overall risk posture of a cloud environment for a security authorization decision. These assessment organizations must demonstrate independence and the technical competence required to test security implementations and collect representative evidence. 3PAOs must:*
>
> - *Plan and perform security assessments of CSP systems*
> - *Review security package artifacts in accordance with FedRAMP requirements*
>
> *The Security Assessment Report (SAR) created by the 3PAO is a key deliverable for leveraging Agencies to use FedRAMP security assessment packages. The FedRAMP JAB requires that a 3PAO be accredited through the FedRAMP 3PAO Program for any JAB P-ATOs. Agencies are highly encouraged to use these organizations for Agency authorizations that meet the FedRAMP requirements. While Agencies are free to use non-3PAO Independent Assessors (IA), use of a 3PAO assessor removes the Agency requirement to provide an attestation to the independence and competency of the security control assessor."*

AND

2.1.2. FEDRAMP AGENCY ATO

> *"CSPs may work directly with an Agency to obtain a FedRAMP Agency ATO. In this case, the Federal Agency will provide the risk review of all documentation provided by the CSP in its security authorization package. CSPs will work directly with the Federal Agency security office and present all documentation to the Authorizing Official (AO) or equivalent for an authorization. As noted in Section 1.6.8, Federal Agencies may elect to use a FedRAMP accredited 3PAO or a non-accredited IA to perform the independent assessment. If a non-accredited assessor is used, the Agency must provide evidence of the assessor's independence and provide a letter of attestation of the assessor's independence with the security authorization package. The FedRAMP PMO highly recommends Agencies select an assessor from the FedRAMP 3PAO accreditation program.*
>
> *Once an Agency authorizes a package, the Agency must inform the FedRAMP PMO by sending an email to info@FedRAMP.gov. The PMO then instructs the CSP how to submit the package for PMO review. After reviewing the package to ensure it meets all of the FedRAMP requirements, the FedRAMP PMO will publish the package in the Secure Repository for other Agencies to leverage."*

TIP: The current OMB A-130 clarifies specific Agency Authorization responsibilities for protecting and managing Federal information resources. Here are some ways OMB A-130 further refines Agency interaction with FedRAMP.

Office of Management and Budget (OMB) Circular A-130 revised 7/28/2016 now explicitly outlines Agency responsibilities for their information and information systems and links their information security program to OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Controls. OMB Circular A-130 Appendix I incorporates requirements of the Federal Information Security Management Act (FISMA) (44 U.S.C. Chapter 35), the E-Government Act of 2002 (44 U.S.C. Chapters 35 and 36), the Paperwork Reduction Act (44 U.S.C. Chapter 35), and the Privacy Act of 1974, and responsibilities assigned in Executive Orders and Presidential Directives.

Agencies are responsible for:

- Ensuring all new Cloud Service Provider (CSP) Cloud Service Offering (CSO) projects minimally use the FedRAMP baseline controls and templates for Low, Moderate, and High baseline systems.
- Ensuring existing cloud projects (implemented or in the acquisition process) meet FedRAMP requirements.
- Adding or modifying contractual provisions that require CSPs and the associated CSO projects meet FedRAMP requirements.
- Updating OMB PortfolioStat data quarterly to identify use of CSPs and Agency plans to meet FedRAMP requirements and provide Agency-specific rationale to support lack of compliance.
- Issuing the initial Agency Authorization.
- Reviewing CSP documentation and test results prior to leveraging a Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) or leveraging the Agency-issued Authorization to Operate (Agency ATO).
- Reviewing Plans of Action and Milestones (POA&Ms) for leveraged CSP CSOs.
- Adding any Agency-specific controls that may exist above the FedRAMP baseline or above the baseline required by a partnering Agency.
- Ensuring the submittal of Agency ATO security packages.
- Reviewing all CSP and 3PAO-provided documentation for the ATO and Continuous Monitoring, as appropriate.

TIP: Use the FedRAMP Package Access Request Form on the FedRAMP website to review a FedRAMP Security Package.

The FedRAMP Package Access Request Form is the form completed by federal employees and government contractors who desire access to view a CSP's security authorization package to determine suitability of the service for use within their individual Agency/organization.

Applicants must be sure to complete every section of the form and make sure to fill in the boxes with initials, as appropriate. Do not use check marks or "X's" in the areas that require initials. The Agency Access Request Form including Attachment A: Federal Contractor Non-Disclosure Agreement for FedRAMP is on the website, under FedRAMP Authorized Products.

Be sure to fill out the FedRAMP Approver sections located at the bottom of Page 1 under “Access Authorization” and page 3 “Agreement for Authorized FedRAMP Approver (CISO; DAA)”, in its entirety. These Approver Sections are often left blank resulting in the PMO sending the forms back to the applicant. This results in delays for the applicant being able to view the packages.

4. GENERAL PROGRAM

Q: Does the “FedRAMP Ready” designation allow CSPs to bid on contracts without having an existing ATO? If not, how will a CSP that does not have a current ATO respond to a RFP? Will the CSP be required to obtain a JAB P-ATO?

A: CSPs without existing ATOs are allowed to bid on contracts. Agencies can request a CSP to have a timeline for obtaining an ATO but should not limit the request to CSPs with ATOs. Please contact the FedRAMP PMO if an Agency is doing such an action.

The “FedRAMP Ready” designation is a market indicator to Agencies that a system has a high likelihood of obtaining a JAB P-ATO or an Agency ATO. Agencies can be confident that systems that meet the FedRAMP Ready requirements actually have the key capabilities needed to fit their security needs. Therefore, a small cloud service provider will have the ability to attain FedRAMP Ready and be available for Agency review in the FedRAMP Marketplace. The Agency can then decide to issue an ATO based on the understanding that the system meets the Readiness Assessment requirements.

Q: Will the same 3PAO be able to perform both the FedRAMP Readiness Assessment and the complete security assessment during a JAB P-ATO process?

A: The same 3PAO can perform both the Readiness Assessment and complete the security assessment for the ATO process without conflict of interest, provided that the 3PAO does NOT provide any consulting duties for the same authorization package. So, a 3PAO can help write the SSP, SAP, SAR, and POA&M but cannot do any of the testing. It is fairly similar to the current ATO process where different 3PAOs do the consulting and testing for a CSP’s authorization package.

Q: What is a major difference between a true cloud service provider (CSP) and a managed service provider (MSP)?

A: The difference between a MSP and a CSP is the delivery of the service.

A MSP provides a service that is specific to an individual customer. The customer dictates both the technology and the operational procedures. That service is governed by a strict Service Level Agreement (SLA) between the individual and the MSP and is limited to the agreement between the customer and the MSP.

A CSP offers the technology and the operational procedures on a subscription basis. If the customer does not accept the technology and the operational procedures, then the customer can shop elsewhere. The CSP provides a full environment that encompasses datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity). This environment is secured, monitored, maintained, and tested for continual effectiveness at planned intervals. This ensures protection from unauthorized interception or damage and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.

Q: How can I ensure I’ve submitted all of the documents required for FedRAMP authorization?

A: The FedRAMP Documentation Checklist (found on FedRAMP.gov) includes a list of the required authorization package documents that must be submitted for review to achieve FedRAMP Authorization. The Checklist specifies the correct format (e.g. Word, or Excel, etc.) that the documentation must be submitted in, as well as if the CSP must use a FedRAMP-provided template for the document. Not only is the Checklist a useful tool for the CSP to help ensure the correct documentation is uploaded, but it is also required to be completed and included with the uploaded material. This is important since it includes fields for each document's file name, date, and version number, so that the FedRAMP Reviewer knows that each uploaded document is the intended version, and not an older draft. Completing and submitting the Checklist with the package helps to enable an efficient review of the authorization package.

Q: If a CSP wants to complete a FedRAMP Readiness Review, but is then going to pursue an Agency-sponsored FedRAMP authorization, can the CSP use the same 3PAO for both assessments?

A: A CSP can use the same 3PAO for completing their Readiness Assessment Report (RAR) and their full security assessment when working with an Agency or the JAB. The same 3PAO, however, cannot consult between assessments – this is outlined in the ISO 17020 requirements and FedRAMP-A2LA 3PAO accreditation requirements.

Additionally, to help ensure successful completion of the RAR, the FedRAMP PMO has created a FedRAMP RAR Guide for 3PAOs that includes useful tips and lessons learned.

Q: What does FedRAMP Ready status mean? Is it a requirement for CSPs who would like to pursue an Agency authorization?

A: FedRAMP Ready is a designation intended to demonstrate a CSP's ability to complete the full FedRAMP Authorization process. It is a mandatory step in pursuing a JAB Provisional Authorization to Operate (P-ATO) and is optional for those pursuing an Agency-based FedRAMP Authorization. Although it is optional for Agencies, some Agencies may prefer to work with CSPs that are "FedRAMP Ready" since it offers key insight into their capabilities and ability to achieve an authorization.

The FedRAMP Authorization process is rigorous and intensive. It involves a lot of hard work and effort, so it makes sense that a CSP would want some assurance that their cloud offering is likely to attain authorization. This is why reaching "FedRAMP Ready" is an important first step in the FedRAMP process.

Q: Could you explain the purpose and process behind requiring a CSP to complete an incident response test and contingency plan test before their 3PAO assessment?

A: If a CSP does not complete an incident response test and contingency plan test before the 3PAO assessment, the Joint Authorization Board (JAB) will not issue the cloud offering a Provisional Authorization to Operate (P-ATO). These tests must be conducted in accordance with NIST SP 800-53, and the results should be made available to the 3PAO for evaluation. Once a P-ATO is granted, the tests should continue to be completed prior to the annual assessment so that the 3PAO can evaluate the results as part of that assessment.

Q: I am developing a cloud system but want to make sure it is FedRAMP compliant before producing it and making it operational. Will FedRAMP evaluate a cloud system (even for FedRAMP Ready) that is not in production and operational?

A: No. FedRAMP only evaluates documentation for systems that exist and are operational. FedRAMP works with CSPs to provide Agencies with secure cloud computing options, so it is required that CSPs have an operational cloud system before engaging with the FedRAMP Team. CSPs can use the FedRAMP Readiness Assessment Report (RAR) as a self-assessment to understand if there are any gaps in their service offering's security prior to pursuing an Authority to Operate (ATO) with an Agency. The Readiness Assessment Report Template for High and Moderate systems can be found on the Templates page of fedramp.gov.

TIP: Your FedRAMP Information System Security Officer (ISSO) or government liaison is here to help guide you through the FedRAMP process. Communication is imperative to get through the FedRAMP process! The better communication you have, the smoother the process will go.

If you have any questions or concerns, or just want to brainstorm ideas, your FedRAMP point-of-contact can share potential impacts of any proposal you have. If you're not sure a control implementation should be "Not Applicable" or an "Alternative Implementation," your ISSO can help! And if you're unclear on how to describe your PIV/CAC implementation, your government liaison can point you in the right direction!

Q: I keep receiving commentary from the JAB on documents in my authorization package and this has extended my review time. What can I do to lessen the amount of comments my authorization package receives?

A: When preparing documentation for final submission to the JAB Technical Representatives, one must remember that the document is telling a story about the effort. If there are gaps in the storyline, there will be comments to address the gaps. The more gaps in the storyline, the more numerous the comments will be created to try to fill in the gaps – which will in turn slow down your review time. The author should frame each answer in a way that the reader can follow the complete thread from the beginning to the end. The author must never assume that the reader already knows "details" about the story without identifying the detail's location in the document. For instance, when providing the Penetration Testing Report, the 3PAO should provide the full name and versions of the tools used, why these were chosen, and then what the outcome was from the testing. These questions are basic to information gathering and reporting. For each section within the documentation, each of these questions must have a factual, detailed answer for the story to be complete.

Q: Why should CSPs spend time and money developing high quality documentation when their goal is to become FedRAMP Authorized?

A: FedRAMP requires quality documentation (i.e., documentation that is clear, concise, consistent, and complete) to provide a clear and complete description of the risk posture of a cloud system. This, in turn, reduces an Agency's level of effort to reuse an Authorization Package. Quality documentation also pays for itself by minimizing costly rework and time-consuming delays caused by clarifying misunderstandings and waiting for missing documentation.

FedRAMP requires CSPs to spend as much time writing and editing the documentation as they do engineering the security.

Q: Is there an OMB memo or any other guidance that states when (or if) there is a "drop dead" date for Federal IT systems to be in the cloud?

A: According to the initial Cloud First Strategy, dated 2010, the Federal Government should have been moved to the cloud within 18 months, so this would be approximately June 9, 2012. However, since the effort to move all Agencies to the cloud was more complex than initially anticipated, the Cloud First Strategy was updated on February 8, 2011 and states:

"Our responsibility in government is to achieve the significant cost, agility and innovation benefits of cloud computing as quickly as possible. The strategy and actions described in this paper are the means for us to get started immediately. Given that each Agency has unique mission needs, security requirements, and IT landscape, we ask that each Agency think through the attached strategy as a next step. Each Agency will evaluate its technology sourcing strategy so that cloud computing options are fully considered, consistent with the Cloud First policy."

Therefore, it is the responsibility of each individual Agency to define its Cloud First Strategy.

Q: What is important to consider for CSPs leveraging other services?

A: It is a very common practice for a SaaS CSP to use some of the services available from an underlying infrastructure (IaaS/PaaS) that the SaaS is hosted on. This is called leveraging. However, buyer beware – some services that an IaaS/PaaS CSP may offer, may not be FedRAMP authorized. Only FedRAMP authorized services may be used by government customers.

If your service offering is leveraging another system, the system you are leveraging itself must be FedRAMP Authorized by having a FedRAMP P-ATO or an Agency ATO. This includes sub-services. For example, a large CSP may have a commercial service offering and a separate service offering with a FedRAMP Authorization. That CSP may offer multiple sub-services – some of which may be included in the FedRAMP-authorized service's authorization boundary, while other sub-services are not. Only service offerings with a FedRAMP Authorization may be leveraged for use by government customers. Please validate that services are FedRAMP authorized and any associated sub-services are within the authorization boundary of a FedRAMP-authorized service before leveraging them for use by your government customers.

Note: This is a mandatory requirement for achieving FedRAMP Ready status under the Readiness Assessment process. 3PAOs are required to validate the FedRAMP authorization of all leveraged services and sub-services.

Q: What happens if a SaaS is hosted at a non-FedRAMP IaaS and on a non-FedRAMP PaaS?

A: When a CSP has its system/service hosted in a non-FedRAMP Authorized cloud service (e.g., IaaS, PaaS) there is no "leveraging/inheritance" relationship. In this situation, the SaaS provider needs to include the infrastructure and platform, as well as its own software application within its authorization boundary. This means that the CSP is responsible for the entire stack. Hence, the CSP is not "leveraging or inheriting " any security controls from an IaaS/PaaS authorization. In order for a SaaS to receive FedRAMP approval, the underlying stack pieces (IaaS/PaaS) must be considered and defined in the system security plan.

Q: I need to develop a Configuration Management Plan (CMP); can you please direct me to some guidance or a template for CMPs?

A: Security Control CM-9 requires CSPs to develop a Configuration Management Plan (CMP) and that Plan is a required document within their security authorization packages. FedRAMP does not provide a template for CMPs however NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, provides a wealth of information about configuration management and also provides a sample outline for a CMP in its Appendix D: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-128.pdf.

TIP: Security control implementations can only be inherited (leveraged) from a Cloud Service Offering (CSO) that has been approved and granted a FedRAMP Provisional Authorization to Operate (P-ATO) or an Agency ATO.

It is very important to clearly identify what controls or sections of controls are inherited. Similar to the Customer Responsibility Requirements, the control writer must identify what sections of the control are inherited from the leveraged Cloud Service Offering or other entity.

The FedRAMP SSP templates all have a section for each control, labeled, "Control Origination". Within this section is the area for the checkbox named, "Inherited from pre-existing FedRAMP Authorization for Click here to enter text., Date of Authorization".

The SSP writer should clearly indicate what sections of the security control are inherited and provide a description of what is inherited. If an entire control is inherited, it must be clear to the Assessor what is inherited. The writer does not need to describe how the leveraged service is performing the particular function. That detail is found in the SSP of the leveraged system from which the control is inherited.

If a policy has been published and is referenced as is the basis for the implementation of the inherited security control, make sure that published document is provided as an attachment, or a supporting artifact with the SSP when submitted for FedRAMP review.

Inheritance

According to NIST SP 800-53 Revision 4, security control inheritance is "a situation in which an information system or application receives (full inheritance) protection from security controls (or portions of security controls, i.e., partial inheritance) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides."

Security capabilities provided by controls can be inherited from many sources including, for example, organizations, organizational mission/business lines, sites, enclaves, environments of operation, or other information systems. Many of the controls needed to protect organizational information systems (e.g., security awareness training, incident response plans, physical access to facilities, rules of behavior) are inheritable by other systems. In addition, there can also be a variety of technology-based inheritable controls (e.g., Public Key Infrastructure [PKI], authorized secure standard configurations for clients/servers, access control systems, boundary protection, cross-domain solutions). By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of inheritable controls, security costs can be amortized across multiple information systems.

Inheritable controls, whether employed in organizational information systems or environments of operation, must be authorized by senior officials with at least the same level of authority/responsibility for managing risk as the authorization officials for the information systems inheriting the controls.

Q: How do I write a Business Impact Analysis required by FedRAMP?

A: FedRAMP does not provide a Business Impact Analysis template. However, a template can be found in NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems, dated May 2010; Appendix B—Sample Business Impact Analysis (BIA) and BIA Template

Q: How do I treat the implementation for SA-11(1)?

A: FedRAMP sees that many CSPs fail the SA-11(1) requirement. This is true not because the control fails but because the Cloud Service Provider (CSP) fails to document this enhancement in the Continuous Monitoring Plan. Please be aware that Control Enhancement SA-11 (1) must be implemented for FedRAMP Cloud Service Offerings. SA-11(1) is "The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis." Then the SA-11(1) Additional FedRAMP Requirement which is also a requirement for SA-11(1) and SA-11(8): The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

Q: Can a CSP simply go from an Agency ATO to a JAB P-ATO without going through the JAB Authorization effort?

A: A CSP interested in transitioning their Agency ATO to a JAB P-ATO must go through the JAB P-ATO process. Each Agency can accept varying levels of risk, per FISMA, when granting an ATO. The JAB works in a similar fashion, in that they must review the entire authorization package to understand associated risk with the system and make a decision whether or not to issue a JAB P-ATO. The JAB P-ATO provides the Agency community with the assurance that the JAB entities (DoD, DHS, and GSA CIOs) reviewed the package and deemed the risk to be acceptable for Agencies to issue their own ATOs. The JAB cannot accept risk on behalf of any Agency which is why the JAB authorization is titled a “Provisional Authorization.” If an Agency decides to use a system with a Provisional Authorization, the Agency will need to issue its own ATO letter to indicate that they accept the risk associated with using the system. We ask that these ATOs are sent to info@fedramp.gov for record-keeping and incident response notifications.

A JAB Provisional Authorization may not necessarily be optimal for every system and every CSP. In general, the JAB grants Provisional Authorizations for those systems leveraged government wide. FedRAMP was designed with the objective to authorize a system once and reuse that authorization many times. If a CSP only has one or two Agency customers showing interest in using their system, it is just as efficient for the CSP to obtain an authorization directly through the one Agency of interest.

TIP: The CSP has the most significant responsibility before beginning the FedRAMP processes - adequately and accurately defining the information system security boundary.

Before a CSP launches into the FedRAMP process, and before getting a 3PAO consultant or assessor involved in the process, a CSP should draft an accurate illustration of the system authorization boundary and all associated data flow diagrams.

The CSP system authorization boundary illustration must include network and architecture diagram(s) and provide a written description of the Authorization Boundary. Ensure each diagram:

- Includes a clearly defined authorization boundary.
- 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.

The CSP system boundary description must clearly define the following:

- 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.

In addition to describing these, all of the services must also be depicted either in the CSP system authorization boundary diagrams or in separate diagrams.

The CSP system data flow diagram(s) must:

- 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 data flow diagrams must be accompanied by a written description of the data flows.

If the CSP boundary is not adequately/accurately represented, the 3PAO will identify boundary deficiencies that could lead to substantial delays in the CSP Readiness Assessment process.

Q: How does an Agency recognize if the CSP's Cloud Service Offering (CSO) accepts Personal Identity Verification (PIV) and Common Access Card (CAC)?

A: The IA-2(12) Identification and Authentication Acceptance of PIV/CAC Credentials is one of FedRAMP's critical controls. In table 4-4 of the Readiness Assessment Report (RAR) the first "Question" asks if the system supports federal user authentication via CAC/PIV credentials. If the CSP’s answer to this question is "no," they fail the Readiness Assessment Review.

In order to securely provide this capability in the current, secure, technology environment, this may be accomplished through a type of Federated Identity Management. Federated Identity Management is available as a service offered by certain FedRAMP CSPs in their CSO. When a CSO accepts Government-issued PIV or CAC, that CSP has likely architected their solution to include some type of Federated Identity Management.

At each CSP level, whether an IaaS, PaaS, or SaaS, the CSP may include in their CSO a Federated Identity Management solution. Agencies should validate that IA-2(12) is indicated as implemented in the CSP's package and should validate that the testing in the SAR indicates the CSP's solution adequately meets the control requirement.

Q: What types of software must be included in the information system boundary?

A: In terms of computing, software is the variable part and hardware the invariable part. FedRAMP software inventory must take into account all the "variable" parts.

Historically, application software is divided into two general classes: systems software and applications software. FedRAMP recognizes applications software and systems software which includes the operating systems and any program that supports application software. Applications software is also called end-user programs and includes such things as database programs, word processors, Web browsers and spreadsheets. An application program (app or application for short) is a computer program designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user. This contrasts with system software, which is mainly involved with running the computer. System software is a type of computer program that is designed to run a computer's hardware and application programs. If we think of the computer system as a layered model, the system software is the interface between the hardware and user applications. The Operating System manages all the other programs in a computer.

FedRAMP recognizes middleware as programming that mediates between application and system software or between two different kinds of application software. Middleware is computer software that provides services to software applications beyond those available from the operating system. It can be described as "software glue". A service-oriented architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. The basic principles of service-oriented architecture are independent of vendors, products, and technologies.

FedRAMP also recognizes utility software, as applicable within the system. Utility software is also known as a utility program, and a utility tool. This utility software may have its own stripped-down OS; can be installed separately and used independently. Utility software is system software designed to help analyze, configure, optimize or maintain a computer. It is a type of system software, used to support the computer infrastructure in contrast to application software, which is aimed at directly performing tasks that benefit ordinary users. A utility program may be one that performs a very specific task, usually related to managing system resources. Operating systems contain a number of utilities for managing disk drives, printers, and other devices.

If you inventory all these types of software (including all relevant information concerning each piece of software, i.e., version, patch level, date, etc.) within your system boundary, then the chances are good that you have included all required software in the FedRAMP software inventory.

Q: For control RA-3, the FedRAMP parameter indicates that the results of the risk assessment should be documented in a "Security Assessment Report." Is this document the same as the SAR the 3PAO produces?

A: Yes - this document is the same. FedRAMP does not require a separate risk assessment; the results of the risk assessment are reported in the 3PAO's SAR.

Q: When adding a new service or feature to a JAB-authorized system, how does a CSP determine which process to follow - the New Services Onboarding process or the Significant Change process?

A: If onboarding the feature or service severely impacts the security posture of the system, the CSP should follow the Significant Change process. To help CSPs and 3PAOs determine which process to follow, FedRAMP has defined the following parameters for what constitutes a feature or service that qualifies for onboarding:

- Does not replace an existing service/feature previously included in the original system assessment;
- Is not an outsourced service belonging to a different CSP;
- Does not change the categorization of the Cloud Service Offering;
- Does not introduce vulnerabilities affecting the current security posture of the system;
- Does not affect the existing security controls implementation details of any controls as captured in the System Security Plan; and/or
- Does not add a unique or alternative implementation of any of the security controls as captured in the System Security Plan

Q: How are data centers treated for FedRAMP Authorizations?

A: Data center facilities are included in FedRAMP authorizations but the data centers, themselves are not specifically authorized separately as "data centers." In other words, a service provider that offers infrastructure, platform, and/or software as a service must include the underlying data center, i.e., the physical property (ping, power, and pipe) within its authorization boundary. FedRAMP authorizes the infrastructure, platform, and/or software as a service.

Q: How should I upload my package documentation? In which file format should the files be and what files is FedRAMP looking for?

A: All package documentation should be uploaded to MAX.gov using the folder structure that has been provided. Files should be uploaded in their native format based on the file, i.e., Word, Excel, PowerPoint. Uploading a file in its native format will facilitate FedRAMP review of your documentation to provide quicker turnaround. For a complete list of the appropriate file formats required in a cloud package, please see the FedRAMP Initial Authorization package checklist (found on fedramp.gov). This checklist can be used for Agency or JAB Authorizations to prepare your package or Annual Assessment for FedRAMP review.

TIP: Authorizations (Provisional Authorizations and Agency Authorizations) are now “ongoing authorizations.”

Office of Management and Budget Circular A-130 (OMB A-130), *Subject: Managing Information as a Strategic Resource, revised 7/28/2016*, enables ongoing authorization to maintain the security state and the risk posture of the system at the level (Low, Moderate, or High) as approved by the initial authorization. OMB A-130 requires that Agencies test information security and privacy controls, in an ongoing manner, at least annually but at a rate that is acceptable to each Agencies’ risk posture. The authorization letter is signed at initial approval. Agencies must collaborate with CSPs to ensure that cloud service offerings are tested and evaluated at least annually.

Please see:

OMB A-130, pg. 33

> *54.“Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the security and privacy state of the information system to determine whether the mission or business risk of continued system operation is acceptable.”*

OMB A-130, Appendix I-19, section e. Security and Privacy Assessments

> *“Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk,* ***but at least annually.*** *However, this general requirement to test and evaluate the effectiveness of information security and privacy policies, procedures, and practices does not imply that Agencies must assess every selected and implemented security and privacy control at least annually. Rather, Agencies must continuously monitor all implemented security and privacy controls (i.e., system-specific, hybrid, and common controls) with a frequency determined by the Agency in accordance with the ISCM and PCM strategies. These strategies will define the specific security and privacy controls selected for assessment during any one-year period (i.e., the annual assessment window) with the understanding that all controls may not be formally assessed every year.”*

TIP: Mandatory requirements for FedRAMP Readiness Reviews are just that - mandatory.

CSPs are responsible for understanding what it takes for them to be "FedRAMP Ready." Any CSP that is considering to opt for Moderate or High baseline FedRAMP Readiness should download the most recent copy of either the Moderate or High baseline Readiness Assessment Report (RAR) Template from fedramp.gov. Each potential CSP applicant should read through the document to understand the compulsory items required within the Cloud Service Offering. These compulsory requirements *cannot* have alternate implementations and must be implemented.

1. The "showstopper" requirements are located in *RAR Section 4.1 Federal Mandates* for both the Moderate and the High Baseline Cloud Service Offerings.
2. Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required?
3. Can the system fully support user authentication via Agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials?
4. Is the system operating at the minimum eAuth level for its FIPS-199 designated level of operation (Level 3 for Moderate, Level 4 for High)?
5. Does the CSP have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days?
6. Does the CSP and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?

If you are a CSP looking at these five requirements and you answer “No” to any one of these, you are not “FedRAMP Ready.” Keep in mind that, while the CSP can include customer responsibilities associated with meeting some of the mandatory requirements, such as PIV Acceptance, they may not pass the responsibility to the customer. As an example, citing the PIV acceptance, the CSP must have the capability to accept PIVs/CACs regardless of the customer's mechanism for use of PIVs/CACs. So an alternative implementation is not acceptable.

FedRAMP recommends that if a CSP is deficient in any of the FedRAMP mandatory requirements areas, they seek assistance to determine the feasibility of architecting/re-architecting the environment to accommodate the FedRAMP Ready requirements.

TIP: A SaaS is responsible for the entire stack if…

If a SaaS is on an infrastructure and/or platform that is not FedRAMP authorized, the SaaS CSP would either need to include the IaaS/PaaS in its own authorization boundary (which would be indicated in the Readiness Assessment Report) OR wait for the the IaaS/PaaS to be authorized separately prior to submitting the RAR. All layers need to be authorized or have the potential to be authorized.

As such, a SaaS Cloud Service Offering is responsible for the entire stack (IaaS/ PaaS/ SaaS) if the underlying IaaS/PaaS does not have a FedRAMP authorization, either a Provisional Authorization through the JAB or an Agency Authorization. The SaaS is responsible for all the security controls that are normally inherited from the IaaS/ Paas, such as the ping/power/pipe and rented cage within the data center, and for the physical, environmental, and all other related controls.

If the IaaS /PaaS are not FedRAMP authorized, the SaaS Cloud Service Offering may work with the data center provider through Service Level Agreements and/or Rental Agreements to ensure that the requirements for the ping, power, pipe, cage, all physical, environmental, and all related security controls are implemented per the appropriate FIPS 199 Level (Low, Moderate, or High). In the agreement(s), the SaaS CSP must ensure that the data center provider has the appropriate level of security implemented to ensure the security of the SaaS.

Q: Why should a CSP use an accredited 3PAO when pursuing a FedRAMP Agency ATO?

A: While there is no specific requirement for an Agency to require that the a CSP use a FedRAMP accredited 3PAO to perform the security assessment, FedRAMP recommends that Agencies require CSPs to engage a FedRAMP Accredited Assessor to evaluate the implementation of the FedRAMP baseline security controls.

CSPs that seek a JAB P-ATO must use a FedRAMP Accredited Assessor. CSPs submitting an Agency Authorization package may have their cloud system assessed by an Agency-validated Independent Assessor. However, FedRAMP has no insight and control over an Agency-validated independent assessor. The Agency has no recourse and must have another assessment performed, if an Agency-validated Independent Assessor provides the Agency a deficient security assessment in which the security of the CSP system is inappropriately/poorly tested. Using a FedRAMP Accredited 3PAO provides greater confidence to other leveraging Agencies as to the rigor of the initial partnering Agency's assessment. Furthermore, if the CSP intends to later pursue a JAB P-ATO, the rigor prescribed by the

FedRAMP Accredited 3PAO to the assessment process provides the CSP with a more accurate understanding of their risk posture from a true FedRAMP perspective and their readiness to pursue a JAB P-ATO.

Q: What are some frequently asked questions for CSPs who currently hold an Agency Authorization to Operate (ATO) at the Moderate level, but wish to apply for an Agency High Baseline Authorization?

A: For some CSPs, the ATO transition between a Moderate baseline and a High baseline is simple because the system in question was originally architected at the High baseline level but the CSP opted for the FedRAMP Moderate because that is all FedRAMP offered at the time.

For other CSPs who wish to transition to the high baseline, FedRAMP recommends that the CSP and the attesting 3PAO download a copy of the FedRAMP High Readiness Assessment Report (RAR) Template from the FedRAMP website and read through the contents of the RAR to understand the depth of scrutiny required for a High Baseline system.

Here are some frequently asked questions regarding this transition:

1. *Is the ATO transition between a Moderate baseline and a High baseline merely an amendment to the Moderate ATO? Or will this process involve a new ATO?*

   Answer: The High Baseline (HBL) Authorization is a new Authorization at the High Baseline level. This requires that the CSP engage with a partnering Agency (either existing or new) and a FedRAMP-accredited 3PAO or other independent assessor to maneuver through the HBL Authorization process; i.e., capturing HBL requirements in the SSP and attachments, undergoing testing of the HBL controls, at a minimum, and re-authorization of the Service at the HBL level. This assumes that the cloud service's moderate-level testing is current and compliant with FedRAMP guidelines.

2. *Is there a FedRAMP-approved document that speaks to the "net-new" controls between the Moderate baseline and the HBL?*

   Answer: No. Based on the extent of the control and parameter changes, the CSP must review the requirements as enumerated in the High Baseline (HBL) SSP template, and the HBL RAR template to ensure that the CSP organizational architecture will support the HBL requirements. Further, the review will ensure that the cloud service architecture can meet the HBL requirements.

3. *Are there any significant new requirements for New Systems?*

   Answer: Yes. There are changes incorporated in the current FedRAMP HBL set of controls posted on the FedRAMP website, based on the FedRAMP PMO and Joint Authorization

Board (JAB) collaboration. Some of the changes were additional controls; other changes were more stringent parameters and Additional Guidance. Please see the requirements in the HBL SSP template, and the HBL Readiness Assessment Report template. Some examples of changes in the HBL requirements include:

a. More emphasis is placed on the use of automation for control implementations
b. All CSO services must be included in the authorization boundary
c. The eAuth requirement is "Level 4" (includes in-person identity proofing) versus the Moderate "Level 3 or higher"

There are added controls that are particularly challenging, either in terms of resources or technical complexity, based upon the cloud service architecture, i.e., SC-3 Security Function Isolation

Q: One of the Moderate and High RAR Federal Mandates that is overlooked is (5.) Does the CSP and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? What does this really mean to a CSP?

A: Since the FedRAMP mandate is a requirement that must be met, it is important that the CSP understands the Federal Records Retention Requirements to achieve compliance. Since CSPs store, transmit, and process Government data, a CSP must be aware that there are retention schedules provided by NARA that govern the disposition of these federal records. From the Agency perspective, the Agency program officials are required to coordinate with Agency records officers and with NARA to identify appropriate retention periods and disposal methods. Since CSPs and the CSOs are now mostly the de facto cloud-based keepers of the federal records, CSPs must understand the NARA and FOIA requirements for the federal data and information that is traversing and being held in the CSP system. The requirements should be fully outlined in the contract award information, but it is incumbent upon the CSP contractors to understand Federal Records Management Requirements. The basic requirements for Federal Records Management can be found at:

https://www.archives.gov/about/regulations/regulations.html

Regarding FOIA, "Since 1967, the Freedom of Information Act (FOIA) has provided the public the right to request access to records from any Federal Agency. It is often described as the law that keeps citizens in the know about their government. Federal Agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement."

Currently, additional information for the FOIA can be found here:

https://www.foia.gov/index.html

The FOIA applies to all federal Agencies, which means it does not apply to:

- The Judicial Branch and Federal Courts
- The Legislative Branch and Congress
- State Governments and Courts

Q: Is there an established process for what is supposed to occur when ownership of an authorized service transfers from one Cloud Service Provider (CSP) to another?

A: If there were NO changes to the service, NO change to the security posture, NO change to the risk management strategy of the overall organization, and it was simply a name change, then the process could be as easy as notifying the Authorizing Official(s) of the name change. This could be addressed as an administrative change based upon the AO determination. The CSP should notify FedRAMP also, of the change. The Cloud Service Offering authorization package documentation should be changed as well to reflect the ownership change.

More often than not, when services change owners, organizational policies and procedures change which changes the security posture and the risk management strategy of the system. Changes like this are significant and must be documented appropriately. If that is the case, the CSP should account for and make associated updates to the CSO package as early as possible. The changes must be clearly documented and submitted to the AO for review and approval.

Of course, the CSP and involved Agencies will need to facilitate contractual changes to reflect the change of ownership.

Q: Does FedRAMP still assign Information System Security Officers (ISSOs) to each Cloud Service Provider (CSP) that is engaged in the Joint Authorization Board (JAB) provisional authorization process?

A: FedRAMP no longer has FedRAMP ISSOs assigned to each CSP. Now, each CSP has a direct relationship with a primary and secondary JAB Reviewer. Each CSP should ensure that the SSP documentation, when referring to designated contacts, is changed (for example, changing "FedRAMP ISSO" to "Primary JAB Reviewer" and "Secondary JAB Reviewer."

Please note that in the recent past, the "JAB Reviewer" was called the "JAB Technical Review-Reviewer." Since the FedRAMP JAB Provisional Authorization adjustments, and the shifting of the responsibilities, the JAB Technical Review-Reviewer is now called the "JAB Reviewer."

Q: When submitting a completed authorization package to FedRAMP, what are the three categories of testing evidence with timeliness criteria? Please define the timeliness criteria required.

A: The three categories of testing evidence with timeliness criteria are penetration testing, security controls testing, and vulnerability scanning. Vulnerability scanning must be for Operating System (OS)/infrastructure, databases, and web application components. The CSP/3PAO must ensure that the associated testing evidence is considered “timely” by the PMO (JAB & PMO follow same requirements).

Timeliness Requirements for Penetration Testing

- When submitting a completed authorization package to FedRAMP to begin the JAB P-ATO process, the Penetration Test ***cannot be older than 6 months***
- CSPs should ensure the Penetration Test is executed as close as possible to a CSP’s submission of the authorization package
- Once a JAB P-ATO is granted, CSPs must have a 3PAO complete a new Penetration Test at minimum once a year

Timeliness Requirements for Security Control Testing

- When submitting a completed authorization package to FedRAMP, security control testing evidence must be current within:
  - ***120 days***, if the system does not have an existing FedRAMP Agency authorization
  - ***12 months***, if the system has an existing FedRAMP Agency authorization

Timeliness Requirements for Vulnerability Scanning

- When submitting a completed authorization package to FedRAMP to begin the JAB P-ATO process or the Agency ATO process, the scans completed by a 3PAO and reflected in the Security Assessment Report (SAR) ***must be current within 120 days***
- Additionally, CSPs must submit scans and a POA&M **current within 30 days** prior to the date of the JAB P-ATO process kickoff
- During the JAB P-ATO process and afterwards, vendors must submit monthly vulnerability scans, in accordance with security controls RA-5 and RA-5 (5); and matching POA&Ms, in accordance with security control CA-5
- Agency ATO systems should be submitting timely monthly scan results and POA&Ms to the partnering Agency(ies)

TIP: When submitting a Readiness Assessment Report or an authorization package, be sure to send an email notification to info@fedramp.gov

Cloud Service Providers (CSPs), Partnering Agencies, and/or Third Party Assessment Organizations (3PAOs) must send an email notification to info@fedramp.gov to let the FedRAMP PMO know exactly when an Agency FedRAMP Package or a Readiness Assessment Report (RAR) is posted to OMB MAX. Because both the RAR and the CSP package culminates in the Security Assessment Report (SAR) and the 3PAO recommendation to the Authorizing Official (AO) concerning the risk posture and/or authorization of the system, it is ideal if the 3PAO uploads the documentation. This email notification facilitates the beginning of the process to get the Cloud Service Offering (CSO) Package into the FedRAMP process or at the least get the AO Memo posted to the website. The OMB MAX facilitator will set up the CSO package skeleton on MAX into which the package is uploaded. Other encryption policies apply if the CSO is a High Baseline package.

Please be advised that OMB Max submissions do not generate an automatic notification to the FedRAMP PMO at this time. If a RAR or authorization package is submitted, but the PMO is not made aware of the submission, the review will be delayed.

Q: Are CSPs required to perform background checks on staff members?

A: Yes. ***Personnel Security (PS) - 3 Personnel Screening*** is required for all FedRAMP defined baselines (High, Moderate, Low, and FedRAMP Tailored). Specifically, the control requirement is that the organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals for national security clearances - a reinvestigation is required during the 5th year for top secret security clearance; the 10th year for secret security clearance; and 15th year for confidential security clearance. Additionally, for moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions.

The objective/ intent of part (a) of this PS-3 control is to ensure that the CSP elaborates upon what type of personnel screening is accomplished before the personnel are allowed system access. The CSP must be aware that when contracting with the Federal Government it is at the discretion of the partnering Agency to determine what level of personnel screening must be accomplished. Since the CSP is contracting and acting on behalf of the Agency, the CSP is required to follow the Agency requirements for suitability to perform services on behalf of the Agency.

Further, for FedRAMP Moderate and High baseline systems, ***PS-3(3) Personnel Screening | Information with Special Protection Measures***, the control requirement is that the organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

a. Have valid access authorizations that are demonstrated by assigned official government duties; and
b. Satisfy personnel screening criteria – as required by specific information.

NIST Supplemental Guidance:

Organizational information requiring special protection includes, for example, Controlled Unclassified Information (CUI) and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.

TIP: A CSP using non-US persons to support their system is FedRAMP compliant but will find their market limited among Federal Agencies.

Using non-US persons to support a FedRAMP system is a business decision the CSP must make. There is no Federal requirement about citizenship. Some Agencies have no issue with the use of non-US persons supporting the system; however, many Agencies have their own citizenship requirements. For some Agencies, the requirement is blanket. For others, it may depend on the sensitivity of the system.

Q: Who do I contact if I have changes to the information that I submitted in my CSP Information Form or the information that is displayed on my FedRAMP Marketplace page?

A: Please email info@fedramp.gov to request any changes and/or updates to information (e.g., offering, description, point of contact).

TIP: US-CERT has updated incident response guidance (effective April 1, 2017).

https://www.us-cert.gov/incident-notification-guidelines

Organizations must report information security incidents, where the confidentiality, integrity, or availability of a federal information system with the required data elements, as well as any other available information, within one hour of being identified by the organization. In some cases, it may not be feasible to have complete and validated information prior to reporting. Organizations should provide their best estimate at the time of notification and report updated information as it becomes available. Events that have been found by the organization not to impact confidentiality, integrity or availability may be reported voluntarily.

Q: What is the first step to move from a moderate system to a high system?

A: Please visit the FedRAMP Templates page and find the FedRAMP FIPS-199 Categorization Change Form Template under the "Continuous Monitoring" section. Once the form is completed, send the form, along with the letter from an Agency demonstrating demand, to info@fedramp.gov. Your JAB reviewer will then contact you regarding the request (with request for clarification, approval, or denial).

Q: How do I get access to my Certificate of Completion after I complete Training module 300-G?

A: To download and print your course certificate you must first complete the 3PAO RAR Training, 3PAO RAR Final Exam, and FedRAMP Course Survey. These trainings can be accessed on our FedRAMP Training page. Once the course survey is complete, click on the box 'Marked Reviewed' below the description. This action will refresh the screen and bring up your course certificate. To view the course certificate, click on the box "Marked Reviewed" and then click on "Certificate" in the upper left-hand index under "Start Here." This action will bring up another window with the certificate and you can print it using the controls on the right.

Q: The Agency I'm working with requires that their data be cryptographically protected. What requirements must I follow?

A: Any system that handles Government data may be the target of a cyber-attack, particularly those systems with sensitive data. Because of this, if an Agency requires that their data must be cryptographically protected, then FIPS 140-2 applies, and cryptomodules must be validated using Transport Layer Security (TLS) services.

Version 1.2 is currently the most secure; however, version 1.3 is in draft and may cause compatibility issues when it is released because it will not support many obsolete crypto features.

To take advantage of the benefits of TLS 1.2, it is important to use a TLS service (e.g. library, web framework, web application server) that has been FIPS 140-2 validated. In addition, the cryptomodule must be installed, configured and operated in either an approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptomodule is providing the expected security services in the expected manner.

If the system is required to use FIPS 140-2 encryption (i.e., owned or operated by or on behalf of the U.S. Government), then TLS must be used, and SSL disabled. For more information on this, see Section 7.1 (now D.2) of Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program.

Cryptographic modules validation listings can be found at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program/module-validation-lists

Cryptographic algorithm validation listings can be found at: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation

Q: I already have a Provisional Authorization to Operate (P-ATO) with the Joint Authorization Board (JAB). Is non-compliance on a particular control or on business issues allowed?

A: Once a CSP achieves a P-ATO, it is incumbent on them to maintain their authorization to the best of their ability. Any non-compliance must be addressed expediently and to the satisfaction of the JAB. This includes ensuring consistent, successful monthly continuous monitoring with remediations and annual assessments. Corrective Action Plans (CAPs) will be instituted if deemed necessary. This level of fidelity is necessary to ensure the security of government data and systems.

5. PROFESSIONAL WRITING TIPS

The FedRAMP authorization process requires cloud service providers (CSPs) and 3PAOs to develop a large number of technically written documents. Here are some tips from our Quality Management team on how to write to a well-written document.

Write short sentences.

Stick to a single idea in each sentence. Structure them with bulleted lists in many cases. Avoid a sentence like this: “In order to fulfill control requirement XX-Y, the system implements feature Q, controlled by parameters initialized to factory settings ZZZ, and changed in accordance with the history of user requests to new settings to solve any revealed problems, reviewed monthly by the product manager.”

Say rather:

- “Control requirement XX-Y is satisfied as follows:
- Feature Q is used to fulfill this requirement.
- Feature Q is initialized to factory settings ZZZ.
- The product manager reviews the past month’s user requests.
- The product manager changes the settings based on the past month’s user requests.
- The new settings are determined according to the following table:” [You should include a table here showing criteria for changing the settings.]

Each time a new version of a document is “published,” the version number should be incremented, and the date of publication should become the document date.

The document should be marked with these two important items on the cover page at a minimum. Ideally (and where required by templates) the version and date appear also in a document revision history and in the header or footer of every page of the document. For major revisions, increment the whole number to the left of the decimal. For minor revisions, increment the number to the right of the decimal.

For example, the initial SSP would start out as Version 1.0. As the CSP revises the CSP in response to JAB TR comments, the SSP version number should increment to 1.1, then 1.2, etc. As a CSP transitions from NIST SP 800-53 Rev 3 to Rev 4, the resulting SSP version number would change to 2.0. Then as the SSP is revised as a result of ISSO or JAB feedback the version would change to 2.1 and then to 2.2 for each "published" revision.

Reviewers, auditors, and users of these documents rely on correct version numbers and dates to ensure they are looking at an appropriate version of a document. Proper management of document version numbers and dates eliminates ambiguity as to which version of a document is the latest and when it went into effect.

Q: When is it appropriate to use "bytes" and when should I use "bits"?

A: You may already know this and there can be exceptions but as a rule of thumb:

When discussing storage, size is expressed in "bytes." When discussing communications, speeds are typically expressed in "bits per second." Storage includes tape backup, SAN, RAM, ROM, disks, thumb-drives, etc. and storing program files such as executables, OS', Microsoft OA files such as Word/Excel, and pictures, size is expressed in bytes (KB, MB, GB and SAN and tape storage can be terabytes (TB) and petabytes (PB)). As an example, GSA's email gateway has a limit of a 45 MB (megabytes) file attachment size.

Communications speeds and sizes, on the other hand, are expressed in "bits per second." GSA's Internet links are probably 1 Gbps (giga bits per second). Corporate Wide Area Networks and data center backbones are typically 10 Gbps and communications between workstations and servers are typically 100 Mbps (megabits per second) or 1 Gbps. Wi-Fi, these days, is at least 54 Mbps and getting faster.

So, bytes for storage, and bits per second for communications.

Be wary of using pronouns in your writing.

Always be absolutely clear who, or what organization, is responsible for an action. It is much better to repeat the responsible party's/organization's name than to leave the reader in doubt as to who or what a pronoun refers to.

In your written work, always refer to the same person, position, or thing by the same name. Avoid, for example, calling "the test team" by other names, like "the test group," "the testers," or "the evaluation team."

Provide all relevant information for the JAB TRs to prevent slowing down the review process.

When reviewing each of the NIST SP 800-53 Revision 4 controls, be sure to read the control description thoroughly to understand the nouns and the verbs in each of the individual requirements for each individual security control. Once the writer identifies who or what should be performing the action(s), then provide a description regarding how the action is and/or the actions are performed within the environment. Be succinct for each action verb, i.e., "monitors" and "updates". The writer must describe how something is monitored and then how something is updated. (Please note that many times the monitors and updates require a specific frequency, as well.) The NIST SP 800-53A Revision 4 testing criteria can be used as the cross reference for each of the security controls in order that the writer understand the objectives for each control.

Q: Which is the better sentence? "The report is sent to the Agency." OR "The Contractor's Project Manager sends the Monthly Status Report to the Agency Program Manager by the fifth day of each month."

A: The first sentence is written in passive voice. It does not specify who sends the report or which Agency will receive it.

Tip: Send all documents and writing in an Active Voice. Writing in active voice gives clarity and specificity – a must for all FedRAMP documentation.

Many readers commonly confuse the meanings of i.e. and e.g. I.e. and e.g. are both abbreviations for Latin terms. I.e. stands for "id est" and means roughly "that is." E.g. stands for "exempli gratia," which means "for example." It is best to write out the meanings of these abbreviations to avoid any misunderstanding.

Avoid using "etc." If an item is important enough to be in a list, then it is important enough to name. Only use "etc." if it is completely clear how the rest of the list will run. Alternatively, explain the characteristics of the items in the list, and then say, "For example."

Be consistent with your naming conventions. Always call the same thing by the same name throughout your written work.

EXAMPLE: "The Emergency Response Team shall resolve all problems within four hours of receiving a report. Once a problem is fixed, the response team lead documents the solution and sends the requesting team the correction report.” This sentence calls “The Emergency Response Team” by another name, “response team.” These are probably the same, but the different names and differing capitalization can be confusing. Additionally, what the Emergency Response Team does is referred to with three different verbs: resolve, fix, and correct. Stick to one name and try to stick to one verb that accurately describes the action.

6. READINESS ASSESSMENT REPORT

TIP: When submitting a RAR or RAR update (3PAOs) or an authorization package (CSPs or Agencies), be sure to send an email notification to info@fedramp.gov.

Submission does not generate an automated notification to PMO at this time. Sometimes RARs and authorization packages are submitted, but PMO is not made aware of the submission, to begin review.

We also ask that you email info@fedramp.gov and give us at least two weeks advance notice BEFORE you submit any authorization for review to OMB MAX.

By giving us advance notice of your anticipated submission date through info@fedramp.gov, the FedRAMP PMO can ensure our reviews are completed in a prompt and efficient manner. Our goal is to complete our reviews as quickly as possible and in turn update your CSP’s status on the FedRAMP Marketplace to “Authorized” as close to your Agency granting an ATO as possible.

Without providing us with an estimated completion date and providing a two-week warning, we will be unable to ensure we have the appropriate resources and commit to you that our review will be completed in a timely manner.

If you have any questions about this request, place do not hesitate to reach out to info@fedramp.gov.

7. SECURITY ASSESSMENT PLAN (SAP) & SECURITY ASSESSMENT REPORT (SAR) DOCUMENTS

TIP: Findings that the 3PAO has validated/determined to be False Positives are NOT included in the P-ATO SAR POA&M.

Otherwise, they are simply “findings” which need to be included in the P-ATO SAR POA&M. However, if the findings that the 3PAO determined to be “False Positives” in the P-ATO SAR are not approved by

JAB, then at Continuous Monitoring phase, those findings must be added to the ConMon POA&M for tracking through the monthly reporting until remediated. (Note: These findings are deliberately not called "False Positives" because at that point they will have been determined to be simply "open findings.")

Q: What is the 3PAO's responsibility if it is not conducting the vulnerability scanning for an assessment?

A: If the 3PAO is not conducting the vulnerability scanning for an assessment, then the Security Assessment Plan (SAP) should identify the alternative methodology. The 3PAO should describe processes to ensure integrity, completeness, accuracy, reliability, and the independent nature of the scan results. At a minimum, the 3PAO is responsible for:

- Reviewing scanning tools to ensure the tools are appropriately configured before the scans are executed (i.e., describing what the appropriate/expected configurations are that will be verified)
- Ensuring scans comply with the FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide
- Overseeing and monitoring scans from initiation to completion
- Describing the procedures to ensure chain-of-custody of the scan results

Q: When developing a System Assessment Plan (SAP), how should a 3PAO select which controls to assess?

A: Guidance documents for selecting controls to include in the SAP can be found on the FedRAMP website. For Annual Assessments, as an example, the 3PAO should select core security controls, as well as other controls required by the CSP, all controls that haven't been tested within the three-year cycle, and controls that were Plan of Action and Milestones (POA&M) items, involved with Deviation Requests, etc.

As a tip: When developing the SAP, 3PAOs should review the controls listed in the closed POA&Ms as a basis for the selection of controls to assess. Then, instead of full testing of the control, simply assess the remediation actions/documentation associated with the closed POA&M to ensure the specific issue noted in that POA&M was addressed.

Q: What is the third party assessment organization's (3PAO) responsibility if it is not conducting the vulnerability scanning for specific controls in an assessment?

A: Generally, an assessment by the 3PAO includes several methodologies: personal interviews, document and evidence reviews, vulnerability scanning, and penetration testing. The Security Assessment Plan (SAP) should address the assessment methodology in detail so that it can be reviewed and approved prior to assessment testing. For vulnerability scanning, 3PAO responsibilities include:

- Reviewing scanning tools to ensure the tools are appropriately configured before the scans are executed (i.e., describing the appropriate/expected configurations that will then be verified)
- Ensuring scans comply with the FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide
- Overseeing and monitoring scans from initiation to completion
- Describing and executing the procedures to ensure 3PAO chain-of-custody of the scan and results

Q: When completing the Security Assessment Report (SAR), is it appropriate to assign the same values to tables ES-1 and F-1/F-2 if there are no POA&M entries in the initial assessment?

A: It is not appropriate to assign the same values to tables ES-1 and F-1/F-2 if there are no POA&M entries in the initial assessment. SAR Table ES-1 represents the total risk to the system being assessed, while tables F-1 and F-2 represent only the findings from the assessment testing itself.

For initial assessments, the findings represent the total risk to the system, thus table ES-1 ends up with the same totals as tables F-1 and F2. For annual assessments, POA&M items not duplicated through testing are also part of the total system risk, thus table ES-1 totals must reflect both testing totals and POA&M totals after duplicates have been identified and removed from the count.

Q: Is the CSP responsible for ensuring the quality of the work performed by the 3PAO?

A: While accredited 3PAOs perform security assessments of FedRAMP cloud services, it is the CSP that is responsible for all 3PAO activities and deliverables related to the assessment of their cloud offering. The CSP manages and oversees these activities accordingly. Exceptions are delivery of the Security Assessment Plan (SAP), Security Assessment Report (SAR), and the SAR results. In order to maintain the integrity and independence of these documents, they must be provided to the PMO directly from the 3PAO. While the 3PAO makes the final determination on the security results in the SAR, the CSP should ensure the quality of the SAR and all 3PAO deliverables provided to FedRAMP.

Q: Are High findings acceptable when submitting a Security Assessment Report (SAR) for an initial Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO)?

A: When submitting a SAR for an initial JAB Provisional Authorization to Operate (P-ATO), there must be no High findings. For High findings that cannot be resolved, such as vendor dependencies, sufficient additional mitigating controls must be in place to justify a risk reduction to Moderate.

Some CSPs incorrectly believe that a High finding is acceptable if it is a vendor dependency or operationally required vulnerability. This is not the case. If a High finding cannot be resolved, it must at least be mitigated down to a Moderate.

Q: Do the tools used for the penetration test need to be listed anywhere else besides in the Penetration Test Plan document?

A: Yes. The tools used for the penetration test must also be listed in the Security Assessment Plan (SAP) and match those listed in the Penetration Test Plan document. When completing Table 5-3 in the SAP, be sure to include each tool used for the security controls assessment, vulnerability scanning, and penetration test.

Q: Are low risk findings tracked on the Plan of Action and Milestones (POA&M)? If so, what is the time window to correct low risk findings? The FedRAMP guidance only states remediation time frames for high/moderate risk items.

A: Yes, all findings must be documented in the POA&M, including low risk findings. Low risk findings should be remediated within 180 days, and the remediation will be validated during the next annual assessment.

Q: What are the roles and responsibilities of the third party assessment organization (3PAO) and the cloud service provider (CSP) during the assessment?

A: While FedRAMP certifies 3PAOs to perform security assessments of FedRAMP cloud services, the CSP is ultimately responsible for all 3PAO activities and deliverables related to the assessment of their cloud offering. The CSP develops and maintains the System Security Plan (SSP), Plan of Action and Milestones (POA&M) and other supporting documents; however, the CSP also manages and oversees the assessment activities accordingly. The 3PAO develops and delivers the Security Assessment Plan (SAP), and Security Assessment Report (SAR), and SAR evidence/attachments. While the 3PAO makes the final determination on the security results in the SAR, the CSP should ensure the quality of the SAR and all other 3PAO deliverables.

Q: When developing the Security Assessment Report (SAR), what is the procedure or method for documenting findings that were corrected during testing or identified as false positives?

A: False positives and vulnerabilities that were corrected during testing are reported in designated SAR tables. Consult the SAR table of contents to identify these locations. When describing what was done to confirm that something was a false positive or corrected during testing, cite the specific item of evidence (screenshot, scan file, etc.) by filename in the table entry. Provide the evidence file(s) with the SAR. This approach will ensure the SAR reviewers can easily navigate the document when evaluating these items.

Q: Can the Security Assessment Plan (SAP) or the Security Assessment Reports (SAR) templates be modified?

A: Templates for the SAP and the SAR can be modified to add content, but content cannot be removed from the template. So you will be able to add information to help bolster security packages, but you cannot eliminate parts or portions of the templates.

Q: How does a 3PAO indicate that a vulnerability is “closed” in the Security Assessment Report (SAR)?

A: For any scan-related finding that was found and corrected during testing, please make sure to include a “targeted” scan that reflects the vulnerability as closed. It is recommended that these remediation scans are targeted scans, where scans are conducted to target the specific vulnerabilities and specifically impacted components proving closure, so as not to skew the assessment results. Please provide these targeted scans as part of the final SAR deliverable that is submitted to FedRAMP.

Q: Are there limitations on the types of findings that can be reported in the Security Assessment Report (SAR)?

A: There cannot be any unmitigated or unremediated high findings reported in the SAR for P-ATO. Hence, Table ES-1, shouldn't have any high's listed within the composite

Q: What does the 3PAO need to provide with regard to vulnerabilities that were fixed during testing, downgraded, operationally required, or false positives?

A: For vulnerabilities that were remediated during assessment testing, risk adjusted, operationally required, or determined to be a false positive, the 3PAO must provide compelling evidence in the form of artifacts and detailed rationale within the appropriate Security Assessment Report (SAR) tables to justify the adjusted status. Please reference the specific evidence file(s) and provide them with the SAR.

Q: Should a Security Assessment Plan (SAP) be submitted if the inventory differs from the System Security Plan (SSP)?

A: At the time the SAP is submitted by the 3PAO, the SSP and SAP should reflect the same inventory. Post testing, if there are devices that are discovered and not disclosed within the SSP and/or SAP, the Security Assessment Report (SAR) must reflect a deviation from the SAP, and the SSP must be updated prior to authorization with the accurate inventory listing.

Q: How does a 3PAO ensure repeatable and consistent results when reporting the results of an assessment method?

A: When reporting the results of an assessment method (document examinations, personal interviews, and system tests), ensure there is enough detail so that the assessment method and result can be repeated by someone else. This generally refers to Appendix B of the Security Assessment Report SAR), spreadsheet tab: "Procedure and Evidence". For each control, there should be sufficient detail to describe the assessment method that includes the procedure, evidence and results. This should have a consistent look and feel from control to control, for repeatability and consistency.

Q: When a 3PAO is providing the Authorization Recommendation for a CSP Provisional Authorization To Operate (P-ATO), the Security Assessment Report (SAR), Section 7 needs to be updated. What updates must be provided in the SAR template section 7-Authorization Recommendation?

A: Section 7 of the SAR is templated so that the 3PAO may provide an executive summary type of overview for the analysis of risk identified within the system environment. The summary includes the numbers of types of vulnerabilities identified (i.e., there were <Number> High risks, <Number> Moderate risks, <Number> Low risks, and <Number> of Operationally Required risks). Operationally required risks must be identified because these vulnerabilities are risks that cannot readily be remediated or mitigated because the remediation or mitigation would adversely affect the operating environment of the system. The FedRAMP Program Management Office (PMO) expects that the 3PAO provides their professional recommendation regarding the analysis of risks for the system based on the results of the security assessment. However, the 3PAO recommendation must be fully validated by collected artifacts and evidence. The recommendation is reviewed by the Joint Authorization Board (JAB) for the Provisional Authorization To Operate (P-ATO) decision and by the Agency Authorizing Official (AO) for the Agency Authorization.

TIP: A Certified 3PAO Penetration Testing Methodology must contain all of the FedRAMP Penetration Testing components.

Every 3PAO has adopted a specific Penetration Testing Methodology. However, in order for the 3PAO to be FedRAMP compliant and perform FedRAMP Compliant Penetration Testing, the FedRAMP Penetration Test Guidance, Version 1.0.1, dated July 6, 2015 and the methodology contained therein must be tightly interwoven in the 3PAO Penetration Testing Methodology.

For instance, if a 3PAO is testing roles, for each role defined, the penetration testing methodology used by the 3PAO must incorporate attack vectors defined, at a minimum:

1. External to Corporate – External Untrusted to Internal Untrusted
2. External to Target System – External Untrusted to External Trusted
3. Target System to CSP Management System – External Trusted to Internal Trusted
4. Tenant to Tenant – External Trusted to External Trusted
5. Corporate to CSP Management System – Internal Untrusted to Internal Trusted
6. Mobile Application – External Untrusted to External Trusted

Even if the networks are called something else and are not referred to as generically as the FedRAMP listing, the proof must be provided that at least the minimum attack vectors listed in the FedRAMP guidance must be penetration tested and must be part of the 3PAO FedRAMP Penetration Testing Methodology for the CSP.

TIP: Assign unique Vulnerability Identifiers for the SAR/Deviation Requests/POA&M workbooks.

This can be in any format or naming convention that produces uniqueness, but FedRAMP recommends the convention V-<incremented number> (for example, V-123). This unique identifier is assigned to a specifically identified vulnerability in the CSP system. The requirement is that if a vulnerability is identified during the annual assessment and/or the monthly continuous monitoring effort, and that vulnerability is the same vulnerability already uniquely identified in the existing POA&M, the CSP and 3PAO must use the same POA&M ID as for pre-existing and open vulnerabilities. In other words, do not assign a different ID to a vulnerability that is already documented in the POA&M.

Q: What are the FedRAMP requirements for vulnerability scanning?

A: Vulnerability scanning must occur for Operating System (OS)/ infrastructure, databases, and web application components in the Cloud Service offering authorization boundary. The scanning parameters for the components must be defined in the Security Assessment Plan (SAP). If the 3PAO has not or is not conducting the vulnerability scanning for the assessment, then the SAP identifies the alternative methodology. This standard then becomes integrated in the methodology. In order to maintain FedRAMP scanning compliance, the 3PAO must describe processes to ensure integrity, completeness, accuracy, reliability, and the independent nature of the scan results.

At a minimum, the 3PAO must:

- Review the scanning tools to ensure the tools are appropriately configured before the scans are executed.
- Oversee and monitor the scans from initiation to completion.
- Describe the procedures to ensure chain-of-custody of the scan results.
- Compare the list of components identified in the scans and those in the inventory and provide an explanation for the difference in the SAR.
- Assess a component through other means (manual methods), if a component cannot be scanned.

Once the methodology is approved via the SAP, the methodology may be followed for the system until there is a significant change or the next annual assessment whereby the methodology may be altered within the next SAP.

Vulnerability scans must be performed using system credentials that allow full access to scanning the entire authorization boundary to include all hardware and software. Scanners must have the ability to perform in-depth vulnerability scanning of all systems (as applicable). Systems scanned without credentials provide limited or no results of the risks. All unauthenticated scans will be rejected unless an exception has been previously granted due to applicability or technical considerations.

Q: For vulnerability scans, do all plugins have to be enabled?

A: All non-destructive plugins must be enabled. To ensure all vulnerabilities are discovered, the scanner must be configured to scan for all non-destructive findings. Any vulnerability scans where plugins are limited or excluded will be rejected. Exceptions may occur based on specific requests from the government for re-scans or targeted scans. These scans must comply with the directions provided by the government.
For more information, please see our FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide.

TIP: What does a typical Third Party Assessment Organization (3PAO) Team performing a Cloud Service Offering (CSO) assessment look like according to FedRAMP?

FedRAMP requires that all assessments must be staffed by an appropriate number of 3PAO team members based on the complexity of the CSO being assessed. This 3PAO staffing includes, but is not limited to, individuals responsible for scanning, interviews, the examining of artifacts, and report writing. The 3PAO team must consist of at least three people from the 3PAO, who participate in and support the assessment, one of which is an individual considered to be the senior representative of the 3PAO, one of which is a penetration tester, and one of which is an individual dedicated to quality management of the 3PAO process.

The senior representative is responsible for ensuring the assessment activities and evidence is completed fully and meets the FedRAMP requirements and standards.

The penetration tester is responsible for ensuring the penetration testing is fully compliant with FedRAMP Penetration Test Guidance.

The individual dedicated to quality management is responsible for ensuring that all deliverables from the 3PAO meet the quality standards set forth by FedRAMP.

Any 3PAO who wishes to complete an assessment with less than three people must seek approval from the FedRAMP PMO. The senior representative must have the authority to sign off on the work of the other individuals who work on the project. During the onsite assessment by A2LA, the 3PAO must demonstrate the ability to meet the team staff requirements.

TIP: What are the basic FedRAMP requirements for 3PAOs delivering a security assessment report or a readiness assessment report?

All deliverables should be signed off by the 3PAO quality management lead before being delivered to a CSP or government authorizing official team. The quality review process for the 3PAO shall include checking all deliverables to ensure the following:

- There are no spelling or punctuation errors.
- All sections of each document delivered are complete, clear, concise, and consistent with each other.
- All team members of the assessment have reviewed the deliverables.
- Documents are prepared using the most recent standard templates, without alterations or deletions, and insertions must be agreed upon.

All SARs written by the 3PAO shall include an authorization recommendation on whether the system can appropriately safeguard government data in accordance with the security classification of the system. The recommendation shall include a summary statement and justification statement.

All SARs written by the 3PAO shall include all scan results in a readable format such that someone without a scanner license can read the results.

All RARs written by the 3PAO must adhere to the guidance within the FedRAMP High Readiness Assessment Report (RAR) template and the FedRAMP Moderate Readiness Assessment Report (RAR) template.

All RARs written by the 3PAO shall include analysis of results from activities including, but not limited to, discovery scans and in person interviews and physical examinations where appropriate. In the event that scan results are requested by the PMO, they should be retained in a readable format such that someone without a scanner license can read the results.

Q: What are the reporting expectations for the penetration test plan?

A: The SSP (and supporting documents) contain information that contributes to the reconnaissance/information gathering phase of the penetration test. This information includes the system and network architecture, inventory, ports, and protocols and services. The SAP should include tailored penetration test assessment steps (including manual steps) that are the unique result of evaluating the information in this documentation.

8. SYSTEM SECURITY PLAN (SSP) DOCUMENTATION

Q: How do I avoid making mistakes when creating/updating the System Security Plan (SSP) document?

For EVERY security control implementation:

1. Describe the solution implemented for this security control and how it meets the security control requirement.
2. Specify the person(s) responsible for implementing/enforcing the solution to this security control.
3. Describe how often (daily, weekly, monthly, quarterly, annually, etc.) this security control and its implementation are periodically reviewed.
    a. Be sure to include:
        i. Who performs the review.
        ii. What triggers a periodic review. Is it a specific date or event?
4. How are specified periodic reviews documented and what artifacts can prove this control is actively implemented and reviewed?
5. If a policy has been published and is referenced as the basis for the implementation of this security control, make sure that published document is provided as an attachment, or a supporting document with the SSP when submitted for FedRAMP review. This is especially true for inherited controls.
    a. Security control implementations can only be inherited (leveraged) from systems that have already been approved and granted a FedRAMP authorization.

Providing a complete response to the items above will greatly improve the likelihood of a successful review on the first submission.

Q: How can a 3PAO ensure high quality assessments and deliverables?

A: The FedRAMP PMO suggests 3PAOs to perform a peer review that asks the following questions to ensure high quality assessments and deliverables:

- Can the documented assessment steps (either described an/or as shown in the evidence files) be easily repeated by someone else?
- Did you perform an examination of the System Security Plan (SSP) or Policies & Procedures (P&P) when an examination of records was required?
- When a test was required, did you perform an interview or use the examine assessment method?
- Was an interview assessment method used when an examination/observation was required?

- Is a reason provided for performing a different assessment method than the one required (e.g. examine in lieu of a test)?
- Is evidence provided?
- Is the evidence specifically cited so it can be easily located?
- Is the evidence specifically cited or provided so that ISSO can verify that the sampling methodology (as described in the Security Assessment Plan) was followed?
- Do the observations and evidence discuss a different control than the control in the test case?
- Are the observations and evidence descriptions consistent with Findings column (found in the "Assessment Test Cases" template)?
- Do the Results show a Contingency Plan (CP) test was conducted?
- Do the Results show the CP test was a table-top exercise rather than a functional test?
- Do the Results show an Incident Response (IR) test was conducted?
- Do the Test cases include results of the vulnerability scans and penetration test?

Q: Does the FedRAMP PMO have file type requirements for documents submitted for review?

A: When submitting documentation to the OMB MAX Secure Repository for FedRAMP PMO Review, the System Security Plan (SSP) must be in Word format and unprotected. The FedRAMP PMO cannot properly conduct a formal review if documentation is in any other format. For concerns regarding this, please address them to the FedRAMP PMO at info@fedramp.gov prior to uploading documentation to MAX.

Q: Could you explain the interdependencies of controls within the System Security Plan (SSP)? Specifically, does having "N/A" for my System Security Plan (SSP) Access Control (AC)-17 for Remote Access have implications on other controls?

A: When creating the System Security Plan (SSP), understand that the plan tells the "story" of the system. While it may not be clear when you begin this task, the security controls are interrelated and have interdependencies. One of the most common issues unfolds when the SSP Access Control (AC) -17 Remote Access has "N/A" for the implementation detail. In our evolving technological world, all access to the system is now remote access. This control is interdependent with many other controls, specifically: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4. So if there is a misinterpretation of AC-17, chances are very good that the inter-related controls will also have issues.

Q: What is a security architecture diagram and what should it include?

A: A security architecture diagram is a component of the security architecture document, which illustrates how technical security controls are implemented in the environment. It also articulates the overall security program strategy in alignment with the position and selection of security control implementations. A security architecture diagram MUST be a stand-alone document and address the requirements outlined in the control supplemental guidance in PL-8, it is not sufficient to reference the SSP or outside product guides.

Architectural and network diagrams must include all possible communication links between the CSP and federal Agencies, as well as paths into the system boundary. If customers are not yet connecting directly, a CSP can identify all planned connection points in the SSP. Describing the architecture that will be offered can help ensure that it will be authorized before a customer needs it. The boundary diagrams should be completed prior to writing implementation statements.

Q: What are some tips to writing a detailed and accurate control implementation?

A: Think of each implementation as a little story. Always include who is responsible, how the control is implemented (be specific–get granular), and what components are affected.

Q: Should I repeat the control requirement?

A: Do not repeat the control requirement. Feel free to use it though as a jumping off point to write a detailed, specific implementation. Additionally, use the same action and key words within the control requirement when describing your implementation so it is clear exactly how the implementation meets the stated requirements.

Q: Why is it important to maintain consistency between the security control implementation statements and the technical diagrams?

A: The security control implementation statements provide a detailed explanation as to how compliance with NIST SP 800-53 and FedRAMP requirements are met. Generally, compliance is met with the implementation of technical components, policy/procedure, and other mechanisms. The Boundary, Network, and Data Flow diagrams provide a visual depiction of these components within the secure environment, so it’s very useful to reviewers to map control implementations to the specific components. Further, many controls are often satisfied with the implementation of the same components and are subject to security test and Continuous Monitoring to assure effectiveness. It’s important, therefore, that the implementation statements and the diagrams are consistent and accurate.

TIP: Avoid adding time to your authorization process by successfully completing the System Security Plan (SSP) review the first time! Here are some tips from the FedRAMP PMO on how to create a strong SSP:

“The Emergency Response Team shall resolve all problems within four hours of receiving a report. Once a problem is fixed, the response team lead documents the solution and sends the requesting team the correction report.”

1. Submit a complete and well-structured SSP.
2. Expertise and knowledge of NIST/FedRAMP security controls.
3. Enough resources – often one writer is not enough, and you may have to allot additional resources and subject matter experts to complete SSP.
4. Employ the four C’s of writing: Clear – straightforward, avoiding convoluted phrases or over-long phrases; Concise – pack the most meaning into your words; Concrete – concrete writing is precise and detail-oriented; and finally, Correct – correct grammar, mechanics, and format are baseline expectations for writing.
5. The writer(s) has knowledge of the system and/or can obtain the information from others and be able to communicate their technical knowledge.
6. Perform quality review on the SSP. Doing these things cannot guarantee a successful SSP review but will greatly enhance your chances.

Another writing tip: For the first control in each family (e.g. AC-1, AU-1 etc.), use the following as a checklist to ensure consistency among all of the “first” controls to ensure they contain the required information in the appropriate part.

Part A:

(1)

- Reference the policy document specifically
- Discuss how/where the policies are made available to personnel

(2)

- Reference the procedures document specifically
- Discuss how/where the procedures are made available to personnel

Part B:

- Identify frequency of review and update of policy
- Identify frequency of review and update of procedures

Note 1: If the policies and procedures are all in one document, there is no issue with referencing that document in both Parts a and b.

Note 2: Be aware that 800-53 Rev 4 reorganized these control requirements.

“Security Procedures” as defined by NIST in SP 800-12: “Procedures normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task (e.g. preparing new user accounts and assigning the appropriate privileges).”

Security Procedures generally explain how to perform a task such as a technical task or a business process.

Examples of procedures are:

- How To Create User Accounts
- How To Test Backups
- How To Authorize A User Account
- How To Perform Friendly Terminations
- How To Perform Unfriendly Terminations
- How To Lockdown a Windows 2012 Server
- How To Manually Turn On a Generator
- Standard Operating Procedures For Adding New Storage Arrays
- Media Sanitization Procedures
- Procedures For Adding Firewall Rules
- Procedure For Configuring Live Migrations of Virtual Machines
- How To Review a Log File for Suspicious Activity
- How To Configure Audit Storage Capacity Alerts
- How To Use Cron To Schedule Alerts
- How To Configure The Log Delivery Service
- How To Test The Contingency Plan

Q: All of the controls listed in the System Security Plan (SSP) do not apply to my system, so I only completed those that are applicable and left the others blank. Is it permissible to leave a control blank if it has not been implemented?

A: Every section within the SSP is required to have an answer – including each control. So simply leaving it blank is not permissible. You must list the control as “n/a” and any appropriate rationale as to why that control does not apply to your system. Very few controls are ever considered “not applicable.” The average FedRAMP CSP system has no more than a handful of controls that are truly not applicable and typically include controls involving “Wi-Fi” and “Mobile,” where these components are simply not used. However, there should be very limited or no controls listed as “not applicable” for technical controls such as AC, AU, IA and SC etc. CSPs must think of the system as a whole when determining applicability. If the control applies to the system in any way from the provider to the consumer, it is applicable. A provider must describe any portion the control that the provider is responsible for as well as any responsibilities of consumers. For example, for IA-2 (12), which requires multi-factor authentication for end users via PIV or CAC cards might not sound applicable for a CSP. Controls like this are tricky because a CSP usually doesn't work with end users at Agencies to issue PIV or CAC cards. However, CSPs are required to have the capabilities in place for end users to authenticate via PIV or CAC cards. In this case, instead of this control being not applicable, a CSP might describe how they accept SAML authentication mechanisms for the end user, and also the customer responsibilities related to PIV/CAC and SAML interactions with the CSP.

Q: There seem to be some inconsistencies in the System Security Plan (SSP) template. For example, the -1 controls do not have as many "checkboxes" as other controls. Am I allowed to alter or update the template to fit my needs?

The SSP template should not be altered by the CSP. For example, do not add "checkboxes" or make any other changes to the original template. Tables may be added, for example, but existing tables cannot be modified. The -1 controls do not have as many "checkboxes" as the other controls, and this is intended by the PMO. The tables are intended to be consistent across all FedRAMP SSPs to facilitate Agency customer reviews.

Q: How do policies and procedures differ from the System Security Plan (SSP)?

A: Policies and procedures are a critical supplement to the SSP and are required by the first control (known as the "dash ones," i.e. AC-1) for each control family. These documents are submitted with the SSP and provide the guidelines under which the procedures are developed and by which the SSP controls are implemented. Policies address what the policy is and its classification, who is responsible for the execution and enforcement of the policy, and why the policy is required. Procedures define the specific instructions necessary to perform a task. Procedures detail who performs the procedure, what steps are performed, when the steps are performed, and how the procedure is performed.

Q: I referenced a document in my System Security Plan (SSP) but did not provide the referenced document because it contains proprietary or sensitive information. How will this affect my review?

A: Every attempt should be made to prevent this situation. The assessment package should stand on its own without referencing documents that require complex retrieval, which can be confusing, time consuming, and cause delays in the assessment. In the rare circumstance this can't be avoided, you might add a statement that says, "The document is available onsite for review upon request or as required for audits and assessments."

Q: How should a cloud service provider (CSP) address platform scope within the System Security Plan (SSP)?

A: There are multiple platforms/platform groups in a system as identified by the inventory. A platform has certain controls (e.g., access controls, audit logging, session lock, etc.) configured uniquely for each device type. It is expected that unique implementations would be addressed by platform for the following controls/control families where applicable: AC, IA, AU, CM, SI-2, SI-3, SI-5, SI-11. We recommend using a standard format for addressing controls by platform (e.g., have a sub header within the control part/parts for "Cisco," "Brocade," etc.).

Q: How do I capture Customer Requirements in my security control implementation detail?

A: Please remember that clarity and consistency is key in security control implementation detail. Once the writer of the SSP makes a determination as to how the Customer Requirement is portrayed for one security control implementation detail, that same format should be used throughout the System Security Plan (SSP) for each control that has a Customer Responsibility requirement. We suggest that you begin the Customer Responsibility section in each security control implementation detail by framing "Customer Responsibility" or "Customer Responsibility Requirements" directly and stay consistent throughout the SSP.

Following the "Customer Responsibility" or "Customer Responsibility Requirements", clearly describe what the customer is expected to do. As the Cloud Service Provider (CSP), you do not have to describe how the customer implements the requirement. That description is the responsibility of each individual customer using your service offering. You must only describe that it is a Customer Requirement as based on the security control implementation. Make sure that all customer requirements in the SSP MATCH the Customer Requirements in the FedRAMP Control Implementation Summary (CIS) for SSP Low Moderate Baseline (CIS) benchmark and in the Customer Responsibility Matrix (CRM). Please note that this CIS template for the Low and Moderate Cloud Service Offerings is located on The FedRAMP website via this url: https://www.fedramp.gov/files/2016/07/A09-FedRAMP-CIS-Workbook-LM-Template-2016-06-20-v02-00.xlsx

The FedRAMP website also has a FedRAMP High Control Implementation Summary (CIS) Workbook template as it may apply to some systems.

Q: What are some common mistakes that arise when addressing Control Implementation statements?

A: There are several mistakes that CSPs encounter when drafting their Control Implementation statements. Some of those include:

- **Customer Responsibility:** The customer specific responsibility should be addressed explicitly and consistently (e.g. addressed under a "Customer Responsibility" heading). This is so customers know exactly what their responsibilities are with regard to meeting the control requirement exclusively or in partnership with the CSP.
- **Control Scope:** There are multiple platforms and device types in a system identified in the system inventory. At a minimum, each device type has (for instance) access controls, audit logging, and flaw remediation. Each device type may have those controls configured uniquely depending upon the location of the device within the defense-in-depth for the overall system risk management strategy. Unique configurations and implementations are addressed by device type and/or location in the security defense strategy for the system. This will normally affect the AC, IA, AU, CM, and SI control families. This means that the security control implementation details for those families and then the particular controls within the families have greater depth of detail required.
- Before attempting to populate the system security plan (SSP), it is recommended that one take a look at the overall system authorization boundary and all the devices and components within the boundary to understand what controls affect which devices and components. This mapping is called a Security Controls Requirements Matrix. Developing a matrix saves time in the long run when documenting the system via the SSP and it becomes easier to use a standard format for addressing controls by device or component (e.g., have a sub header within the security control implementation detail for "Cisco", "Brocade", “Windows”, “Linux”, and/or “Oracle”). Additionally, where applicable, each facility should be addressed including alternate, backup, and operational facilities.
- **Document References:** Policies and procedures as well as supporting documents should be explicitly referenced (title, date and version) so it is clear which is active.
  If the entire referenced document does not apply, specific sections references should be provided so the applicable sections can be located easily.
  The reviewer should not have to rely solely on following the references to understand the control implementation. An overview of what the referenced document addresses and direct relevancy to the control requirement should be provided so the SSP can stand on its own.

You can have a table at the end of the SSP that specifies all referenced documents, their title, date, and version. Then reference that table when a document is cited. This way you only have to maintain date and version in one place.

Q: Does FedRAMP provide a template for an Incident Response Plan?

A: Security Control IR-8 requires CSPs to develop an Incident Response Plan (IRP). The IRP is a required document within security authorization packages. FedRAMP does not provide a template for IRPs; however, NIST SP 800-61 Rev 2, Computer Security Incident Handling Guide, provides guidance on the development of Incident Response Policies and Procedures, as well as guidance on the development of an Incident Response Plan.

Q: Although the FedRAMP PMO does not provide a template for Contingency Plans and Incident Response Plans, is there any information that needs to be included?

A: For Contingency Plans and Incident Response Plans, it is helpful to include the following information:

- Name/Title of attendees
- Date and time of the exercise
- Description specific exercise
- Expected results
- Actual results
- Was the particular exercise successful?
- Who performed the specific part of the exercise?
- Lessons learned

For Low systems, a tabletop exercise is sufficient. For moderate and high systems, we require a functional exercise.

TIP: Incident Response plans must include the response time for Federal Agency Incident Categories.

Minimum response times are provided by US CERT at https://www.us-cert.gov/government-users/reporting-requirements. FedRAMP is especially concerned with the response time for CAT 1 incidents, unauthorized access. FedRAMP expects reporting of suspected unauthorized access within one hour of when the impacted customer Agency is identified. The CSP should not wait for a full analysis to be complete before reporting the suspected breach.

TIP: If a CSP's or Authorizing Official's information has changed, be sure to make these changes in the role section of the System Security Plan (SSP) immediately after the change.

There have been a lot of personnel changes in CSPs and Agencies. It's critical that CSPs update their SSPs to reflect these changes, as this is something that is vital, but often overlooked.

TIP: AC-2 and IA-2 are closely related.

Every group, account, or role defined in AC-2 must be explicitly addressed in IA-2. AC-2 is used to define the groups, accounts, and roles, who may be assigned to one, and how they are managed (approval process, creation & modification procedures, monitoring, etc.). IA-2 defines the authenticators used for each group, account, or role, as well as the types of access to the system utilized by these groups, accounts, and roles. Different roles or activities require differing strengths/levels of authentication. Each authentication mechanism and use case must be clearly documented to ensure complete and adequate coverage of authentication.

TIP: The System Security Plan (SSP) Boundary, Network, and Data Flow Diagrams should be as detailed as possible to clearly define the Authorization Boundary and services, as well as show major hardware and software components and interconnectivity.

Each component should also appear with the same description in the Hardware and Software Inventories. Deviation Requests and Plan of Action & Milestones (POA&Ms) that reference these components should include the same descriptions so that they are easily cross-referenced between documents. Data Flow Diagrams should identify where federal data is processed and stored and describe all data traffic in and out of the boundary. It is also necessary to describe data flow for privileged (such as systems administrators) and customer access and address ports, protocols and services for managing this traffic. This assures a much better mapping between documents and helps eliminate confusion.

Q: Can a CSP mark a control as both "Implemented" and "Alternative Implemented" in the System Security Plan (SSP)?

A: Usually not. If a control is fully implemented, then only the "Implemented" box is checked. If there is an "Alternative Implementation" or "Partial Implementation" of any component of the control, then either Alternative or Partial is selected as appropriate. As an example, there may be 2 types of Access Control methods: one for an administrator with elevated privileges that is fully "Implemented;" and the second access type is for non-privileged users that has an "Alternative Implementation." The CSP would only check the box for Alternative Implementation but explain the two implementations in the dialog box for that control. This is because during testing, the 3PAO will only determine whether the control is Implemented, Alternative Implementation, Partial Implementation etc., but no combination. Then, the 3PAO will determine if the control implementation is Satisfied or Other than Satisfied for the implementation type provided.

Q: Can shareware or freeware be an integral part of the operational infrastructure of a CSP?

A: Shareware and freeware products that are typically available for PC or mobile device usage are not permitted in FedRAMP environments.

Open Source (no product or support costs) products, however, are permitted from reputable sources where the CSP has control over the source and executable code. The product must be subjected to continuous monitoring functions and vulnerability remediation.

9. OTHER DOCUMENTATION – PLAN OF ACTIONS AND MILESTONES (POA&M), READINESS ASSESSMENT REPORT (RAR), SCANS, AND INFORMATION SYSTEM CONTINGENCY PLAN (ISCP)

TIP: When submitting the monthly Plan of Actions and Milestones (POA&M) spreadsheet, the findings on the spreadsheet must be reconciled each month with the scan results to ensure POA&M accuracy. This means that any items that have closed throughout the month should be marked as such and appropriate artifacts should be provided to validate closure.

All findings must be recorded on the open tab of the POA&M. A false positive (FP) vulnerability remains in the open tab until the deviation request (DR) is approved. An operationally required (OR) vulnerability remains on the open tab indefinitely and is only closed if the circumstances creating the OR are resolved, such as migration to a new technology. A vendor dependency also remains on the open tab indefinitely and is only closed once the CSP resolves the issue by applying a vendor approved fix or upgrade.

Q: Is the FedRAMP High requirement, in NIST 800-53 Identification and Authentication (1A)- 2(4), met by a second device (such as a smart phone) receiving a one-time password or must a hardware token (i.e. CAC/PIV) be used? The glossary seems to indicate they are equivalent as far as meeting the requirement, since the "Something You Have" category lists both.

A: The FedRAMP High baseline requires the use of FIPS Pub 201-compliant credentials – and PIVs/CACs meet this requirement. OMB Memo 11-11 requires federal Agencies to continue implementing the requirements specified in HSPD-12 to enable Agency-wide use of PIV credentials. Please see this link for more info:

http://www.nist.org/nist_plugins/content/content.php?content.49

The FedRAMP JAB has provided the following Guidance to CSPs on the subject:

- When first factor is Password, second factor must be one of the following:
- Look-up Secret – e.g., bingo card where you look up the OTP
- Out of Band – e.g., smart phone with secure communications protocol to receive OTP
- Single Factor OTP Device – e.g., RSA SecureID or OTP generator on CMDs
- Single Factor Cryptographic Device – e.g., digitally signed nonce using 'embedded' 'non-exportable' keys
- Email is not permitted for OTP
- SMS is not permitted for OTP

Q: What are the current vulnerability remediation timelines required to be FedRAMP Authorized?

A: The FedRAMP PMO does not differentiate between "Critical" and "High." However, FedRAMP requires mitigation of High-risk vulnerabilities within 30 days from discovery, Moderate-risk vulnerabilities within 90 days from discovery, and Low-risk vulnerabilities within 180 days from discovery.

Q: Our CSP client has data centers in multiple locations throughout the United States. As part of the Readiness Assessment Report (RAR), FedRAMP requires in-person interviews. Does visiting one data center satisfy FedRAMP's requirement, or do we need to visit each location?

A: Visiting data centers is a best practice to enable you to view the security at the facility first-hand as part of your verification and validation efforts. If a CSP has multiple data centers, you are not required to visit each one as part of the RAR effort; however, during the Security Assessment Report (SAR) phase, we expect the 3PAO to visit each data center to perform in-person interviews, review documents as necessary, and validate some of the controls. Most CSPs remotely manage their systems, and the 3PAO needs to validate that the security capabilities are actually in place.

Q: What is the purpose of an Information System Contingency Plan (ISCP)?

A: Each CSP must develop and maintain contingency plans to address operational disruptions. The contingency plan (and test results) provides management with an evaluation of the preparedness of the CSP's cloud service offering in the event of a major disruption and/or a catastrophic event. The contingency plan ensures that operations resume and are eventually restored to a known state. The ISCP and Service Level Agreements drive the recovery test frequency and complexity and recovery time frames. These contingency plans are a component of an effective security operations implementation.

Q: What types of databases are required to be scanned and how should they be tested?

A: The database scanning or manual testing requirements apply to all databases within the security boundary (i.e., those that reside/are embedded in a host/application as well as other databases). Databases that reside in a host (such as an appliance) need to be tested and may require the tester to work with the relevant vendor to ensure the appropriate security posture of the database that resides in a host is secure. If the databases are not accessible by the scanners, alternate methods of database testing (such as manual tests) should be explored. The host on which the databases reside should be scanned as part of the infrastructure scanning.

Q: What can a CSP do to prepare for penetration testing and what risks are involved?

A: The FedRAMP Penetration Testing Methodology is comprehensive and follows NIST SP 800-115. Before considering this activity, a CSP should work with a Third Party Assessment Organization (3PAO) assessment team to discuss the ramifications of utilizing the FedRAMP Penetration Testing Methodology. Both the 3PAO assessment team and the CSP must determine, in writing and prior to the onset of the testing, the level of risk they are willing to accept for the assessment and tailor the approach accordingly.

Once the parameters have been tentatively agreed upon, the 3PAO penetration tester and assessment team should begin the security assessment activities with a planning phase that includes gathering information about the CSP environment and developing the test procedures. Only after completing the planning phase should the 3PAO assessment team proceed to the execution phase.

During execution phase, the assessment team identifies vulnerabilities and validates that the vulnerabilities are not false positives. At the conclusion of the execution phase, the assessment team has a list of technical and process vulnerabilities. This list is used during the post-execution phase to determine root causes of vulnerabilities, recommend remediation actions, and document the test results in the Security Assessment Report (SAR).

Penetration testing risks can range from not gathering sufficient information on the organization's security posture for fear of impacting system functionality to affecting the system or network availability by executing techniques without the proper safeguards in place.

Communication and thorough understanding is key.

Q: What purpose does the Plan of Action & Milestones (POA&M) document serve?

A: The purpose of the POA&M is to facilitate a disciplined and structured approach to mitigating risks in accordance with the CSP's risk mitigation strategy. The POA&Ms include the findings and recommendations of the security assessment report and the continual security assessments. The POA&M identifies: (i) the tasks the CSP plans to accomplish with a recommendation for completion either before or after information system implementation; (ii) any milestones the CSP has set in place for meeting the tasks; and (iii) the scheduled completion dates the CSP has set for the milestones.

FedRAMP uses the POA&M to monitor CSP progress in correcting weaknesses or deficiencies noted during the initial assessment, annual security control assessment, and throughout the continuous monitoring process. The POA&M has columns labeled from A through Z which must be filled in for each row which is a uniquely identified vulnerability.

Use the FedRAMP's Plan of Action and Milestones (POA&M) Template to track and manage POA&Ms. *Please note that www.fedramp.gov is the official website from which to download FedRAMP templates.*

The POA&M workbook has two spreadsheets, the “Open” tab and the “Closed” tab. The Open POA&M spreadsheet includes known security weaknesses within the cloud information system. Open POA&M items must comply with the following:

- If a finding is reported in the Security Assessment Report (SAR) and/or in the continuous monitoring activities, the finding must be included as an item on the POA&M.
- False positives identified in the SAR (Appendices C, D, and E), along with supporting evidence (for example, clean scan report) do not have to be included in the POA&M.
- Each line item on the POA&M must have a unique identifier. This unique identifier must pair with a respective SAR finding and/or any continuous monitoring vulnerability.
- All high and critical risk findings must be remediated prior to receiving a JAB Provisional Authorization.
- High and critical risk findings identified following JAB Provisional Authorization through continuous monitoring activities must be mitigated within 30 days after identification.
- Moderate findings shall have a mitigation date within 90 days of JAB Provisional Authorization date or within 90 days of identification as part of continuous monitoring activities.
- The POA&M must be submitted in an appropriate format for the FedRAMP automated processes.

Q: What criteria must a Plan of Actions & Milestones (POA&M) document meet in order to accurately record the findings of the annual assessment Security Assessment Report (SAR)?

A: When recording the findings of the Annual Assessment SAR in the POA&M, a Cloud Service Provider (CSP) needs to ensure that they are utilizing the most current FedRAMP POA&M template available on the FedRAMP website. If the template has been updated since the last annual assessment, the CSP should update and transfer data and information to the latest version.

The Annual Assessment POA&M differs from the initial POA&M as the initial POA&M does not track POA&M items through the Continuous Monitoring process. If a CSP has an existing POA&M workbook that has been maintained since P-ATO, the POA&M is updated with all of the items from the Annual Assessment SAR. The findings in the SAR must exactly match the items recorded in the POA&M “Open” tab so that during the Third Party Assessment Organization (3PAO) assessment, a 3PAO can investigate and validate the status of any “Open” POA&M items.

The SAR must then accurately report all risk items that are still open (recorded on the "Open" tab of the POA&M), and then record any new items identified during the assessment. If a CSP has an existing POA&M that has been maintained since P-ATO, all the findings from the Annual Assessment needs to be appended to the POA&M in the “Open” tab. Until the SAR is JAB-approved, the new items derived from the Annual Assessment will be in a pending status, but are still valid risks identified by the 3PAO for the system. Once the SAR is approved, the CSP will reconcile the JAB approvals/concerns with what is in the existing POA&M. The updated POA&M is then the POA&M of record for the next monthly Continuous Monitoring cycle.

TIP: When submitting the monthly Plan of Actions and Milestones (POA&M) spreadsheet, the date at the top of the sheet (header) needs to be updated.

This date, along with dates from the individual scans provided by the CSP, is used by the Continuous Monitoring team as the reference point for different date-related issues/items in the POA&M. For example, any vendor dependency check-in dates listed in the POA&M will be referenced against the date in the header of the POA&M.

Missing or incorrect listings in that header could be considered as non-adherence to scanning requirements or non-compliant delivery of scan results (bad scans, bad POA&Ms, etc.) and result in a CAP.

Q: A service previously documented in the System Security Plan (SSP) was renamed. How do we reflect the name change when we submit a Deviation Request (DR) for a vulnerability that affects the renamed service?

A: Please provide a brief contextual description of the renamed service and reference its documented name in the SSP. This enables the reviewer to look up the service by its original name in the SSP.

Q: Are CSPs expected to maintain Continuous Monitoring activities while undergoing an annual assessment?

A: Yes. CSPs are expected to maintain Continuous Monitoring activities while undergoing an annual assessment, including timely remediation of POA&Ms and submission of monthly deliverables. FedRAMP does not allow exceptions for this.

TIP: When submitting a Significant Change Request (SCR), always discuss the change with your reviewer prior to submitting the form.

A CSP is often inclined to err on the side of caution and evaluate a change as significant when it may not be (or vice versa), and the reviewer can assist in this decision. Additionally, the reviewer will be able to assist the CSP with wording on the form, as well as the timing of when it is submitted. As an example, the reviewer may advise that a changed deemed as “significant”, requiring more extensive testing, may be done in conjunction with an upcoming Annual Assessment.

TIP: CSPs should be sure to include closure dates for Plan of Action & Milestones (POA&M) items even if they have been moved to the closed tabs.

Please be sure to include these dates boldly in the comment section. This provides a clear picture of the status of POA&M items.

TIP: When submitting the Annual Assessment (AA) package, the final Security Assessment Plan (SAP), Security Assessment Review (SAR), System Security Plan (SSP) and Plan of Action & Milestones (POA&M) documents must be submitted no later than the P-ATO anniversary date.

CSPs should plan carefully to ensure all documents are completed and submitted for the Annual Assessment no later than the P-ATO anniversary date. FedRAMP often receives partial packages (e.g. with only the SAP and SAR and not the SSP and POA&M). If FedRAMP does not receive a complete package (with documents in a final draft form) by the P-ATO anniversary date, the package is considered late and the CSP will be placed on a corrective action plan (CAP) in accordance with the FedRAMP P-ATO Management and Revocation Guide.

The POA&M provided must be updated to include the findings from the SAR. For the SSP provided, the NIST SP 800-53 controls in that SSP must be updated to match the status reflected in the SAR. The CSPs and 3PAO should allow for these POA&M and SSP update tasks in the annual assessment schedule.

TIP: In the "Description of Risk to the System" section of the Deviation Request, do NOT copy and paste the vulnerability description from the source.

It is necessary to explain the vulnerability within the context of the system and the potential risk should a threat exploit that vulnerability.

A vulnerability description from a scanner does not provide the description of risk presented to the system. The reviewers should be able to discern the risk presented. Reviewers can generally research the vulnerabilities themselves, but the CSP needs to provide the risk presented to the system.

TIP: Deviation Requests (DRs) should be submitted early enough for a reasonable expectation of approval before the initial expected remediation date.

DRs should not be submitted on or after the expected closure date of the Plan of Action & Milestones (POA&M). A DR for a High vulnerability should be submitted along with the initial POA&M listing the vulnerability, or at least before the next month’s PO&M submission. A Moderate risk adjustment should be submitted before the 3rd POA&M submission. Deviation requests that are submitted at the due date can demonstrate a reactive approach to security, rather than a proactive approach.

TIP: Deviation Requests (DRs) should be submitted early enough for a reasonable expectation of approval before the initial expected remediation date.

DRs should not be submitted on or after the expected closure date of the Plan of Action & Milestones (POA&M). A DR for a High vulnerability should be submitted along with the initial POA&M listing the vulnerability, or at least before the next month’s PO&M submission. A Moderate risk adjustment should be submitted before the 3rd POA&M submission. Deviation requests that are submitted at the due date can demonstrate a reactive approach to security, rather than a proactive approach.

TIP: When submitting a Microsoft Outlook, Gmail, or email from other messaging systems as evidence, ensure that it is captured in a common format such as a Microsoft Word file or Adobe PDF.

This helps to eliminate issues with dissimilar email systems. The preferred method is to avoid the use of email all together and use secure methods for transmitting and storing evidence.