

# 2015 **Tips & Cues**





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've received a lot of positive feedback about these posts and as an end of the year release, we've compiled every tip published this year for all of our readers.

We hope you'll use this tips compilation in the future and continue to look for more tips and cues from the FedRAMP PMO in 2016!

Happy Holidays,

A handwritten signature in blue ink, appearing to read "Matt Goodrich".

Matt Goodrich  
FedRAMP Director

# Contents

Continuous Monitoring	4
Federal Agency	6
General Program	8
Professional Writing Tips	11
Revision 4 Transition	15
SAP & SAR Documentation	19
System Security Plan (SSP) Documentation	22



# Continuous Monitoring



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?



Risk adjustments will typically be rejected when submitted as a remediation deadline approaches. Risk adjustments submitted after the remediation effort and/or costs are understood are generally viewed as an attempt to avoid non-compliance. This type of risk adjustment is rarely accepted and only with an exceedingly compelling justification.

Submit valid risk adjustments as soon as possible after a new vulnerability is discovered. You must show what has changed about the vulnerability or environment that now justifies a risk reduction.

 <https://www.fedramp.gov/?p=40372>



What is the procedure to submit a Continuous Monitoring (ConMon) High deviation request?



Any High Vulnerability Deviation Requests must be submitted to your ISSO via OMB MAX as soon as they are discovered. Please do not wait to submit as part of

your regularly scheduled Monthly ConMon Submission.

 <https://www.fedramp.gov/?p=26422>

# Federal Agency



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



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.

 <https://www.fedramp.gov/?p=26422>



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



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 standard.

 <https://www.fedramp.gov/?p=38332>



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 Federal Agencies?



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.

 <https://www.fedramp.gov/?p=37802>

# General Program



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?



No. FedRAMP only evaluates documentation for systems that exist and are operational. FedRAMP works with CSPs to provide Federal agencies with secure cloud computing options, so it is required that CSP's have an operational cloud system before engaging with the FedRAMP Team. If it is questionable

whether or not a CSP's system is operational while going through interviews with the FedRAMP PMO, a CSP may be asked to provide vulnerability scan results of their system to demonstrate operational capabilities.

 <https://www.fedramp.gov/?p=29882>



Your FedRAMP Information System Security Officer (ISSO) or government liaison are 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!

 <https://www.fedramp.gov/?p=41882>



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?



When preparing documentation for final submission to the JAB Technical Representatives-Rs, 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.

<https://www.fedramp.gov/?p=38332>



# Professional Writing Tips



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.”



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.

 <https://www.fedramp.gov/?p=26422>



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.

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.”

 <https://www.fedramp.gov/?p=27542>

Avoid using “etc.” If an item is important enough to be in a list, then it is important



Overly-long sentences are hard to understand and may cause confusion. They can leave out necessary information, which is not easily noticed.

Avoid sentences like “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.”

It is better to write short sentences that stick to a single idea through the use of bulleted lists:

“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.]”

 <https://www.fedramp.gov/?p=41882>



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.

 <https://www.fedramp.gov/?p=26912>



Writing in active voice is the best way to pass the FedRAMP PMO document acceptance criteria for readability, relevance, sufficiency, and consistency.

Here’s a special Halloween-edition writing tip from Grammarly:

If you can insert “by Zombies” after the verb and the sentence makes sense, then it is written in passive voice.

Passive	Active
The house was haunted <i>by zombies</i> .	Zombies haunt the house.
The town was attacked <i>by zombies</i> .	Zombies attacked the town.

 <https://www.fedramp.gov/?p=39522>

# Revision 4 Transition



How do I avoid making mistakes when updating the System Security Plan (SSP) from Revision 3 to Revision 4?



If you are updating your FedRAMP SSP from NIST 800-53 Revision 3 to Revision 4, watch out for controls where the content is the same but the information has been rearranged. For example, a control in Revision 3 may have moved Part A of that control to Part C in Revision 4.

If you want to easily see what has been changed, the PMO recommends performing Microsoft Word document comparison that analyzes the SSP by each control family. Follow these steps to perform a document comparison in Microsoft Word (this examples uses the Access Control (AC) family):

1. **Copy and paste Revision 3 AC family into a new document.**
2. **Copy and the Revision 4 AC family into a second document.**
3. **On the “Review” tab, click the “Compare” button.**
4. **On the drop-down list, choose Compare to compare the original Revision 3 AC to the Revision 4 AC edition.**
5. **Click “Ok” and you will see the changes between the two versions of the AC control family.**

It is important to compare the documents to avoid incorrectly inputting information or missing new requirements when transitioning from Revision 3 to Revision 4. Update your SSP according to the comparison.



<https://www.fedramp.gov/?p=42361>



Are there significant changes to Continuous Monitoring requirements for CSPs & 3PAOs under Revision 4?



Revision 4 Risk Assessment control (RA)-5 requires monthly Operating System (OS), Web Application, and Database scanning be performed and reported to FedRAMP. Under Revision 3, CSPs were only required to submit Web Application and Database scans quarterly and OS scans monthly. FedRAMP recommends that the scanning be performed as as soon as possible following system maintenance activities.

For RA-5(a), the FedRAMP Revision 4 Test Cases require a 3PAO to determine if its

CSP performs monthly scans of the system and hosted applications for vulnerabilities, and also when new vulnerabilities potentially affecting the system and/or applications are identified and reported. The 3PAO is also required to perform scanning for the initial assessment and at least annually. Those scans are submitted by the 3PAO as part of the Security Assessment Report (SAR), per the FedRAMP Continuous Monitoring Strategy Guide.



<https://www.fedramp.gov/?p=42361>



***Beginning January 1, 2016, the FedRAMP PMO will only accept materials aligned to the National Institutes of Standards and Technology (NIST) Revision 4 standards. My current System Security Plan (SSP) is written for Revision 3. In Revision 4, FedRAMP broke out many control requirements into separate requirements (or subparts).***

Can I copy and paste the Revision 3 control implementation into each of the subparts?



While it's important to provide complete implementation statements that address the "what, how and who," it is equally important to refrain from including extraneous information. Copying and pasting Revision 3 control implementation statements into the Revision 4 documentation will add potential additional information.

So it is best not to copy and paste in order to avoid this mistake. This will allow the reviewer to easily and quickly verify that the control requirement has been addressed, without having to sift through multiple paragraphs to find the answer.



<https://www.fedramp.gov/?p=40372>



When updating an System Security Plan (SSP) from Rev 3 to Rev 4, can a Cloud Service Provider (CSP) simply copy and paste?



Copying and pasting will not suffice for updating an SSP from Rev 3 to Rev 4. For example, NIST reorganized the “Policy and Procedures” control requirements for NIST SP 800-53 Rev 4. So all of the -1 controls for each control family must be updated and cannot be a simply copy and

paste from Rev 3 documentation when updating the SSP for the transition to Rev 4. You must read the control requirement and input a fully formed and original answer. CSPs should do this analysis for each control.

 <https://www.fedramp.gov/?p=28742>



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



The PMO is unable to evaluate authorization packages which 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**



<https://www.fedramp.gov/?p=37202>

# SAP & SAR Documentation



Can the Security Assessment Plan (SAP) and/or the Security Assessment Reports (SAR) templates be modified?



The SAP and/or the SAR template 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.



<https://www.fedramp.gov/?p=26912>



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



For any scan-related finding that was found during testing and corrected during testing, please make sure to include a targeted scan that reflects the vulnerabil-

ity as closed. Please provide these targeted scans as part of the final SAR deliverable that is submitted to FedRAMP.



<https://www.fedramp.gov/?p=37202>



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



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



<https://www.fedramp.gov/?p=27542>



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



For vulnerabilities that were fixed during testing, downgraded, operationally required or false positives, the 3PAO must provide compelling evidence in the form of artifacts and detailed rationale within the appropriate SAR tables to justify the

remediated status. Please reference the specific evidence file(s) and provide them with the SAR.



<https://www.fedramp.gov/?p=28092>



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



At the time the SAP is submitted to the ISSO 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.



<https://www.fedramp.gov/?p=29882>



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



When reporting the results of an assessment method (examines, interviews, and tests), ensure there is enough detail so

that the assessment method and result can be repeated by someone else.



<https://www.fedramp.gov/?p=28252>

# System Security Plan (SSP) Documentation



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



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.

 <https://www.fedramp.gov/?p=26912>



Should I repeat the control requirement?



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.

 <https://www.fedramp.gov/?p=27542>



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



The security control implementation statements that are described in the System Security Plan (SSP) must not only address National Institutes of Standards and Technology (NIST) Revision 4 and FedRAMP security requirements, but must also be incorporated in the technical diagrams (where applicable) for conformity and sound security engineering design.

Inconsistencies between the implementation statements and technical drawings are a red flag for JAB Technical Reviewers. The JAB Technical Reviewers will note this as a major finding to be corrected in the SSP, which may cause delays in your security assessment.

 <https://www.fedramp.gov/?p=26912>



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.



<https://www.fedramp.gov/?p=28252>



“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



<https://www.fedramp.gov/?p=28742>



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?



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. 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.

<https://www.fedramp.gov/?p=39522>





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.

 <https://www.fedramp.gov/?p=40582>



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



Policies and procedures are a critical supplement to the SSP. Policies are the guidelines under which the procedures are developed. 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.

 <https://www.fedramp.gov/?p=28092>



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



Referencing documents that contain proprietary or sensitive information without providing the actual documents could confuse the reviewer. The reviewer may have to stop, ask questions and clarify why this document is not available, which will slow down your review.

To avoid this slowdown, the PMO suggests you add a statement to this effect:

“The document is available onsite for review upon request or as required for audits and assessments.”

 <https://www.fedramp.gov/?p=37802>



How should a Cloud Service Provider (CSP) address platform scope within the System Security Plan (SSP)?



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.).

 <https://www.fedramp.gov/?p=28252>



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:

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.*

 <https://www.fedramp.gov/?p=29432>