FedRAMP® Review Initiation Checks (RIC)

Part 2: Post-Assessment

<Version ALPHA>

<2024-12-26>

info@fedramp.gov

fedramp.gov

TABLE OF CONTENTS

OVERVIEW

Optional FedRAMP Review Initiation Checks (RIC) help cloud service providers, independent assessors, and federal agency partners understand how FedRAMP evaluates and verifies the completeness, consistency, accuracy, and clarity of an authorization package. Following these checks properly will enable expedited review by FedRAMP and increase the likelihood of a smooth FedRAMP authorization process.

- **RIC Part 1** may be used by the cloud service provider to self-assess after the preparation of the System Security Plan but prior to the independent security assessment of the cloud service offering.

- **RIC Part 2** may be used by the cloud service provider to self-assess after the completion of the independent security assessment of the cloud service offering and after the preparation of the Security Assessment Plan and Security Assessment Report.

This document contains the RIC Part 2.

RIC PART 2

The RIC Part 2 checks are to be performed after the initial assessment has been completed and the Security Assessment Plan, Security Assessment Report, and corresponding artifacts have been produced. Each item within each check will generate one of the following results:

- Yes, indicating that this item is fully met
- No, indicating that this item is applicable but is not fully met
- N/A, indicating that this item does not apply (only an option for items in certain checks)

If any item within a check results in No, be aware that your cloud service offering may not be ready to have its package submitted to FedRAMP. Strongly consider addressing the deficiencies before continuing.

The appropriate personnel to perform the checks for a cloud service offering will vary by organization. All checks require a solid understanding of cybersecurity and the cloud service offering itself.

Some parts of checks are strictly editorial in nature – for example, ensuring that a file is present, a diagram is legible, or a plan contains all the sections specified by a template. These parts are labeled as [Editorial].

Check 5: SAR Breadth and Depth

The following checks are to be performed primarily on the SAR, with other documents mentioned specifically when needed.

Check 5A: Validation of N/A controls

1. If any controls are listed as N/A in the SSP, have they all been validated by the IA as being N/A?	☐ Yes ☐ No ☐ N/A

Check 5B: Validation of O&E and scan results for specific controls

Consult the Observations and Evidence (O&E) information for the specified assessment objectives and, where applicable, artifacts and vulnerability/compliance scan results to answer the following questions:

1. Regarding CM-6.a and CM-6.b: a. Did the IA specify the IT products that were validated to have configuration settings applied? b. Do the vulnerability/compliance scans validate that hardening is actually occurring on all production components?	☐ Yes ☐ No
2. Regarding CP-9: Do the O&Es describe how the IA validated that all parts of the controls are implemented correctly and operating as intended (versus simply echoing the control requirement)?	☐ Yes ☐ No
3. Regarding IA-2(6) [Rev. 5] or IA-2(11) [Rev. 4]: a. Do the O&Es describe how the IA validated that all parts of the controls are implemented correctly and operating as intended (versus simply echoing the control requirement)? b. If the IA issued a SAR finding because the MFA is not FIPS-validated or NSA-approved, is the remediation plan in the POA&M reasonable? For example, migrating from an MFA that is not FIPS-validated to a MFA that is FIPS-validated should not take a year.	☐ Yes ☐ No
4. Regarding IA-5, if the cloud service offering provides identity management as a part of the service offering, does the O&E describe all of the following? a. How authentication is implemented for cloud service offering access	☐ Yes ☐ No ☐ N/A

b. How AAL authentication is supported for customer deployment. In particular: i. The cloud service offering's capability to meet the requirements in item 1 of check 4L for each impact level. ii. The customer responsibilities for compliant configuration at each impact level. c. How IAL and FAL are supported for customer deployment (as appropriate) d. At least one compliant configuration exists for the capabilities described for items 5b and 5c of check 4L	
5. Regarding IA-8(1): Do the O&Es describe how the IA validated that the control is implemented correctly and operating as intended (versus simply echoing the control requirement)? *Validating that there is a PIV option on the application front-end is not sufficient.*	☐ Yes ☐ No
6. Regarding RA-5 and RA-5(5): Do the vulnerability scans validate the completeness and scope of the subnet range targets against the Inventory and SSP Ports, Protocols and Services table?	☐ Yes ☐ No
7. Regarding SC-7: Do the O&Es describe how the IA validated that the control is implemented correctly and operating as intended (versus simply repeating the control requirement)?	☐ Yes ☐ No
8. Regarding SC-13: a. Do the O&Es describe how the IA validated that the controls are implemented correctly and operating as intended (versus simply repeating the control requirement)? b. Do the O&Es discuss each flow (source to destination) that was reviewed and specify the associated FIPS-validated or NSA-approved cryptographic module (CM) (and its certificate number) that is encrypting that flow? c. For information traversing certain components (e.g., firewalls) that is being decrypted, do the O&Es validate that the same information that is de-encrypted is also re-encrypted by the same component and that FIPS-validated or NSA-approved CMs are in use? d. Do the O&Es discuss each data store that was reviewed and the associated FIPS-validated or NSA-approved CM that is encrypting that store? e. Do the vulnerability scans confirm that there are no findings around the use of insecure or non-FIPS approved cryptographic algorithms?	☐ Yes ☐ No

9. If the assessment result for any of the above assessment objectives is "Other than Satisfied," are all control failures documented as follows? o Rev. 4: If the control failure was corrected during testing, it was captured in SAR Section 5.1 (Risks Corrected During Testing). o Rev. 4: If the control failure was not corrected during testing, it was captured in the SAR RET with a corresponding item in the POA&M. o Rev. 5: If the control failure was corrected during testing, it was captured in the SAR RET on the “Risks Corrected During Testing” tab. o Rev. 5: If the control failure was not corrected during testing, it was captured in the SAR RET on the “Risk Exposure Table (RET)” tab, with a corresponding item in the POA&M.	☐ Yes ☐ No ☐ N/A

Check 5C: SAR Executive Summary text

NOTE: This check only applies to the FedRAMP Rev. 5 SAR Template.

1. Does the first paragraph of SAR Section 2 (Executive Summary) read as follows: “*This is an initial assessment SAR as required by FedRAMP. This SAR aggregates the results of the required FedRAMP security assessment of the <CSO Name> environment as recorded in the <CSO Name> SSP*”? [Editorial]	☐ Yes ☐ No ☐ N/A

Check 5D: Clear IA recommendation

NOTE: FedRAMP will not accept a package that includes a non-recommendation from the IA. If the IA has issued a non-recommendation, the cloud service provider must remediate the risks that led to the non-recommendation AND the IA must validate the remediations in order to get to a favorable recommendation before the package is submitted to FedRAMP for review.

1. For Rev. 5, review SAR Section 2 (Executive Summary). Regarding the recommendation: a. Does it use one of the "templated" statements provided in the “Executive Summary” section of the SAR? [Editorial] b. Is it NOT contingent on other factors? Does it NOT include caveats or qualifying/conditional statements?	☐ Yes ☐ No ☐ N/A
2. For Rev. 4, review SAR Section 7 (Authorization Recommendation). Regarding the recommendation: a. Does it use the "templated" language in the SAR? [Editorial]	☐ Yes ☐ No ☐ N/A

b. Is it NOT contingent on other factors? Does it NOT include caveats or qualifying/conditional statements?	

Check 5E: Penetration test report

NOTE: The penetration test report document may be uploaded separately to the secure repository if not embedded within the SAR. If embedded, it is in Appendix F for Rev. 5 and Appendix J for Rev. 4.

1. Does the penetration test report include testing of all of the attack vectors specified in the *FedRAMP Penetration Test Guidance*?	☐ Yes ☐ No
2. If an IA determined that a certain attack vector is not applicable, does the penetration test report clearly state the rationale for its exclusion from testing? For example, mobile application testing was not performed because there is no mobile application within the authorization boundary.	☐ Yes ☐ No ☐ N/A

Check 5F: SAR Risk Exposure Table (RET)

1. Is the RET template unaltered? [Editorial]	☐ Yes ☐ No
2. Does the RET account for all scan findings?	☐ Yes ☐ No

Check 5G: SAR consistency cross-checks

Instructions for Rev. 5

1. Do the number of findings and risk categories documented in SAR Section 2-2 (Summary of Risks That Remained Open at the Conclusion of this Assessment) match the number of findings and risk ratings documented in the RET? Filter on the specific columns in a variety of combinations in the RET to determine original and adjusted risk ratings, operational requirements (OR), and vendor dependencies (VD). For example: o In the RET, filter column L (“Adjusted Risk Rating”) to determine the number of findings for each risk-adjusted category (L, M, H).	☐ Yes ☐ No

o In the RET, filter column N (“Operational Requirements”) to determine the number of ORs findings by each original and risk-adjusted category (L, M, H).	
2. Are the findings captured consistently within SAR Appendix B? The values in the “System” tab and “CrtlSummary” tab are auto populated as each individual control family tab is completed. Perform the following spot checks to verify the formulas are calculating correctly: o On the “CrtlSummary” tab, filter column D (“Assessment Result”) by “Other than Satisfied”. The result should match the number in cell B11 of the “System” tab. o Cross-check a sampling of test results between the “System” tab, “CrtlSummary” tab, and individual control family tabs. For example, in the “AC” tab, filter column N (“Risk Exposure Level”) by Low, Moderate, or High. The result for each risk exposure level should match the AC Summary Risk Exposure Levels of the “System” tab.	☐ Yes ☐ No
3. Are findings captured consistently between the SAR Appendix B and the RET? Validate this by performing the following: o In the “CrtlSummary” tab, filter column D (“Assessment Result”) by “Other than Satisfied”. o In the RET, validate that the “Other Than Satisfied” items noted in the SRTM are in only one of the following tabs: ▪ In the “Risk Exposure Table (RET)” tab (if still an open risk), or ▪ In the “Risks Corrected During Testing” tab (if the risk was addressed and validated by the IA as corrected before the SAR was completed). o Verify consistency with other key concerns noted in the “CrtlSummary” tab such as Risk Exposure Level and SSP Differential. o If SSP Differentials are indicated ("1" in column F of the “CrtlSummary” tab), there should be a corresponding PL-2 finding(s) in the RET, if not listed in the “Risks Corrected During Testing” tab.	☐ Yes ☐ No
4. Are findings documented in the penetration test report included in the RET? o Penetration testing results are typically represented in the Weakness Detector Source as “Penetration Test” or “Manual Testing”.	☐ Yes ☐ No

Instructions for Rev. 4

1. Do the number of findings and risk ratings documented in SAR Section 7 (Authorization Recommendation) match the number of findings and risk ratings documented in both Table F-1 (Assessment Findings) and the RET? o In the RET, filter column N (Risk Exposure after Mitigating Controls / Factors) to determine the number of findings for each impact level (L, M, H).	☐ Yes ☐ No
2. Is the source of discovery (Assessment Test Cases, OS scans, etc.) in Table F-1 consistent with column C (Source of Discovery) in the RET? o In the RET, filter column C to determine the number of findings for each source (Assessment Test Cases, OS scans, etc.).	☐ Yes ☐ No
3. Is the RET consistent with Tables 5-2 and 5-3 in the SAR? o Compare Table 5-2 in the SAR to columns I through N in the RET for consistency. o Compare Table 5-3 in the SAR to column O for consistency. NOTE: The RET does not include a column for "Operational Requirements". IAs use column O (“Recommendation”) to document validated ORs.	☐ Yes ☐ No
4. Are the findings captured consistently within SAR Appendix B? The values in the “System” tab and “CtrlSummary” tab are auto populated as each individual control family tab is completed. Perform the following spot checks to verify the formulas are calculating correctly: o In the “CrtlSummary” tab, filter column D (“Assessment Result”) by “Other than Satisfied”. The result should match the number in cell B11 in the “System” tab. o Cross-check a sampling of test results between the “System” tab, “CrtlSummary” tab, and individual control family tabs. For example, on the “AC” tab, filter column N (“Risk Exposure Level”) by Low, Moderate, or High. The result for each risk exposure level should match the Access Control - Summary Risk Exposure Levels in the “System” tab.	☐ Yes ☐ No
5. Are findings captured consistently between the SAR Appendix B and the RET? o In the “CrtlSummary” tab, filter column E (“Assessment Result”) by “Other than Satisfied”. Each control finding must be documented in one of two places: ▪ In the SAR RET (if still an open risk), or	☐ Yes ☐ No

▪ In the SAR Table 5-1 (if the risk was addressed and validated by the IA as corrected before the SAR was completed). o Verify consistency with other key concerns noted in the “CrtlSummary” tab such as Risk Exposure Level and SSP Implementation Statement Differential. o If SSP Differentials are indicated ("Yes" in column G of the “CrtlSummary” tab), there should be a corresponding PL-2 finding(s) in the RET (if not listed in the SAR Table 5-1).	
6. Are the findings documented in the penetration test report included in the RET?	☐ Yes ☐ No

Check 5H: SAR and POA&M consistency cross-checks

1. Does the POA&M identifier track with the RET identifier for traceability? o Rev. 4: Use the RET identifier as the POA&M identifier or alternatively add the corresponding RET identifier to column Z (“Comments”) in the POA&M. o Rev. 5: IAs are instructed to use the cloud service provider-established POA&M identifier schema to assign a unique identifier to each RET item.	☐ Yes ☐ No
2. For each finding documented in the RET, is there at least one corresponding finding in the POA&M’s “Open” items tab?	☐ Yes ☐ No ☐ N/A
3. For risks corrected during testing, is there a corresponding finding in the POA&M’s “Closed” items tab? This must include all findings identified during initial testing and then validated as closed (i.e., "corrected") by an IA. o Rev. 4: Compare SAR Table 5-1 to the POA&M’s “Closed” items tab. o Rev. 5: Compare the RET’s “Risks Corrected During Testing” tab to the POA&M’s “Closed” items tab.	☐ Yes ☐ No ☐ N/A
4. Do POA&Ms associated with vulnerability findings map to the relevant IIW/vulnerability scan target components where the vulnerability was found?	☐ Yes ☐ No

Check 5I: Rationales for FPs, RAs, and ORs

Review the IA-provided rationales for validated false positives (FPs), risk adjustments (RAs), and operational requirements (ORs). For Rev. 5, see SAR Appendix A. For Rev. 4, see SAR Tables 5-2 and 5-3.

1. Does each RA include a description of the rationale for it and mitigating factors or compensating controls in place that reduce likelihood and/or impact of exploitation? o Adjustments from a High-risk rating to a Low-risk rating will be heavily scrutinized by FedRAMP and (in most cases) are NOT acceptable.	☐ Yes ☐ No ☐ N/A
2. An OR is a finding that cannot be remediated, often because the system will not function as intended or because a vendor explicitly indicated it does not intend to offer a fix to their product. Does each OR have a sufficient description of the rationale for it? o FedRAMP will not approve an OR for a High vulnerability; however, cloud service providers may mitigate the risk to enable it to be downgraded.	☐ Yes ☐ No ☐ N/A
3. Did the IA objectively validate with supporting evidence that claimed FPs were accurate? Was a well-established source (e.g., CISA VEX, vendor-supplied information) leveraged?	☐ Yes ☐ No ☐ N/A

Check 5J: Monthly ConMon deliverables

Review the monthly POA&M deliverable, monthly IIW deliverable, and monthly scan deliverables (OS/Network, Web, DB, and container) if the cloud service provider is responsible for vulnerability scans to answer the following questions:

NOTE: This check is only relevant if one or more months have passed since the independent assessment concluded.

1. Is the cloud service provider uploading ConMon deliverables on a monthly basis? This includes raw scan files and scan reports, an up-to-date inventory, and up-to-date POA&M.	☐ Yes ☐ No
2. Is the date of the POA&M accurate? The date is reflected in cell D3 of the POA&M's "Open" items tab.	☐ Yes ☐ No
3. Are POA&M items documented in accordance with the *FedRAMP POA&M Template Completion Guide*?	☐ Yes ☐ No
4. Is the cloud service provider tracking each unique vulnerability scan finding as an individual POA&M item? POA&M findings must be based on the scanning tool's unique vulnerability reference identifier. The cloud service provider may break a unique vulnerability into multiple POA&M items to track the vulnerability	☐ Yes ☐ No ☐ N/A

at a more granular level (e.g., a vulnerability that applies to different asset types that will be remediated in different ways); however, a cloud service provider must not group multiple unique vulnerabilities into a single POA&M item.	
5. Are VDs and DRs correctly captured in the POA&M? Are vendor dependencies being reviewed each month? Is there evidence that the vendor has announced concrete plans to issue a patch? The *FedRAMP CSP Authorization Playbook* (Section 5.1 - General POA&M Guidance) describes how to correctly capture VDs and DRs in the POA&M.	☐ Yes ☐ No ☐ N/A
6. Has the cloud service provider maintained the POA&M's "Scheduled Completion Date" in the template? The scheduled completion date is automatically populated based on the POA&M's "Original Detection Date" and risk rating. Cloud service providers must not modify the "Scheduled Completion Date" column. Any date changes should be reflected in the "Planned Milestones" or "Milestone Changes" column.	☐ Yes ☐ No
7. Does the POA&M indicate that the cloud service provider is consistently remediating risks for the cloud service offering within the FedRAMP remediation timeframes?	☐ Yes ☐ No
8. Do the scans cover the full breadth of the system inventory, including ports and protocols listed in the SSP and configuration validations?	☐ Yes ☐ No
9. Are the scans being performed with privileged access? Is the percentage of authentication failures under 10%?	☐ Yes ☐ No
10. Do the scans provide all necessary data fields?	☐ Yes ☐ No
11. Does the inventory and scans show consistency? For example, no added/removed components without significant change requests month over a month? o Investigate ports in the ephemeral ranges that are consistently open across multiple scans.	☐ Yes ☐ No
12. Do the configuration baselines drift from the initial SAR scans (or current baseline)?	☐ Yes ☐ No

13. Are all findings in the scan that reflect inadequate control implementation documented as manual POA&M findings in addition to the vulnerability finding (unsupported components are an SA-22 finding, insecure cryptographic algorithms are an SC-13 finding, etc.)?	☐ Yes ☐ No ☐ N/A

RIC ATTESTATION FORM

The RIC attestation form is illustrated here for informational purposes. The final version of this form to be completed and submitted as part of each package will be made available in an editable form outside of this document.

The [Federal Agency Name], [Cloud Service Provider Name], and [Independent Assessor Organization Name] attest that the checks from RIC Parts 1 and 2 have been completed and validated, and represent the *[Cloud Service Offering Name]* authorization package as accurately as possible. All failed RIC checks are documented and explained below as comments.

Agency Partner Comments: _____

CSP Comments: _____

IA Comments: _____

Agency Partner Representative: _____
Date: _____

CSP Representative: _____
Date: _____

IA Representative: _____
Date:_____

v1.4