FedRAMP® Review Initiation Checks (RIC)

Part 1: Pre-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 1.

RIC Part 1

The cloud service provider performs the Part 1 checks on the System Security Plan and related attachments/appendices prior to the initial assessment. 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 undergo an assessment or 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 1: Scope

The cloud service provider must perform an analysis of the Integrated Inventory Workbook (IIW), vulnerability scans, authorization boundary diagram (ABD), and the associated SSP sections to answer the following questions.

NOTE: For Rev. 5, see SSP Sections 8.1 and 9.1 and Appendix Q. For Rev. 4, see SSP Sections 9.2, 9.4, and 10.1.

1. Are all asset types (operating systems, web servers, container images, etc.) that are listed in SSP System Diagram and System Description reflected in the IIW?	☐ Yes ☐ No
2. Are raw vulnerability scan files provided in machine-readable format and with the following data fields? o IP Address o FQDN/hostname o Ports, Protocols, Services o Cryptographic modules o Unique detection identifier (tool-specific) o CVE identifier o Relevant CVSS score o CVSS temporal and environmental vectors o Original detection date	☐ Yes ☐ No
3. Are all components listed in the IIW targeted in the scans, and vice versa?	☐ Yes ☐ No
4. Are all ports (non-ephemeral/ephemeral), protocols, and services listed in the SSP Ports & Protocols Table in alignment with open ports found in the scans?	☐ Yes ☐ No
5. For Rev. 5, do IIW components match all listed cryptographic modules in SSP Appendix Q, and vice versa?	☐ Yes ☐ No ☐ N/A

Check 2: Visibility

The cloud service provider must perform an analysis of the IIW, vulnerability scans, and POA&M deliverables to answer the following questions:

1. Are the scans performed with elevated privileges (<10% authentication failure rate)?	☐ Yes ☐ No

2. Are Network, OS, DB, Web, Container, and SAST/SCA scans performed as applicable on all IIW components?	□ Yes □ No

Check 3: Governance

The cloud service provider must perform an analysis of the SSP (table where the System Owner, Model, and ISSO are identified) to answer the following questions.

NOTE: FedRAMP does not review packages for private clouds, grant a FedRAMP Authorized designation, or list private clouds on the FedRAMP Marketplace because the concept of "reuse" does not apply.

1. Is the deployment model for the service offering applicable to the agency's use and potential government data involved (public vs. government-only community)?	□ Yes □ No
2. If applicable, does the SSP annotate why "hybrid" was selected, and does this actually apply to the service offering based on the architecture?	□ Yes □ No □ N/A
3. Is the deployment model listed in the SSP the same as the cloud service offering's FedRAMP Marketplace listing?	□ Yes □ No
4. If the cloud service offering is listed as non-public, do the SSP and Access Control Policy document how customer restrictions are enforced via the sales pipeline?	□ Yes □ No □ N/A
5. Does the System Owner have the organizational authority to address risk for *all* components, processes, and people included in the scope of system policies (budget, resources, charter, etc.)?	□ Yes □ No

Check 4: SSP Front Matter and Attachments/Appendices

The cloud service provider must perform the following checks around the SSP front matter and attachments/appendices.

Check 4A: ISCP and CP test report

1. Does the package include an Information System Contingency Plan (ISCP)? [Rev. 5 - SSP Appendix G; Rev. 4 - SSP Attachment 6] [Editorial]	□ Yes □ No
2. Does the ISCP include a corresponding CP test report? [Rev. 5 - ISCP Appendix F; Rev. 4 - ISCP Appendix G] It may be included in the associated template, or it may be provided as a separate attachment. [Editorial]	□ Yes □ No
3. Does the ISCP use the FedRAMP ISCP Template associated with Revision 4 or Revision 5 (as appropriate)? Are all portions of the template present? (Information may be added to the template.) Have all sections of the template been completed? [Editorial]	□ Yes □ No
4. Is the CP test report from within the last 12 months? [Editorial]	□ Yes □ No
5. Does the CP test report include the parts (date, lessons learned, etc.) from the FedRAMP ISCP Template? Does the test indicate whether the cloud service provider is able to meet its RTO and RPO objectives?	□ Yes □ No

Check 4B: Rationale for N/A controls

Review the CIS Worksheet tab in the CIS/CRM workbook to quickly identify the controls that are marked N/A. [Rev. 5 - SSP Appendix J; Rev. 4 - SSP Attachment 9] If there are none, this check does not apply, so skip to the next check (check 4C).

Cloud service providers often misidentify controls as N/A when the capability exists but is not authorized for use per system policies. For example, many cloud service providers consider AC-2(2) to be N/A because temporary/emergency accounts are not used in the environment. FedRAMP considers this control to be applicable. In the AC-2(2) implementation statement, the cloud service provider should reference the policy that prohibits the creation of temporary/emergency accounts and describe any technical controls in place to prevent the creation of and/or audit unauthorized accounts.

1. For each control that is marked N/A, is a rationale provided in the corresponding control implementation statement in the SSP as to why the control is not needed? [Rev. 5 - SSP Appendix A; Rev. 4 - SSP Section 13]	□ Yes □ No
2. Are controls marked N/A only if they are not technically or functionally applicable to the system?	□ Yes □ No

Check 4C: Consistency between CRM and SSP

1. Do the control originations specified in the SSP Control Summary Information table match the CIS/CRM workbook entries? [Rev. 5 - SSP Appendix J; Rev. 4 - SSP Attachment 9]	☐ Yes ☐ No
2. Are customer responsibilities clearly delineated in the SSP control implementation statement from the cloud service provider's responsibilities?	☐ Yes ☐ No
3. Do controls address what the customer must do to fulfill their responsibilities for the control?	☐ Yes ☐ No
4. For controls that indicate a customer responsibility, is there a corresponding entry in the CRM within the CIS/CRM workbook that addresses every distinct use case (e.g., unique services or features) where customer responsibilities apply?	☐ Yes ☐ No
5. For controls inherited from other cloud service offering vendors, does the CRM match the vendors' CRM lists of inheritable controls?	☐ Yes ☐ No ☐ N/A

Check 4D: Diagram readability and consistency

The SSP's authorization boundary diagram (ABD), network diagram, and data flow diagram (DFD) are either included within the SSP [Rev. 5 - Section 8.1; Rev. 4 - Sections 9.2, 9.4, and 10.1] or are provided as separate attachments. Some cloud service providers choose to combine the ABD, network diagram, and DFDs into a single holistic diagram. This is acceptable.

1. For all these diagram(s), is the resolution fully legible, including all characters being clearly distinguishable? [Editorial]	☐ Yes ☐ No
2. If separate files are provided for diagrams, are all of the following true for each of those files? a. The file opens properly. [Editorial] b. The specific filename is referenced in the associated SSP section with versioning information. [Editorial] c. Each diagram within the separate file(s) has the same figure number corresponding with the figure number used in the SSP.	☐ Yes ☐ No ☐ N/A

d. All text within the diagrams is searchable. [Editorial]	

Check 4E: ABD and narrative consistency

This involves comparing the ABD to the narrative sections and tables within the SSP to identify any inconsistencies in documenting the services used by the cloud service offering.

Note: For Rev. 5, see SSP Sections 8.1 and 8.2, and Tables 6.1 and 7.1. For Rev. 4, see Section 9.2, Tables 8-3 and 11-1, and Control CA-3 in Table 13-3.

1. Are all flows to/from external services clearly depicted on the ABD?	□ Yes □ No
2. Are all services depicted on the ABD also explained in the narrative description? Are all services explained in the narrative description also depicted on the ABD?	□ Yes □ No
3. Is each external service identified either as FedRAMP Authorized or as lacking FedRAMP authorization?	□ Yes □ No
4. For each service identified as FedRAMP Authorized, does its name match the FedRAMP Marketplace naming convention?	□ Yes □ No □ N/A
5. For each transport service, is its destination depicted? Does supporting text describe the purpose of data delivered to its destination?	□ Yes □ No

Check 4F: External services with federal data/metadata

1. For each interconnected external service that stores/processes federal government data and/or metadata, is one of the following true? a. The external service is FedRAMP-authorized or FISMA-authorized at the same or higher impact level as the cloud service offering, based on the impact level (high, moderate, low) of federal government data and/or metadata that is stored/processed in the external service. b. The external service is either lacking a FedRAMP or FISMA authorization altogether OR is not authorized at the same or higher impact level, but there is a corresponding POA&M that describes the cloud service provider's plans to remediate the risk by moving impacted functionality to a FedRAMP or	□ Yes □ No □ N/A

FISMA authorized service at the same or higher impact level that describes mitigating factors that may reduce the risk.	

Check 4G: Architecture documentation content review

1. Are all data flows crossing the boundary depicted in the ABD and include the following? a. All customer and cloud service offering administrator access b. The flow of software releases from update services to production components (e.g., application updates or patches) c. Flows to the customer's site (e.g., access to agency's identity management service) d. Component-to-component flows o In general, depicting flows to groups such as VPCs is insufficient. o cloud service providers may make reasonable exceptions, such as depicting a single flow from a scanner going to a text box that describes the components accessed by the scanner (rather than a separate flow to each scanned component).	☐ Yes ☐ No
2. At a minimum, does the ABD depict access flows for the following? a. Customer users b. Customer administrators c. cloud service offering administrator to cloud service offering d. cloud service offering administrator to IaaS/PaaS console e. Non-human account access flows	☐ Yes ☐ No
3. Does access flow have a high-level depiction of MFA in the ABD?	☐ Yes ☐ No
4. Does a corresponding narrative description provide details about the ABD's access flows?	☐ Yes ☐ No
5. Do the ABD and narrative address the following? a. Authentication consistent with IA-5 (see Check 4L in RIC Part 1 and Check 5B in RIC Part 2). b. Authentication tokens must be generated by an identity provider (IdP) where:	☐ Yes ☐ No

i. The IdP is inside an authorized boundary, OR ii. The IdP authorization is at the same, or higher, impact level. c. Authentication tokens must be encrypted when passed through a browser.	
6. Does the ABD depict the alternate processing and storage site? Is there a corresponding narrative description? Are differences between alternate site configuration and primary site configuration depicted and described?	□ Yes □ No
7. In the network diagram, are all of the following true? a. Is the authoritative DNS server for external access to the cloud service offering (SC-20) depicted? b. Is the recursive DNS server for external access from the cloud service offering's boundary (SC-21) depicted? c. Is the recursive server inside a FedRAMP Authorized boundary? d. Are the connections from cloud service offering components to the recursive server trusted? e. Are subnets clearly depicted and consistent with SSP narratives, including SC-7 control description? f. Do subnets adhere to structures described in the FedRAMP Subnets White Paper, including publicly accessible components in separate subnets and operational and management components in separate subnets?	□ Yes □ No

Check 4H: Data flow documentation review

For the following checks, see SSP sections 8.1 and 8.2 (for Rev. 5) and 10.1 (for Rev. 4).

1. Are the DFD(s) consistent with their own narrative descriptions in the SSP and with relevant control descriptions (e.g., SC-8(1), SC-13, SC-28)?	□ Yes □ No
2. If multiple DFDs are used: a. Does each child diagram include a descriptive name that specifies what the particular diagram is depicting in relation to the parent diagram? b. Does the parent diagram indicate where a child diagram fits into the overall cloud service offering using the same descriptive name of the child diagram?	□ Yes □ No □ N/A
3. On the DFD(s), is the encryption status of all data in transit (data flows) and data at rest (data stores) clearly depicted as one of the following?	□ Yes □ No

a. Encrypted with FIPS-validated modules b. Encrypted without FIPS-validated modules c. Unencrypted data flows and stores	
4. On the DFD(s), do the flows to data stores include the following? a. All encryption in the management VPC b. Flows from management tools required for their work (log collection, scanning, etc.) c. Flows and stores associated with disk/block storage attached to compute components d. Flows and stores inside container environments	☐ Yes ☐ No
5. Are flows for backup and alternate processing sites shown on the DFD(s)?	☐ Yes ☐ No
6. Are network components where encryption can terminate (e.g., load balancers and firewalls) included on the DFD(s)?	☐ Yes ☐ No

Check 4I: CM-6 control narrative

Review the control narrative for CM-6. [Rev. 5 - SSP appendix A; Rev. 4 - SSP section 13]

1. Does it explicitly specify the IT products (e.g., database, operating system, web server) where configuration settings have been applied? For example, Solaris 11 SPARC STIG – Ver. 2, Rel 9. a. For Rev. 4, are all baseline configuration settings using at least CIS Benchmarks level 1 for all applicable components? b. For Rev. 5, are all baseline configuration settings using DoD STIGs for all applicable components?	☐ Yes ☐ No
2. Does it state that all relevant STIGs have been applied based on the core DoD Security Requirement Guides (SRGs) and corresponding Technology SRGs? (e.g., Application SRG, Network SRG, Operating System SRG, Policy SRG)	☐ Yes ☐ No

Check 4J: CP-9 control narrative

Review the control description for CP-9. [Rev. 5 - SSP appendix A; Rev. 4 - SSP section 13] NOTE: Data must be backed up and not "mirrored" or "replicated."

1. Does part (a) specify the user-level information that is being backed up, frequency and type of backups (at least daily incremental and weekly full), where backups are retained, and how many copies (at least three copies [one copy online])?	□ Yes □ No
2. Does part (b) specify the system-level information that is being backed up, frequency and type of backups (at least daily incremental and weekly full), where backups are retained, and how many copies (at least three copies [one copy online])?	□ Yes □ No
3. Does part (c) specify the system documentation that is being backed up, frequency and type of backups (at least daily incremental and weekly full), where backups are retained, and how many copies (at least three copies [one copy online])?	□ Yes □ No

Check 4K: IA-2 control narrative

Review the control description for IA-2(6) [Rev. 5] or IA-2(11) [Rev. 4]. [Rev. 5 - SSP appendix A; Rev. 4 - SSP section 13]

1. Is MFA used to authenticate into all privileged and non-privileged accounts within the authorization boundary?	□ Yes □ No
2. Is MFA used to authenticate at the first "hop" within the authorization boundary? For example, logging into the jump host, bastion host, server, management console, etc.	□ Yes □ No
3. Does MFA involve a separate device than the system being accessed? For example, using an authenticator app on a mobile device.	□ Yes □ No
4. Are the make and model (e.g., OTP, hardware token) of the MFA specified, as well as the FIPS-validated certificate number (if applicable)? a. If the MFA is included in a FedRAMP Authorized service, is the associated leveraged service referenced? (Doing so is sufficient.) b. If an NSA-approved product is used, is the source document listed for obtaining information related to the NSA approval?	□ Yes □ No
5. Are all modes of MFA access consistent with those depicted in the ABD?	□ Yes □ No

6. Does each have a tool (by vendor) and protocol level (e.g., PIV, OTP, Push) depiction of MFA?	☐ Yes ☐ No
7. Is PIV/CAC support indicated for all federal government personnel access?	☐ Yes ☐ No

Check 4L: IA-5 control narrative

1. Does each access mode meet authenticator requirements? o Low baseline, Rev. 5: MFA is required per the FedRAMP baseline. o Low baseline, Rev. 4: Single-factor is acceptable per NIST SP 800-63B AAL1. o Moderate baseline, Rev. 5 and Rev. 4: MFA is required per NIST SP 800-63B AAL2. o High baseline, Rev. 5: MFA is required per NIST SP 800-63B AAL3. Password and hard token OTP are no longer accepted. o High baseline, Rev. 4: MFA is required per NIST SP 800-63B AAL3. Password and hard token OTP will also be accepted.	☐ Yes ☐ No
2. Does each access mode meet phishing resistance requirements? o Low and moderate baselines, Rev. 5: Required for federal agency, contractor, and cloud service provider access. Must be an available option for public access. o Low and moderate baselines, Rev. 4: Not required. o High baseline, Rev. 5 and Rev. 4: Required.	☐ Yes ☐ No
3. Does each access mode meet FIPS 140 requirements for the authenticator and the verifier?: o Low baseline: Not required for authenticators. Required for verifiers. o Moderate baseline: Required for federal agency, contractor, and cloud service provider access. Not required for public access. o High baseline, Rev. 5: NIST SP 800-63 Rev. 3 is required until the final version of NIST SP 800-63 Rev. 4 is published and becomes effective. o High baseline, Rev. 4: A hard token is required with any FIPS 140 validation. FedRAMP will continue to accept FIPS 140 validated hard tokens.	☐ Yes ☐ No
4. Does each access mode meet SP 800-63B requirements (e.g., soft tokens acceptable for Moderate baseline, hard tokens required for High baseline)?	☐ Yes ☐ No

5. If the cloud service offering provides identity management as a part of the service offering, does the SSP control description include all of the following: a. How authentication is implemented for cloud service offering access b. How AAL authentication is supported for customer deployment. In particular: o The cloud service offering's capability to meet the requirements in item 1 of this check for each impact level o 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 this check	☐ Yes ☐ No

Check 4M: IA-8 control narrative

NOTE: This control applies regardless of whether the customer is or is not using PIV to access the service.

1. Does the SSP control narrative for IA-8(1) indicate that the back-end technical implementation supports an agency customer's use of PIV (e.g., can accept SAML assertions)? Does it include having a capability in place for accepting and validating PIV when coupled with a customer's identity provider (IdP)?	☐ Yes ☐ No

Check 4N: RA-5 control narrative

1. Does the control narrative for RA-5 indicate the vulnerability scanning tool(s) used, the frequency of scanning performed (at least monthly), and the types of components being scanned (at minimum, the network infrastructure components, operating systems, databases, web applications, and container images where used)?	☐ Yes ☐ No
2. Does the control narrative for RA-5(5) indicate that all of the vulnerability scans performed are via privileged or credentialed access?	☐ Yes ☐ No

Check 4O: SC-7 control narrative

1. Is a logical or physical (where applicable/appropriate) subnet structure in place consistent with the *FedRAMP Subnets White Paper*?	☐ Yes ☐ No ☐ N/A

2. For the management planes and the operations planes, are their publicly accessible components in a public subnet? Are their other components in a private subnet?	□ Yes □ No

Check 4P: SC-13 control narrative

Review the control description for SC-13 to answer the following for all components within the authorization boundary:

1. For each data-in-transit (DIT) flow traversing the boundary (e.g., administrator and user access, APIs, and updates) or inside the boundary (e.g., VPC to VPC, server to server, access to IaaS/PaaS services, and backups to storage), is one of the following true? a. The flow is encrypted by FIPS-validated or documented NSA-approved cryptographic modules (CMs). b. The flow is encrypted through the appropriate technical implementation of a FedRAMP Authorized service and completion of appropriate customer responsibilities (e.g., the use of FIPS endpoints). c. The flow is encrypted by CMs that are not FIPS-validated or NSA-approved, but these CMs are documented in the POA&M.	□ Yes □ No
2. For each area of data-at-rest (DAR) (e.g., residing in databases, logs, backups, and storage), is one of the following true? a. The data-at-rest is encrypted using FIPS-validated or documented NSA-approved CMs. b. The data-at-rest is encrypted through the appropriate technical implementation of a FedRAMP Authorized service and completion of appropriate customer responsibilities (enabling encryption on the database, etc.) c. The data-at-rest is encrypted by CMs that are not FIPS-validated or NSA-approved, but these CMs are documented in the POA&M.	□ Yes □ No

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