# READ ME for the Agency ATO Review Template

Below is the template that the FedRAMP Program Management Office (PMO) uses when reviewing an Agency ATO package.

Agencies and CSPs should be cautious to not overly focus on these questions as FedRAMP PMO reviewers also spot-check other areas for compliance.

Any questions on this can be forwarded to info@fedramp.gov.

# Agency ATO Report

#N/A

| | | | |
|---|---|---|---|
| **FedRAMP Review for:** | **(select CSP)** | | |
| **Recommendation:** | **(select action)** | **Date:** | MM/DD/YYYY |
| **NIST SP 800-53 Revision (Rev 3 or Rev 4):** | **(select)** | **Deployment Model:** | **(select)** |
| **Document Versions Reviewed:** | **SSP (vx.x MM/DD/YY), SAP (vx.x MM/DD/YY), SAR (vx.x MM/DD/YY) and POA&M (vx.x MM/DD/YY)** | | |
| **Assessor (3PAO or Agency Selected):** | **(enter assessor info)** | | |
| **Service Model:** | **(select)** | **System Categorization:** | **(select)** |

## Section A: Executive Summary

*The purpose of this report is to summarize the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office's (PMO) analysis of the <CSP and Package Name> security package. The intended audience for this report is the initial partnering agency (<INSERT AGENCY NAME=XXX>) and any Agency that is considering use of this cloud service.*

*The FedRAMP PMO reviewed the <PACKAGE NAME> security package, including the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Results (SAR), Plan of Action and Milestones (POA&M), and all attachments. Based on this analysis, the FedRAMP PMO has determined that this package is <acceptable for any Agency considering authorization of the cloud service>.*

*[For FedRAMP Authorized Packages] Agencies reviewing this package should consider the following items of note:*
*<numbered list>*

*[For FedRAMP Authorized Packages that we want to encourage continued improvement of package -- add below statement]*

*As part of normal review/update efforts, the CSP should develop and implement a Continuous Monitoring Plan <if missing> and address the recommendations within this report, or as directed by the Partnering Agency. In consideration of the items addressed in this report, the CSP should review and update its security documentation for similar errors and omissions.*

## Section B: Documents Provided Check

| # | Description | Provided? |
|---|---|---|
| 1.0 | Initial Authorization Package Checklist | ---- |
| 2.0 | System Security Plan (SSP)* | |
| 2.1 | Att. 1: Information Security Policies & Procedures* | ---- |
| 2.2 | Att. 2: User Guide | ---- |
| 2.3 | Att. 3: Electronic Authentication (E-Authentication) Plan* | ---- |
| 2.4 | Att. 4: Privacy Impact Assessment (PIA) | ---- |
| 2.5 | Att. 5: Rules of Behavior (ROB) | ---- |
| 2.6 | Att. 6: Information System Contingency Plan (ISCP)* | ---- |
| 2.7 | Att. 7: Configuration Management Plan (CMP)* | ---- |
| 2.8 | Att. 8: Incident Response Plan (IRP)* | ---- |
| 2.9 | Att. 9: Control Implementation Summary (CIS) Workbook | ---- |
| 2.10 | Att. 10: Federal Information Processing Standard (FIPS) 199 Categorization | ---- |
| 2.11 | Att. 11: Separation of Duties Matrix | ---- |
| 2.12 | Att. 12: Laws and Regulations | ---- |
| 2.13 | Att. 13: Integrated Inventory Workbook | ---- |
| 3.0 | Security Assessment Plan (SAP)* | ---- |
| 3.1 | App. A - Security Test Case Procedures | ---- |
| 3.2 | App. B - Penetration Testing Plan and Methodology | ---- |
| 3.3 | App. C - 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement and Sampling Methodology) | ---- |
| 4.0 | Security Assessment Report (SAR) * | ---- |
| 4.1 | App. A - Risk Exposure Table | ---- |
| 4.2 | App. B - Security Test Case Procedures | ---- |
| 4.3 | App. C - Infrastructure Scan Results | ---- |
| 4.4 | App. D - Database Scan Results | ---- |

| | | |
|---|---|---|
| 4.5 | App. E - Web Application Scan Results | ---- |
| 4.6 | App. F - Assessment Results | ---- |
| 4.7 | App. G - Manual Test Results | ---- |
| 4.8 | App. H - Documentation Review Findings | ---- |
| 4.9 | App. I - Auxiliary Documents | ---- |
| 4.10 | App. J - Penetration Test Report | ---- |
| 5.0 | Plan of Action and Milestones (POA&M)* | ---- |
| 6.0 | Continuous Monitoring Plan (ConMon Plan) | ---- |
| 7.0 | ATO Letter | ---- |
| **Other Comments:** | | |

**Key:** ✔ = Doc provided ✖ = Doc not provided * Key Doc (Agency review only)

## Section C: Overall SSP Checks

| # | Description | Yes/No | Comments |
|---|---|---|---|
| 1 | Do all controls have at least one implementation status checkbox selected? | ---- | |
| 2 | Are all critical controls implemented? | ---- | *List critical controls not implemented; check the control to validate implementation, not only that the "Implemented" checkbox was selected.* |
| 3 | Are the customer responsibilities clearly identified (by checkbox selected and in the implementation description)? | ---- | *Sample a few critical controls - there should be clear control implementation text about customer responsibilities; sometimes there are separate "Customer Responsibility" subsections.* |
| 4 | Does the Roles Table (User Roles and Privileges) sufficiently describe the range of user roles, responsibilities, and access privileges? | ---- | |
| 5 | In the control summary tables, does the information in the Responsible Role row correctly describe the required entities responsible for fulfilling the control? | ---- | |
| 6 | Was the appropriate e-Authentication Level selected? | ---- | *Level 3 is required for Moderate-impact systems; Low-impact systems may be Level 2 or Level 3.* |
| 7 | Is the authorization boundary explicitly identified in the network diagram? | ---- | |
| 8 | Is there a data flow diagram that clearly illustrates the flow and protection of data going in and out of the service boundary and including all traffic flows for both internal and external users? | ---- | |
| 9a | If this is a SaaS or a PaaS, is it "leveraging" another IaaS with an ATO? | ---- | |
| 9b | If 9a is Yes, are the "inherited" controls clearly identified in the control descriptions? | ---- | |

| | | |
|---|---|---|
| 10 | Are all required controls present? | ---- |
| 11 | Is the inventory provided in the FedRAMP Integrated Inventory Workbook? | ---- |

**Other Comments:**

*Reviewer: Include stats on control implementation status: "Control implementation status: xxx - Implemented, xx - Alternative Implementation, xx - Partially Implemented, xx - Planned, and xx - Not Applicable." Unusual stats, such as more than 11 N/As require a note in exec in Exec Summary such as " Twenty-two controls are indicated as N/A; the selection of N/A controls should be judicious and include solid rationale." (or similar wording).*

*Additional considerations: Service model and deployment model -- does the Service model make sense for the deployment model selected? If the CSP indicates "Public" cloud is it deployed to a cloud that allows public access (i.e., not Government only IaaS)?*

## Section D: SSP Critical Control Checks

| Control | Control | Yes/No | Comments |
|---|---|---|---|
| AC-2 | Account Management | ---- | |
| AC-4 | Information Flow Enforcement | ---- | |
| AC-17 | Remote Access | ---- | |
| CA-1 | Security Assessment and Authorization Policies and Procedures | ---- | |
| CM-6 | Configuration Settings | ---- | |
| CP-7 | Alternate Processing Site | ---- | |
| CP-9 | Information System Backup | ---- | |
| IA-2(1) | Identification and Authentication (Organizational Users) - network access to privileged accounts. | ---- | |
| IA-2(2) | Identification and Authentication (Organizational Users) - for Network Access to Non-privileged Accounts | ---- | |
| IA-2(3) | Identification and Authentication - Local Access to Privileged Accounts | ---- | |
| IA-2(11) | Identification and Authentication - Acct. Mgmt. Separate Device Authentication | ---- | |
| IA-2(12) | Identification and Authentication - Acct. Mgmt. PIV Verification | ---- | |
| IR-8 | Incident Response Plan | ---- | |
| RA-5 | Vulnerability Scanning | ---- | |
| RA-5(5) | Vulner. Scan. - Privileged Access Authorization | ---- | |
| RA-5(8) | Vulner. Scan. - Historic Log Review for High Vulnerabilities | ---- | |
| SA-11 | Developer Security Testing and Evaluation | ---- | |
| SA-11(1) | Developer Security Testing and Evaluation - Code Analysis | ---- | |
| SC-4 | Information in Shared Resources | ---- | |

| | | |
|---|---|---|
| SC-7 | Boundary Protection | ---- |
| SC-13 | FIPS-validated or NSA-approved Cryptography | ---- |
| **Other Comments:** | | |

## Section E: SAP Checks (for CSP and Agency Reviews)

| # | Description | Yes/No | Comments |
|---|---|---|---|
| 1 | FedRAMP SAP template used, including all sections? | ---- | |
| 2 | Security Assessment Test Cases present? | ---- | |
| 3a | Rules of Engagement present? | ---- | |
| 3b | Penetration Test Plan present (may be combined with Rules of Engagement)? | ---- | |
| 4 | Is there an inventory of items to be tested? | ---- | |
| 5 | If a sampling methodology was used for technical testing, was the sampling methodology/plan described? | ---- | |
| **Other Comments:** | | | |

## Section F: SAR Checks (for CSP and Agency Reviews)

| # | Description | Yes/No | Comments |
|---|---|---|---|
| 1 | FedRAMP SAR template used, including all sections? | ---- | |
| 2 | Are risks documented? | ---- | |
| 3 | Was evidence provided, or was there a statement that evidence can be provided upon request? | ---- | |
| 4 | Completed Security Assessment Test Cases present and in accordance with FedRAMP template? | ---- | |
| 5 | Security scan results present? | ---- | |
| 6 | Penetration Test Report present and consistent with the SAR? | ---- | *Is the date within one year of the date of the SAR?* |
| 7 | Are deviations from the SAP documented? | ---- | |
| 8 | Does the 3PAO provide an attestation statement or recommendation for authorization? | ---- | |

| | | |
|---|---|---|
| 9 | Are there zero High findings identified in the SAR? If there are any high findings, provide number and comments. | ---- |
| 10 | Are the numbers of risks/findings consistently stated within the SAR, where appropriate? | ---- |
| 11 | Are the inventory lists within the SAR and SSP consistent? | ---- |

**Other Comments:**

*Reviewer: Include stats on # high, Mod, and Low risks; and # risks downgraded (by level) due to mitigating factors*

## Section G: POA&M Checks (for CSP and Agency Reviews)

| # | Description | Yes/No | Comments |
|---|---|---|---|
| 1 | Is the POA&M in the FedRAMP POA&M template? | ---- | |
| 2 | POA&M consistent with SAR Risk Exposure Summary Table | ---- | |
| 3 | Is there an inventory, either in a POA&M Inventory Tab, or in the SSP? | ---- | |

**Other Comments:**



## Section H: Additional Comments