<u>README for the Agency ATO Review Template</u>

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

Package ID:

FedRAMP Review for:	**(select CSP)**		
Recommendation:	**(select action)**	**Date:**	MM/DD/YYY
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)**		
Service Model:	**(select)**	**System Categorization:**	**(select)**

Section A: Executive Summary

Section B: Documents Provided Check

#	Description	Provided?
1.0	System Security Plan (SSP)*	----
1.1	FIPS Pub 199*	----
1.2	e-Authentication*	----
1.3	Information System Security Policies & Procedures*	----
1.4	Configuration Management Plan (CM) Plan*	----
1.5	Control Implementation Summary (CIS) Worksheet	----
1.6	IT Contingency Plan (CP) and CP Test Report*	----
1.7	Incident Response Plan (IRP)*	----
1.8	Privacy Threshold Analysis (PTA) / Privacy Impact Assessment (PIA)	----
1.9	User Guide	----
1.10	Rules of Behavior (ROB)	----
2.0	Security Assessment Plan (SAP)*	----
3.0	Security Assessment Report (SAR)*	----
4.0	Plan of Action and Milestones (POA&M)*	----
5.0	ATO Letter (only required for Agency Review)	----
6.0	Continuous Monitoring Plan (ConMon Plan)	----

Other Comments:

Agency ATO Report

Package ID:

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?	----	
3	Are the customer responsibilities clearly identified (by checkbox selected and in the implementation description)?	----	
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?	----	
7	Is the authorization boundary explicitly identified in the network diagram?	----	
8a	If this is a SaaS or a PaaS, is it "leveraging" another IaaS with an ATO?	----	
8b	If 8a is Yes, are the "inherited" controls clearly identified in the control descriptions?	----	
9	Are all required controls present?	----	

Other Comments:

Agency ATO Report

Package ID:

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:

Agency ATO Report

Package ID:

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	Does the test plan include sampling of components for technical testing?	----	

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?	----	
7	Are deviations from the SAP documented?	----	

Agency ATO Report

Package ID:

8	Does the 3PAO provide an attestation statement or recommendation for authorization?	----
9	Are there any High findings identified in the SAR? If so, provide number and details.	----
10	Are the numbers in the Risk Exposure Table and the Executive Summary consistent?	----

Other Comments:

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