U.S. DEPARTMENT OF ENERGY

Department of Energy (DOE) FedRAMP Agency Authorization Process Guide



September 2023

Version 1.2

Controlled Unclassified Information
May be exempt from public release under
the Freedom of Information Act (5 U.S.C. 552),
Exemption number and category: 7
Name/Org: Cybersecurity Compliance and Oversight, IM-32
Date: September 2023
Guidance: N/A

Document Revision History

Date	Version	Page(s)	Description	Author
03/26/2020	V1.0	All	Initial Publication	OCIO, IM-32
11/17/2022	V1.1	3, 5	Minor Updates	OCIO, IM-32
08/30/2023	V1.2	All	Major uplift to the entire document	OCIO, IM-32

Signatures of Approval

I have reviewed this FedRAMP Agency Authorization to Operate (ATO) Guide for the Department of Energy and concur that the information presented in this document is true and accurate to the best of my knowledge.

Approved by: William R. Wright Digitally signed by William R. Wright Date: 2023.08.30 16:18:46 -04'00' _____

William Wright
Security Control Assessor

Date

Approved by: Ignatius P. Liberto Digitally signed by Ignatius P. Liberto Date: 2023.08.31 12:22:40 -04'00' _____

Ignatius Liberto
Authorizing Official Designated Representative

Date

Table of Contents

1. Introduction

Agencies are required under the *FedRAMP Authorization Act* as part of the National Defense Authorization Act (NDAA) to protect federal data stored within the cloud. This is done by authorizing cloud services that demonstrate their compliance with one of the Federal Risk and Authorization Management Program (FedRAMP) security baselines. FedRAMP provides a standardized approach to security authorization in accordance with Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) security requirements. One of the goals is to prevent Agencies from reinventing the wheel; a "do once, use many", approach which promotes re-use of security assessments to save Agencies time and resources. FedRAMP facilitates collaboration across the federal government. It provides guidance and support to help Agencies through the authorization process.

The FedRAMP Authorization Act codifies the FedRAMP program as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information. The FedRAMP Authorization Act aims to improve FedRAMP by streamlining the approval process for Cloud services and by allowing agencies to rely on previous approvals from other agencies[1].

1.1 Purpose

As Federal agencies move to the cloud, all cloud services are required under the *FedRAMP Authorization Act* to demonstrate their compliance with one of the FedRAMP security baselines. The desired cloud service may have not yet been authorized by FedRAMP, particularly those that are Software as a Service (SaaS)[2]. In such cases, when an alternative already-authorized cloud service is not available, an option is for the site to request the vendor's cloud service be sponsored by the Department of Energy (DOE) for a FedRAMP Agency Authorization to Operate (ATO). The Office of the Chief Information Officer (OCIO) serves as the sponsoring organization for FedRAMP for DOE, with the Chief Information Security Officer (CISO) serving as the Department's sponsoring and Authorizing Official (AO). This process leverages and incorporates by reference, the FedRAMP Agency Authorization Playbook process found at : https://www.fedramp.gov/assets/resources/documents/CSP_Authorization_Playbook_Getting_Started_with_FedRAMP.pdf

1.2 Scope

Any DOE organization may request and/or recommend a FedRAMP Agency ATO and coordinate that activity with the DOE CISO through this Process.

1.3 Key Points

All cloud services used by DOE organizations must have a FedRAMP ATO or at a minimum demonstrate their compliance with one of the FedRAMP security baselines in accordance with the *FedRAMP Authorization Act*.

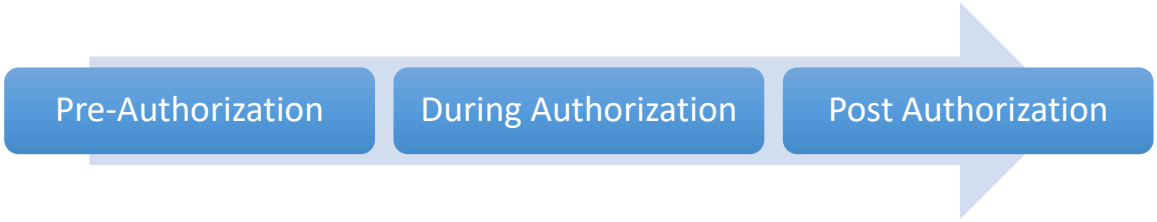
DOE OCIO is the sponsoring organization and the CISO and the principal deputy Chief Information Officer are the sponsoring officials for all FedRAMP Agency ATOs performed by DOE.

[1] FY23 National Defense Authorization Act (NDAA) (See Sec. 5921, page 1055).

[2] OMB Security Authorization of Information Systems in Cloud Computing Environments Memo; Dec. 2011.

If a DOE organization needs to use a cloud service that is not yet authorized, it may request DOE sponsorship through the OCIO Cybersecurity Compliance and Oversight Office.

2. FedRAMP Step by Step Guidance for Agency Authorization



A FedRAMP Agency ATO process includes 3 main steps: pre-authorization, during authorization, and post authorization [3]. The details of each step are outlined below.

2.1 Pre-Authorization

The pre-authorization process is broken down into 2 steps: partnership establishment and authorization planning.

Step 1: Partnership Establishment (~1-2 weeks)

- **Agency selects a Cloud Service Offering (CSO) that will meet the mission needs.**
- **Establish working relationship with the Cloud Service Provider (CSP), FedRAMP Program Management Office (PMO), and other relevant Agencies.**
- **Confirm the CSP's dedication to taking on the FedRAMP authorization process.**
- **Clearly outline the level of effort involved in the authorization process and the Agency's specific requirements.**
- **As soon as a CSO is selected, send an email to info@fedramp.gov advising of the intent to authorize the selected CSO in accordance with FedRAMP's "In Process" Requirements.**

Step 2: Authorization Planning (~4 weeks)

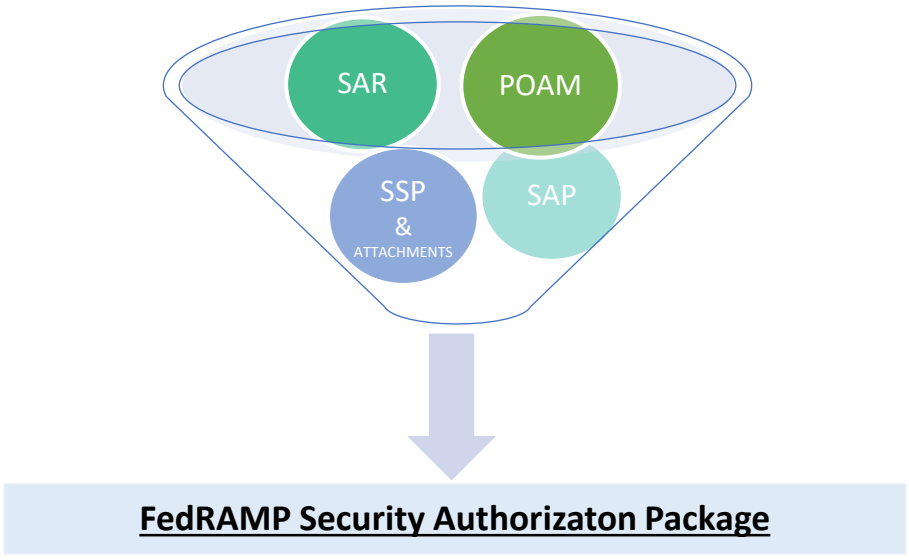
- **Agency AO is identified.**
- **Confirm resources (an Agency should have at least one technical reviewer [TR], Information System Security Officer [ISSO] / Information System Security Manager [ISSM] assigned to the authorization process). The TR works closely with the CSP to obtain timely answers to questions and with the Agency AO for the final approval and authorization of the CSO.**
- **Engage the FedRAMP PMO when needed to provide clarification on the authorization process.**
- **Determine authorization approach. The authorization approach has 2 primary methods.**

[3] FedRAMP Agency Authorization Playbook: www.fedramp.gov/agencyauthorizationplaybook ; Oct 2021.

- **Just-In-Time Linear Approach**: each FedRAMP deliverable builds upon another starting with the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M) in a linear fashion.
- **All Deliverables Provided Simultaneously**: all FedRAMP deliverables (SSP + attachments, SAP, SAR, and POA&M) are completed by the CSP and submitted to the agency by project kick-off. The Agency reviews all deliverables at once and work collaboratively with the CSP to remediate weaknesses (if any).
- Identify and provide additional Agency-specific requirements above the FedRAMP security control baseline (if applicable).
- Develop an initial project plan. Map the various milestones associated with the authorization and provide a notional schedule for CSP and 3rd Party Assessment Organization's (3PAO) input.
- Coordinate with the CSP to define Agency and CSP roles and responsibilities.
- Request access to FedRAMP's secure repository, which is where the CSP and 3PAO will upload security documents.
- Submit notional authorization schedule and notional authorization dates to the PMO once there is consensus (Agency, CSP, and 3PAO) for posting to the FedRAMP marketplace.

2.2 Authorization

The following documents make up a complete FedRAMP security authorization package for Low, Moderate, and High impact systems:



The following documents are included in the FedRAMP tailored Low-Impact Software as a Service (LI-SaaS) security package:

Appendix – B provides mandatory templates and tailored test cases specific for FedRAMP tailored LI-SaaS systems.

Appendix – E contains the FedRAMP controls recommended for self-attestation by the CSP.

There are 4 main steps that are executed during a FedRAMP Agency Authorization. During the authorization process, the CSO's security authorization package is reviewed for quality and risk. Some outcomes of the review include a deep understanding of the technical makeup and security of the CSO and the ability to determine the level of risk associated with the system, the agency's understanding of the responsibilities associated with the customer responsible controls, and the agency's ability to provide the CSP with timely feedback based on the agency's risk analysis to modify the FedRAMP deliverables. The authorization steps are outlined below.

1. Step 1: Kick-off (~1 week)

The kick-off meeting is intended to review roles and responsibilities, key security items to consider, project schedule, and future meeting cadence. Identify materials from the CSP and 3PAO that would be reviewed at the kick-off session and ask that those materials be uploaded via FedRAMP's secure repository ahead of time.

Suggested materials to review if available at time of kick-off are:

- Readiness Assessment Report
- SSP Highlights – Network topography, interconnections, system boundary diagram
- FedRAMP's critical controls: AC-2, AC-4, AC-17, CA-1, CM-6, CP-7, CP-9, IA-2(1), IA-2(2), IA-2(3), IA-2(11), IA-8(1), IR-8, RA-5, RA-5(5), RA-5(8), SA-11, SA-11(1), SC-4, SC-7, SC-8, SC-8(1), SC-13, SC-28
- Control Implementation Summary (CIS)/Customer Responsibility Matrix (CRM)
- Security Assessment Plan (SAP) – Testing methodology and sample sizes
- Security Assessment Report (SAR) – Table 4-1
- Plan of Action and Milestones (POA&M)
- Monthly scan results

Create a kick-off agenda and meeting design. An agenda lays out the order of topics and a meeting design details how those topics will be discussed.

If there are any additional Agency requirements, gaining consensus on those at the kick-off is key, as well as any Agency specific security concerns.

2. Step 2: Quality & Risk Review (~3-4 weeks)

During the quality and risk review phase the agency reviewer follows the steps listed below:

1. Begin the review based on the approach determined in the Authorization planning phase (Just-in-Time Linear or All Deliverables Provided Simultaneously).
2. Understand the impact of the customer implemented control set that was initially agreed upon with the CSP at the kick-off session.
3. Review CSP and 3PAO documentation via the FedRAMP secure repository.
4. Analyze Agency specific controls compared to the FedRAMP baseline and address any delta of controls outside of the FedRAMP baseline.
5. Review the CSP's monthly scans submissions throughout the quality review process.
6. When assessing the overall quality and risk of the authorization package, it is important for the agency reviewer to check for major issues or concerns in meeting federal requirements (FIPS

140-2 compliance, level 3 e-authentication, Multi-Factor Authentication, logical and physical separation for customers).

As part of the CSPs security package, the agency reviewer will review the following for accuracy:

The FedRAMP agency authorization review report sample template can be accessed in the following link. The FedRAMP PMO uses this template to review agency ATO packages. This template can be leveraged by agencies as it provides pertinent information and additional questions to address when reviewing a CSP's ATO package.

https://www.fedramp.gov/assets/resources/templates/FedRAMP_Agency_Authorization_Review_Report_Sample_Template.pdf

3. Step 3: Remediation (~3 weeks)

1. The CSP is responsible for remediating all weaknesses identified by the agency during the quality review phase.
2. The agency defines the remediation plan and key measures of success that address all key findings from the quality and risk review up front.
3. Provide timely feedback to the CSP to ensure updates are made as quickly as possible.
4. Be available to address questions throughout the remediation process.
5. If applicable, review the delta testing results as they come in so that weaknesses remediated are not all reviewed at once at the end of the process.

4. Step 4: Final Review (~4 weeks)

1. Submit the CSO's authorization package to the Agency AO for final approval and issuance of the ATO.
2. It is optional for agencies to use the FedRAMP ATO Letter Template when issuing ATO.
3. If the AO authorizes the system for use, submit the authorization package to the FedRAMP secure repository.
4. Inform the FedRAMP PMO at info@fedramp.gov that the CSP's authorization package has been submitted for review.
5. DOE only issues ATOs for the Agency's use of a particular cloud service. Other Agencies that are interested in authorizing the system will review the security deliverables and issue their own ATO through the re-use model.
6. Complete the review. Pay close attention to details.

2.3 Post Authorization (Continuous Monitoring)

The final phase of the FedRAMP Agency ATO process is Continuous Monitoring (ConMon) as outlined in FedRAMPs Continuous Monitoring Performance Guide. This is an ongoing process during which the agency ensures that the security posture of the CSO at time of authorization is maintained throughout the system's lifecycle. The ConMon process occurs as follows:

1. **Request Monthly ConMon Meetings:**
    - The agency will coordinate a monthly meeting cadence with the CSP (and 3PAO if needed) at least one week after the monthly ConMon deliverables are submitted by the CSP, to review ConMon deliverables and ask questions and/or share any concerns with the CSP.
2. **Annual Security Assessments:**
    - The agency will oversee performance of annual assessments by the CSP's 3PAO.
3. **Questions and Recommendations:**
    - DOE OCIO encourage the departmental elements System Owners and Information System Security Officers to review the monthly ConMon deliverables in detail if they decide to attend the ConMon meetings. Departmental elements leveraging the CSO should be aware of the CSP's reported weaknesses or vulnerabilities prior to attending the meeting. This will allow them to investigate reported weaknesses or vulnerabilities and mitigation timelines accordingly.
4. **Agenda for Monthly ConMon Meeting:**
    - Discuss any overdue Plan of Action and Milestones (POA&Ms) items.
    - Review and approval of any pending Deviation Requests and or Significant Change Requests.
    - Discussion and status updates on Significant Change Request, including planned changes, those pending approval, and the status of implementation and testing.
    - Status update on Annual Assessments.

DOEs Escalation Process for Non-Compliance:

The escalation process for non-compliance is a crucial aspect of FedRAMP's ConMon. It ensures timely resolution of identified non-compliance issues.

1. **Identification:** The agency's ConMon team identifies non-compliance and documents it.
2. **Notification:** The agency's ConMon team promptly notifies the CSP of the non-compliance issue.
3. **CSP Response:** CSP investigates and responds with proposed remediation actions.
4. **Agency Review:** The agency analyzes the CSP's response.
5. **Escalation:** If necessary, OCIO will escalate the issue between the CSP and the Agency's AO.
6. **Deviation request or Mitigation Plan:** Consider these options if non-compliance persists.
7. **Reporting:** If the CSP fails to provide a plan acceptable to the Agency or fails to meet the dates identified in the plan, the Agency may increase the escalation level to the FedRAMP PMO.
8. **Remediation:** The agency's ConMon team monitors the CSP's remediation progress. Retire the FedRAMP Agency ATO (if necessary) due to compliance non-compliance, cloud service reaching end-of-life, or any other security reason.

3. DOE – OCIO's Continuous Monitoring Program (ConMon)

The implementation of standardized ConMon activities and economies of scale for cloud offerings brings benefits such as leveraging existing reports, increased cybersecurity risk awareness, easy access to information, risk-based decision-making, operational visibility, cost savings, and standardized processes. The ConMon program reviews security artifacts, maintains visibility for stakeholders, manages the reporting repository, conducts reviews with service providers, and generates reports for risk sharing. The reports are used by the SAT Team to report inherited risks and provide a summary of risks for each organization. Trend analysis helps identify patterns and changes overtime.

3.1 Scope of Reporting

The scope of the reports includes the following components: Penetration Testing, O/S and Database Scans, Web application/Vulnerability Scans, 3PAO Testing/Annual Assessment results, Significant Changes, and POA&M Submissions/Inventories. These elements contribute to the overall assessment of security and risk posture, providing valuable information on the state of the systems, applications, and vulnerabilities.

Gaining Access to DOEs OMB MAX ConMon Repository

1. To gain access to the reports customers must first register for OMB Max credentials.
2. Registration for OMB MAX can be completed at https://omb.max.gov.
3. Agency employees and contractors must use their DOE - abc@hq.doe.gov email addresses when registering for access.
4. Enterprise Authorization to Operate (eATO) ConMon reports and any available associated security package using the eATO - \\Doe.local\dfsfr\ORG_IM\im\eATO\eATO ConMon Reporting\User Guide\Portal Access.docx .

OMB MAX Repository Login and Navigation

- The DOE Cybersecurity Community of Practice (CoP) hosted on the OMB MAX Portal.
- Access all the CoP resources and repositories based on roles/need-to-know.
- User Guide for IM-30 CoP OMB Max PORTAL - eATO Repository Available on Request.

Appendix A: Acronyms

Acronym	Definition
3PAO	3rd Party Assessment Organization
AO	Authorizing Official
ATO	Authorization to Operate
CIS	Control Implementation Summary
CISO	Chief Information Security Officer
ConMon	Continuous Monitoring
CoP	Community of Practice
CRM	Customer Responsibility Matrix
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DOE	Department of Energy
eATO	Enterprise Authorization to Operate
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
ISSM	Information System Security Manager
ISSO	Information System Security Officer
Li-SaaS	Low-Impact Software as a Service
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and budget
PMO	Program Management Office
POA&M	Plan of Action and Milestones
SaaS	Software as a Service
SAP	Security Assessment Plan
SAR	Security Assessment Report
SAT	Security Assessment Team
SSP	System Security Plan
TR	Technical Reviewer

Appendix B: Resources

FedRAMP Agency Authorization Playbook

- https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf

FedRAMP Continuous Monitoring Performance Management Guide

- https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Performance_Management_Guide.pdf

FY23 NDAA National Defense Authorization Act

- https://www.govinfo.gov/content/pkg/CRPT-117hrpt397/pdf/CRPT-117hrpt397.pdf

OMB Security Authorization of Information Systems in Cloud Computing Environments Memo; Dec. 2011.

- https://www.fismacenter.com/fedrampmemo.pdf