

FedRAMP Guide for Managing Multi-Agency
Continuous Monitoring



FedRAMP

Version 1.0

August 6, 2015

Revision History

Date	Version	Page(s)	Description	Author
August 6, 2015	1.0	All	Initial Publication	FedRAMP PMO

Table of Contents

1. Introduction.....	1
1.1. Background.....	1
1.2. Purpose of This Document	1
1.3. Agency ATO Governance Issues.....	1
2. fedramp collaboration Group.....	1
2.1. Initial Authorization.....	2
2.2. ConMon	2
2.2.1. Collaboration Group Role.....	3
3. Collaboration Group Charter	3
3.1. Collaboration Group Members	4
3.2. Collaboration Group Officers	4
3.3. Collaboration Group Committees.....	4
3.4. Collaboration Group Roles and Responsibilities.....	4
3.5. Collaboration Group Meetings	6
3.6. Collaboration Group Decision-Making	6
3.7. Charter Review	6
3.8. Charter Revisions.....	6
Appendix A: Table of Acronyms.....	7

HOW TO CONTACT US

For questions about FedRAMP or this document, email to info@fedramp.gov.

For more information about FedRAMP, visit the website at <http://www.fedramp.gov>.

1. INTRODUCTION

1.1. BACKGROUND

The Federal Risk and Authorization Management Program (FedRAMP) provides a framework for Cloud Service Providers (CSP) to meet Federal Information Security Management Act (FISMA) requirements. Cloud systems that comply with FedRAMP may be re-used by government agencies, reducing the cost and time associated with each agency's use of that cloud system. Cloud systems can meet FedRAMP compliance through three different paths: Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO), Agency Authorization to Operate (ATO), or CSP supplied. This document focuses specifically on the Agency ATO path.

1.2. PURPOSE OF THIS DOCUMENT

This document provides guidance to agencies and CSPs to assist with a framework for collaboration when managing Agency ATOs.

1.3. AGENCY ATO GOVERNANCE ISSUES

Governance of Agency ATOs can be inefficient since there is no central authority to manage the authorization. FedRAMP was not designed to force the initial authorizing agency to manage the cloud system's authorization forever. Therefore, collaboration across the government is required to successfully manage agency ATOs.

The total responsibility of maintaining a cloud system ATO through continuous monitoring should not always lie with the initial authorizing agency. While this model is acceptable, it places undue responsibility on the initial authorizing agency, makes the subsequent leveraging agencies overly dependent on the initial authorizing agency, and it does not foster the collaborative nature of FedRAMP.

2. FEDRAMP COLLABORATION GROUP

FedRAMP recommends agencies create a FedRAMP Collaboration Group (Collaboration Group) to manage the continuous monitoring (ConMon) of a common cloud system. This Collaboration Group should include members from all the agencies currently using and/or committed to using the cloud service.

Collaboration Groups allow the member agencies to share the responsibility of ConMon; reduce the dependency of leveraging agencies on the initial authorizing agency; and collaborate with the CSP and other member agencies to ensure the cloud service continues to meet the member agencies' needs. The Collaboration Group members should establish a charter for sharing this responsibility and for collaborating amongst themselves.

A Collaboration Group can be established whenever there are two or more agencies currently using or committed to using the same cloud system. Agencies may find it easier to establish a Collaboration Group amongst current cloud service users because the agencies are already committed to the service and all have contractual relationships with the CSP.

The Collaboration Group membership will change over time as new agencies leverage the cloud service and other agencies discontinue using the cloud service. CSPs with multiple FedRAMP Agency ATO system offerings should maintain Collaboration Groups for each of their service offerings to ensure the correct agencies are engaged.

2.1. INITIAL AUTHORIZATION

Although this document does not provide specific guidance on how to establish a Collaboration Group for initial authorization, agencies may establish such a Collaboration Group of committed agencies to collaborate on and share the responsibility of obtaining the initial authorization¹.

2.2. CONMON

To maintain FedRAMP compliance, CSPs must monitor their cloud system's security controls, assess them on a regular basis, and demonstrate the security posture of their service offering is continuously acceptable. CSPs satisfy this requirement by implementing ConMon activities, as documented in FedRAMP's ConMon requirements and the cloud system's ConMon Plan. See the *FedRAMP Continuous Monitoring Strategy & Guide*, available at <http://www.fedramp.gov>, for more information on ConMon and FedRAMP's ConMon requirements.

The goal of ConMon is to provide operational visibility, managed change control, and incident response.

Operational Visibility

To accomplish this goal the CSP must provide evidentiary information to Authorizing Officials (AO) monthly, annually, every 3 years, and on an as-needed frequency after authorization is granted. *Table A-1 – Summary of Continuous Monitoring Activities & Deliverables* included in the *FedRAMP Continuous Monitoring Strategy & Guide* describes the activities, deliverables, and actors (CSP or 3PAOs) who are required to meet these ConMon goals.

Managed Change Control

To accomplish this goal the CSP must develop and maintain a configuration management plan and notify the AO of any planned significant changes. Before a significant change is implemented the CSP must complete a *Significant Change Security Impact Analysis Form* (available on FedRAMP.gov) and a *Security Assessment Plan (SAP)* for testing the change and provide to the AO for their analysis and approval. After approved changes are implemented, the CSP must submit a new *Security Assessment Report (SAR)* along with any updated documents (*System Security Plan (SSP)* and any associated attachments) to the AO based on a security assessment performed by a Third-Party Assessment Organization (3PAO) in accordance with the SAP.

Incident Response

To accomplish this goal the CSP must develop and maintain an incident response guide, which is approved by the AO at time of authorization. The CSP must also follow the incident response and reporting guidance contained in the *FedRAMP Incident Communications Procedure*. During

¹ FedRAMP plans on releasing guidance on how to create a collaboration group for initial authorization by the end of CY15.

incident response, both the CSP and leveraging agencies are responsible for coordinating incident handling activities together, and with US-CERT, and notifying FedRAMP.

2.2.1. COLLABORATION GROUP ROLE

A Collaboration Group must develop an ConMon framework based on the *FedRAMP Continuous Monitoring Strategy & Guide* that describes the security assessment process the CSP must use to maintain the high water mark of the Collaboration Group's member agencies and FedRAMP's ConMon requirements. In addition, the framework should identify any additional ConMon requirements that the member agencies need to meet their own agency specific FISMA reporting requirements. The Framework should also identify any required procedures within their respective agencies.

The purpose of this framework will allow the CSP to fully understand all of the required deliverables, method for delivery, and any agency specific additions or exceptions they must manage for continuous monitoring. It will allow the CSP to more efficiently complete ConMon and be more responsive to all government customers. Once this assessment framework is developed, it must be reviewed and agreed to by the CSP and approved by the member agencies.

After the Collaboration Group approves the ConMon framework, the Collaboration Group performs oversight of the CSP's ConMon activities to ensure that the CSP maintains the security posture of their cloud system in accordance with the ConMon Framework. The Collaboration Group must collaborate and share the responsibilities for performing the following activities:

- Establishing criteria for and overseeing continuous, periodic, and ad-hoc cloud system monitoring
- Serving as focal point for coordinating and monitoring the CSP's ConMon activities
- Verifying the CSP is submitting all required ConMon artifacts to the required recipients in a timely manner
- Analyzing monthly Plan of Action and Milestones (POA&M) vulnerability scans and inventories; tracking actions and milestones through completion
- Ensuring significant changes are reviewed and approved by all the member agencies
- Ensuring updated documentation describing the newly implemented changes is submitted to the member agencies and FedRAMP
- Coordinating and monitoring the CSP's incident handling activities and reporting
- Ensure all documentation is uploaded and stored within the FedRAMP repository on OMB MAX.

3. COLLABORATION GROUP CHARTER

A Collaboration Group requires some sort of forming document to establish members, roles, responsibilities, meeting frequency, and decision making authorities. FedRAMP recommends a Collaboration Group Charter (charter) to do this. This charter should be developed by the member agencies and be reviewed and approved by them in accordance with other similar multi-agency agreements.

3.1. COLLABORATION GROUP MEMBERS

The FedRAMP Collaboration Group should consist of all stakeholders for the cloud service offering, including but not limited to:

- Agencies currently using the cloud service
- Agencies committed to using the cloud service (typically for new agency instances)
- Agencies considering utilizing the cloud service (optional)
- The Cloud Service Provider

3PAOs may be requested to provide information to the Collaboration Group, but are not typically included as members of the Collaboration Group unless a CSP is using a 3PAO to perform the monthly ConMon. In such a case, the 3PAO should be a member of the Collaboration Group.

The CSP is a critical member of the Collaboration Group. The CSP may be the only member that knows all of the agencies considering or using the cloud service and has a relationship with all of them.

Agencies should consider having voting and non-voting members to clarify which members are decision makers. Non-voting members might include the CSP, 3PAO, and agencies considering utilizing the cloud service.

3.2. COLLABORATION GROUP OFFICERS

The Collaboration Group should have a Chair and a Vice-Chair. The Chair should be selected by a majority vote of the voting membership. The Chair must be a government employee from a voting member of the Collaboration Group. The Chair can nominate a Vice-Chair from the voting membership upon appointment to role or the Vice-Chair can be voted upon as well. The Chair may delegate responsibility to the Vice-Chair temporarily via any mechanism provided all voting members are notified.

3.3. COLLABORATION GROUP COMMITTEES

The Collaboration Group may establish standing and temporary or ad-hoc committees to conduct on-going business and consider items of concern on an as needed basis. These committees may include things like reviewing ConMon deviation requests on a monthly basis, reviews of significant change requests, responses to cross-service incidents, and overall risk management among others.

3.4. COLLABORATION GROUP ROLES AND RESPONSIBILITIES

Collaboration Group members should decide the roles and responsibilities required to accomplish their objectives and delegate their staff to the roles. Collaboration Group members should include the CSP the Collaboration Group is collaborating with and the 3PAO performing the monthly ConMon. Table 1 includes **examples** of Collaboration Group roles required to implement the proposed Collaboration Group governance approach.

Table 1. Roles and Responsibilities

Role	Responsibilities
Chair	<ul style="list-style-type: none"> ▪ Chair Collaboration Group meeting ▪ Direct and coordinate Collaboration Group activities ▪ Appoint a Vice-Chair (optional) ▪ Delegate activities to the Vice-Chair as needed ▪ Promote and maintain FedRAMP compliance
Vice-Chair	<ul style="list-style-type: none"> ▪ Chair the Collaboration Group meetings in the absence of the Chair ▪ Direct and coordinate Collaboration Group activities in the absence of the Chair ▪ Other duties as delegated by the Chair or determined by the Collaboration Group
Secretary	<ul style="list-style-type: none"> ▪ Capture all minutes from meetings ▪ Capture any and all action items from meetings ▪ Distribute notes to the Collaboration Group members within 2 business days of the meeting ▪ Begin each meeting with a recap of last week's minutes and outcomes of any action items.
User Agencies	<ul style="list-style-type: none"> ▪ Attend Collaboration Group Meetings ▪ Collaborate and share the responsibilities of ConMon ▪ Contribute staff for officers and committees ▪ Contribute and collaborate to ensure the cloud system meets all the member agencies' needs
Committed Agencies	<ul style="list-style-type: none"> ▪ Attend Work Group Meetings ▪ Collaborate and share the responsibilities of ConMon ▪ Provide temporary support staff as requested/required for major infrequent tasks such as significant change reviews and incident management
Reviewers	<ul style="list-style-type: none"> ▪ Review artifacts and provide comments and recommendations to the Collaboration Group
CSP Representatives	<ul style="list-style-type: none"> ▪ Facilitate the creation of Collaboration Groups for their cloud services ▪ Respond to Collaboration Group requests for information ▪ Review and agree on additional ConMon requirements to meet unique member agency needs
3PAO Representatives	<ul style="list-style-type: none"> ▪ Respond to Collaboration Group requests for information ▪ Review and agree on additional ConMon requirements to meet unique member agency needs
Committees (if formed)	<ul style="list-style-type: none"> ▪ Perform their assigned duties ▪ Advise the Collaboration Group

Role	Responsibilities
FedRAMP PMO	<ul style="list-style-type: none"> ▪ Attend Collaboration Group meetings as a special advisor when requested by the Collaboration Group Chair ▪ Respond to Collaboration Group requests for information <p>Note: The FedRAMP PMO will only attend meetings when requested. The FedRAMP PMO will not initiate, drive, or facilitate Collaboration Group meetings.</p>

3.5. COLLABORATION GROUP MEETINGS

Collaboration Group members will determine the frequency and attendees of periodic and ad hoc meetings to conduct Collaboration Group business and make decisions. It is recommended that meetings happen minimally on a monthly basis due to monthly deliverables by the CSP in accordance with the ConMon requirements. More frequent meetings may be required during annual assessment, significant change requests, and major incidents. Collaboration Group members should determine a default forum for periodic meetings. Collaboration Group meetings do not necessarily have to be in-person at a specified location. Teleconference, web conference, and other mutually agreeable alternative forums are acceptable and may even be desirable for geographically dispersed members.

3.6. COLLABORATION GROUP DECISION-MAKING

At a minimum, all Collaboration Group decisions should be agreed to by a majority of the voting members. The Collaboration Group may determine some decisions require a unanimous votes or consensus agreements. Voting may occur during the monthly meeting or through remote means such as e-mail or letter. The Collaboration Group should determine a quorum to hold a vote, expressed as a minimum percentage or number of voting members. The Collaboration Group may elect to grant certain members and committees limited decision-making powers.

3.7. CHARTER REVIEW

This charter is a living document. The Collaboration Group should review this Charter and revise it as often as necessary to keep it current and relevant. The Collaboration Group should evaluate its effectiveness on at least an annual basis, and consider changes as necessary.

3.8. CHARTER REVISIONS

Changes to the Charter should be approved by the voting members by a vote greater than a simple majority, as stated in the Charter. Once the changes have been approved, the “Record of Changes” section of this document will reflect the date, revision, and changes accepted for historical tracking.

APPENDIX A: TABLE OF ACRONYMS

Acronym	Meaning
3PAO	Third-Party Assessment Organization
AO	Authorizing Official
ATO	Authorization to Operate
ConMon	Continuous Monitoring
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
JAB	Joint Authorization Board
P-ATO	Provisional Authorization to Operate
PMO	Program Management Office
SAR	Security Analysis Report