FedRAMP *Tailored* Low Impact

Software as a Service (LI-SaaS)
Continuous Monitoring Guide



Federal Risk and Authorization Management Program

Version 2.0

August 23, 2017

Executive Summary

The Office of Management (OMB) Circular No. A-130, Appendix I (OMB A-130), issued July 28, 2016, requires the implementation of continuous monitoring (ConMon) as a means for maintaining ongoing awareness of the information security, vulnerabilities, threats, and incidents to support the agency risk management decisions. OMB A-130 defines “ongoing authorization” as “the means for determining risk and for making risk acceptance decision subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency’s mission or business requirements and agency risk tolerance.” OMB A-130 further defines ongoing authorization as a time-driven or event-driven authorization process whereby the Authorizing Official (AO) is provided with the necessary and sufficient information regarding the security state of the information system to determine whether the mission or business risk of continued system operation is acceptable.

Consistent with OMB A-130 and in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, FedRAMP developed an ongoing assessment and authorization program for the purpose of maintaining the authorization of FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) Cloud Service Providers (CSP).

This continuous monitoring guide describes the FedRAMP strategy and *minimum* requirements for a CSP to use once it has received a FedRAMP Authorization based on the FedRAMP *Tailored*
LI-SaaS requirements. CSPs must continuously monitor the cloud service offering to detect changes in the security posture of the system to enable well-informed risk-based decision making.

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Description** | **Version** | **Author** |
| 6/19/2017 | Initial Document | 1.0 | FedRAMP PMO |
| 7/23/2017 | Final baseline for publication/use | 2.0 | FedRAMP PMO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Overview 1](#_Toc490669230)

[1.1. Purpose of This Document 2](#_Toc490669231)

[1.2. Continuous Monitoring Process 2](#_Toc490669232)

[2. Continuous Monitoring Roles And Responsibilities 4](#_Toc490669233)

[2.1. Authorizing Official 4](#_Toc490669234)

[2.2. FedRAMP PMO 4](#_Toc490669235)

[2.3. Department of homeland security (DHS) 4](#_Toc490669236)

[2.4. Independent Security Assessment 5](#_Toc490669237)

[2.5. FedRAMP Tailored LI-SaaS CSP 5](#_Toc490669238)

[3. Continuous Monitoring Process 6](#_Toc490669239)

[3.1. Operational Visibility 6](#_Toc490669240)

[3.2. Ongoing Continuous Monitoring Requirements 6](#_Toc490669241)

[3.3. Annual Continuous Monitoring Requirements 7](#_Toc490669242)

[3.4. Change Control 8](#_Toc490669243)

[3.5. Incident Response 9](#_Toc490669244)

[4. Authorizing Official (AO) Continuous Monitoring Analysis Process 10](#_Toc490669245)

[5. Appendix A - Control Frequencies 11](#_Toc490669246)

List of Figures & Tables

[Figure 1 – NIST Special Publication 800-137 ConMon Process 3](#_Toc490665531)

[Table 3-1 – Criteria for AO Selection of Additional Testing 8](#_Toc490665532)

[Table A-1 – Summary of FedRAMP Tailored LI-SaaS ConMon Activities and Deliverables 11](#_Toc490665533)

**About This Document**

This document has been developed to provide guidance on continuous monitoring (ConMon) and ongoing authorization, in support of maintaining a security authorization that meets FedRAMP *Tailored* Low Impact Software as a Service (LI-SaaS) requirements. This document is not a FedRAMP template – there is nothing to fill out in this document.

**Who Should Use this Document?**

This document is intended to be used by Cloud Service Providers (CSPs), Independent Assessors, Government contractors working on FedRAMP projects, and Government employees working on FedRAMP projects. This document may also prove useful for other organizations that are developing a ConMon program.

**How This Document is Organized**

This document is divided into four sections and one appendix.

|  |  |
| --- | --- |
| Section 1 | Provides an overview of the ConMon process. |
| Section 2 | Describes roles and responsibilities of ConMon. |
| Section 3 | Describes the ConMon process. |
| Section 4 | Describes the Authorizing Official (AO) ConMon analysis process. |
| Appendix A | Describes the security control frequencies.  |

**How to Contact Us**

Questions about FedRAMP or this document may be directed to *info@fedramp.gov**.*

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

# Overview

Once initial authorization has been granted, in accordance with the FedRAMP *Tailored* LI-SaaS Framework, the CSP’s security posture is monitored according to the ongoing assessment and authorization process. Monitoring security controls is part of the overall risk management framework for information security, and is a requirement for CSPs to maintain a security authorization that continues to meet the FedRAMP *Tailored* LI-SaaS requirements following initial authorization.

The Office of Management (OMB) Circular No. A-130, Appendix I (OMB A-130), issued July 28, 2016, requires the implementation of ConMon as a means for maintaining an ongoing awareness of the information security, vulnerabilities, threats, and incidents to support the agency risk management decisions. OMB A-130 defines ongoing authorization as the means for determining risk and for making risk acceptance decision subsequent to the initial authorization, taken at agreed-upon and documented frequencies in accordance with the agency’s mission or business requirements and agency risk tolerance. OMB A-130 further defines ongoing authorization as a time-driven or event-driven authorization process whereby the Authorizing Official (AO) is provided with the necessary and sufficient information regarding the security state of the information system to determine whether the mission or business risk of continued system operation is acceptable.[[1]](#footnote-1)

Traditionally, this process has been referred to as “Continuous Monitoring,” (or “ConMon”) as noted in National Institute of Standards and Technology Special Publication 800-137 (NIST SP 800-137), *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. It is important to note that both the terms “Continuous Monitoring” and “Ongoing Security Assessments and Authorization” mean essentially the same thing, and should be interpreted as such.

Performing ongoing security assessments determines whether the set of deployed security controls in a cloud information system remains effective in light of new exploits and attacks, and planned and unplanned changes that occur in the system and its environment over time. To maintain an authorization that meets the FedRAMP *Tailored* LI-SaaS requirements, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

Ongoing assessment of security controls results in greater control over the security posture of the CSP system and enables timely risk-management decisions. Security-related information collected through ConMon is used to make recurring updates to the security assessment package. Ongoing due diligence and review of security controls enables the security authorization package to remain current, which allows agencies to make informed risk management decisions as they use cloud services.

## Purpose of This Document

This document provides guidance and instructions to CSPs that have been issued an Agency Authorization to Operate (ATO) in accordance with the FedRAMP *Tailored*, as well as to the agencies leveraging the system’s ATO.

## Continuous Monitoring Process

The FedRAMP *Tailored* LI-SaaS ConMon program is based on the ConMon process described in NIST SP 800-137*, Information Security Continuous Monitoring (ISConMon) for Federal Information Systems and Organizations*. The goal is to provide: (i) operational visibility; (ii) managed change control; (iii) and attendance to incident response duties. For more information on incident response, review the FedRAMP *Incident Communications Procedure* available on the FedRAMP website (www.fedramp.gov).

The effectiveness of a CSP’s ConMon capability supports ongoing authorization and reauthorization decisions. Security-related information collected during ConMon is used to make updates to the security authorization package. Updated documents provide evidence that FedRAMP *Tailored* LI-SaaS baseline security controls continue to safeguard the system as originally planned and that they are operating as intended.

As defined by NIST, the process for continuous monitoring includes the following initiatives:

* **Define** a ConMon strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.
* **Establish** measures, metrics, and status monitoring and control assessments frequencies that make known organizational security status and detect changes to information system infrastructure and environments of operation, and status of security control effectiveness in a manner that supports continued operation within acceptable risk tolerances.
* **Implement** a ConMon program to collect the data required for the defined measures and report on findings; automate collection, analysis, and reporting of data where possible.
* **Analyze** the data gathered and **Report** findings accompanied by recommendations. It may become necessary to collect additional information to clarify or supplement existing monitoring data.
* **Respond** to assessment findings by making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority.
* **Review** and **Update** the monitoring program, revising the ConMon strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enhance data driven control of the security of an organization’s information infrastructure; and increase organizational flexibility.



Figure 1 – NIST Special Publication 800-137 ConMon Process

Security control assessments performed periodically validate whether stated security controls are implemented correctly, operating as intended, and continue to meet FedRAMP *Tailored* LI-SaaS baseline security controls. Security status reporting provides Federal officials with information necessary to make risk-based decisions and provides assurance to existing customer agencies regarding the security posture of the system.

# Continuous Monitoring Roles And Responsibilities

## Authorizing Official

The AOs and their teams serve as the focal point for coordination of ConMon activities for CSPs. The AOs monitor the security posture of the CSP and any major significant changes and reporting artifacts (such as vulnerability scan reports) associated with the CSP service offering. AOs use this information so that risk-based decisions can be made about ongoing authorization. Agency customers must perform the following tasks in support of CSP ConMon:

* Notify the CSP if the agency becomes aware of an incident that a CSP has not yet reported.
* Provide primary and secondary points of contact (POCs) for CSPs and United States Computer Emergency Readiness Team (US-CERT), as described in agency and CSP Incident Response Plans.
* Notify US-CERT when a CSP reports an incident.
* Work with CSPs to resolve incidents, providing coordination with US-CERT if necessary.
* Monitor security controls that are agency responsibilities.

During incident response, both CSPs and agencies are responsible for coordinating incident handling activities together with US-CERT. A team-based approach to incident handling ensures that all parties are informed and enables incidents to be closed as quickly as possible.

## FedRAMP PMO

The FedRAMP Program Management Office (PMO) acts as the liaison for the Joint Authorization Board (JAB) for ensuring that CSPs with a FedRAMP JAB Provisional Authorization (P-ATO) strictly adhere to their established ConMon plan. The JAB and FedRAMP PMO only perform ConMon activities for those CSPs that have a JAB P-ATO. The JAB and FedRAMP PMO provide this guidance to agencies and CSPs in support of FedRAMP *Tailored* LI-SaaS authorizations issued by agency AOs.

## Department of homeland security (DHS)

The FedRAMP Policy Memorandum released by OMB on December 8, 2011, defines the DHS FedRAMP responsibilities to include:

* Assisting Government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity.
* Coordinating cybersecurity operations and incident response and providing appropriate assistance.
* Developing ConMon standards for ongoing cybersecurity of Federal information systems to include real-time monitoring and continuously verified operating configurations.
* Developing guidance on agency implementation of the Trusted Internet Connection (TIC) program for cloud services.

The FedRAMP PMO works with DHS to incorporate DHS guidance into the FedRAMP program guidance and documents.

## Independent Security Assessment

Independent assessment organizations are responsible for verifying and validating the control implementations are in place and operating as intended for FedRAMP *Tailored* LI-SaaS CSPs in the ConMon phase of the FedRAMP process.[[2]](#footnote-2) Specifically, the independent assessors are responsible for:

* Assessing all of the FedRAMP *Tailored* LI-SaaS required and conditional controls annually.
* Submitting the assessment report to the AO one year after the CSP’s authorization date and each year thereafter.
* Performing annual scans of web applications, databases, and operating systems, as applicable.
* Assessing changed controls on an *ad hoc* basis as requested by the AOs for any changes made to the system by the CSP.

In order to be effective in this role, independent assessors are responsible for ensuring that the chain of custody is maintained for any authored documentation. The assessor must also be able to vouch for the veracity and integrity of data provided by the CSP for inclusion in the authored documentation. As an example:

* If scans are performed by the CSP, the independent assessor must either be on site and observe the CSP performing the scans, or be able to monitor or verify the results of the scans through other means documented and approved by the AO.
* Documentation provided to the CSP must be placed in a format that allows the assessor to verify the integrity of the document.

## FedRAMP Tailored LI-SaaS CSP

CSPs must coordinate with their AOs and assessors to provide security control artifacts, at a minimum monthly and annually, to demonstrate the ongoing security posture of the system. The submission of these deliverables allows AOs to evaluate the risk posture of the CSP and to make risk-based decisions on whether to continue the authorization.

# Continuous Monitoring Process

## Operational Visibility

An important aspect of a CSP’s ConMon program is to provide evidence that demonstrates the efficacy of its program. CSPs and the independent assessors are required to provide evidentiary information to AOs monthly and annually, at a minimum, as well as on an as-needed frequency after authorization is granted.

Table A-1 in Appendix A, notes which deliverables are required as part of ConMon activities. These deliverables include providing evidence, such as monthly vulnerability scans of CSP operating systems, databases, and web applications, as applicable.

## Ongoing Continuous Monitoring Requirements

As part of the ConMon process, FedRAMP *Tailored* LI-SaaS CSPs are required to perform the following activities:

* Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
* Install security-relevant software and firmware updates within thirty (30) days of release of the updates.
* Incorporate flaw remediation into the organizational configuration management process.
* Scan monthly for vulnerabilities in the FedRAMP *Tailored* LI-SaaS system operating system, web application(s), and database(s), as applicable, and when new vulnerabilities potentially affecting the system/applications are identified and reported.
* Ensure scanning tools have the latest vendor updates before performing monthly scans.
* Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
* Enumerating platforms, software flaws, and improper configurations;
* Formatting and making transparent checklists and test procedures; and
* Measuring vulnerability impact.
* Analyze vulnerability scan reports and results from security control assessments.
* Remediate High-risk vulnerabilities within thirty (30) days from date of discovery and Moderate-risk vulnerabilities within ninety (90) days from date of discovery, in accordance with an organizational assessment of risk.
* Report monthly on the status of all identified vulnerabilities and weaknesses to the AO, including a summary report of the overall risk posture and requests for deviation (e.g., risk impact level adjustment, false positive, operational requirement).
* Share information obtained from the vulnerability scanning process and security control assessments within the FedRAMP *Tailored* LI-SaaS CSP organization, the AO, and independent assessors to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

## Annual Continuous Monitoring Requirements

As part of the ConMon process FedRAMP *Tailored* LI-SaaS CSPs are required to have an independent assessor perform the following on an annual basis:

* Validate all FedRAMP *Tailored* LI-SaaS “required” and applicable “conditional” controls implemented on the system continue to operate as intended.
* Validate applicable changes to the FedRAMP *Tailored* LI-SaaS CSP system to ensure risk posture is maintained at an acceptable level.
* Confirm controls “inherited” from the underlying IaaS/PaaS have not changed or assess the impact of changes to inherited controls.
* Validate vulnerability scanning of applicable web applications, databases, and operating systems performed by the FedRAMP *Tailored* LI-SaaS CSP.
* Validate FedRAMP *Tailored* LI-SaaS CSP has completed other ConMon activities on a periodic basis.

The AO may request additional testing based on the criteria in Table 3-1, below.

Table 3-1 – Criteria for AO Selection of Additional Testing

| **Criteria** | **Description** |
| --- | --- |
| 1. | Condition of previous assessment | Any conditions made by the AO in the authorization letter or during a previous assessment. This would include the resolution of vulnerabilities within certain timeframes, implementation of new capabilities, etc. |
| 2. | Weakness identified since the last assessment | Any areas in which a cloud system has had known vulnerabilities or enhanced risk related to specific controls. Examples might include actual or suspected intrusion, compromise, malware event, loss of data, or Department of State (DoS)/Distributed Denial of Service (DDoS) attacks. |
| 3.  | Known or suspected testing/ConMon failure | Any areas where the cloud system has demonstrated a weakness or vulnerability in ConMon and testing related to specific security controls. Examples might include those controls related to patch management, configuration management, or vulnerability scanning. |
| 4. | Control implementation that has changed since last assessment | Any control implementations that have changed since the last assessment. These changes might not reach the level of a significant change but due to their change in implementation status would require an independent assessment of that implementation. |
| 5. | Newly discovered vulnerability, zero-day attack, or exploit | Select additional controls for testing when the system is affected by newly discovered vulnerabilities or zero-day exploits. Examples would include the “Heartbleed” vulnerability. |
| 6. | Recommendation of AO or Organization  | Based on direct knowledge and use of a cloud system, AOs or organizations can require the CSP to test additional controls based on unique mission concerns or based on the CSP’s performance since their last assessment. |

The results of the annual assessments may be provided to the AO as an addendum to the System Security Plan (SSP)/ Security Assessment Plan (SAP)/ Security Assessment Report (SAR) document approved at the time of initial ATO.

As part of the ConMon process, FedRAMP *Tailored* LI-SaaS CSPs are required to submit an updated Attestation documenting the CSP’s continued implementation of security controls and requirements included in the FedRAMP *Tailored* LI-SaaS Baseline that have not been designated as “Required” or “Required, Conditional” and any additional controls required by the agency AO.

## Change Control

Systems are dynamic, and FedRAMP anticipates that all systems are in a constant state of change. ConMon and change control processes help maintain a secure baseline configuration of the CSP’s system. Routine, day-to-day changes are managed through the CSP’s change management process. However, before a planned significant change takes place, CSPs must perform a Security Impact Analysis (SIA) to determine if the change will adversely affect the security of the system. The SIA is a standard part of a CSP’s change control process.

CSPs must notify their AO within a minimum of thirty (30) days before implementing any planned major significant changes. The AOs might require more time, based on the severity of the change being implemented, so CSPs must work closely with their AOs to understand how much time is needed in advance of major system changes. All plans for significant changes must include the rationale for making the change, and a plan for testing the change prior to, and following implementation in the production system.

If any anticipated change adds residual risk, or creates other risk exposure that the AO finds unacceptable, the ATO could be revoked if the change is made without prior notification. The goal is for CSPs to make planned changes in a controlled manner so that the security integrity of the system remains at an acceptable level.

An AO may require an independent assessment of the change prior to implementation. At a minimum, the FedRAMP *Tailored* LI-SaaS CSP must include the change as part of the scope of the independent annual assessment.

## Incident Response

FedRAMP requires that CSPs demonstrate that they are able to adequately respond to security incidents. As part of the FedRAMP requirements, CSPs are required to implement a process for addressing, monitoring, and reporting incidents to the AO and other customers as applicable. FedRAMP *Tailored* LI-SaaS CSPs are also required to follow the incident response and reporting guidance contained in the *FedRAMP Incident Communications Procedure* guidelines.

# Authorizing Official (AO) Continuous Monitoring Analysis Process

AOs will be monitoring the risk posture of the FedRAMP *Tailored* LI-SaaS CSPs on a monthly basis to ensure that the CSP maintains an appropriate risk posture. This typically means the risk level remains at or better than at the time of authorization.

This monthly analysis and review of the CSP risk posture allows the AO to make authorization decisions every month.

FedRAMP *Tailored* LI-SaaS CSPs will provide summary information to assist in the analysis of monthly reporting, including explanations for late remediation of high and moderate risks. It is normal to request deviation for adjustment of risk, false positives, and for risks that cannot be corrected because it could negatively impact the operation of the system. These deviations must be defined in the summary report. However, a repeated history of late remediation of risks may indicate to the AO there is a misalignment with business processes and operations and negatively impact the risk posture of the system.

# Appendix A - Control Frequencies

Security controls have different frequencies for performance and review, and some require review more often than others. Table A-1 below summarizes the required ConMon activities. Some ConMon activities require that the FedRAMP *Tailored* LI-SaaS CSP submit a deliverable to their AO. Note that CSPs are required to submit the deliverables listed in Table A-1 if they have full or shared responsibility for the listed control. However, inherited controls do not require the submission of a deliverable.

Some ConMon activities do not require a deliverable, and will be reviewed by the independent assessor during security assessments. CSPs must be able to demonstrate to the independent assessor that ongoing ConMon activities are in place, and have been occurring as required. For example, if a CSP has indicated in the control implementation description that it monitors unsuccessful login attempts on an ongoing basis, the independent assessor may ask to see log files, along with the CSP analysis of the log files.

In Table A-1, refer to the “Description” column for information about what is required and when it is required to be submitted. A checkmark in either the “CSP Responsibility” column or “Independent Assessor Responsibility” column of Table A-1 indicates which entity is responsible for meeting the requirement.

AOs may ask for a security artifact at any point in time especially if concerns arise about the security posture of the FedRAMP *Tailored* LI-SaaS CSP system. CSPs should anticipate that, aside from scheduled ConMon deliverables, and testing performed by the independent assessor, AOs may request certain system artifacts on an ad hoc basis if there are concerns.

FedRAMP *Tailored* LI-SaaS CSPs are required to submit a schedule of activities within fifteen (15) days of the date of their authorization to their AOs, and annually thereafter. This schedule assists AOs in monitoring ConMon activities.

***Note:*** For controls that do not have a check in either the “CSP Responsibility” or “Independent Assessor Responsibility” columns in Table A-1, FedRAMP *Tailored* LI-SaaS CSPs is required to provide evidence of compliance, minimally during annual assessment and upon request.

Table A-1 – Summary of FedRAMP Tailored LI-SaaS ConMon Activities and Deliverables

| **Row #** | **Control ID** | **Control Name** | **Continuous Monitoring Activity** | **CSP Responsibility** | **Independent Assessor Responsibility** | **Notes** |
| --- | --- | --- | --- | --- | --- | --- |
| **Ongoing** |
| **1** | CP-9 | Information System Backup | CSP determines what elements of the cloud environment require information system backup control (e.g., user-level information, system-level information). The service provider shall determine how information system backup is going to be verified and periodically checked (e.g., daily incremental; weekly full). CSP determines how backups are maintained (e.g., online, offline). | X |   |   |
| **2** | SI-2 | Flaw Remediation | Installs security-relevant software and firmware updates within thirty (30) days of the release of the updates. | X |   |   |
| **Weekly** |
| **3** | AU-6 | Audit Review, Analysis, and Reporting | CSPs must review and analyze information system audit records for indications of inappropriate or unusual activity. Reports findings of inappropriate or unusual activity to incident response team.  | X |   |   |
| **Monthly** |
| **4** | CA-7 | Continuous Monitoring | CSPs must report the security state of the system to the AOs on a monthly basis.  | X |   |   |
| **5** | CM-8 | Information System Component Inventory | CSPs must review and update the information system component inventory and deliver to AO at least monthly. | X |   |   |
| **6** | RA-5 | Vulnerability Scanning | CSPs must scan for vulnerabilities in the information system (operating system, database, and web applications) monthly and when new high-impact vulnerabilities are identified that potentially affect the LI-SaaS. CSPs must remediate legitimate high risk vulnerabilities within thirty (30) days from date of discovery; moderate risk vulnerabilities within ninety (90) days from date of discovery, in accordance with organization assessment of risk. | X |   |   |
| **Quarterly** |
| **7** | AC-22 | Publicly Accessible Content | CSPs must review content on publicly-accessible systems and look for non-public information. | X |   |   |
| **Annually** |
| **8** | CA-2 | Security Assessments | CSPs must have an independent assessor perform assessment of all LI-SaaS security controls annually. Assessed results must be submitted to the AO one year from the ATO date and each year thereafter. |   | X |   |
| **9** | PL-2 | System Security Plan | CSPs must review and update the System Security Plan annually.  | X |   |   |
| **10** | RA-3 | Risk Assessment | Conducts risk assessment annually or whenever there is a significant change. |   | X |   |
| **11** | RA-5 | Vulnerability Scanning | An independent assessor scans applicable operating systems, web applications, and databases once annually. |   | X |   |
| **12** |  | Attestation | CSP must submit an attestation annually that addresses all controls not designated as *required* or *required (conditional)* in the FedRAMP *Tailored* LI-SaaS Baseline are implemented and continue to operate as intended. This also includes any additional controls as designated by an agency AO. | X |  |  |

1. OMB A-130, dated 7/28/2016, Appendix I, Section 5. [↑](#footnote-ref-1)
2. Independent assessments of FedRAMP *Tailored* LI-SaaS CSPs may be conducted by an authorizing agency organization or a FedRAMP Third Party Assessment Organization (3PAO). [↑](#footnote-ref-2)