FEDRAMP 3PAO OBLIGATIONS AND PERFORMANCE GUIDE

Version 2.0

December 7, 2017

FedRAMP

REVISION HISTORY

Date	Version	Page(s)	Description	Author
07/29/2015	1.0	All	Initial Publication	FedRAMP
6/6/2017	1.0	Cover	Updated FedRAMP logo	FedRAMP PMO
12/7/2017	2.0	All	Updated to the new template	FedRAMP PMO

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/.

TABLE OF CONTENTS

1. INTRODUCTION

The Federal Risk and Authorization Management Program (FedRAMP) created a conformity assessment process to accredit Third-Party Assessment Organizations (3PAOs) to ensure that 3PAOs meet quality, independence, and knowledge requirements necessary to perform the independent security assessments required for FedRAMP. To maintain accreditation, 3PAOs must continue to demonstrate quality, independence, and FedRAMP knowledge as they perform security assessments on cloud systems.

2. 3PAO ACCREDITATION STANDARDS

3PAO accreditation by FedRAMP includes an assessment by the American Association for Laboratory Accreditation (A2LA). A2LA performs an initial assessment of each 3PAO required for accreditation by FedRAMP, a yearly surveillance, and a full re-assessment every 2 years for continued accreditation.

The A2LA assessment ensures that 3PAOs meet the FedRAMP requirements of ISO 17020 (as revised) and FedRAMP specific knowledge requirements related to the FedRAMP Security Assessment Framework. The A2LA provides an assessment report to FedRAMP that documents the 3PAO:

- Is competent to perform inspections of Cloud Service Provider (CSP) documents
- Has a documented and fully operational quality system
- Quality system meets the standards of ISO/IEC 17020-2012
- Is operating in accordance with its quality system

A2LA also assesses 3PAOs with specific FedRAMP and FISMA knowledge. A 3PAO must demonstrate technical competence through reviews of System Security Plans, creation of a Security Assessment Plan, and documenting the results in Security Assessment Test Cases as well as a Security Assessment Report.

3. 3PAO OBLIGATIONS

FedRAMP requires all 3PAOs to adhere strictly and continuously to the FedRAMP accreditation requirements and follow their ISO 17020 quality manual as described in their application and evaluated by A2LA. Among these requirements, a few key items are:

- The 3PAO must be independent from any CSP they assess. A 3PAO is only allowed to be a Type A or type C Inspection Body.
- All the assessment work that 3PAOs perform for CSPs must meet a high standard of independence and performance, especially quality, completeness, and timeliness.
- 3PAOs must demonstrate knowledge of FISMA and FedRAMP specific requirements when conducting their assessments.

3PAOs must continuously meet and demonstrate they are performing in accordance with these standards, which they demonstrated in their A2LA assessment. If a 3PAO has any questions on these matters, they should consult with FedRAMP.

During a FedRAMP assessment, 3PAOs produce the following documents as a part of the overall security authorization package submitted for authorization to a government Authorizing Official:

- Security Assessment Plans (SAP)

  - Inventories
  - Rules of Engagement

- Security Assessment Reports (SAR)

  - Security Assessment Test Case Workbook
  - Risk Exposure Table
  - Penetration Test Report
  - Vulnerability Scan Data Files
  - Test Artifacts

These 3PAO documents must meet the following standards, reflective of their FedRAMP accreditation:

FedRAMP Standard	Details
Completeness	Complete and thoroughly prepared documents are expected on first submission. If any issues are identified, the 3PAO shall quickly and efficiently respond to the comments, and incorporate updates to resolve all the comments.
Timeliness	Documents are delivered on time, according to the schedule agreed to between the government, the CSP, and the 3PAO.
Standard templates	Documents are prepared using the most recent standard templates, without alterations or deletions, and insertions must be agreed upon.
Document Quality and Acceptance Criteria	The 3PAO must meet all quality and acceptance criteria as published by FedRAMP on the fedramp.gov website.
Testing Quality	Complete and accurate testing is an essential responsibility of a 3PAO. This responsibility derives from the 3PAO's A2LA assessment and the FedRAMP requirements for the highest quality testing.

Failure of a 3PAO to perform according to these standards affects the government's ability to authorize based on a 3PAO's assessment. FedRAMP will pursue corrective actions and possible removal of accreditations if 3PAO products do not meet the above standards.

4. 3PAO PERFORMANCE

The government evaluates all 3PAO products, and expects superior quality and performance. Quality is expected across the government, regardless of the whether a 3PAO is working directly with the FedRAMP PMO or JAB. In the event that a 3PAO's performance is not meeting standards, FedRAMP has the authority and responsibility to pursue corrective actions, including the following:

FedRAMP Action	Details
Consultation	If a 3PAO has minor deficiencies in their performance: • FedRAMP will require a meeting with 3PAO representatives to discuss the specific deficiencies in the 3PAO's performance. • This will result in an internal Corrective Action Plan (CAP) being developed by the 3PAO and submitted to FedRAMP. • The CAP will be shared with A2LA during the 3PAOs next assessment.
Remediation	If a 3PAO has deficiencies in their performance or fails to complete the internal CAP: • A letter will be sent from the FedRAMP Director to the 3PAO notifying the 3PAO of specific deficiencies in 3PAOs performance. • This letter would also inform that the 3PAO's status is "In Remediation" and noted as such on www.FedRAMP.gov. • This letter will also require a 3PAO to provide a formal CAP to be submitted to FedRAMP within 7 days. • The CAP would need to include specific dates and actions for a 3PAO to complete in response the deficiencies noted in the letter from the FedRAMP Director. • As a part of this CAP, FedRAMP may require a re-assessment by A2LA for validation of the successful completion of the Corrective Action Plan.
Revocation	If a 3PAO has severe deficiencies in their performance or fails to complete a formal CAP from an "In Remediation" Status: • A letter will be sent from the FedRAMP Director to the 3PAO notifying the 3PAO of specific deficiencies in 3PAOs performance and that the 3PAO's status is being revoked and removed from the accredited list on www.FedRAMP.gov. • Revocations will last for a minimum of 6 months. • Revoked vendors are no longer authorized to provide assessment services to FedRAMP CSPs. • If 3PAO wishes to continue to be accredited, FedRAMP will require a 3PAO to commit to a formal CAP or revised CAP if revocation is due to failure to complete a CAP while in remediation status. • The CAP must include specific dates and actions for a 3PAO to correct the deficiencies noted in the letter from the FedRAMP Director and must be approved by the FedRAMP Director. • FedRAMP will require a re-assessment by A2LA for validation of the successful completion of the Corrective Action Plan.

5. REFERENCES

The following documents are references 3PAOs should review and incorporate in to their quality systems. These references will have regular updates as FedRAMP provides additional clarity and expectations.

- **FedRAMP General Document Acceptance Criteria:** The *FedRAMP General Document Acceptance Criteria* details general acceptance criteria for documents submitted to FedRAMP focused on clarity, completeness, conciseness, and consistency. Technical content is not addressed by these acceptance criteria.
- **SAP Review Checklist:** The *SAP Checklist* is a document that lists review items for SAP documents, specific to the SAP subject matter.
- **SAR Review Checklist:** The *SAR Checklist* is a document that lists review items for SAR documents, specific to the SAR subject matter.

APPENDIX A   FEDRAMP ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.