R311 - Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)

March 13, 2017

R311 – Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)

Table of Contents

I. SCOPE 3
II. REFERENCES 3
III. DEFINITIONS 3
IV. GENERAL APPLICATION REQUIREMENTS 4
V. GENERAL 3PAO REQUIREMENTS 5
VI. ISO/IEC 17020 ADDITIONAL REQUIREMENTS 6

Introduction

I. Scope

This document describes the requirements for Third Party Assessment Organizations (3PAOs) seeking A2LA accreditation in the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services.

All 3PAOs seeking accreditation under FedRAMP must meet the general requirements of ISO/IEC 17020:2012.

3PAOs seeking accreditation under FedRAMP through A2LA must also meet A2LA policy and requirements documents listed below.

A 3PAO which also has an affiliated testing laboratory in information technology may apply for accreditation for its testing laboratory concurrently with its application for accreditation for FedRAMP.

II. References

- *R102 – Conditions for Accreditation.*
- *R105 – Requirements When Making Reference to A2LA Accredited Status.*
- *R301 – General Requirements: Accreditation of ISO/IEC 17020 Inspection Bodies.*
- National Institute of Standards and Technology (NIST) Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.* December 2014. Available here: http://dx.doi.org/10.6028/NIST.SP.800-53Ar4
- *FedRAMP Security Assessment Framework (SAF).*
- *FedRAMP System Security Plan (SSP) Template.*
- *FedRAMP System Assessment Plan (SAP) Template.*
- *FedRAMP System Assessment Report (SAR) Template.*
- *FedRAMP Readiness Assessment Report (RAR) Template.*

III. Definitions

3.1 For the purposes of these requirements, the relevant terms and definitions given in ISO/IEC 17000, ISO/IEC 17020, and ISO/IEC Guide 2 apply. As used herein, the following terms shall have the meanings specified:

3.2 Key Inspection Body Personnel**:** Any personnel critical to the accredited inspection process(es) and/or the running of the Inspection Body.

Along with ISO/IEC 17020:2012, applicant 3PAOs must, at a minimum, meet all applicable A2LA policy and requirement documents as specified in Section II of this document, and the requirements listed below.

IV. General Application Requirements

4.1 Applicant and accredited organizations under this program consent to permit A2LA to provide assessment documentation (i.e., assessor reports, checklists, etc.), corrective action plans, and any associated objective evidence of resolution of deficiencies (where applicable) to the FedRAMP Program Management Office (PMO) upon request.

4.2 The organizational chart shall clearly show the functions and lines of authority for staff within the applicant's organization and the relationship, if any, between the FedRAMP Security Assessment functions and other activities of the applicant's organization.

4.3 If the Third Party Assessment Organization (3PAO) is part of an organization that offers consulting services to cloud service providers (CSPs), the 3PAO must provide a customer list for both consulting services and FedRAMP services to A2LA as part of their surveillance assessment application, annual review application, and renewal application. The customer list must include all customers from the previous three years.

4.4 To assess knowledge of the FedRAMP Security Assessment Framework (SAF), new applicants to the program are provided a sample System Security Plan (SSP) for a notional system and they are required to analyze the sample SSP to identify any issues within the document and then record these discrepancies in the template provided. The issues compiled in the template format are then submitted to A2LA. These results will be graded by A2LA during the application review. The applicant's score must be at least 70% to continue through the application process. If a score of less than 70% is achieved, A2LA and the FedRAMP PMO will decide how to proceed with the applicant.

4.5 Once the notional SSP exercise is passed, the applicant must submit a sample System Assessment Plan (SAP) and a sample System Assessment Report (SAR) that describes findings related to deficient controls found in the notional system via the sample SSP. The 3PAO candidate must use the latest versions of the FedRAMP templates when completing the SAP and the SAR. When the SAP and the SAR are submitted to A2LA, A2LA will assign an assessor to complete the on-site assessment. The assessor will review the provided documents prior to the assessment. If the SAP or SAR is deemed to have sufficient technical issues, an applicant will have one chance to re-submit. If an applicant fails to submit an acceptable SAP and/or SAR in the second submission, the application will be halted and the organization will be barred from submitting an application for a period of at least one year. Please note that the submitted deposit will be used to reimburse the assessor for their time.

4.6 As part of a renewal application, if a 3PAO is a type C organization and provides consulting services on FedRAMP, the consulting services may be requested to provide a SAP and SAR based on the notional SSP, for the 3PAO services to evaluate, in order to ensure the consulting services adequately understand FedRAMP.

4.7 As part of their renewal and surveillance application, the 3PAO must provide a list of all FedRAMP engagements completed since the last assessment. The assigned A2LA assessor will choose up to four engagements to review on-site. The SSP, SAP,

SAR, and After Action Reports for these engagements must be available for the assessor's review.

4.8 As part of the annual documentation review, the 3PAO must provide all first SAR submissions along with the final accepted SAR by the Joint Authorization Board (JAB) or Agency Authorizing Officials in the last year. 3PAOs should also provide a copy of all comments provided by the JAB or Agency Authorizing Officials and the detailed corrective actions based on those comments. The scope, number, and severity of comments across engagements will be analyzed to understand the 3PAO's technical knowledge and understanding of FedRAMP.

4.9 For the purpose of onsite A2LA assessments of 3PAOs that have not performed any FedRAMP assessments since the previous A2LA onsite assessment, the 3PAO must:

4.9.1 Provide evidence that its organization has individuals on staff that are knowledgeable on FedRAMP assessments (and assessments that are similar in scope such as cloud assessments, cybersecurity assessments, and other risk assessments).
4.9.2 Submit a new SAP and SAR based on review of a notional SSP.
4.9.3 Provide resumes of all FedRAMP designated assessors.
4.9.4 Provide evidence that all assessors have completed the required training.
4.9.5 Provide evidence that their Quality Management system is still effectively operating.
4.9.6 Provide access to have their facility evaluated, if deemed necessary, by A2LA or the FedRAMP PMO.

V. General 3PAO Requirements

5.1 The 3PAO must accommodate assessments by A2LA and/or the FedRAMP PMO when requested. "Unannounced" assessments are required to occur within ten business days from initial notification.

5.2 A2LA will assess all 3PAO candidates on their knowledge of the technical requirements listed in the FedRAMP Security Assessment Framework in accordance with accompanying NIST 800 series documents.

5.3 A2LA makes recommendations to FedRAMP on whether or not to accredit a 3PAO. A recommendation from A2LA does not imply acceptance to the FedRAMP program. A2LA submits the entire 3PAO assessment package (including the assessor report, corrective actions, correspondences and any Accreditation Council comments) to the FedRAMP PMO for final approval and acceptance in to the FedRAMP program.

5.4 The 3PAO must not submit any actual client records (i.e., SSP, SAP, SAR, etc.) to A2LA. These documents may be reviewed during the on-site assessment, but all confidential information must remain with the 3PAO.

VI. ISO/IEC 17020 Additional Requirements

Additional specific requirements for this program approved by the A2LA Criteria Council are described below. The numbering system for each section below corresponds to the major sections of ISO/IEC 17020. If a section is not listed below, there are no program specific requirements in addition to what is already stated in ISO/IEC 17020.

4.1-Impartiality and Independence

4.1.6 F.1 The 3PAO must meet the requirements of either a Type A or Type C Inspection Body as defined in ISO/IEC 17020:2012. Type B Inspection Bodies are not permitted.

4.1.6 F.2 If a 3PAO is a Type C Inspection Body, the quality of all deliverables (from both assessment and consulting services) must meet all FedRAMP quality standards as defined through the FedRAMP General Document Acceptance Criteria on www.fedramp.gov. Deficiencies in meeting these quality requirements may affect a 3PAO's accreditation through FedRAMP.

4.1.6 F.3 FedRAMP reserves the right to request customer records, policies, procedures, training records, and other similar records for FedRAMP consulting services of 3PAOs who are Type C organizations.

5.1-Administrative Requirements

5.1.4 F.1 The 3PAO must maintain appropriate insurance commensurate with the types of systems they provide assessments for and must disclose to A2LA what insurance policies they currently maintain.

5.2- Organization and Management

5.2.4 F.1 If a 3PAO is part of an organization that offers consulting services to CSPs, the 3PAO is not permitted to inspect a CSP system that it has provided consulting services on.

5.2.4 F.2 If the 3PAO is part of an organization that is also a CSP, the 3PAO is not permitted to inspect the work of their organization's CSP.

5.2.4 F.3 If the 3PAO completes a FedRAMP Readiness Assessment Report (RAR) on behalf of a CSP and the CSP does not submit the report to FedRAMP, the 3PAO can be hired by the CSP for consulting services to fix deficiencies found in the initial report. However, the CSP is required to hire another 3PAO to complete the RAR delivered to FedRAMP.

6.1-Personnel

6.1.2 F.1 All assessments must be staffed by an appropriate number of team members based on the complexity of the cloud system being assessed. This includes, but is not limited to, individuals responsible for scanning, interviews, the examining of artifacts, and report writing. The team must consist of at least three people from the 3PAO, who participate in and support the assessment, one of which is an individual considered to be the senior representative of the 3PAO, one of which is a penetration tester, and one of which is an individual dedicated to quality management of the 3PAO process. The senior representative is responsible for ensuring the assessment activities and evidence is completed fully and meets the FedRAMP requirements and standards. The penetration tester is responsible for ensuring the penetration testing is fully compliant with FedRAMP Penetration Test Guidance. The individual dedicated to quality management is responsible for ensuring that all deliverables from the 3PAO meet the quality standards set forth by FedRAMP. Any 3PAO who wishes to complete an assessment with less than three people must seek approval from the FedRAMP PMO. The senior representative must have the authority to sign off on the work of the other individuals who work on the project. During the onsite assessment by A2LA, the 3PAO must demonstrate the ability to meet the team staff requirements.

6.1.2 F.2 3PAOs must have at least one designated penetration tester on staff or on contract. A penetration tester must be engaged and complete the penetration testing for each assessment of a CSP. If a 3PAO subcontracts the penetration testing to another organization, the penetration tester must adhere to the relevant requirements in Sections 6.2 and 6.3 below.

6.1.5 F.1 The 3PAO must develop a training program for its assessors including, at a minimum, content incorporating FISMA, cloud computing, FedRAMP, and cyber security. This training program can include industry standard certifications or 3PAO developed training content. The 3PAOs must maintain a list of all training courses and a statement for each item on the list as to how the training is related to these knowledge areas. The training program will be analyzed to determine if there is sufficient technical training of assessors for understanding FedRAMP, FISMA, cloud computing, and cyber security.

6.1.7 F.1 Current 3PAO employees must register for all 3PAO training modules and program update sessions provided by FedRAMP within 30 days of the training announcement. All new trainings will be announced by the FedRAMP PMO to the 3PAO's POC on file with the FedRAMP PMO. The 3PAO must maintain certificates of completion for all authorized 3PAO assessors from their organization. Any exceptions to this must be approved by the FedRAMP PMO.

IB1 F.1 Subcontractors who will be used for multiple engagements must be included in the Inspector Witnessing Plan, as required by R301 Section VIII.

6.1.10 F.1 All training records shall list the name of the organization that provided the training, the date the training occurred, and the topic of the training course.

6.1.10 F.2 The 3PAO must maintain training records for all their staff that has been involved with FedRAMP assessments for the past year.

6.2-Facilities and Equipment

6.2.2 F.1 The subcontractor's equipment must fall under the 3PAO's equipment control policies from ISO/IEC 17020:2012 for identification, security, and maintenance.

6.2.13.b F.1 The 3PAO's procedures for protecting and securing the integrity of data (ISO/IEC 17020:2012 clause 6.2.13b) must also address collection, transmission and storage of data collected by the subcontractor and that data shall be held secure by the subcontractor until it is transferred to the 3PAO for final review and reporting.

6.3-Subcontracting

6.3.1 F.1 If a 3PAO subcontracts out any part of the assessment, it must ensure and be able to demonstrate that the subcontractor is competent to perform the tasks and must comply with the relevant requirements and standards.

6.3.1 F.2 The subcontractor must be trained on the 3PAO's quality management system in order to ensure compliance with ISO/IEC 17020:2012. These training records must be maintained by the 3PAO.

6.3.1 F.3 All subcontractors must also meet the same position description requirements of similar positions within the 3PAO organization.

6.3.3 F.1 Whenever subcontracted companies or contracted employees (1099 employees) perform part of the assessment, the responsibility for ensuring that all work is performed in conformance with A2LA and FedRAMP requirements must remain with the 3PAO.

6.3.3 F.2 If a 3PAO chooses to subcontract part of a FedRAMP engagement to another company, the requirements listed above can be waived if the subcontracted company is an accredited 3PAO.

7.1-Inspection Methods and Procedures

7.1.1 F.1 The 3PAO must participate in all quality management checks required by the FedRAMP PMO including any new quality management checks released during the course of the year.

7.1.5 F.1 During the contract review process, the CSP shall be informed of their ability to proactively provide feedback on the 3PAO's performance directly to A2LA and the FedRAMP PMO at any time throughout the process. The *F338 – CSP Evaluation Form* is available on the A2LA CAB portal and the A2LA public website and should be provided to the CSP once the work has begun. The CSP may provide feedback as they see fit throughout the 3PAO assessment process.

7.4-Inspection Reports

7.4.1 F.1 3PAOs must have a documented quality review process for ensuring the quality of deliverables to CSPs and government authorizing official teams.

7.4.1 F.2 All deliverables should be signed off by the 3PAO quality management lead before being delivered to a CSP or government authorizing official team. The quality review process for the 3PAO shall include checking all deliverables to ensure the following:

1. There are no spelling or punctuation errors.
2. All sections of each document delivered are complete, clear, concise, and consistent with each other.
3. All team members of the assessment have reviewed the deliverables.
4. Documents are prepared using the most recent standard templates, without alterations or deletions, and insertions must be agreed upon.

7.4.2 F.1 All SARs written by the 3PAO shall include an authorization recommendation on whether the system can appropriately safeguard government data in accordance with the security classification of the system. The recommendation shall include a summary statement and justification statement.

7.4.2 F.2 All SARs written by the 3PAO shall include all scan results in a readable format such that someone without a scanner license can read the results.

7.4.2 F.3 All RARs written by the 3PAO must adhere to the guidance within the *FedRAMP Readiness Assessment Report (RAR)* template.

7.4.2 F.4 All RARs written by the 3PAO shall include analysis of results from activities including, but not limited to, discovery scans and in person interviews and physical examinations where appropriate. In the event that scan results are requested by the PMO, they should be retained in a readable format such that someone without a scanner license can read the results.

7.4.4 F.1 After each engagement (either readiness or full engagements), the 3PAO must create an After Action Report. 3PAOs should download the *F337 – After Action Report Form* from the A2LA CAB portal. The completed reports should be submitted to the FedRAMP PMO at 3PAO@FedRAMP.gov and to A2LA at FedRAMP@A2LA.org within 30 days of the end of the engagement.

8.1-Options

8.1.1 F.1 As long as the 3PAO maintains accreditation, it must continue to implement its ISO/IEC 17020:2012 management system even if they are not working on any FedRAMP engagements.

8.1.1 F.2 Along with ISO/IEC 17020:2012, applicant 3PAOs must, at a minimum, meet all applicable A2LA requirements.

8.1.1 F.3 If compliance to ISO/IEC 17020 is new for the organization, the organization must use their ISO/IEC 17020 quality management system for six months prior to applying to become an accredited 3PAO.

8.1.3 F.1 All 3PAO applicants will be assessed on the management system requirements listed in Section 8, Option A of ISO/IEC 17020:2012.

REVISION HISTORY

DATE	REVISION
11/8/2013	Initial publication.
12/22/2016	Complete document re-write
03/13/2017	Removal of requirement that a 3PAO cannot assess a CSP that inherits or leverages a portion of its security requirements from a CSP the 3PAO has previously consulted on.