

FedRAMP 3PAO Requirements



FedRAMP

Version 1.0

July 20, 2015

2. General Requirements

- 2.1** Along with ISO/IEC 17020:2012, applicant Third Party Assessment Organizations (3PAO) must at a minimum, meet all applicable A2LA policy and requirement documents as specified in Section 2.3 of this document, and the requirements listed below.
- 2.2** The 3PAO must either meet the requirements of a Type A or Type C Inspection Body as defined in ISO/IEC 17020:2012; Type B Inspection Bodies are not permitted.
 - 2.2.1** If a 3PAO is a type C organization, the quality of deliverables of any consulting for FedRAMP must meet all FedRAMP quality standards as defined through guidance documents on www.FedRAMP.gov. Deficiencies in meeting these quality requirements for consulting on FedRAMP may affect a 3PAO's accreditation through FedRAMP.
 - 2.2.2** 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.
- 2.3** The 3PAO must sign and return F311a – FedRAMP 3PAO Consent Agreement with all applications.
- 2.4** If compliance to ISO/IEC 17020 is new for the organization, the organization must use their ISO/IEC 17020 quality management system for 6 months prior to applying to become an accredited 3PAO.
- 2.5** All 3PAO applicants will be assessed on the management system requirements listed in Section 8, Option A of ISO/IEC 17020:2012.
 - 2.5.1** As long as the 3PAO maintains accreditation, they shall continue to implement their ISO/IEC 17020 management system even if they are not working on any FedRAMP engagements.
- 2.6** The 3PAO must accommodate unannounced assessments by A2LA and/or the FedRAMP Program Management Office (PMO) when requested.
- 2.7** If the 3PAO is part of an organization that offers consulting services to Cloud Service Providers (CSPs), the 3PAO is not permitted to inspect the work of any CSP that it has provided consulting services to.
- 2.8** If the 3PAO is part of an organization that offers consulting services to CSPs, the 3PAO must provide a customer list for both consulting services and FedRAMP services to A2LA at the time of their initial application, as part of their surveillance assessment application, annual review application, and renewal application. The customer list must include all customers from

the previous 3 years.

- 2.9** To assess knowledge of the FedRAMP Security Assessment Framework, new applicants to the program will be provided a sample System Security Plan and must submit with their application a sample Security Assessment Plan (SAP), and a sample Security Assessment Report (SAR) that describes findings related to systems described in the System Security Plan provided to them. The 3PAO candidate must use the FedRAMP templates when completing the SAP and the SAR.
- 2.10** As part of their renewal application, the 3PAO must provide a list of all FedRAMP-related engagements completed since the last assessment. The assigned A2LA assessor will choose up to four assessment engagements to review on-site. The System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), and After Action Reports for these engagements must be available for the assessor's review.
- 2.11** As part of the annual review, the 3PAO must provide a list of all SARs (from the last review year) that required multiple revisions such that an After Action Report was required.
- 2.12** 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. *Additional information on training requirements can be found in section 9 below.*
- 2.13** The 3PAO must maintain appropriate insurance commiserate with the types of systems they provide assessments for and must disclose what insurance policies they currently maintain to A2LA.
- 2.14** Accreditation granted to a 3PAO 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.
- 2.15** The 3PAO must participate in all quality management checks required by the FedRAMP program including any new quality management checks released during the course of the year.
- 2.16** During annual assessments, for 3PAOs that have not performed any FedRAMP assessments in the last year, the 3PAO must provide: 1) evidence that their organization has individuals on staff that are knowledgeable of FedRAMP and any updates over the last year, this should also include a list of any assessments of similar scope and nature to FedRAMP assessments; 2) submit a new SAP and SAR based on a review of a new SSP that new 3PAOs must review and

respond to when they first apply; 4) all assessors have completed the required training (see Section 9 below); 5) evidence that their Quality Management system is still effectively operating; 6) access to have their facility evaluated if deemed necessary by A2LA or the FedRAMP PMO.

3. 3PAO Resource Requirements for Assessments

- 3.1** All assessments shall require that a minimum of three people from the 3PAO be present, one of which is an individual considered the senior representative of the 3PAO, and one of which is an individual dedicated to quality management of the 3PAO process. Any exceptions to this must be approved by 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.
- 3.2** In addition to the 3 people required for the assessment, 3PAOs must at a minimum have one qualified penetration tester on staff. A qualified penetration tester must be engaged and complete the penetration testing for each assessment of a 3PAO. If a 3PAO subcontracts the penetration testing, they must follow all provisions in section 7.6 below.
- 3.3** If the 3PAO is part of an organization that is also a Cloud Service Provider (CSP), the 3PAO is not permitted to inspect the work of their organization's CSP.
- 3.4** 3PAOs must have position descriptions for each position within its organization involved in security assessment activities. The position descriptions must include required years of experience, education, and training. The position descriptions for a senior representative of the 3PAO must include at least 5 years of FISMA experience and at least 2 industry standard cybersecurity certifications.
- 3.5** If a 3PAO subcontracts out any part of the assessment, it shall ensure and be able to demonstrate that the subcontractor is competent to perform the tasks and, where applicable, complies with the relevant requirements and standards.
- 3.6** 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 shall remain with the 3PAO.
 - 3.6.1** The 3PAO management system shall address ISO/IEC 17020 Section 6.1 with respect to the subcontractors.

- 3.6.2 The subcontractor shall be trained on the 3PAO's quality management system in order to ensure compliance with ISO/IEC 17020. These training records shall be maintained.
- 3.6.3 The subcontractor's equipment shall fall under the 3PAO's equipment control policies from ISO/IEC 17020 for identification, security, and maintenance.
- 3.6.4 The 3PAO's procedures for protecting and securing the integrity of data (ISO/IEC 17020 clause 6.2.13b) shall 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.
- 3.6.5 Subcontractors who will be used for multiple engagements shall be included in the Inspector Witnessing Plan, as required by R301 Section VIII.
- 3.6.6 All subcontractors must also meet the same position description requirements of similar positions within the 3PAO organization.

4. Protection of Sensitive Information

- 4.1 The 3PAO shall have documented policies and procedures established for protecting CSP data and information.
- 4.2 The 3PAO must not submit any actual client records (SSP, SAP, SAR) to A2LA. These documents may be reviewed during the on-site assessment but all confidential information shall remain with the 3PAO.

5. Training

- 5.1 3PAOs must attend/register for all mandatory training and program update sessions provided by FedRAMP within 30 days of the training being announced by FedRAMP. All new trainings will be announced by the FedRAMP PMO to the 3PAOs POC on file with the FedRAMP PMO. The FedRAMP 3PAO POC must provide a copy of all assessor training certificates to the FedRAMP PMO within 30 days of this announcement. Any exceptions to this must be approved by the FedRAMP PMO.
- 5.2 The 3PAO must develop a training program for assessors. This training program can include industry standard certifications or 3PAO developed training programs. If a 3PAO develops an internal training program, all training program materials must be made available for A2LA and the FedRAMP PMO to review.

- 5.3** The 3PAO training program must incorporate FISMA, cloud computing, FedRAMP, and cyber security. Each individual working on a FedRAMP assessment must ensure that they obtain 60 hours of training each year in one or more of these knowledge areas. The 60 hours is in addition to the mandatory trainings through the FedRAMP PMO.
- 5.4** All training records shall list the name of the organization that provided the training and the date the training occurred. These records shall be submitted to A2LA during each annual review and at the time of the initial application.
- 5.5** The 3PAO must provide training records for all staff that has been involved with FedRAMP assessments for the past year during their annual review.
- 5.6** All training records shall indicate if the training courses listed included training related to cloud computing, FISMA, or FedRAMP.

6. Quality Control of Assessments

- 6.1** When developing a SAR, the 3PAO must indicate the name of the person responsible for attesting to the accuracy of the testing for all items in the SAR. The name and contact information of the responsible person(s) shall be noted at the bottom of each section. If different people created different content for different sections of the SAR, then the different team(s) and/or members shall be listed with the responsible person(s) name, phone number, and email address. If the SAR does not yet have signatory indicators, the senior person responsible for attesting to the accuracy of the information should insert or attach a table at the end of the SAR with names next to each section number.
- 6.2** 3PAOs must develop a quality review process for ensuring the quality of deliverables to CSPs and government authorizing official teams.
- 6.3** The quality review process for the 3PAO shall include checking all deliverables to ensure the following:
 - a) No spelling and punctuation errors
 - b) All sections of each document delivered are consistent with each other
 - c) All sections of the SAR have a responsible name next to it
 - d) All team members of the assessment have reviewed the deliverables

All deliverables should be signed off by the 3PAO quality management lead before being delivered to a CSP or government

authorizing official team.

6.4 After each assessment, the 3PAO must create an After Action Report that includes the following information:

- a) Name of CSP
- b) Names of all members on 3PAO Assessment Team
- c) Number of times the SAR was returned (by the Authorizing Official) to the 3PAO for revision¹
- d) List of items from SAR that required revisions
- e) Indication if Quality Management process was updated after assessment
- f) Lessons Learned
- g) All After Action Reports must be signed by the senior 3PAO representative responsible for the assessment.

6.5 At the end of each engagement, the 3PAO must ask the CSP to perform an evaluation of the 3PAO service provided to them. The 3PAO should indicate to the CSP how to send the evaluation to A2LA. The 3PAO must be able to provide evidence that an evaluation form was sent to the CSP. (The 3PAO has no responsibility for ensuring that the CSP fills out the evaluation and actually sends it in to A2LA.)

- a) Each 3PAO evaluation by a CSP shall be sent in to A2LA by the CSP directly without participation or review by the 3PAO.
- b) The evaluation shall include the following rating criteria:

Response Scale	
Strongly Agree	5
Agree	4
Undecided	3
Disagree	2
Strongly Disagree	1
Not Applicable	0

	Criteria	Response
1)	The 3PAO is knowledgeable about FedRAMP.	
2)	The 3PAO was able to identify security vulnerabilities on our system.	
3)	The 3PAO was able to communicate issues to us so we could understand them.	

¹ This requirement must be consistent with what the government authorizing official team would confirm if A2LA or the FedRAMP PMO were to be contacted by the authorizing official team.

4)	The 3PAO is well organized and able to forecast scheduling activities.	
5)	The 3PAO had adequate follow-up skills.	
6)	The 3PAO is knowledgeable about FISMA.	
7)	The 3PAO is knowledgeable about cyber security.	
8)	I would consider hiring the 3PAO again in the future.	
9)	Please provide strengths of the 3PAO	
10)	Please provide a listing of any issues experienced during the assessment with the 3PAOs performance.	

7. Assessment Report Requirements

- 7.1** 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.
- 7.2** 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.