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

November 2013

© 2013 by A2LA.

All rights reserved. No part of this document may be reproduced in any form or by any means without the prior written permission of A2LA.
R311 – Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)

Table of Contents

1.0 SCOPE.................................................................................................................................................................... 3
2.0 REFERENCES ...................................................................................................................................................... 3
3.0 DEFINITIONS....................................................................................................................................................... 4
4.0 GENERAL REQUIREMENTS............................................................................................................................. 4
5.0 SPECIFIC REQUIREMENTS............................................................................................................................... 4
Introduction

1.0 Scope

This document describes the requirements for Third Party Assessment Organizations (3PAO) 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 the 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:

- P101 – Rules for Making Reference to A2LA Accredited Status
- R102 – Conditions of Accreditation
- R301 – General Requirements: Accreditation of ISO/IEC 17020 Inspection Bodies

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.

2.0 References

- FedRAMP Security Assessment Framework.
- P101 – Rules for Making Reference to A2LA Accredited Status.
- R102 – Conditions for Accreditation.
- R301 – General Requirements: Accreditation of ISO/IEC 17020 Inspection Bodies.
3.0 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.

4.0 General Requirements

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 1.0 of this document, and the requirements listed below.

4.1 The 3PAO must either meet the requirements of a Type A or Type C Inspection Body; Type B Inspection Bodies are not permitted.

4.2 The organization 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 3PAO is part of an organization that is also a Cloud Service Provider (CSP) the 3PAO is not permitted to inspect the work of the CSP as part of FedRAMP related activities.

4.4 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.

4.5 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 as part of their surveillance assessment application, annual review application, and renewal application. The customer list must include all customers.

4.6 The 3PAO must participate in quality checks offered through the FedRAMP program when they become available.

4.7 Attend all mandatory training and program update sessions provided by FedRAMP.
4.8 The 3PAO must sign and return *F311a – FedRAMP 3PAO Consent Agreement* with all applications.

4.9 Per *FedRAMP Security Assessment Framework* new applicants to the program must submit with their application a sample System Security Plan (SSP), Security Assessment Plan (SAP), and Security Assessment Report (SAR), using the FedRAMP templates and assessment cases located within the application.

4.10 As part of their renewal and surveillance applications, the 3PAO must provide a list of all FedRAMP related jobs completed since the last on-site assessment. The assigned assessor will choose up to four of these jobs to review. The System Security Plan (SSP), Security Assessment Plan (SAP) and Security Assessment Report (SAR) for these jobs must be submitted to the assessor prior to the assessment for the assessor’s review.

4.11 As part of the annual review submission documentation, the 3PAO must provide a list of all SARs that have been rejected by the Joint Authorization Board (JAB) that have occurred since the last on-site assessment.

4.12 The 3PAO must provide training records for all staff that has been involved with FedRAMP inspections for the past year during their annual review.

4.13 The 3PAO must report to A2LA within thirty (30) business days, and in writing, of changes or pending changes in any aspect of the 3PAO’s status or operation that affects the:

a. Legal, commercial, organizational, or ownership status;
b. Organization and management, including key inspection body personnel;
c. Location;
d. Facilities, working environment, or other resources;
e. Accepted 3PAO authorized representative (point of contact) or alternate representative; or
f. Other such matters that may otherwise materially affect its ability to perform assessments.

Note: All 3PAO applicants will be assessed to the management system requirements listed in Section 8, Option A of ISO/IEC 17020:2012.
5.0 Technical Requirements

5.1 All 3PAOs will also be assessed to the technical requirements listed in the FedRAMP Security Assessment Framework in accordance with accompanying NIST 800 series documents such as NIST SP 800-53A.

5.2 All scopes for the FedRAMP program will include the following footnote for FedRAMP accredited work:

   Accreditation to the requirements of the FedRAMP program does not imply acceptance to the FedRAMP program. Please see the FedRAMP website www.fedramp.gov for a listing of accredited 3PAOs.

5.3 After the accreditation process is completed the application will be forwarded to FedRAMP for their review. Final acceptance into the FedRAMP program is maintained by FedRAMP.

REVISION HISTORY

<table>
<thead>
<tr>
<th>DATE</th>
<th>REVISION</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/8/2013</td>
<td>Initial publication.</td>
</tr>
</tbody>
</table>