

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP 3PAO Application & Approval Process

Lisa Carnahan

Computer Scientist - NIST Services

National Institute of Standards & Technology





3PAO Acceptance Process

Review Application

- Potential 3PAO reviews application materials found at gsa.gov/FedRAMP.

Gather Materials

- Potential 3PAO completes application and gathers artifacts.

Security Assessment Report	System Security Plan	Applicant Assessment Test Procedures
----------------------------	----------------------	--------------------------------------

Submit Application

- Potential 3PAO submits application to FedRAMP office to demonstrate technical competency & ability to conform with technical requirements.

Review by ERB

- Expert Review Board (ERB) composed of parts of GSA and ISO independent cybersecurity experts review the application.

Applicant Decision

- FedRAMP PMO reviews ERB recommendation and provides 3PAO an acceptance decision.

Accepted

Accredited 3PAO for Use by Agency and CSPs



Application and Process Description

- <http://www.fedramp.gov>
- Program Description: what, how & when
- Application: Form and document submission requirements

The screenshot shows a Microsoft Internet Explorer browser window displaying the GSA website page for Third Party Assessment Organizations (3PAOs). The browser's address bar shows the URL <http://www.gsa.gov/portal/category/102387>. The page header includes the GSA logo and navigation links such as Home, Newsroom, Regions, Staff Directory, Careers, Forms, e-Tools, and Quick. A search bar is also present. The main content area features a sidebar with a navigation menu for FedRAMP, including links for Overview, About FedRAMP, Agencies, Third Party Assessment Organizations (3PAOs), 3PAO Application Materials, 3PAO Application Process, FedRAMP Industry Day, Cloud Service Providers (CSPs), and FAQs. The main heading is "Third Party Assessment Organizations (3PAOs)". The text explains that as part of the FedRAMP process, cloud service providers (CSPs) must use a FedRAMP approved third party assessor to independently validate and verify that they meet the FedRAMP requirements. It also states that in coordination with NIST, FedRAMP implemented a conformity assessment process to qualify 3PAOs. This conformity assessment process qualifies 3PAOs according to two requirements:

- Independence and quality management in accordance with ISO standards
- Technical competence through FISMA knowledge testing

The text further explains that Third Party Assessment Organizations (3PAO) perform initial and periodic assessment of CSP systems per FedRAMP requirements, provide evidence of compliance, and play an on-going role in ensuring CSPs meet requirements. FedRAMP provisional authorizations must include an assessment by an accredited 3PAO to ensure a consistent assessment process.

Registration for the December 16, 2011 3PAO Industry Day is now over capacity - thank you very much for your interest. Video from the session will be made available by...

The right sidebar contains a "CONTACTS" section with the following information:

CONTACTS
General Inquiries
info@fedramp.gov
Press Inquiries
Bob Lesino
202-501-9113

The bottom of the browser window shows the address bar with the URL <http://www.gsa.gov/portal/category/102379> and the status bar indicating "Internet" and "100%" zoom.



Applicant Review: Key Dates and Process

- Provided in 3PAO Program Description
- Application accepted for initial list: Jan 6 thru Jan 20
 - Application received will be considered for initial list
 - Applications will be queued in order received
 - Applicant undergoes a FedRAMP requirements evaluation by FedRAMP PMO and Expert Review Board (GSA & NIST)
 - Completeness check
 - Review of documents and evidence received with application form
 - Determination that applicant meets ISO/IEC 17020:1998
 - Determination that applicant has required technical competence
 - Determination that applicant meets additional FedRAMP program-specific requirements



Applicant Process (cont.)

- If requirement(s) are not met
 - Applicant receives a non-conformity letter
 - Applicant may address with a revised application
 - Non-conformance letters received prior to Jan 20 indicates that applicant will not be considered for initial list; however can be listed subsequently
- All applicants meeting the requirements
 - Receive an accreditation memo stating acceptance as FedRAMP 3PAO
 - Will be listed, AS A GROUP, on the initial list of FedRAMP-accredited 3PAOs
- Subsequent accredited 3PAOs will be added to the list, in real-time upon release of accreditation memo



Industry Questions

- 3PAO / CSP Conflict of Interest, Firewall
- Teaming
- 3PAO Application due date
- Notional / Hypothetical Systems
- Measures of Success for Accredited 3PAOs