300-0: 3PAO Obligations and Performance Guide

Slide	Audio Script
	Welcome to the 3rd Party Assessment Organization (3PAO) Introduction training course, with a focus on obligations and performance standards. While these training modules are designed for 3PAOs, all FedRAMP stakeholders can participate. Participants will gain a better understanding of the level of analysis and testing that a 3PAO must conduct on a Cloud Service Offering, as the FedRAMP assessment requires a comprehensive understanding of cloud technologies and requirements from the Federal Information Security Modernization Act or FISMA.
	This course consists of 4 microlearning modules, ranging from 4.5 minutes to 15.5 minutes, with a total course time of 41 minutes. This is the first of 8 required FedRAMP training courses for Third Party Assessment Organizations, or 3PAOs. **This first course, 300-0**: 3PAO Obligations and Performance Guide, provides 3PAOs with the FedRAMP requirements for attaining and maintaining good standing in the FedRAMP 3PAO Program. It focuses on organizations that wish to be accredited as a FedRAMP Third Party Assessment Organization. A FedRAMP 3PAO must be assessed by the American Association for Laboratory Accreditation (A2LA), to the requirements of ISO/IEC 17020:2012 for the Operation of Various Types of Bodies Performing Inspection. Accreditation refers to the recognition given to an organization (such as an inspection body or 3PAO) by an authoritative body. **The second course is 300-A**: The importance of a Readiness Assessment Report, or RAR. This course provides guidance on how the FedRAMP security requirements must align with a CSP's system security capabilities before the CSP system can be approved as FedRAMP Ready.

The third course, 300-B: 3PAO Security Assessment Plan, or (SAP) Guidance, provides 3PAOs with guidance on FedRAMP requirements for creating a robust SAP.

The fourth course, 300-C: 3PAO Security Assessment Report Guidance or SAR, provides 3PAOs with guidance on FedRAMP requirements for creating a robust SAR.

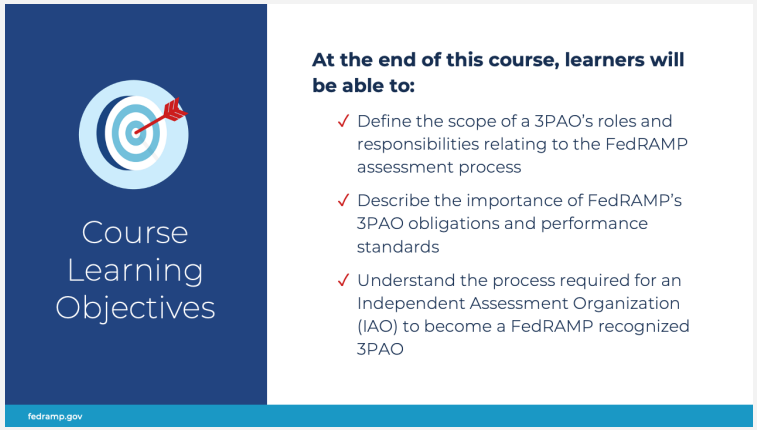
The fifth course 300-D: 3PAO Documenting Evidence Procedures, provides 3PAOs with guidance on FedRAMP requirements for documenting evidence collected during the assessment and how to populate the SAR.

The sixth course, 300-E: 3PAO Vulnerability Scanning Methodology and Documentation, provides 3PAOs with guidance on FedRAMP requirements for conducting vulnerability scanning on a system and how the results must be documented to meet FedRAMP requirements for initial authorization assessments and annual assessments.

The seventh course, 300-F: Review of Security Assessment Report (SAR) Tables, provides 3PAOs with guidance on FedRAMP requirements for populating SAR tables to ensure that all tables are correctly populated.

The eighth and last course, 300-G: Review of Penetration Testing Guidance, provides an overview of the rigor and attention to detail required to complete a FedRAMP Penetration Test.

Each course within this learning path is segmented into micro modules in order to make the material easier to digest and concentrate on one concept at a time.



Course Learning Objectives.

At the end of this 300-0 course, learners will be able to:

- Define the scope of the 3PAO roles and responsibilities relating to the FedRAMP assessment processes
- Describe the importance of the of the 3PAO obligation and performance standards
- Recall the process required for an Independent Assessment Organization (IAO) to become a FedRAMP recognized 3PAO

The shift to cloud-based services and the use of third-party providers have become integral to modernizing many government agencies, but it is important to understand the risks associated and how to mitigate them with regulatory requirements.

This is where FedRAMP comes in. FedRAMP provides a cost-effective, risk-based approach to the adoption and use of cloud services by making them available to federal agencies.

FedRAMP reduces duplicative efforts, inconsistencies, and cost inefficiencies associated with the security authorization process. Back in 2011, through the original OMB Memo, FedRAMP established a public-private partnership to promote innovation and the advancement of more secure information technologies. By using an agile and flexible framework, FedRAMP enables the federal government to continue advancing the agencies' adoption of cloud computing by creating transparent standards and processes for security authorizations at scale.

Within FedRAMP's compliance process, 3PAOs play a critical role. 3PAOs are tasked with assessing the security of the offerings of cloud service providers (CSPs) to help them satisfy FedRAMP's compliance regulations. The 3PAOs' security assessment expertise allows federal agencies to make informed, risk-based decisions regarding the authorization and secure use of cloud service offerings (CSOs).

As you will see through this training, the path to becoming a 3PAO is just as important as the 3PAO role itself.

So who is involved in this process? The four main stakeholders are:

FedRAMP: The Federal Risk and Authorization Management Program.

This is a United States federal government-wide program, recently made into federal law as part of the “FedRAMP Authorization Act”. FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Next is:

A2LA: American Association for Laboratory Accreditation.

This is a non-profit organization dedicated to the formal certification of competent testing and calibration laboratories, inspection bodies, proficiency testing providers, and reference material producers.

Next is:

3PAOs: Third-party assessment organizations.

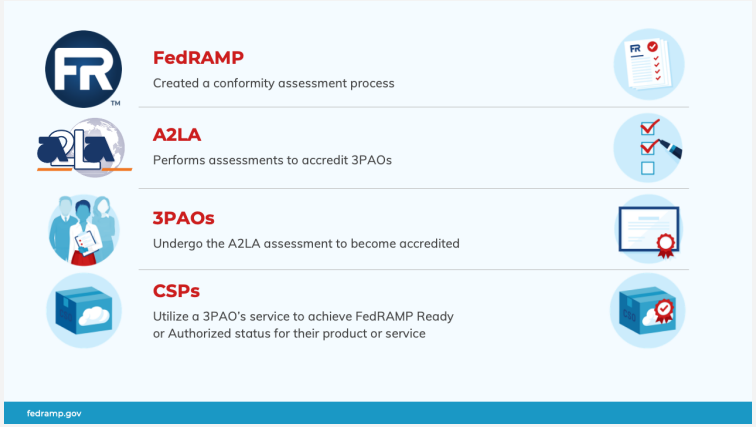
These are organizations designated as the evaluators of cloud service offerings to ensure transparency between government and cloud providers and consistency in data security strategies.

And lastly, we have:

CSPs: Cloud Service Providers

These are the companies that are offering a cloud-based platform, infrastructure, and/or application service that are seeking FedRAMP Authorization status based on a favorable 3PAO recommendation.

Each party plays an important role in making informed decisions regarding the security of Cloud Service Offerings to federal agencies.



Throughout the 3PAO process, each stakeholder holds a significant role:

- **First is FedRAMP.** FedRAMP coordinated and collaborated with NIST to develop and implement the conformity assessment program and process to recognize 3PAOs through accreditation under ISO/IEC standards. This provides assurance that the FedRAMP process is consistently applied across all CSPs that seek to provide services to the federal government. The 3PAO is a "conformity assessment body" that is assessed annually in order to provide consistent assessment services. This "conformity assessment body" is the 3PAO who, in turn provides assessment services, the outcome of which serves as the basis from which the federal government makes informed, risk-based authorization decisions for the government's use of cloud products and services.
- **Next is A2LA.** A2LA performs the ISO conformity assessment to accredit 3PAOs under 17020. A2LA then provides a recommendation to FedRAMP as to whether the 3PAO's technical competence and experience in inspecting CSP systems could be acceptable for FedRAMP. The FedRAMP PMO then either approves or disapproves the recommendation.
- **Next is the 3PAOs.** The 3PAOs begin as Independent Assessment Organizations under the ISO 17020 standard to provide proof that the organization is well-equipped to a FedRAMP-recognized 3PAO.
- **And lastly we have the CSPs.** Once the Independent Assessment Organization has been FedRAMP-recognized as a 3PAO, they are able to provide independent assessments of CSPs' implementation of FedRAMP security authorization requirements.

This process ensures 3PAOs have the ISO 17020 accreditation and meet the necessary quality, independence, impartiality, and FedRAMP knowledge requirements to perform independent security assessments required by FedRAMP. This process is also critical for producing consistent, independent, and impartial third-party assessments of security controls implemented by CSPs.

The 4 key roles and responsibilities of a 3PAO are:

- Quality,
- Independence,
- Impartiality, and
- FedRAMP Knowledge.

In order to maintain favorable status in the FedRAMP Program, 3PAOs must consistently demonstrate impartiality, independence, quality, and FedRAMP knowledge as they perform security assessments.

The key elements of quality, independence, impartiality, and FedRAMP Knowledge are:

- 3PAO assessments are captured in FedRAMP security documentation/templates, which must be delivered with high quality and consistency
- 3PAOs are required to independently assess the effectiveness of security controls associated with cloud service offerings (CSOs)
- 3PAOs are required to provide proof that their ownership, governance, personnel, finances, and payments for work align with all U.S. laws, policies, and regulations to maintain impartiality
- 3PAO personnel must demonstrate technical competence and FedRAMP knowledge through education, training, technical knowledge, skills, and experience

These standards are critical because a 3PAO evaluates a CSO from a security and risk perspective using dependable and repeatable processes. They verify the vendor's security implementations, compare them with the controls specified in FedRAMP, and confirm whether the implementations match the controls requirements. The 3PAO also gathers and reviews the artifacts or documents of a CSP's security authorization package in accordance with FedRAMP requirements. They consider the overall risk posture of the vendor's cloud environment when making authorization recommendations to Authorizing Officials.

The 3PAO plays a role at various stages of the CSP assessment and authorization process:

The first stage is the **Readiness Assessment**. The intent of the Readiness Assessment is to have a 3PAO attest to a CSP's readiness for the FedRAMP authorization process at either the Moderate or High impact level. By completing a Readiness Assessment Report, or (RAR), a CSP should be able to understand if their Cloud Service Offering (CSO) has the key technical capabilities in place, and operating as intended in a production environment, to obtain a FedRAMP authorization.

In the RAR, a 3PAO documents and validates a CSP's full implementation of the technical capabilities required to meet FedRAMP security requirements, which is the biggest hurdle for CSPs to obtain FedRAMP authorization. For a Readiness Assessment, the 3PAO must:

- Ensure the system being assessed is operational
- Follow all requirements in accordance with the FedRAMP High RAR template or FedRAMP Moderate RAR template
- Provide a clear attestation in the RAR with no conditional or ambiguous attestations - (all attestations must be logical and align with the proposed residual risk of operating the system)
- Notify FedRAMP, at least two weeks prior to submission of a RAR, via info@fedramp.gov
- Upload the RAR to the appropriate repository for the FedRAMP PMO review
- Provide notification email to info@fedramp.gov of the availability of the RAR
- Accept feedback from FedRAMP to facilitate FedRAMP Ready decisions
- Collect additional artifacts, as may be required from the CSP, to clarify the security posture of the system
- Maintain proper chain of custody, as applicable, for artifacts and documents associated with the readiness assessment
- Review 3PAO performance feedback, from FedRAMP, and utilize the 3PAO's QMS or corrective action plans, as needed to ensure that any errors with process are addressed

Next is the Initial Authorization Assessment. During the Initial Authorization Assessment, the 3PAO:

- Assesses the security controls implemented by CSPs through observation, interviews, and/or manual testing per 800-53 requirements

- Follows all requirement documents available on the FedRAMP website, as per the 3PAO Obligations and Performance Standards Guide
- Coordinates with the CSP, then notifies the PMO at least two weeks prior to package submission via info@fedramp.gov
- Uploads all documentation for which they are responsible (e.g., SAP, SAR, scan files, evidence) and see to it that CSP documentation is uploaded by the CSP in a timely manner
- Accepts SAP, SAR, and Penetration Testing Reports product feedback from FedRAMP to facilitate CSP/CSO FedRAMP approval
- Collects additional artifacts as required from the CSP to clarify its security posture
- Reviews organizational feedback from FedRAMP and utilizes the 3PAO Quality Management System (QMS), corrective actions, and complaints process, as needed

The next stage is the Annual Assessment. FedRAMP requires CSPs to undergo an annual security assessment of their Cloud Service Offering or CSO per security control CA-2. Both CSPs and 3PAOs are responsible for submitting components of a complete Annual Assessment package. For the annual assessment, FedRAMP relies heavily on the 3PAO to:

- Ensure the system being assessed is still operational
- Ensure all significant changes to the system, since the last assessment, have appropriate documentation and are uploaded into the respective package repository
- Ensure all requirements are followed in accordance with the FedRAMP Annual Assessment templates
- Notify FedRAMP, at least two weeks prior to annual security assessment submission, via info@fedramp.gov
- Upload all 3PAO-required documentation to the appropriate repository and provide a notification email to info@fedramp.gov, as well as applicable stakeholders to include the agency representative
- Accept and incorporate SAP, SAR, and Penetration Testing Report feedback and work with FedRAMP agency AOs to facilitate continued FedRAMP Authorization decisions
- Collect additional artifacts, as required, from the CSP to clarify the system's security posture
- Maintain proper chain of custody, as applicable, for artifacts and documents associated with

the annual security assessment

- Just as with the initial authorization, review organizational feedback from FedRAMP and utilize the 3PAO's QMS and corrective action plans, as needed

The last phase is the Significant Changes to FedRAMP Authorized Cloud offerings. FedRAMP recognizes that the marketplace is constantly changing and that to remain competitive, CSPs need to make changes to their cloud services. FedRAMP considers a change to be "significant" if it affects the security state of the information system, which was the original state that formed the AO's decision to issue the authorization of the cloud service. During the significant change phase the 3PAO:

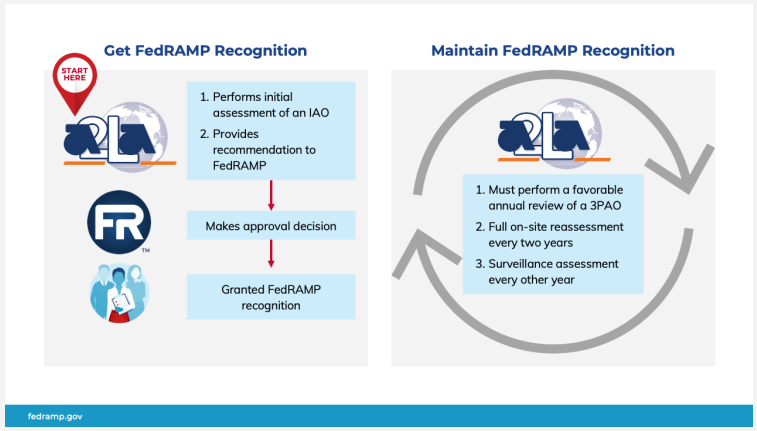
- Reviews the Significant Change Request to determine the scope of testing required
- Develops the Security Assessment Plan which defines the scope of testing
- Conducts testing and provides recommendations and status updates to FedRAMP and agency AOs related to significant changes
- Uploads all required documentation to the appropriate repository, and provides a notification email to info@fedramp.gov, as well as applicable stakeholders to include the agency representative
- Maintains proper chain of custody, as applicable, for artifacts and documents associated with significant change assessments

A 3PAO may perform one or all of these types of assessments for Cloud Service Offerings. Many 3PAOs often choose to perform consulting services for CSPs, rather than provide assessments. This is fine and acceptable as long as the 3PAO does not consult and then assess the same system.

The Independent Assessment Organization (IAO) accreditation process is very rigorous, as it requires these assessment organizations to meet very high standards for quality and technical competence. An accredited IAO has demonstrated technical competence and compliance with the general requirements of ISO/IEC 17020:2012, supplemented by R311, as well as FedRAMP specific requirements to the degree in which they have been recommended and accepted. Once the IAO has met the A2LA requirements and A2LA feels that the organization would be a good fit for FedRAMP, A2LA makes a formal recommendation to the FedRAMP PMO to accept this IAO as a FedRAMP 3PAO. If FedRAMP agrees, the IAO then must go through a series of steps before the organization is listed on the FedRAMP Marketplace as a FedRAMP-recognized 3PAO.

Since a FedRAMP 3PAO is a certified, independent assessor that has been recognized by the FedRAMP PMO, this certification tells CSPs who are looking to pursue certification through the FedRAMP process, that this organization has passed the necessary rigor and can help them pursue FedRAMP authorization.

These next few slides will dive into the process and rigor required of 3PAOs to demonstrate, in order to receive certification and maintain it.



In order for an Independent Assessment Organization, or IAO, to become a FedRAMP-recognized 3PAO:

- An IAO must complete the one year A2LA Cybersecurity Inspection Body Program conformity assessment requirement
- An IAO must be interested in becoming highly process-oriented, which is the basis for the ISO 17020 conformity assessment
- Each organization must also set up a quality management system (QMS) internally to ensure that every assessment is completed on every cloud service offering in a Firm, Fair, and Consistent, or “FFC” manner
- Each organization must send one team (3 members as required by the R311) to successfully complete the Baltimore Cyber Range Proficiency exercise (failure is not an option for continued participation)
- The IAO must demonstrate proficiency to A2LA in the context of their defined scope of

accreditation throughout the course of one year

- As long as the requirements are met, after the one-year period, the “independent assessment organization” petitions A2LA which may recommend them to FedRAMP for 3PAO status
- Success in the Cybersecurity Assessment Body Program is ultimately measured by A2LA recommending the IAO to become a FedRAMP 3PAO

After successfully completing the A2LA Cybersecurity Inspection Body Program, to become a 3PAO, the IAO must complete these additional steps and rigor as outlined:

- The FedRAMP PMO may ask for additional artifacts from the IAO to support the PMO’s decision to accept the IAO into the FedRAMP 3PAO Program
- FedRAMP PMO approves or disapproves the A2LA recommendation based on the artifacts provided
- If approved, a new 3PAO must coordinate with the FedRAMP PMO to schedule a FedRAMP 3PAO Kickoff Meeting
- After the Kickoff Meeting, the 3PAO must review the most recent FedRAMP branding guidance and ensure adherence in all branding and marketing materials when referencing FedRAMP
- Each individual member of the IAO must attest in writing to their proficiency in FISMA and FedRAMP as well as what the IAO has chosen as its scope of accreditation
- The new 3PAO must now successfully complete the Baltimore Cyber Range proficiency exercise. The entire assessor team (or multiple teams) as defined in the R311 must successfully complete the Range proficiency exercise
- Only the individual members of the 3PAO who meet all the competency requirements as outlined in the R311 may perform “FedRAMP” assessments

It is important to note that If an assessing organization IS NOT LISTED on the FedRAMP Marketplace, that organization is not a FedRAMP 3PAO as they have not achieved the FedRAMP recognition.

Note that a 3PAO which allows its 17020 accreditation to lapse is also no longer a FedRAMP 3PAO. Recognition will be removed immediately. The organization will be required to re-enter the FedRAMP-qualification process through the A2LA Cybersecurity Inspection Body Program.

After a 3PAO has become FedRAMP-recognized, they must be reviewed and assessed ***at least annually*** to maintain their FedRAMP recognition. This process includes:

1. A favorable annual review by A2LA
2. A full on-site reassessment every two years
3. Surveillance assessment every other year

All 3PAOs must maintain FedRAMP-recognition by demonstrating that they operate impartially and independently, in accordance with ISO/IEC 17020 and FedRAMP requirements.

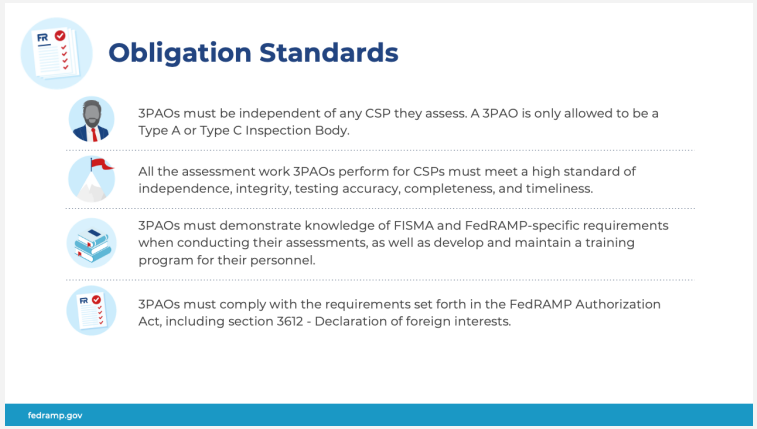
All 3PAO assessments must adhere to FedRAMP requirements for quality, accuracy, integrity, and timeliness.

All of the outlined processes, standards, and rigor that are demanded of 3PAOs must be upheld to ensure the sanctity of the process as a whole.

The obligations and performance standards of a 3PAO are upheld throughout the time the 3PAO is operating under the FedRAMP recognition. Integrity and consistency is expected. If a 3PAO does not abide by the expectations set forth, a series of performance management actions take place to correct the issues, which may result in removal of the 3PAO's FedRAMP recognition.

Following the next few slides, we will explore the obligations standards as mandated by 3PAOs, as well as the performance management process, what it entails, and what the consequences are for not adhering to it.

Finally, please read and reference FedRAMP's 3PAO Obligations and Performance Standards document on the FedRAMP website for additional details.



As part of FedRAMP accreditation, all 3PAOs are obligated to adhere strictly and continuously to the FedRAMP accreditation requirements and follow their ISO 17020 quality management system as described in their application and evaluated by A2LA.

These requirements include the following key items:

- The 3PAO must be independent of any CSP they assess. A 3PAO is only allowed to be a Type A or Type C Inspection Body.
    - A type A inspection body is an independent “third party” that receives external orders for the inspection of products, processes, or services. This is true of most of the FedRAMP “third party” organizations.
    - Type C bodies are identifiable entities but may not be a separate part of the organization. Type C can also supply inspection services to parties other than the parent organization. There are several auditing firms that have been approved by FedRAMP to provide 3PAO assessments.
- 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. They must also develop and maintain a training program for their personnel including, at a minimum, content incorporating FISMA, FedRAMP, cloud computing, and cybersecurity.
- 3PAOs must comply with requirements set forth in the FedRAMP Authorization Act including section 3612 - Declaration of foreign interests

It is the responsibility of 3PAOs to continuously demonstrate they are performing in accordance with ISO/IEC 17020 as revised and FedRAMP requirements to maintain their FedRAMP recognition. It is also important to note that 3PAOs must always have three team members (minimally) for each assessment, Senior Assessor, Junior Assessor, and a Penetration Testers. Each of these team members must also meet:

- The personnel requirements for years of experience and,
- The certification and technical proficiency activities
- As set forth by FedRAMP for every assessment.

FedRAMP assessments require 3PAOs to submit the following documents to government Authorizing Officials as part of the overall security authorization package:

- Security Assessment Plans or SAP, which includes
  - A detailed accounting of how the security testing will proceed as agreed upon by the CSP and 3PAO
  - The Rules of Engagement supporting this testing.
- Security Assessment Reports or SAR, which includes
  - Security Assessment Test Case Workbook
  - Risk Exposure Table
  - Penetration Test Report
  - Vulnerability Scan Data Files
  - Test Artifacts

Based on their FedRAMP accreditation, these 3PAO documents **must meet the following standards**:

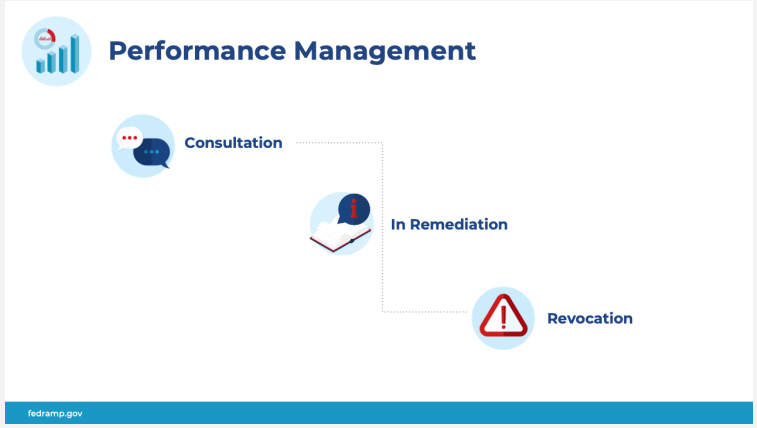
- **Complete Authorization Package:** First-time submissions should be complete and thoroughly prepared. Any issues uncovered will be promptly and efficiently addressed by the 3PAO, and updates will be incorporated to correct any issues identified.
- **Document Quality**: All quality and acceptance criteria must be met by the 3PAO as outlined by FedRAMP on the fedramp.gov website. This includes all requirements in the FedRAMP General Document Acceptance Criteria Guidance. Note, that the documents must be prepared using the most recent FedRAMP template without any alterations or deletions.
- **Timeliness & Responsiveness**: In accordance with the schedule agreed to by the government, the CSP, and the 3PAO, all documents are delivered on time.
- **Testing Accuracy & Completeness:** It is the 3PAO's responsibility to carry out this testing based on the ISO/IEC 17020 conformity assessment standards and FedRAMP's highest-quality testing requirements and assure accurate and complete testing of a CSP's offering.
- **Assessment Integrity:** All independent assessments of the CSP's security posture must be submitted without influence by CSP demands. This ensures that the security assessment is

impartial and independent, as well.

- **Personnel Qualifications:** Every personnel requirement must be met as listed by the A2LA in the R311- Specific Requirements: Federal Risk and Authorization Management Program policy.

If a 3PAO fails to meet these standards, all stakeholders are affected:

- The CSP assessment package might be invalidated.
- The Agency cannot rely on the system until the package is FedRAMP-authorized,
- And the 3PAO is disciplined.



Excellence is expected across the government.

The government evaluates all 3PAO products and expects superior quality and performance. In the event that a 3PAO's performance does not meet FedRAMP standards, FedRAMP has the authority and responsibility to pursue corrective actions related to the 3PAO's FedRAMP recognition status.

The first is **Consultation**.

If a 3PAO has minor deficiencies associated with FedRAMP's 3PAO performance standards, such as incomplete testing, poor document quality, inaccurate testing

- A notice is sent. FedRAMP will require a meeting with the 3PAO representatives to discuss the specific deficiencies in the 3PAO's performance
- The 3PAO then must develop and submit an internal Corrective Action Plan or CAP to info@fedramp.gov within 10 business days of the meeting
- The internal CAP:
    - Outlines details of all the deficiencies as identified by FedRAMP, the root cause of the deficiencies, and how and when they will remediate the deficiencies
    - Requires FedRAMP Director approval, and
    - Is documented in the 3PAO's performance records and shared with A2LA during the 3PAO's next assessment

It is imperative that the 3PAO adhere to the Consultation guidelines and timeframes in order to avoid escalation and/or the removal of their FedRAMP recognition.

If a 3PAO is placed in **Consultation** for a first instance of utilizing unqualified personnel

- The PMO will reject the assessment work provided by the 3PAO. The 3PAO will need to provide an internal CAP response that is approved by the Director, and the assessment will need to be redone by qualified personnel/resubmitted for FedRAMP review.
- For personnel issues that result in a 3PAO being In Consultation, the 3PAO may still conduct assessment work for their client (per their direction), but FedRAMP will not accept new deliverables from the 3PAO until their remediation plan is approved by the Director.
- If a 3PAO has a repeat instance of using unqualified personnel, the 3PAO will be placed In Remediation. The 3PAO will need to provide a formal CAP response that is approved by the Director, and the assessment will need to be redone by qualified personnel/resubmitted for FedRAMP review.

Next is **In Remediation.**

If a 3PAO has deficiencies, such as repeated performance issues, submission of conditional CSP authorization recommendations, or fails to complete the internal CAP as part of the "Consultation" status corrective action requirements include:

- An In-Remediation letter is sent from FedRAMP to the 3PAO and CSP for RAR submissions, or it is sent to the 3PAO, CSP, and Authorizing Official, for both initial and annual package submissions, notifying the 3PAO of specific deficiencies in the 3PAO's performance
- The 3PAO must then submit a formal CAP to FedRAMP, via info@fedramp.gov, within 10 business days of the date of the letter from FedRAMP
- FedRAMP's review of the associated authorization package or RAR will be placed on hold until the FedRAMP Director approves the 3PAO's formal CAP response
- A "in-remediation" label will be placed next to their name in the marketplace during this period

If a 3PAO is placed In **Remediation** for personnel or other assessment issues, this means that the 3PAO must first submit a formal CAP response that is accepted by the Director before any new assessment work can be submitted to FedRAMP. This applies to all 3PAO assessment work underway, which means multiple assessments may be impacted. The 3PAO may still conduct assessment work for their client (per client direction), but FedRAMP will not accept new deliverables from the 3PAO until their remediation plan is approved by the Director.

It is imperative that the 3PAO adhere to the In-Remediation guidelines and timeframes in order to avoid escalation and/or the removal of their FedRAMP recognition.

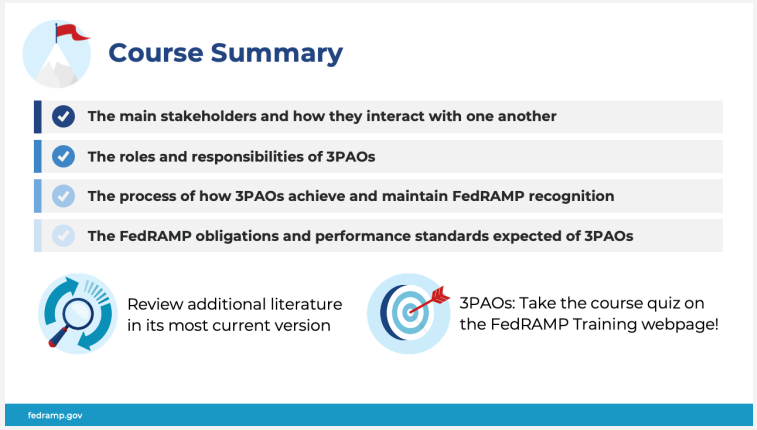
The last status is **Revoked**.

If a 3PAO has severe deficiencies in their performance or a 3PAO fails to complete the formal CAP, as required while in the "In-Remediation" status:

- A letter is sent from FedRAMP to the 3PAO and CSP for RAR submissions, or it is sent to the 3PAO, CSP, and Authorizing Official, for both initial and annual package submissions, notifying the 3PAO of:
  - the revocation of its FedRAMP recognition status,
  - why the revocation occurred, and
  - that its organization's page has been removed from the FedRAMP Marketplace.
- Revoked organizations are not authorized to provide FedRAMP assessment services for CSPs pursuing or maintaining FedRAMP authorizations
- If a 3PAO's FedRAMP recognition is revoked, the organization will be required to re-enter the qualification process through the A2LA Cybersecurity Inspection Body Program that is detailed in Appendix A, which includes performing successfully under A2LA's standards ISO/IEC 17020 and R335 for one year prior to seeking recognition
- A 3PAO who has had their recognition "revoked "will be removed from the FedRAMP marketplace immediately

It is imperative that the 3PAO adhere to the Revoked guidelines and timeframes in order to avoid losing their FedRAMP recognition and being subject to a one-year wait before reapplying. Please note that If a 3PAO is **revoked a second time**, the 3PAO is **not eligible to be recognized by the FedRAMP Program again**.

300-0: 3PAO Obligations and Performance Guide



This course covered the foundational elements of the FedRAMP 3PAO program. We covered:

- Who the main stakeholders are and how they interact with one another
- The roles and responsibilities of 3PAOs
- The process of how 3PAOs get and maintain FedRAMP Recognition and
- The Obligations and Performance Standards expected of 3PAOs

These topics will help frame the information you will continue to learn through this learning path.

Please review all the additional information on these topics in their latest version to provide you with further context.

Remember to complete the course quiz at the conclusion of this training by clicking on the 'Take Quiz' link in the YouTube description, or by going directly to the FedRAMP Training webpage and clicking on the 'Take Quiz' link next to the course you just viewed. If you are a 3PAO, the quiz is obligatory, and you need to achieve a score of 80% or higher to pass. However, if you are not a 3PAO, you can take the quiz, but it is not required.