FedRAMP

CSP Timeliness and Accuracy of Testing Requirements

Version 3.0

12/11/2020

GSA

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
09/27/2016	1.0	All	Initial publication	FedRAMP PMO
11/20/2017	2.0	All	Updated to the new template	FedRAMP PMO
12/11/2020	3.0	All	Updated to the new template and updated references	FedRAMP PMO

How to Contact Us

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

1. Purpose

This document outlines the timeliness and accuracy of testing requirements for evidence associated with an authorization package prior to a cloud service provider (CSP) entering the FedRAMP Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) process.

CSPs will only enter the JAB P-ATO process after they have been prioritized by the JAB. To ensure timeliness of testing it is recommended that CSPs wait to begin full testing of their cloud systems until after they have been prioritized.

2. Background

The JAB grants provisional authorizations for cloud systems they believe could be authorized government-wide by any other Executive level department or agency. This requires a rigorous review of the risk posture of these cloud systems. Thus, the testing evidence associated with the authorization package must accurately reflect the current risk posture of these cloud systems.

3. Timeliness and Accuracy of Testing Overview

There are three categories of evidence associated with testing in an authorization package: (1) Penetration Testing, (2) Vulnerability Scanning, and (3) Security Controls Testing. The following sections describe the three categories of testing as well as how CSPs can ensure the associated testing evidence is considered current by the JAB.

4. Penetration Testing Requirements

Penetration Tests determine exploitable security weaknesses in an information system. They may also evaluate an organization's security policy compliance, its employees' security awareness, and the organization's ability to identify and respond to security incidents. All penetration tests must comply with the FedRAMP Penetration Testing Guidance.

At the beginning of the JAB P-ATO process, as part of the authorization package, a FedRAMP recognized third party assessment organization (3PAO) must submit a 1) Penetration test plan and a 2) Penetration test report on behalf of their CSP. In order to ensure a penetration test is current, the following must apply:

Timeliness Requirements:

- When submitting a completed authorization package, to FedRAMP to begin the JAB P-ATO process, the penetration test cannot be older than 6 months.
    - NOTE: CSPs should ensure the penetration test is executed as close as possible to a CSP's submission of the authorization package.

- Once a JAB P-ATO is granted, CSPs must complete a new penetration test, at a minimum, once a year by a 3PAO.

Accuracy of Testing Requirements:

- Penetration tests must accurately reflect the current security capabilities and services of the cloud system being authorized.
- If there are any significant changes to the security capabilities of the cloud system since the completion of the last penetration test, the JAB may require a new penetration test.
    - Examples include: new ports, protocols, or services.

5. Vulnerability Scan Requirements

Vulnerability scans are a primary source of evidence for continuously monitoring a CSP's risk posture and enabling authorizing officials to continue to authorize the use of a CSP system. FedRAMP requires CSPs to complete vulnerability scans in accordance with the *FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide*.

At the beginning of the JAB P-ATO process, as part of the authorization package, the CSP must 1) submit vulnerability scans provided by the 3PAO as a part of the authorization package 2) submit monthly scans provided by the CSP. These scans provide the JAB with a view into a CSP's ability to remediate findings and provides input for the JAB's authorization decision on the CSP's risk posture. To ensure the vulnerability scans are current, the following must apply:

Timeliness Requirements:

- When submitting a completed authorization package to FedRAMP, to begin the JAB P-ATO process, the scans completed by a 3PAO and reflected in the Security Assessment Report (SAR) must be current within 120 days.
- Additionally, CSPs must submit scans and a Plan of Action and Milestones (POA&M) current, within 30 days prior, to the date of the JAB P-ATO process kick-off.

Monthly Scanning Requirements during JAB P-ATO Process:

- During the JAB P-ATO process, vendors must submit monthly vulnerability scans, in accordance with security controls RA-5 and RA-5 (5), and matching POA&Ms, in accordance with security control CA-5.
- These vulnerability scans and POA&Ms will be treated as monthly continuous monitoring scans that identify all high, moderate, and low vulnerabilities on a CSP's system. In order to be eligible for a P-ATO, a vendor must have monthly scans and POA&Ms demonstrating:
    1. There are no late high vulnerabilities on the system open for longer than 30 days from the date of discovery.

2. The CSP provides a POA&M to remediate all open high vulnerabilities within the 30-day remediation timeframe.
3. The CSP remains in compliance with the applicable requirements in the *Continuous Monitoring Performance Management Guide*.
4. These scans must use the same scan tools and configurations as the scans run by the 3PAO reflected in the SAR.

6. Security Control Testing Requirements

FedRAMP requires CSPs to complete security control implementation testing required by the *FedRAMP Security Controls Baseline*. Each security control within the baseline must be tested by a 3PAO with the appropriate evidence and results documented within the authorization package.

To ensure the testing of security controls by a 3PAO are current, the following must apply:

Timeliness Requirements:

- When submitting a completed authorization package to FedRAMP, security control testing evidence must be current within:
    - 120 days, if the system does not have an existing FedRAMP Agency Authorization.
    - 12 months, if the system has an existing FedRAMP Agency Authorization.

Accuracy of Testing Requirements:

- All security control testing evidence must accurately reflect the current implementations.
- All security control testing evidence must be completed by the same 3PAO.

7. Policy for Treating High Vulnerabilities

The JAB does not accept any open and unmitigated high vulnerabilities found during testing documented in the SAR. There are almost always high risks identified by vulnerability scans during a 3PAO assessment. Any high findings found during the JAB P-ATO process should be closed within 30 days. In order to close any high findings identified by vulnerability scans for a SAR submission, 3PAOs can do one of the following:

- Perform targeted scans to verify closure of a high vulnerability (preferred), or
- Gather evidence to verify closure of a high vulnerability.

3PAOs may not do a complete re-scan of the environment unless that scan identifies zero additional vulnerabilities (at low, moderate, or high).