FedRAMP™

FedRAMP Penetration Test Guidance

Version 4.0

03/04/2024

GSA

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s	Description	Author
06/30/2015	1.0	All	First Release	FedRAMP PMO
07/06/2015	1.0.1	All	Minor corrections and edits	FedRAMP PMO
06/06/2017	1.0.1	Cover	Updated FedRAMP Logo	FedRAMP PMO
11/24/2017	2.0	All	Updated to the new template	FedRAMP PMO
06/30/2022	3.0	All	Updated to reflect current best practices in penetration testing	FedRAMP PMO
03/04/2024	4.0	All	Updates to some penetration testing requirements and added red team requirements	FedRAMP PMO

About This Document

The purpose of this document is to provide requirements for organizations planning to conduct a FedRAMP penetration test, as well as the associated attack vectors and overall reporting requirements.

A penetration test is a proactive and authorized exercise to break through the security of an IT system. The main objective of a penetration test is to identify exploitable security weaknesses in an information system.

These vulnerabilities may include service and application flaws, insecure configurations, improper role-based privilege assignments, and risky end-user behavior. A penetration test 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. Threat actors work diligently to bypass initial system defenses. Penetration testing ensures that the depth of defense goes beyond initial compromise and/or takes into account things like proper coding practices being followed.

Zero Trust Protection mechanisms should be defined as part of the system boundary and are better addressed and included in the SSP front matter discussions.

This document uses the term authorizing official (AO). For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says agency AO. For systems with a FedRAMP Agency authorization to operate (ATO), AO refers to each leveraging agency's AO.

The term authorization refers to either a FedRAMP JAB P-ATO or a FedRAMP Agency ATO.

The term third-party assessment organization (3PAO) refers to a FedRAMP-recognized 3PAO. The use of a FedRAMP-recognized 3PAO is required for systems with a FedRAMP JAB P-ATO; however, for systems with a FedRAMP Agency ATO this may refer to any assessment organization designated by the agency AO.

Who Should Use This Document?

The following **individuals should review this document**:

- Cloud Service Providers (CSPs) when preparing to perform a penetration test on their cloud system
- Third Party Assessment Organizations (3PAOs) when planning, executing, and reporting on FedRAMP penetration testing activities
- AOs when developing and evaluating penetration test plans.

How to Contact Us

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

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

Table of Contents

1. Scope of Testing

The Federal Risk and Authorization Management Program (FedRAMP) requires that penetration testing be **conducted in compliance with the following guidance**:

- NIST SP 800-115 (Current Revision)Technical Guide to Information Security Testing and Assessment
- NIST SP 800-145 (Current Revision) The NIST Definition of Cloud Computing
- NIST SP 800-53 (Current Revision) Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-53A (Current Revision) Assessing Security and Privacy Controls in Federal Information Systems and Organizations

FedRAMP also requires that a CSP's products and solutions (cloud services) undergoing a FedRAMP assessment and penetration test must be classified as a SaaS, PaaS, and/or IaaS (see definitions in Table 2). In some scenarios, it may be appropriate to apply multiple cloud service models to a cloud service.

1.1 Table 2: Cloud Service Classification

Cloud Service Model	NIST Description (Current Revision)
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin-client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls).

In the final Penetration Test Plan, all components, associated services, and access paths (internal/external) within the defined test boundary of the CSP's system must be scoped and assessed. A set of attack vectors will be mandatory, regardless of classification (SaaS, IaaS, PaaS, or hybrid) and is outlined in Section 3.1. CSPs will work, in coordination with their 3PAO, to identify and scope-in other attack vectors prescribed in this guidance. Any deviations from the mandatory or scoped-in attack vectors must be approved by an Authorizing Official (AO). The Rules of Engagement (ROE) must identify and define the appropriate testing method(s) and techniques associated with exploitation of the relevant devices and/or services.

The Penetration Test Plan must address all attack vectors described in Section 3 or explain why a particular attack vector was deemed out of scope or not applicable. 3PAOs may include additional attack vectors they believe are appropriate based on the cloud service offering being assessed. See Appendix C: Rules of Engagement (ROE)/Test Plan Template for more information regarding test plans.

2. Threats

CSPs should consult with their 3PAO to derive the most efficient and effective risk profiling for their cloud service offering (CSO).

2.1 Threat Models

FedRAMP penetration testing follows multiple threat models developed to align with current adversarial tactics and techniques. These threat models are built into each attack vector to ensure real-world threats and risks are analyzed, assessed, mitigated, and accepted by an authorizing authority. 3PAOs shall **assess the risk and security of a CSP minimally through the following threat models:**

- Internet based (Untrusted)
  - Network threat actor
  - Attack on CSP managed user
  - Email attack against CSP managed user
  - Application threat actor
  - Physical based attack
- CSP Corporate (Untrusted and Trusted)
  - Breach of CSP management systems
  - Breach of CSP managed support system and/or networks
  - Breach of CSP managed enclave of authorized systems
  - Corporate insider threat
  - Lost CSP managed system

    - Interconnected networks including international entities, foreign adversaries internally pivoting to US CSO enclave
    - Ransomware spread from CSP Corporate
    - Unauthorized physical access to authorized system
- Internal Threat (Untrusted and Trusted)
    - Weak permissions and access control
    - Abuse of services of authorized system
    - Ransomware spread from government system
    - Multi organization access to authorized system
    - Unauthorized physical access to authorized system

If a 3PAO determines additional threat models are warranted in order to provide an adequate FedRAMP assessment, a CSP must be willing to consider what the 3PAO recommends. If a 3PAO and CSP cannot come to terms, and an AO determines that this additional testing should be performed, this may extend a CSP's time to FedRAMP authorization.

2.2 Attack Models

Depending on the authorized service architecture (IaaS, PaaS, SaaS, hybrid), all or some attack models may apply. Additionally, attack models may be tested in different or multiple ways, and testers are required to demonstrate the ability to exploit vulnerabilities or verify exploits when not feasible. The penetration test should not be strictly limited to automated scanning techniques but manual techniques as well.

A 3PAO's penetration testing methodology and report should provide an AO with a clear picture of attack models leveraged against the authorized system. The report shall outline the specific attack narratives of verification and validation of vulnerabilities identified during testing. This requirement will ensure that the approach and attack models were properly met. While not a comprehensive list, the goal of penetration testing should be to attain all of the following, per the MITRE ATT&CK® knowledge base:

Enterprise	Mobile
• Reconnaissance • Resource Development • Initial Access • Execution • Persistence • Privilege Escalation • Defense Evasion • Credential Access • Discovery • Lateral Movement • Collection • Command and Control • Exfiltration • Impact	• Initial Access • Execution • Persistence • Privilege Escalation • Defense Evasion • Credential Access • Discovery • Lateral Movement • Collection • Command and Control • Exfiltration • Impact • Network Effects • Remote Service Effects

FedRAMP realizes that the goal of testing to attain all of the above is not feasible for every CSO. It is up to CSPs and 3PAOs to determine the tactics and techniques that most assuredly could affect the particular system. FedRAMP relies extensively on a 3PAO's penetration testing expertise to identify and test the most applicable tactics that would be adopted by a malicious actor. 3PAOs shall explain the rationale for choosing the specific penetration testing tactics for the system. A CSP should be aware that an AO may ask for additional testing during the review if common tactics for a CSO are not tested. This can delay the time for FedRAMP authorization.

3. Attack Vectors

Attack vectors are defined as potential avenues of compromise that may lead to a loss or degradation of system integrity, confidentiality, or availability. FedRAMP has identified and developed several risk scenarios for 3PAOs to review and address during penetration testing. CSPs and 3PAOs shall agree on the attack vectors. If a specific attack vector cannot be performed, the deviation must be included in the SAR as a deviation from the Penetration Testing Guidance. CSPs must understand that a 3PAO might see non-conformance to testing a particular attack vector as a High Risk finding in the SAR Risk Exposure Table (RET). If a CSP feels strongly that testing the attack vector may result in a significant negative impact to the production system, then the CSP is encouraged to submit a non-conformance justification for why a 3PAO-recommended attack vector cannot be tested to an AO. CSPs and 3PAOs must both be aware that any deviations or non-conformance to established guidance may result in a longer time to FedRAMP authorization due to the time required for an AO to understand and agree to the deviation or non-conformance.

3.1 Mandatory Attack Vectors

Techniques to test each system may vary depending on the service offering (IaaS, PaaS, SaaS, and Hybrid). Due to system commonalities, the following are **mandatory attack vectors for all authorized systems**:

- External to Corporate
- External to CSP Target System
- Tenant to CSP Management System
- Tenant to Tenant
- Mobile Application to Target System
- Client-side Application and/or Agents to Target System

3.1.1 Attack Vector 1: External to Corporate

The External to Corporate attack vector requires the execution of a social engineering (phishing) attack against a CSP's system administrators, and managing personnel who may influence system administrators. If sampling is performed, it must be documented in the ROE and approved by an AO prior to test execution. An attacker's originating IPs and email domains will be allowed on all perimeter security devices such as firewalls, web application firewalls, SPAM filters, and intrusion protection systems.

Email Phish Campaign

A phishing test is a coordinated assessment between a 3PAO and CSP. The intent is to test the user and the technical mechanisms providing email security. Users must be tested as the last line of defense, and the 3PAOs must test the security mechanisms of the CSP's email systems. The testing of the technical security mechanisms will provide tracking metrics for how any phishing messages are handled, including information about how many messages are opened, forwarded, filtered, and blocked. For user testing, emails shall be allow-listed on all security systems and be presented to the user unflagged, unmodified, and unaltered in any way.

3PAOs must coordinate with CSP security teams to ensure testing is not manipulated in any way. All CSP users with access to CSP management, authorized systems, applications, or support systems are in-scope for this attack vector. Additionally, any system administrators with privileged-level access to CSP management endpoints shall be considered in-scope of this assessment.

3PAOs are authorized to coordinate with CSPs to utilize established user phishing programs to facilitate testing. 3PAOs will provide or approve email templates and landing pages used in testing. 3PAOs must either perform this attack vector themselves or independently evaluate the effectiveness of a third party phishing campaign.

Landing pages for CSP personnel who are victims of the phishing attack shall immediately identify that the email was a phishing attempt and provide supplemental information on how to identify phishing attacks in the future.

The email campaign will consist of the following:

- Email with user name in body
- Link to landing page
- Ability to capture emails opened (hidden pixel)
- Landing page
- Ability to tie landing page visits by user
- Username and password capture
- Ability to track user submission

False positives created by CSP security systems, e.g. sandboxing and link clicking, are to be included in totals due to requirements of CSPs to bypass these protections. 3PAOs shall not keep credentials and

must destroy them after the test due to privacy and security risks. FedRAMP requires that the 3PAO report back roles and/or metrics but not specific names. CSPs shall also require all passwords changed post-test. Any data submitted to the application, real or not, is to be considered a failure of the test.

Metrics for failures and severity can be based on the most current Common Vulnerability Scoring System (CVSS) and the 3PAO expertise. For instance, the number of clicks and credential submissions shall be reported along with the 3PAO justification for the scoring. All phishing campaigns shall last at least one (1) week and user tests shall ensure that the phishing emails are left in the user's inbox and not automatically removed for the duration of the exercise. If the user reports the email, the test for that user can be considered as complete.

Non-Credentialed-Based Phishing Attack

The objective of this testing is to determine if a user can run an untrusted script. 3PAOs shall determine if remote code execution, credential harvesting, privilege escalation, or injection of malware is possible. 3PAOs are not required to capture credentials or execute any remote attack on the target system but shall track items such as when the script was run, under what circumstances was it run, and the role allowed to run it. Successful execution of these types of attacks is not the goal of the phishing attack. No matter the success level of the attack, a 3PAO shall provide evidence of a macro or script execution in lieu of credentials.

3.1.2 Attack Vector 2: External to CSP Target System

The External to CSP Target System attack vector simulates and tests vulnerabilities from external threat actors and untrusted Internet-based attacks; internal threats such as weak permissions/access controls and abuse of system services; and poor customer separation measures (e.g., improper network segmentation and poor implementation of security controls).

Internal Threats

CISA states that "Insider threats present a complex and dynamic risk affecting the public and private domains of all critical infrastructure sectors." Insider threats are unintentional or intentional. CISA defines the unintentional and intentional threats very clearly. These threats are synopsized here for ease of use.

Unintentional Threat (Negligence, Accidental)

Human beings are one of the biggest threat vectors to any computing device. Human beings are sometimes impatient, careless, tired, make mistakes, and procrastinate.

Accidental threats are mostly carried out mistakenly but can be the result of a negligent event. Negligence is the failure to exercise reasonable care or due diligence. We look at accidental threats as caused by those people who mistakenly introduce risk to an organization. Mainly, this accidental threat happens because a person does not understand security principles and applications. For instance, this type of person may not understand privacy data and could send a list of employee Social Security Numbers as an unencrypted attachment to an external email. Or a person may unknowingly forward

an email thread with sensitive company data to a business competitor. This type of person may love to forward email attachments or jokes to others and not realize that the attachment contains malware.

Intentional Threats

Intentional threats are purposefully harmful to another person or an organization. These threats are the result of malcontents or disgruntled employees. Malcontents cause issues because they seek to disrupt life as part of some internal rebellion. Disgruntled employees may cause issues because they feel they were treated unfairly. These types of people may try to sabotage equipment or inflict other types of disruptions and violence. Other people may steal proprietary data or intellectual property in the false hope of advancing their career.

Other Threats

Additional threats include collusion, third-party actors, and direct and indirect threats. 3PAOs and CSPs are urged to consider each type of insider threat and determine how to best test the CSO to minimize these threats.

Poor Separation Measures and Defense In Depth

Applications and systems currently exposed to the public internet shall be tested and risk-assigned based on the footprint provided as part of the external boundary of the information system. Application, API, and services testing shall be done in sessions or a "less than ideal scenario" where all external endpoints are known to an attacker. Application systems shall be tested through the passive and active blocking security devices (i.e. web application firewalls and software-based security controls) and shall be tested either from the inside the network or the passive and active blocking security devices shall be bypassed to facilitate testing. "Attack Vector 2" may be tested along with "Attack Vector 3" and "Attack Vector 4", as long as all attack scenarios are covered and user/management experiences do not differ. 3PAOs are also required to elevate risk ratings higher for compromised scenarios originating from public access.

- **IaaS** – Testing shall originate from public internet attacking exterior IPs or URLs used to host or manage authorized systems. This should include out-of-band, break glass, VPNs, or site-to-site connection interfaces (non-authenticated). 3PAOs must take into consideration corporate shared services and systems and the direct or indirect impact exploitation of these may have on Federal Government data and metadata. These systems usually reside on CSP "corporate networks" and the interconnections shall be assessed due to their impact on the accredited system.
- **PaaS** – Testing shall originate from public internet attacking exterior IPs or URLs used to host and manage authorized systems and within the application or applicable database.
- **SaaS** – Testing shall originate from public internet attacking exterior IPs or URLs used to host and manage authorized systems and within the application or applicable database.

3.1.3 Attack Vector 3: Tenant to CSP Management System

This Tenant to CSP Management System attack vector simulates and tests vulnerabilities, untrusted internal threats, and trusted internal threats that emanate from network threat actors, application threat actors, and abuse of services of the authorized system.

This attack vector is performed by conducting a full application test attempting to access CSP management systems due to misconfiguration, flaw in system design, abuse of intended function, low-code or no-code software deployment, and/or command line interface (CLI) that allows access to the CSP management zone.

Privileged and Unprivileged Users

CSPs will provide privileged level accounts to applications within the production environment in order to facilitate and identify scenarios where the attacker may go from unauthenticated access to authenticated access to privileged level access. All Tenant to CSP Management System attacks are to be conducted using the highest level of permissions available to customer users of the information system. The intent is to identify any opportunity that privileged customer accounts would have to compromise the underlying system architecture.

While cloud providers may prefer to evaluate a tenant within the development/test environments, these are rarely identical to the production deployment, and will not be used as a valid representation for the FedRAMP penetration test vectors. A CSP's production environment should be sufficiently resilient to sustain a FedRAMP penetration test.

- **IaaS** – Testing shall originate from hosted Virtual Private Cloud (VPC) service, server, or platform. Agents, APIs, and applications that allow for communications between tenant space and infrastructure or platform layers are in scope to ensure host compromise is limited to VPC or platform.
- **PaaS** – Testing shall originate from the platform provided and attempt to gain access to lower-level PaaS management systems or IaaS level systems. Due to inherent PaaS customizations and modifications (based on the Service Level Agreement [SLA]), the probability that the PaaS implementation may affect the security of underlying IaaS is high. Automated code deployment tools or CLIs to deploy SaaS solutions are considered in-scope and are required to be tested.
- **SaaS** – Testing shall originate from an application, API, or CLI if provided as a tool that is presented as part of an authorized system.

3.1.4 Attack Vector 4: Tenant-to-Tenant

This attack vector simulates and tests vulnerabilities from untrusted internal threats and trusted internal threats that emanate from issues such as ransomware spread from government and multi organization access to the authorized system.

This attack vector is performed by conducting a full application test which attempts to use provisional access of one tenant to compromise another tenant. Environments are required to be set up to test all aspects of the service provided, to include authentication, data access, user permissions, and sessions. Access to the cloud service offering shall mirror the methods used by system customers. 3PAOs shall be provisioned with two full production customer tenants for performing the Tenant-to-Tenant attack vector.

3.1.5 Attack Vector 5: Mobile Application to Target System

The Mobile Application to Target System attack vector consists of emulating a mobile application user attempting to access a CSP target system or CSP management system. This attack vector is tested on a representative mobile device and does not directly impact a CSP target system or infrastructure.

Information derived from this activity can be used to inform testing of other attack vectors. If a mobile application is not part of a CSP's CSO, then this attack vector can be marked as out-of-scope.

3.1.6 Attack Vector 6: Client-side Application and/or Agents to Target System

For this attack vector, if a CSP provides client-side components (i.e., components installed locally within a customer environment), those components must be included in the CSP's authorization boundary and tested as part of a CSP's system boundary security assessment if the components are essential for their customer's use of their CSO. Such client-side applications or components may include (though not exclusively) software applications, servers, appliances, browser extensions, thick clients, and agents. If a CSP provides optional-use, client-side components, such components may be included in the CSP's tested authorization boundary, if agreed upon between the CSP and customer.

CSPs shall include in their SSP–and 3PAOs in their testing–any controls out of a customer's ability to remediate such as encryption and software development. It is recognized that many of these controls will have a significant customer responsibility. These shared responsibilities shall be clearly called out in the SSP and assessed by a 3PAO.

FedRAMP encourages inclusion of optional-use components within a CSP's tested boundary as it reduces the burden on customers for component assessment, authorization, and continuous monitoring.

When scoping the system boundaries for the assessment, it is important to consider the legal ramifications of performing penetration testing activities on third-party environments. All testing

activities must be limited to the in-scope test boundary for the system to ensure adherence to all agreements and to limit legal liability. Penetration testing shall not be performed on assets for which permission has not been explicitly documented. Obtaining permissions for any third-party assets are required to be in-scope and are a CSP's responsibility.

4. Scoping the Penetration Test

The authorization boundaries of a proposed cloud service will be initially determined based on the SSP and attachments. Section 9 of the SSP should clearly define authorization boundaries of the cloud system in a diagram and in words. During penetration test scoping discussions, individual system components will be reviewed and deemed as "in-scope" or "out-of-scope" for the penetration test. The aggregate of the agreed upon and authorized in-scope components will comprise the system boundary for the penetration test.

When scoping the system boundaries for an assessment, it is important to consider the legal ramifications of performing penetration testing activities on third-party environments. All testing activities must be limited to the in-scope test boundary for the system to ensure adherence to all agreements and to limit legal liability. If adjacent assets or vectors that are not defined in the scope of testing are discovered that have possible or known exploits, the 3PAO shall document all discovered exploits. The 3PAO may test the additional vectors or assets only if the CSP is notified and gives permission to increase the scope of testing. Any updates to the scope shall be documented in the penetration testing report. If the CSP declines the increase in scope of testing, the 3PAO shall not test those additional assets or vectors and shall document the discovery of possible or definite exploits in the findings summary. Obtaining permissions for any third-party assets are required to be in-scope and is a CSP's responsibility.

Service models intending to use FedRAMP Authorized services lower in the "cloud stack" can leverage the FedRAMP compliance and security features of those services. As a result, attack vectors already addressed by other FedRAMP Authorized services lower in the "cloud stack" are not required to be re-evaluated. For example, if a PaaS and SaaS leverage another layer (i.e., IaaS) that is FedRAMP Authorized, then penetration testing of the lower layer is not required. However, a CSP must determine the authorization system boundaries and provide justification for any controls they intend to claim as inherited from the supporting service. If the PaaS and/or SaaS are including FedRAMP Authorized security features for the lower layers, then penetration testing of the lower layers is required and a CSP needs to obtain all the authorizations required for a 3PAO to perform penetration testing for the lower layers.

Penetration testing may require:

- Negotiation and agreement with third parties such as internet service providers (ISPs), managed security service providers (MSSPs), facility leaseholders, hosting services, and/or other organizations involved in, or affected by, the test. In such scenarios, a CSP is

responsible for coordination and obtaining approvals from third parties prior to the commencement of testing.

- When a cloud system has multiple tenants, CSPs must build a temporary tenant environment if another tenant environment suitable for testing does not exist. Use of production to development instances to meet multi-tenancy may be used if a 3PAO validates attack vectors and models are effectively tested.

5. Rules of Engagement (ROE)

The penetration test plan must include:

- A description of the approach, constraints, and methodologies for each planned attack.
- A detailed test schedule that specifies the start and end date/times and content of each test period and the overall penetration test beginning and end dates.
- Technical points of contact (POC) with a backup for each subsystem and/or application that may be included in the penetration test.

The penetration test ROE describes the target systems, scope, constraints, and proper notifications and disclosures of the penetration test. 3PAOs develop a ROE based on the parameters provided by a CSP. The ROE must be developed in accordance with NIST Special Publication (SP) 800-115, Appendix B, and be approved by an AO prior to testing. Additionally, NIST SP 800-115, Section 7, Security Assessment Execution states, "appropriate personnel such as the CIO, CISO, and ISSO are informed of any critical high-impact vulnerabilities as soon as they are discovered." FedRAMP requires that the ROE must contain this clause and include the AO, in addition to the CIO, CISO, and ISSO. See Section 6, Rules of Engagement, of the FedRAMP Security Assessment Plan Template for more information on the ROE. 3PAOs must include a copy of the ROE in the FedRAMP Security Assessment Plan submitted to FedRAMP.

The ROE shall also include:

- Local computer incident response team or capability and their requirements for exercising the penetration test
- Physical penetration constraints
- Acceptable social engineering pretext(s) to be fully worked out prior to the ROE being signed. Note:
    - Social engineering tests are based upon a 3PAO's expertise in challenging a CSP's users' failures to follow documented CSO policies and procedures
    - Can be evaluated against the effectiveness of a CSP's security awareness and training program

- There is no "one size fits all" social engineering testing. 3PAOs shall consider the threats, at the time of testing and incorporate these methods, as applicable, into their penetration testing methodology.

A summary and reference to any third-party agreements, including POCs for third parties that may be affected by the penetration test, must be included in the documentation. The time to authorization will be extended if the additional testing is required to be done based on an AOs review–prior to FedRAMP authorizing the package. 3PAOs are required to fully document in the Penetration Testing Report section 6.0 the rationale behind a CSP not agreeing to a social engineering test. Also, CSPs are encouraged to report to FedRAMP any proposed 3PAO penetration testing exercises that seem too severe given the nature of the CSO being offered.

6. Reporting

Penetration test assessment activities and results must be organized and compiled into a comprehensive penetration test report to be included in the SAR. There is no template provided for the penetration test report.

The penetration test report shall include appropriate confidentiality and sensitivity markings in compliance with a CSP's organizational policy. 3PAOs shall provide the report to a CSP via a secure means in compliance with the CSP organization's policies. Any information included in the report that could contain sensitive data (screenshots, tables, figures) must be sanitized or masked using techniques that render the sensitive data permanently unrecoverable by recipients of the report. 3PAOs must not include passwords (including those in encrypted form) in the final report or must mask them to ensure recipients of the report cannot recreate or guess the password.

The report is required to address the following sections, but not necessarily in this order:

6.1 Scope of Target System

Outline the target system that was assessed and if any deviations were made from the ROE/TP document.

6.2 Attack Vectors Assessed During the Penetration Test

Describe the attack vector(s) tested and the threat model(s) followed for executing the penetration test.

6.3 Timeline for Assessment Activity

Document when penetration testing activity was performed.

6.4 Actual Tests Performed and Results

Document the actual tests performed to address the penetration test requirements outlined in this document and document the results of each test.

6.5 Findings and Evidence

Findings shall include a description of the issue, the impact on the target system, a recommendation to the CSP, a risk rating, and relevant evidence to provide context for each finding.

6.6 Access Paths

Access paths are the chain of attack vectors, exploitations, and post-exploitations that lead to a degradation of system integrity, confidentiality, or availability. 3PAOs must describe the access path and the penetration test impact if multiple vulnerabilities could be coupled to form a sophisticated attack against a CSP.

7. Testing Schedule Requirements

For each initial security authorization, a penetration test must be completed by a 3PAO as a part of the assessment process described in the SAP. This initial penetration test must be performed no more than 6 months prior to the submission of the SAR. Once within the continuous monitoring phase of the FedRAMP process, additional penetration testing activities must be performed **at least every twelve (12) months**, unless otherwise approved by an authorizing body with documented rationale.

8. Third Party Assessment Organizations (3PAOs) Staffing Requirements

All penetration test activities must be performed by a 3PAO that has demonstrated penetration testing proficiency and maintains a defined penetration test methodology. The penetration test team lead must have an industry-recognized credential for penetration testing and equivalent education and experience as required in the R311 Federal Risk and Authorization Management Program (FedRAMP): Specific Requirements.

Appendix A: Definitions

The following is a list of definitions for this document:

- **Attack Vector** – A prescribed attack scenario based on attack models and real-world threats.
- **Cloud Service Provider (CSP)** – The entity responsible for the deployment, maintenance, and security of the authorized system.
- **Cloud Service Offering (CSO)** – The service, platform or capability that is being offered and accredited by the government customer.
- **Corporate** – An internal CSP network accessed outside the authorization boundary. This corporate boundary includes all resources owned, operated, maintained by the CSP to administer services of the system. This includes networks, laptops, mobile phones, systems that touch any part of the authorized system.
- **CSP Management System** – The backend applications, systems, services, hardware, infrastructure, or out of band management that facilitates administrative access to the cloud service. The management system is the support infrastructure only accessible to CSP personnel and authorized individuals.
- **Insider Threat** – An individual that is an employee, contractor, government employee or third party with access to a corporate or authorized system with malicious intent.
- **Microservices** – The capabilities provided or used to provide services.
- **Penetration Test** – A combination of automated and manual testing of technical security controls.
- **Target** – The intended end product being offered to the government customer.
- **Tenant** – A customer instance of a cloud service.

Appendix B: References

The publications referenced in this document are available at the following URLs:

- FedRAMP Documents and Templates: https://www.fedramp.gov/documents-templates/
- NIST Special Publication (SP) 800-115 Technical Guide to Information Security Testing and Assessment: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- NIST SP 800-53 Current Revision Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-145 The NIST Definition of Cloud Computing: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- MITRE ATT&CK® Matrix for Enterprise: https://attack.mitre.org/matrices/enterprise/cloud/
- NIST Red Team Definition: https://csrc.nist.gov/glossary/term/red_team

Appendix C: Rules of Engagement / Test Plan Template

Rules of Engagement / Test Plan

The Penetration Test Rules of Engagement (ROE) and Test Plan (TP) documents describe the target systems, scope, constraints, and proper notifications and disclosures of the Penetration Test. 3PAOs are required to develop a ROE and TP based on the parameters and system information provided by a CSP.

The ROE and TP document must be developed in accordance with NIST SP 800-115, Appendix B, and be approved by an AO prior to testing. 3PAOs must include a copy of the ROE in the FedRAMP Security Assessment Plan submitted to FedRAMP.

Penetration test planning **must include or account for the following considerations**:

- Penetration
    - Network penetration
    - Wireless network penetration
    - Physical penetration
    - Social engineering penetration
- Affected IP ranges and domains
- Acceptable social engineering pretexts

- Targeted organization's capabilities and technologies
- Investigative tools
- Specific testing periods (start and end date/times)
- CSP reporting requirements (format, content, media, encryption)

The Penetration Test Plan **must describe**:

- Target locations
- Categories of information such as open source intelligence, human intelligence
- Type of information such as physical, relationship, logical, electronic, metadata
- Gathering techniques such as active, passive, on- and off-location
- Pervasiveness
- Constraints that do not exploit business relationships (customer, supplier, joint venture, or teaming partners). The CSO control baseline provides the means to thoroughly test these relationships, especially supply chain controls

3PAOs must justify omitting any attack vectors described in Section 3 above in the ROE/TP and the Penetration Test Report.

System Scope

Provide a description of the boundaries and scope of the cloud service system, along with any identified supporting services or systems. System scope shall account for all Internet Protocol (IP) addresses, Uniform Resource Identifiers (URLs), devices, components, software, and hardware.

Assumptions and Limitations

Provide a description of the assumptions, dependencies, and limitations identified that may have an impact on penetration testing activities or results. Include references to local and federal legal constraints that may be relevant to testing or results. Assumptions also include any assumed agreement, or access to third party software, systems, or facilities.

Testing Schedule

Provide a schedule that describes testing phases, initiation/completion dates, and allows for tracking of penetration test deliverables.

Testing Methodology

The methodology section will address relevant penetration testing activities as described in Section 5, above.

Relevant Personnel

Provide a list of key personnel involved in the management and execution of the penetration test. The list shall include, at a minimum:

- System Owner (CSP)
- Trusted Agent (CSP)
- Penetration Test Team Lead (3PAO)
- Penetration Test Team Member(s) (3PAO)
- Escalation Points of Contact (CSP and 3PAO)

Incident Response Procedures

Provide a description of the chain of communications and procedures to be followed should an event requiring incident response intervention be initiated during penetration testing.

Evidence Handling Procedures

Provide a description of procedures for transmission and storage of penetration test evidence collected during the course of the assessment.

Appendix D: Red Team Exercises

Requirement

NIST defines Red Team as:

> *A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.*

The transition to NIST SP 800-53 Revision 5 outlined the addition of the CA-8(2) security control to the FedRAMP Moderate and High baselines. This control requires cloud service providers to:

> *Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].*

NIST further stipulated that:

> *Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.*

Objective

Appendix D defines the FedRAMP PMO's expectations when it comes to Red Team exercises. The primary objective of a Red Team exercise is to test the organization's detection, defense, and response capabilities and by simulating a real-world cyber-attack using current tactics, techniques, and procedures (TTPs) seen in the wild. A red team exercise differs from a penetration test in that the focus is not to find and exploit as many vulnerabilities as possible within the defined timeframe but rather help identify weaknesses in the organization and provide a framework for continuous improvement. The following phases are to be employed while conducting a red team exercise:

- **Phase I** – Objective Setting: Understand the business context, the scope of the engagement, and the key assets that need to be protected. Agree on the overall objectives and scope of the engagement. Define what red team success means aligned to objectives. Determine if initial

access is gained through external breach or if the engagement is to begin with an assumed breach approach.

- **Phase II** – Reconnaissance and Threat Modeling: Research and gather as much information as possible about the target with the underlying objectives in mind. This may include identifying IP ranges, domain names, and employee details. Identify potential threats and assess the level of risk associated with the identified assets. Engagement can be constructed to model TTPs of known threat actors by utilizing the MITRE ATT&CK framework.
- **Phase III** – Initial Access: Leverage identified data and vulnerabilities to exploit systems or people to gain initial access. This can be achieved through various techniques such as social engineering, physical attacks, or vulnerability exploitation on the external attack surface.
- **Phase IV** – Establish Persistence: Once the initial foothold has been established, actions will be taken to maintain access, such as setting up backdoors, creating new accounts, and leveraging Command and Control (C2) frameworks.
- **Phase V** – Escalation/Lateral Movement: Escalate privileges and move laterally using defense evasion techniques within the organization to achieve the defined objectives. This could include further exploitation of vulnerabilities, password cracking, accessing credential stores, and/or social engineering techniques, etc.
- **Phase VI** – Data Exfiltration: Discover, collect, and exfiltrate target data.
- **Phase VII** – Reporting and Debrief: Present a detailed report of the findings, which includes an executive summary, detailed findings, control successes and failures, and recommendations for improvement.

The FedRAMP Penetration Test against the CSP/CSO is distinctly different from a Red Team exercise. However, Red Team exercises can be performed by the 3PAO, a separate third party (non-3PAO), or internally if the CSP has the capability and appropriate skill sets. It should be noted that Red Teaming is an enterprise-focused activity. It is not solely focused on the CSO, but rather the CSP and its ability to detect, defend, and respond to an attack. This will provide a framework that a CSP can implement for continuous improvement. The exercise shall be modeled on the MITRE ATT&CK framework (which most of the above Red Team activities are built upon), and the assessment organization shall leverage the CSP's threat intelligence avenues to establish agreed upon objectives of the Red Team engagement.

Deliverables

The organization performing the Red Team exercise is responsible for creating a Red Team Test Plan (RTTP), executing the test, and documenting the results in a Red Team Test Report (RTTR).

The RTTP shall describe the scope, methodology for the test, activities slated to be performed, schedule of testing activities, organizational resources performing the test, and appropriate authorizations from the CSP.

The RTTR shall summarize the results of the test, annotate any findings from the test, assign a risk rating to each finding from the test, and provide associated recommendations for remediation.