FedRAMP PENETRATION TEST GUIDANCE

Version 2.0

November 24, 2017

FedRAMP

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

ABOUT THIS DOCUMENT

The purpose of this document is to provide guidelines for organizations regarding planning and conducting Penetration Testing and analyzing and reporting on the findings.

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, improper configurations, and risky end-user behavior. A Penetration Test also may evaluate an organization's security policy compliance, its employees' security awareness, and the organization's ability to identify and respond to security incidents.

WHO SHOULD USE THIS DOCUMENT

The following individuals should read this document:

- Cloud Service Providers (CSP) should use this document when preparing to perform a Penetration Test on their cloud system
- Third Party Assessor Organizations (3PAO) should use this document when planning, executing, and reporting on Penetration Testing activities
- Authorizing Officials (AO) should use this document when developing and evaluating Penetration Test plans.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into the following primary sections and appendices:

Table 1: Document Section Table

SECTION	CONTENTS
Section 1	Document Scope
Section 2	Definitions and Assumptions
Section 3	Attack Vectors
Section 4	Scoping The Penetration Test
Section 5	Penetration Test Methodology and Requirements
Section 6	Reporting
Section 7	Test Schedule Requirements
Section 8	3PAO Staffing Requirements
Appendix A	Table of acronyms used in this document
Appendix B	References
Appendix C	Rules of Engagement/Test Plan

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

LIST OF FIGURES

LIST OF TABLES

1. SCOPE

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

- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, September 2008
- NIST SP 800-145 The NIST Definition of Cloud Computing, September 2011
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013, with updates as of January 2015
- NIST SP 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Revision 4, December 2014

FedRAMP also requires that CSP products and solutions (cloud service) undergoing a FedRAMP assessment and Penetration Test must be classified as a SaaS, PaaS, or IaaS. In some scenarios, it may be appropriate to apply multiple designations to a cloud service. Table 2 below shows the definitions of these three service types.

Table 2 – Cloud Service Classification

CLOUD SERVICE MODEL	NIST DESCRIPTION
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, with the possible exception of 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 is able to 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).

All components, associated services, and access paths (internal/external) within the defined test boundary of the CSP system must be scoped and assessed. 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.

Penetration Testing may require:

- Negotiation and agreement with third parties such as Internet Service Providers (ISP), Managed Security Service Providers (MSSP), facility leaseholders, hosting services, and/or other organizations involved in, or affected by, the test. In such scenarios, the CSP is responsible for coordination and obtaining approvals from third parties prior to the commencement of testing.
- To limit impact on business operations, the complete or partial testing may be conducted in a non-production environment as long as it is identical to the production environment and has been validated by the 3PAO. For instance, if a CSP has two identical locations, a Penetration Test on one location may suffice. In this case, the environments must be *exactly* the same, not *almost*, *nearly,* or *virtually.*
- When the cloud system has multiple tenants, the CSP must build a temporary tenant environment if another tenant environment suitable for testing does not exist.

The Penetration Test plan must include actual testing of all the attack vectors described in Section 3 below or explain why a particular vector was not applicable. The Independent Assessors (IA) may include additional attack vectors they believe are appropriate. See *Appendix C: ROE/Test Plan Template* for more information regarding test plans.

2. DEFINITIONS & THREATS

To establish a baseline and context for FedRAMP Penetration Testing, the following terms are used to describe proposed cloud services.

2.1. DEFINITIONS

The following is a list of definitions for this document.

- **Corporate** – Internal CSP network access outside the authorization boundary.
- **Insider Threat** – A threat that is posed by an employee or a third party acting on behalf of the CSP.
- **Management System** – A backend application or infrastructure setup that facilitates administrative access to the cloud service. The Management System is accessible only by CSP personnel.

- **Roles** – Access levels and privileges of a user.
- **System** – The cloud service that is offered to government customers.
- **Target** – The application or cloud service that will be evaluated during the Penetration Test.
- **Tenant** – A customer instance of the cloud service.

2.2. THREAT MODELS

For FedRAMP threat models with multiple tenants, the CSP must build a temporary tenant environment if another tenant environment suitable for testing does not exist.

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 Rules of Engagement (ROE) describes the target systems, scope, constraints, and proper notifications and disclosures of the Penetration Test. The IA develops the ROE based on the parameters provided by the CSP. The ROE must be developed in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115, Appendix B, and be approved by the authorizing officials of the CSP prior to testing. See Section 6, Rules of Engagement, of the *FedRAMP Security Assessment Plan Template* for more information on the ROE. The IA must include a copy of the ROE in the *FedRAMP Security Assessment Plan* submitted to FedRAMP.

The ROE should 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)
- A summary and reference to any Third Party agreements, including Points of Contact (POC) for Third Parties that may be affected by the Penetration Test

2.3. THREAT MODELING

The IA must ensure the Penetration Test is appropriate for the size and complexity of the cloud system and takes into account the most critical security risks. The IA must perform the Penetration Test in accordance with industry best practices and standards. Typical goals for Penetration Testing include:

- Gaining access to sensitive information
- Circumventing access controls and privilege escalation
- Exploiting vulnerabilities to gain access to systems or information
- Confirming that remediated items are no longer a risk

The IA should test all or a sufficient sample of access points and locations (for physical Penetration Testing). When the IA tests a sample, the IA must describe how and why the sample was selected, and why it is sufficient.

The IA should attempt to exploit vulnerabilities and weaknesses throughout the cloud system environment, including physical Penetration Testing. At a minimum, the IA should verify security doors are locked, security alarms work, and security guards are present and alert as required by the CSP organization's security policies and procedures. These situations must be identified during scoping sessions and accounted for accordingly in the Rules of Engagement/Test Plan (ROE/TP).

The types of attacks must be repeatable and present a consistent representation of threats, threat capabilities, and organization-specific threat qualifications. In addition, the types of attacks must address the goals of the Penetration Test and include both internal and external attacks.

- **Internal** – Employees or users who are employed by the CSP, including both privileged and non-privileged users, in the context of the target system.
- **External** – Users and non-users of the system who are not employed by the CSP. This includes government users of the application, as well as third parties who do not have access rights to the target system.
- **Trusted** – Users with approved access rights to the target system. Trusted users include both internal CSP employees with management access to the system, as well as external users with credentialed access to the tenant environment.
- **Untrusted** – Non-users of the target system. Untrusted users include both internal CSP employees who lack credentialed access to the target system, as well as any individual attempting to access the target system from the Internet.

See Table 3 below for the relationships between Trusted/Untrusted and Internal/External attacks.

Table 3 – Types of Attacks

	INTERNAL	EXTERNAL
Trusted	CSP employee responsible for setup, maintenance, or administrative access to the CSP target system.	Any user of the target system, regardless of assigned roles or access rights.
Untrusted	An employee of the CSP without direct access to the target system.	Any individual, without authorized credentials, attempting to access the target system from the Internet.

3. ATTACK VECTORS

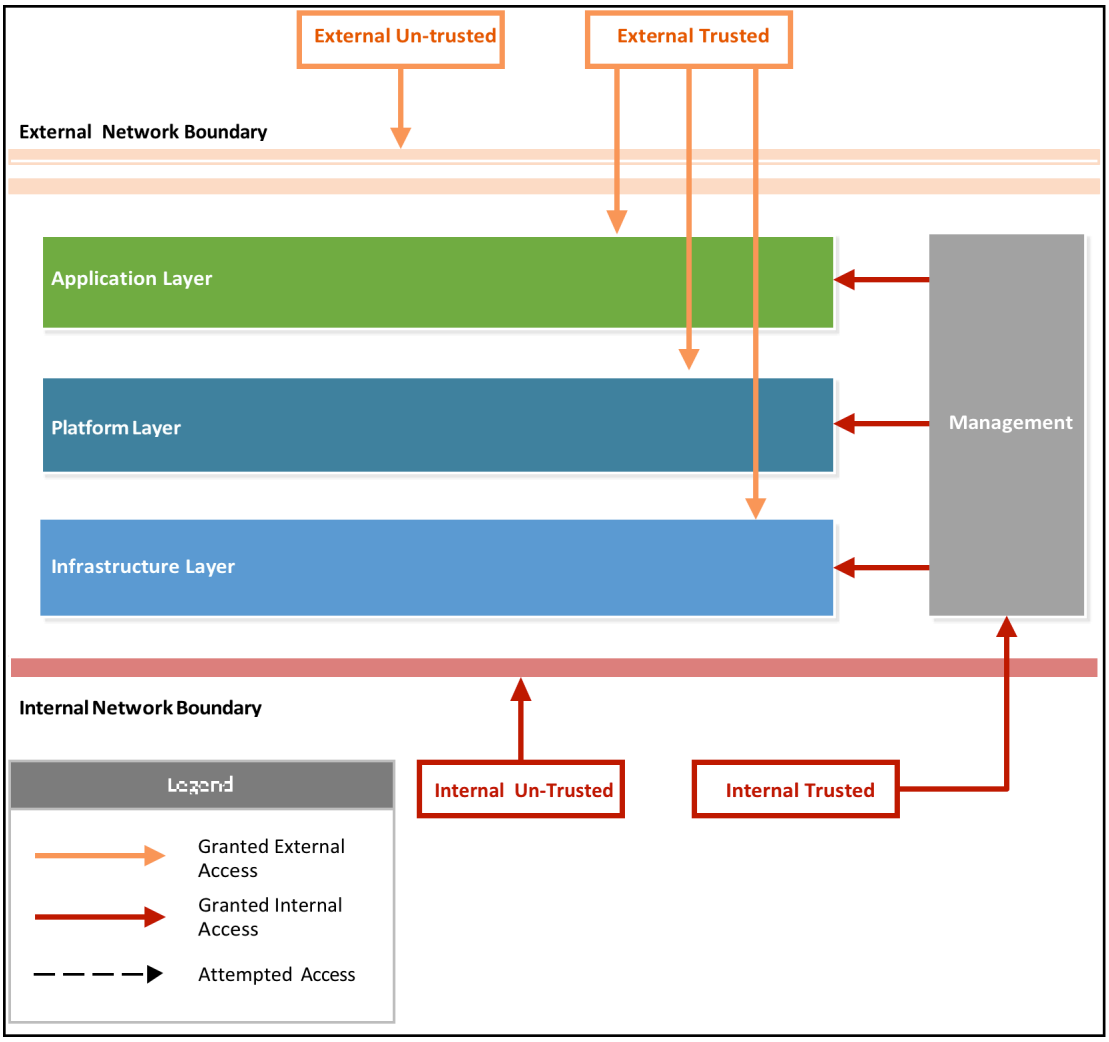
Attack vectors can be defined as potential avenues of compromise which may lead to a degradation of system integrity, confidentiality, or availability. FedRAMP has identified and developed several risk scenarios for the 3PAO organization to review and address during Penetration Testing. Table 4 below lists the identified attack vectors, which are detailed in the sections below.

Table 4 – Attack Vector Summary

TITLE	DESCRIPTION
External to Corporate – External Untrusted to Internal Untrusted	An internet-based attack attempting to gain useful information about or access the target cloud system through an external corporate network owned and operated by the CSP.
External to Target System – External Untrusted to External Trusted	An internet-based attack as an un-credentialed third party attempting to gain unauthorized access to the target system.
Target System to CSP Management System – External Trusted to Internal Trusted	An external attack as a credentialed system user attempting to access the CSP management system or infrastructure.
Tenant to Tenant – External Trusted to External Trusted	An external attack as a credentialed system user, originating from a tenant environment instance, attempting to access or compromise a secondary tenant instance within the target system.
Corporate to CSP Management System – Internal Untrusted to Internal Trusted	An internal attack attempting to access the target management system from a system with an identified or simulated security weakness on the CSP corporate network that mimics a malicious device.
Mobile Application – External Untrusted to External Trusted	An attack that emulates a mobile application user attempting to access the CSP target system or the CSP's target system's mobile application.

Figure 1 below illustrates a sample target cloud system to give context to the attack vectors illustrated in Figures 2 through 6 below. Each attack vector has been paired with its relevant threat model as a general guide for designing test cases. Note that physical attack vectors are not included in the attack vector descriptions below and a specific cloud service may differ from the represented system. The 3PAO must demonstrate how the Penetration Test will address these attack vectors.

Figure 1. Sample Target System

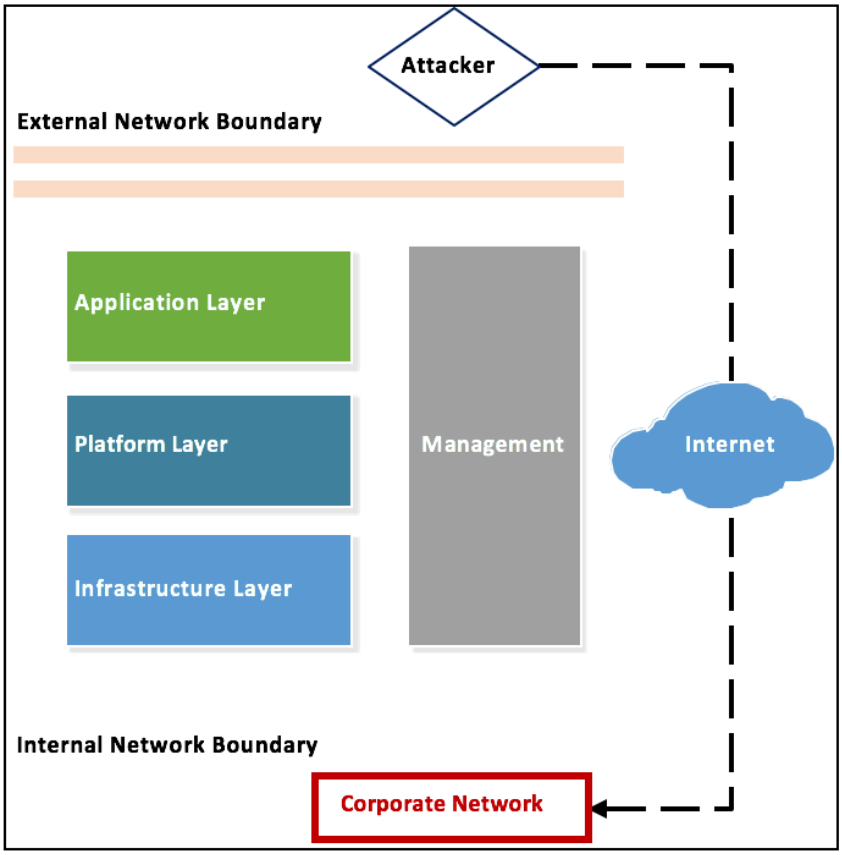


3.1. EXTERNAL TO CORPORATE – EXTERNAL UNTRUSTED TO INTERNAL UNTRUSTED

Figure 2 illustrates an internet-based attack attempting to gain useful information about or access to the target cloud system through an external corporate network owned and operated by the CSP. Only

employees who are directly responsible for the target system will need to be included in this attack vector. See Section 5.5 Social Engineering, for information about this attack vector.

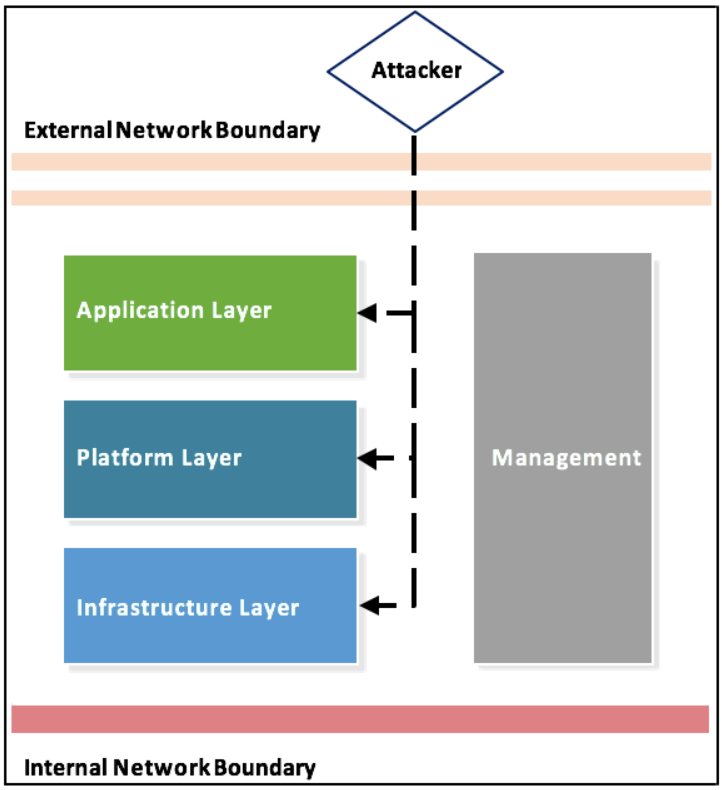
Figure 2. External to Corporate Attack Vector



3.2. EXTERNAL TO TARGET SYSTEM – EXTERNAL UNTRUSTED TO EXTERNAL TRUSTED

Figure 3 below illustrates an internet-based attack as an un-credentialed third party attempting to gain unauthorized access to the target system.

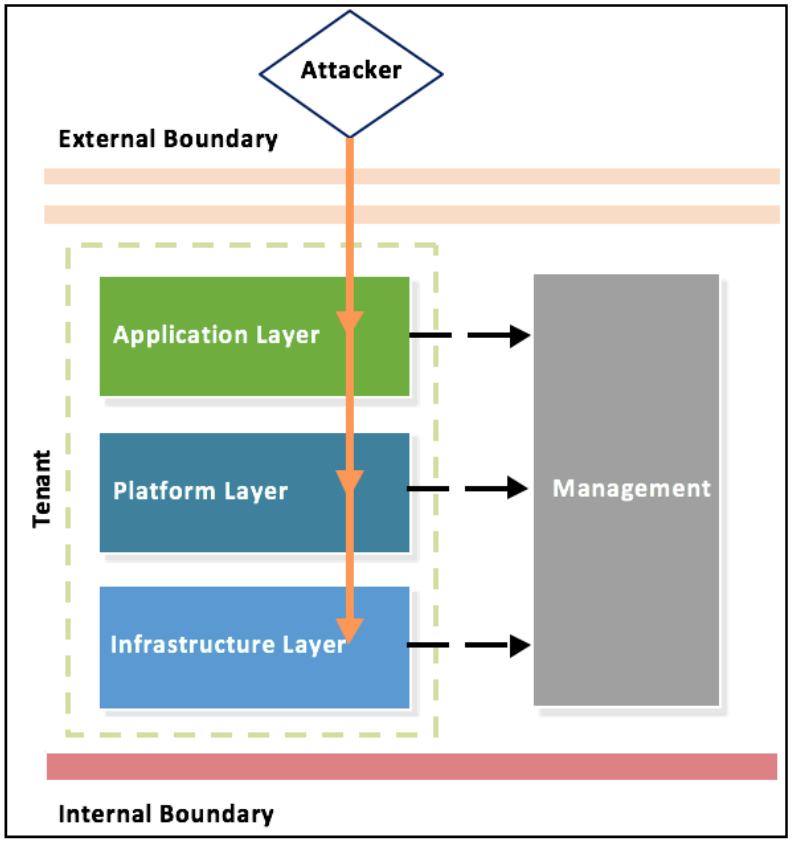
Figure 3. External to Target System Attack Vector



3.3. TARGET SYSTEM TO CSP MANAGEMENT SYSTEM – EXTERNAL TRUSTED TO INTERNAL TRUSTED

Figure 4 below illustrates an external attack as a credentialed system user attempting to access the CSP management system or infrastructure.

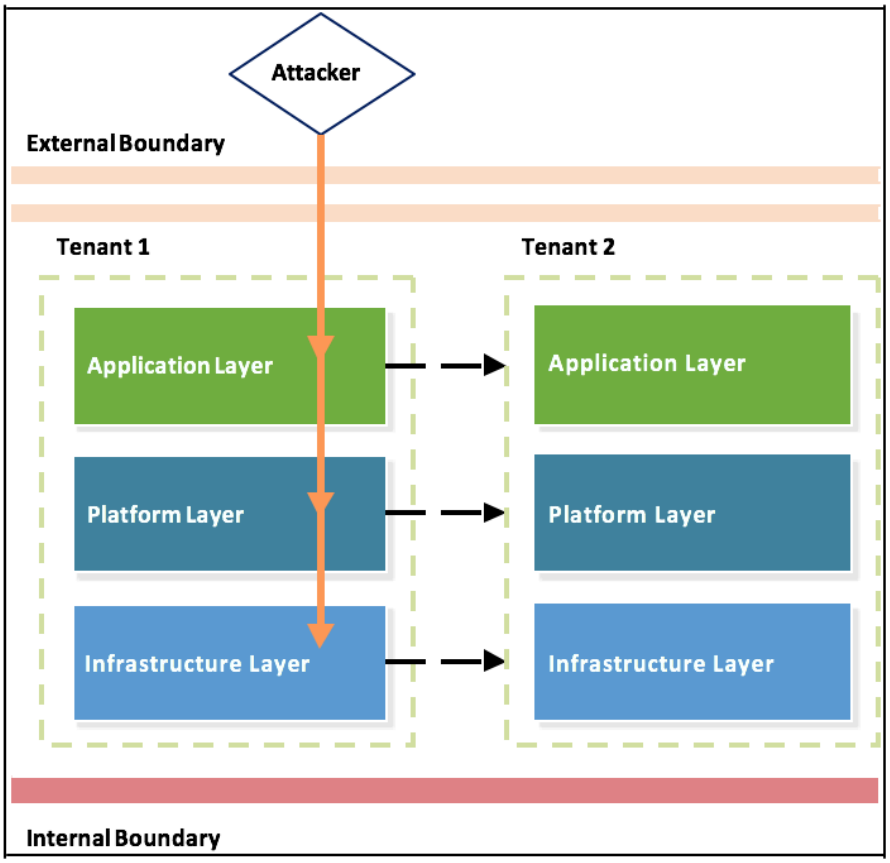
Figure 4. Target System to CSP Management System



3.4. TENANT TO TENANT – EXTERNAL TRUSTED TO EXTERNAL TRUSTED

Figure 5 below illustrates an external attack as a credentialed system user, originating from a tenant environment instance, attempting to access or compromise a secondary tenant instance within the target system.

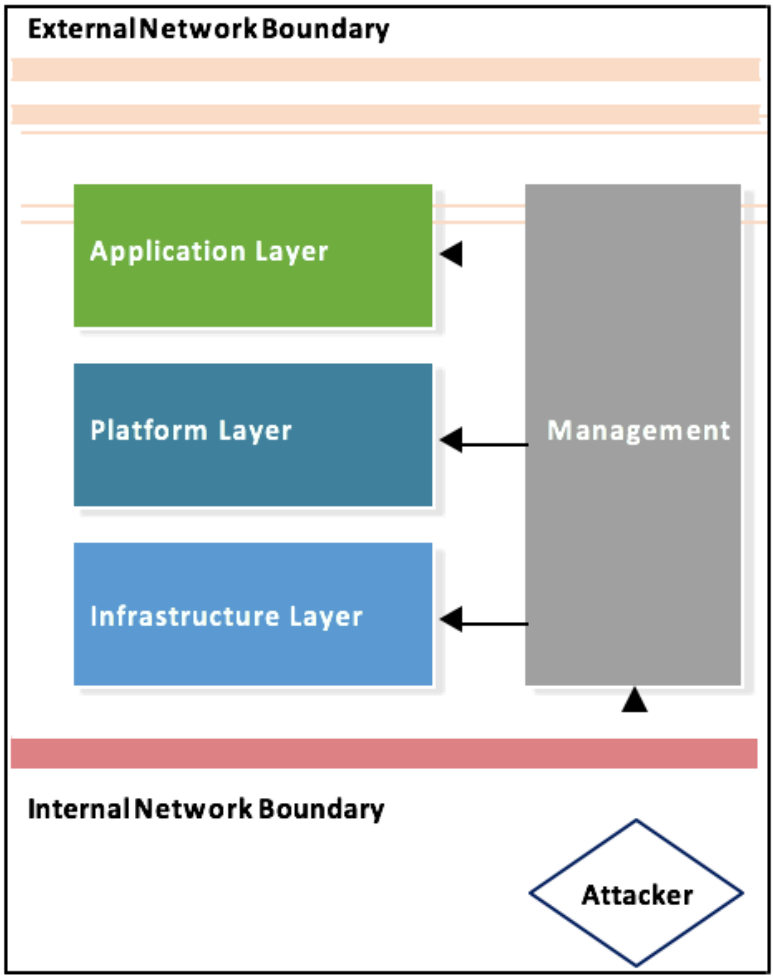
Figure 5. Tenant to Tenant Attack Vector



3.5. CORPORATE TO CSP MANAGEMENT SYSTEM – INTERNAL UNTRUSTED TO INTERNAL TRUSTED

Figure 6 below illustrates an internal attack attempting to access the target management system from a system with an identified or simulated security weakness on the CSP corporate network that mimics a malicious device (as if the organization has been infiltrated) or remotely compromised host on the corporate network.

Figure 6. Corporate to CSP Management System Attack Vector



3.6. MOBILE APPLICATION – EXTERNAL UNTRUSTED TO EXTERNAL TRUSTED

This attack vector consists of emulating a mobile application user attempting to access the CSP target system or the CSP's target system's mobile application. This attack vector is tested on a representative mobile device and does not directly impact the CSP target system or infrastructure. Information derived from this activity can be used to inform testing of other attack vectors.

4. SCOPING THE PENETRATION TEST

The authorization boundaries of the proposed cloud service will be initially determined based on the System Security Plan (SSP) and attachments provided to the FedRAMP PMO. Section 9 of the SSP should clearly define authorization boundaries of the cloud system in a diagram and words. During the

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 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 limitation of legal liability. Penetration Testing should **not** be performed on assets for which permission has not been explicitly documented. Obtaining permission for any third-party assets that are required to be in-scope is the responsibility of the CSP.

Service models intending to use FedRAMP-compliant 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-compliant services lower in the "cloud stack" are not required to be re-evaluated. For example: If a PaaS and SaaS leverage another layer that is FedRAMP compliant, then Penetration Testing of the lower layer is not required. However, the 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-compliant security features for the lower layers, then Penetration Testing of the lower layers is required and the CSP needs to obtain all the authorizations required for the 3PAO to perform Penetration Testing for the lower layers.

5. PENETRATION TEST METHODOLOGY AND REQUIREMENTS

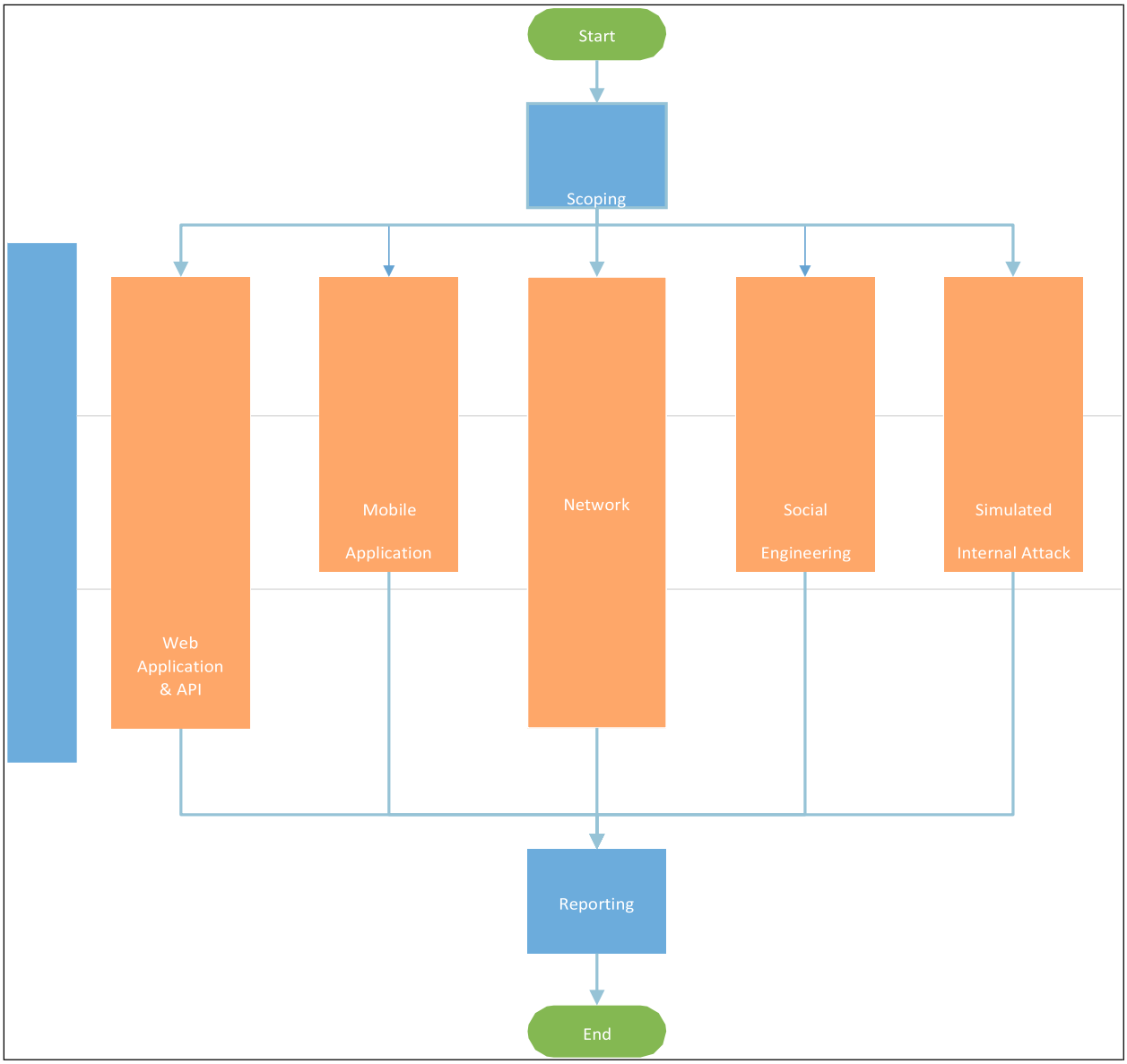
The Penetration Test methodology and requirements are constructed to follow industry best practices. Figure 7 below illustrates the key elements of a CSP Penetration Test FedRAMP identified based on the technology used within the cloud service. The depth of testing and technologies to be tested is dependent on the Penetration Test system boundary and system scope. This guidance will cover the following:

- Web Application/Application Program Interface (API) Testing
- Mobile Application Testing
- Network Testing
- Social Engineering Testing
- Simulated Internal Attack Vectors

The methodology has been organized according to common assessment steps followed by industry-practiced frameworks. The required level of effort regarding the appropriate Penetration Testing methodology will be determined by the 3PAO based on the technologies in the in-scope test boundary, regardless of how the CSP has self-identified the cloud service (SaaS, PaaS, or IaaS). For example: If

operating system/host-level access is offered by a CSP in a cloud service in which the CSP self-identifies as a SaaS or PaaS cloud service, network Penetration Testing requirements will still apply.

Figure 7. Elements of a Penetration Test



5.1. INFORMATION GATHERING & DISCOVERY

Information gathering and discovery activities occur prior to exploitation and are intended to accurately and comprehensively map the attack surface of the target system. Several requirements are outlined below.

5.2. WEB APPLICATION/API TESTING INFORMATION GATHERING/DISCOVERY

For API testing, sample workflows and test cases should be provided by the CSP to serve as a basic interface for common use cases of the application's functionality. The following activities in Table 5 below must be completed.

Table 5 – Discovery Activities

ACTVITY	DESCRIPTION
Perform internet searches to identify any publicly available information on the target web application	Identify any publicly available documentation that can be leveraged to gain insight into potential attack vectors of the target web application. Determine if any publicly available vulnerability has been disclosed, which could potentially be leveraged to attack the target web application.
Identify the target application architecture	Identify all layers of the application including application servers, databases, middleware, and other technologies to determine communication flow and patterns within the application.
Identify account roles and authorization bounds	Identify the roles associated with the cloud service and determine access limitations.
Map all content and functionality	Create a sitemap detailing all levels of functionality within the web application. Please note: different account roles may have different access levels to functionality within the target web application.
Identify all user-controlled input entry points	Map all areas of the application that take input from the user of the application.
Perform web application server configuration checks	Perform web vulnerability scanning activity to determine if common web server configuration flaws are present that could lead to an access path.

5.3. MOBILE APPLICATION INFORMATION GATHERING/DISCOVERY

Conduct information gathering and discovery activities against a mobile application. Please note that all platforms (iOS, Android, BlackBerry, etc.) for which the mobile application is offered should be tested independently. The following activities in Table 6 below must be completed.

Table 6 – Mobile Application Information Gathering/Discovery

ACTVITY	DESCRIPTION
Perform internet searches to identify any publicly available information on the target web application	Identify any publicly available documentation that can be leveraged to gain insight into potential attack vectors of the target mobile application. Determine if any publicly available vulnerability has been disclosed, which could potentially be leveraged to attack the target mobile application.
Map all content and functionality	Navigate through the application to determine functionality and workflow.
Identify all permission sets requested by the application	Inventory the permissions that the mobile application requests from the phone. Determine if there are any differences across mobile platforms.

5.4. NETWORK INFORMATION GATHERING/DISCOVERY

Conduct information gathering and discovery activities against externally available network ranges and endpoints. The following activities in Table 7 below must be completed.

Table 7 – Network Information Gathering/Discovery

ACTVITY	DESCRIPTION
Perform Open Source Intelligence (OSINT) Gathering Activities	Conduct an analysis of the public profile of the target system including information disseminated about public Internet Protocol (IP) ranges, technologies implemented within the target network or organization, and details around previous public attacks against the target system.
Enumerate and Inventory Live Network Endpoints	Conduct a scan to identify active network endpoints on the network environment.
Enumerate and Inventory Network Service Availability	Conduct an inventory of network services to identify potential attack vectors.
Fingerprint Operating Systems and Network	Determine service types and versions numbers.
Perform Vulnerability Identification	Conduct network scanning activity to identify publicly available vulnerabilities.

5.5. SOCIAL ENGINEERING INFORMATION GATHERING/DISCOVERY

Conduct external information gathering and discovery activities against CSP employees and system administrators for the system to be tested. The following activities in Table 8 below must be completed.

Table 8 – Social Engineering Information Gathering/Discovery

ACTVITY	DESCRIPTION
Perform internet searches to identify CSP personnel of interest responsible for target system management.	Inventory publicly available information that details CSP personnel roles and responsibilities for the target system. *Note: The CSP must approve a final list of system administrators to target for a spear phishing exercise.*

5.6. SIMULATED INTERNAL ATTACK INFORMATION GATHERING/DISCOVERY

Conduct internal information gathering and discovery activities against CSP employees and system administrators for the system to be tested. A representative corporate workstation/environment with general user access commensurate with a typical CSP corporate user must be given to the 3PAO to conduct this analysis. The following activities in Table 9 below must be completed.

Table 9 – Simulated Internal Attack Gathering/Discovery

ACTVITY	DESCRIPTION
Perform a scoping exercise with the CSP to determine potential attack vectors.	Identify valid attack chains assuming an internal CSP user was compromised by a social engineering attack.
Perform Vulnerability Identification	Conduct credentialed network scanning activity to identify publicly available vulnerabilities and privilege escalation vectors.

5.7. EXPLOITATION

During exploitation, the 3PAO Penetration Testing team will attempt to leverage attack vectors identified during information gathering and discovery to gain initial access into the target system, based on the attack vector being tested. Several attack vectors are outlined below.

5.7.1. WEB APPLICATION/API EXPLOITATION

Conduct web application exploitation activities against target web applications/APIs. The following activities in Table 10 below must be completed.

Table 10 – Web Application/API Exploitation

ACTVITY	DESCRIPTION
Authentication and Session Management	Assess the application to determine how the target application creates and maintains a session state. Analyze account creation and management process.
Authorization	Identify issues related to role privilege enforcement across common customer roles in the cloud service. Attempt to bypass authorization restrictions.
Application Logic	Attempt to circumvent controls to prevent bypass on intended logic patterns and application flows.
Input Validation	Perform injection attacks against all data inputs to determine if information or files can be inserted or extracted from the target application. Attempt to alter the backend.

5.7.2. MOBILE APPLICATION EXPLOITATION

Conduct local mobile exploitation activities against application content installed onto end-user mobile devices. Please note that all available platforms should be tested if the application is developed for multiple mobile device operating systems. Also note that interaction between the mobile application and the cloud service is not addressed under this section, as it is covered in

Section 5.8.1: Web Application/API Exploitation. The following activities in Table 11 below must be completed.

Table 11 – Mobile Application Exploitation

ACTVITY	DESCRIPTION
Authorization	Identify issues related to role privilege enforcement across common customer roles in the cloud service. Attempt to bypass authorization restrictions.
Data Storage	Identify and inventory data being stored on the device. Determine if encryption is being utilized outside of platform level controls.
Information Disclosure	Identify what information is being disclosed in log files and local cache stores.

5.7.3. NETWORK EXPLOITATION

Conduct network-level exploitation activities to analyze the risk of identified vulnerabilities by demonstrating attacks against hosts to determine the sensitivity of the information that can be

retrieved. Specific requirements are not given in this section, as the nature of the exploitation will be highly differentiated by the identified service or endpoint vulnerabilities; instead, general guidelines for performing exploitation attacks are provided. The following activities in Table 12 below must be completed.

Table 12 – Network Exploitation

ACTVITY	DESCRIPTION
Attack Scenarios	Present identified attack scenarios to the CSP for approval of execution. Note that if the CSP does not approve a potential exploitation path, this must be documented in the Penetration Test report.
Exploitation	Perform exploitation activity with the intent of gaining access to the target systems and elevating privileges, if possible. If unsuccessful, attempt to adapt the exploitation approach to work against the target environment.
Record Results	If exploitation attack scenarios were successful, document the results. If exploitation attack scenarios were unsuccessful, document why the exploit failed and what protections (if any) prevented the exploit from executing.

5.7.4. SOCIAL ENGINEERING EXPLOITATION

A social engineering exercise will target CSP employees responsible for administering the CSP management system. While this exercise will differ based on the agreements and scope of the test plan, the assumption is that the system administrators are operating outside of the target system test boundary and its security controls (relying on CSP corporate security controls). The intent of this test is to assess the likelihood of an external untrusted threat achieving compromise of an internal trusted user responsible for system administration or management. The following activities in Table 13 must be completed.

Table 13 – Social Engineering Exploitation

ACTVITY	DESCRIPTION
Authorization	Identify issues related to role privilege enforcement across common customer roles in the cloud service. Attempt to bypass authorization restrictions.

5.7.5. SIMULATED INTERNAL ATTACK EXPLOITATION

Attempt to identify and potentially exploit attack vectors that could allow access to systems within the test system boundary from within the CSP corporate network environment. This attack vector simulates a breach of a corporate asset with the intent of pivoting access to the target system and will be simulated through analysis of a representative corporate image/workstation.

An assumption is made that if escalation and pivoting vectors are identified, the target system would eventually be compromised. Although the corporate asset is outside the system boundary, the results of the simulated internal attack will be documented in the Penetration Test report for remediation by the CSP. Utilizing this methodology simulates an internal attack without conducting Penetration Testing activities of the corporate CSP network environment. The following activities in Table 14 below must be completed.

Table 14 – Simulated Internal Attack Exploitation

ACTVITY	DESCRIPTION
Escalate to Administrative Privileges	Attempt to gain administrative privileges on the CSP standard workstation image. If the CSP provisions users as local system administrators by default, testing should still be conducted to determine the likelihood of a successful pivot to additional workstations or servers in the CSP environment.
Recording Results	If exploitation attack scenarios were successful, document the results. If exploitation attack scenarios were unsuccessful, document why the exploit failed and what protections (if any) prevented the exploit from executing.

5.8. POST-EXPLOITATION

During post-exploitation, the 3PAO Penetration Testing team will attempt to exercise vulnerabilities discovered during exploitation. The 3APO Penetration Testing team will conduct post-exploitation activities with the intent of demonstrating the impact of exploitation by laterally moving to additional endpoints with the intent to compromise sensitive CSP data, information, or control of the target system infrastructure. Post-exploitation activities will be determined by the level of access gained by exploitation and the technologies utilized by the system. They should broadly cover the activities listed below. The following activities in Table 15 must be completed.

Table 15 – Post-Exploitation

ACTVITY	DESCRIPTION
Escalate to Administrative Privileges	Attempt to gain administrative privileges on the CSP standard workstation image. If the CSP provisions users as local system administrators by default, testing should still be conducted to determine the likelihood of a successful pivot to additional workstations or servers in the CSP environment.
Recording Results	If exploitation attack scenarios were successful, document the results. If exploitation attack scenarios were unsuccessful, document why the exploit failed and what protections (if any) prevented the exploit from executing.

5.8.1. WEB APPLICATION/API POST-EXPLOITATION

Conduct web application post-exploitation activities against target web applications/APIs. The following activities in Table 16 must be completed.

Table 16 – Web Application/API Post-Exploitation

ACTVITY	DESCRIPTION
Unauthorized Management Access	Use access to application to attempt to gain control of underlying infrastructure or management systems.
Unauthorized Data Access	Attempt to demonstrate the potential to access additional data from sources outside the cloud service's intended scope.

5.8.2. MOBILE APPLICATION POST-EXPLOITATION

This attack vector is not applicable since the Penetration Test will be assessing only the local application on the test platform. The device on which the mobile application resides is considered out of scope for the Penetration Test.

5.8.3. NETWORK POST-EXPLOITATION

Conduct network post-exploitation activities against the target infrastructure to attempt to access management networks, applications, and other customer instances. The following activities in Table 17 below must be completed.

Table 17 – Network Post-Exploitation

ACTVITY	DESCRIPTION
Gain Situational Awareness	Determine what level of access was gained following a successful exploitation attempt.
Privilege Escalation	If applicable, attempt to escalate privileges to allow for additional access on the exploited endpoint or other endpoints within the network environment.
Lateral Movement	Perform further discovery and enumeration to identify hosts on the network that may respond only to the compromised system. Leverage compromised systems and credentials to pivot to additional hosts with the intent of gaining unauthorized access to management systems or other customer systems.
Identification and Exfiltration of Sensitive Systems or Data	Identify sensitive or critical information that may be accessed or compromised through a successful attack (criteria for sensitive data to be determined during the scoping phase). Attempt to exfiltrate sensitive information undetected.

5.8.4. SOCIAL ENGINEERING POST-EXPLOITATION

Conduct network post-exploitation activities against the target infrastructure to attempt to access management networks, applications, and other customer instances. The following activities in Table 16 below must be completed.

5.8.5. SIMULATED INTERNAL ATTACK POST-EXPLOITATION

This attack vector is not applicable. The CSP will assume corporate breach; eventually leading to management access into the CSP target system given the 3PAO is able to identify privilege escalation and pivoting avenues and attack chains.

6. REPORTING

Penetration Test assessment activities and results must be organized and compiled into a comprehensive Penetration Test report to be included in the Security Assessment Report (SAR). The report is required to address the following sections.

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 ADDRESSED DURING THE PENETRATION TEST

Described 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 should 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. The 3PAO must describe the access path and the Penetration Test impact if multiple vulnerabilities could be coupled to form a sophisticated attack against the CSP.

The Penetration Test report should include appropriate confidentiality and sensitivity markings in compliance with the CSP organizational policy. The 3PAO should provide the report to the 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. The 3PAO 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.

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 Security Assessment Plan (SAP). Thereafter, FedRAMP requires a complete Penetration Test **at least every 12 months**, unless otherwise approved by the authorizing body with documented rationale.

8. THIRD PARTY ASSESSMENT ORGANIZATION (3PAO) 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 on each Penetration Test must be approved by the Assessment Organization and either have an industry-recognized credential for Penetration Testing or equivalent education and experience. Industry-recognized credentials are identified in Table 18 below.

Table 18 – 3PAO Staffing Requirements

ACTVITY	DESCRIPTION
Global Information Assurance Certification (GIAC)	GWAPT - GIAC Web Application Penetration Tester GPEN - GIAC Network Penetration Tester GXPN - GIAC Exploit Researcher and Advanced Penetration Tester
Offensive Security	OSCP - Offensive Security Certified Professional OSCE - Offensive Security Certified Expert
International Council of Electronic Commerce Consultants (EC-Council)	CEH - Certified Ethical Hacker LPT - Licensed Penetration Tester

APPENDIX A: FedRAMP ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

APPENDIX B: REFERENCES

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

- https://www.fedramp.gov/resources/documents-2016/
- https://www.fedramp.gov/files/2015/03/Guide-to-Understanding-FedRAMP-v2.0-4.docx
- http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- http://dx.doi.org/10.6028/NIST.SP.800-53Ar4
- http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf
- https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Mobile_Security_Testing
- http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- https://azure.microsoft.com/blog/2014/11/11/red-teaming-using-cutting-edge-threat-simulation-to-harden-the-microsoft-enterprise-cloud/

APPENDIX C: ROE/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. The 3PAO is required to develop the ROE and TP based on the parameters and system information provided by the CSP.

The ROE and Test Plan document must be developed in accordance with NIST SP 800-115, Appendix B, and be approved by the Authorizing Official of the CSP prior to testing. The 3PAO 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 3PAO must justify omitting any attack vectors described in Section 3 above in the ROE/Test Plan 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 should account for all 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 should 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.