Guide to Understanding FedRAMP



Version 2.0

June 6, 2014



Executive Summary

The Federal Risk and Authorization Management Program (FedRAMP) provides a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

* Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
* A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by Cloud Service Providers (CSPs);
* Authorization packages of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA;
* Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition; and
* A repository of authorization packages for cloud services that can be leveraged government-wide.

This document provides helpful hints and guidance to make it easier to understand FedRAMP’s requirements and aid government employees and contractors, CSPs and Third-Party Assessment Organizations (3PAOs) in achieving authorization.

FedRAMP supports the U.S. government’s mandate that all U.S. federal information systems comply with the Federal Information Security Management Act of 2002 (FISMA).

Document Revision History

| **Date** | **Page(s)** | **Description** | **Author** |
| --- | --- | --- | --- |
| 06/06/2014 |  | Major revision for SP800-53 Revision 4. Includes new template and formatting changes. | FedRAMP PMO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Guide to Understanding FedRAMP 1](#_Toc389813262)

[Executive Summary 2](#_Toc389813263)

[Document Revision History 3](#_Toc389813264)

[Table of Contents 4](#_Toc389813265)

[List of Figures 6](#_Toc389813266)

[List of Tables 7](#_Toc389813267)

[About this document 8](#_Toc389813268)

[Who should use this document? 8](#_Toc389813269)

[How this document is organized 8](#_Toc389813270)

[How to contact us 8](#_Toc389813271)

[1. FedRAMP Introduction 9](#_Toc389813272)

[1.1. Purpose 9](#_Toc389813273)

[1.2. Applicable Laws and Regulations 10](#_Toc389813274)

[1.3. Applicable Standards and Guidance 10](#_Toc389813275)

[1.4. FedRAMP Governance 11](#_Toc389813276)

[1.5. Federal Compliance and Dates 12](#_Toc389813277)

[1.6. Key Stakeholders 12](#_Toc389813278)

[2. FedRAMP Package Categories and Lifecycle 14](#_Toc389813279)

[2.1. FedRAMP Category: Agency 16](#_Toc389813280)

[2.2. FedRAMP Category: JAB 16](#_Toc389813281)

[2.3. FedRAMP Category: CSP Supplied 17](#_Toc389813282)

[3. Third-Party Assessment Organizations Guidelines 17](#_Toc389813283)

[3.1. How to Become A 3PAO 18](#_Toc389813284)

[3.2. Security Testing 18](#_Toc389813285)

[4. Agency Guidelines 20](#_Toc389813286)

[4.1. Reviewing a FedRAMP Security Package 20](#_Toc389813287)

[4.2. Packages Available for Review 20](#_Toc389813288)

[4.3. Obtaining Approvals and Requesting Access 20](#_Toc389813289)

[4.4. Submitting Existing CSP Security Packages to FedRAMP 23](#_Toc389813290)

[4.5. Migrating Existing Systems to FedRAMP 23](#_Toc389813291)

[4.6. Inventory Cloud Systems 24](#_Toc389813292)

[4.7. Perform GAP Analysis of Missing Controls 24](#_Toc389813293)

[4.8. Review CSP Contracts 25](#_Toc389813294)

[4.9. Obtain Commitment from CSP 25](#_Toc389813295)

[4.10. Migrate Security Documents to FedRAMP Templates 25](#_Toc389813296)

[5. Cloud Service PRovider Guidelines 26](#_Toc389813297)

[5.1. Pre-FedRAMP Initiation 26](#_Toc389813298)

[5.2. Initiating the Process 27](#_Toc389813299)

[5.3. After Acceptance into the FedRAMP Program 28](#_Toc389813300)

[5.4. FIPS 199 Template 28](#_Toc389813301)

[5.5. E-Authentication Template 29](#_Toc389813302)

[5.6. Privacy Threshold Analysis & Privacy Impact Assessment 29](#_Toc389813303)

[5.7. CTW Template 30](#_Toc389813304)

[5.8. CIS Template 30](#_Toc389813305)

[5.9. User Guide 32](#_Toc389813306)

[5.10. Components, Boundaries, and Architecture 32](#_Toc389813307)

[6. Maintaining an Authorization 38](#_Toc389813308)

[7. General Documentation Information for CSPS 39](#_Toc389813309)

[7.1. Formatting and SEction Numbers 39](#_Toc389813310)

[7.2. Sensitivity Markings 39](#_Toc389813311)

[7.3. Items That Are Not Applicable 39](#_Toc389813312)

[8. Layering One Package on top of Another 39](#_Toc389813313)

[Appendix A – Acronyms 41](#_Toc389813314)

[Appendix B – Department of Defense Memo 42](#_Toc389813315)

[Appendix C – Use Cases 43](#_Toc389813316)

[Appendix D – FedRAMP Security Control Guidance 52](#_Toc389813317)

List of Figures

[Figure 1-1 – FedRAMP Key Stakeholders 13](#_Toc389813341)

[Figure 2-1 – Authorization Timeline 15](#_Toc389813342)

[Figure 4-1 – FedRAMP Package Access Process 22](#_Toc389813343)

[Figure 4-1 – Submitting Package to FedRAMP PMO 23](#_Toc389813344)

[Figure 5-1 – Screenshot from CTW 30](#_Toc389813345)

[Figure 5-2 – Select the Implementation Status in the CIS 31](#_Toc389813346)

[Figure 5-3 – Select the Control Origination Responsibility 31](#_Toc389813347)

[Figure 5-4 – Example of Components Described by Name 33](#_Toc389813348)

[Figure 5-5 – Example of Components Described by Function 33](#_Toc389813349)

[Figure 5-6 – Example of Storage Array Illustration 37](#_Toc389813350)

[Figure 5-7 – Data Flow Diagram Example 38](#_Toc389813351)

[Figure C-1 – One IaaS Provider 43](#_Toc389813352)

[Figure C-2 – One Provider for Iaas and PaaS 44](#_Toc389813353)

[Figure C-3 – One Provider, IaaS, Paas, Saas 45](#_Toc389813354)

[Figure C-4 – One Provider, Just SaaS 46](#_Toc389813355)

[Figure C-5 – Two Providers, One IaaS and One PaaS (or Saas) 47](#_Toc389813356)

[Figure C-6 – Three Providers, One IaaS, One PaaS, and One SaaS 48](#_Toc389813357)

[Figure C-7 – Two IaaS Providers 49](#_Toc389813358)

[Figure C-8 – Two IaaS and One PaaS Provider 50](#_Toc389813359)

[Figure C-9 – Three Providers, One IaaS and Two PaaS 51](#_Toc389813360)

[Figure D-1 – TIC Compliant Architecture 59](#_Toc389813361)

[Figure D-2 – Module Validation Lists 61](#_Toc389813362)

List of Tables

[Table 2-1 – FedRAMP Security Package Categories 14](#_Toc389813363)

[Table 4-1 – Required FedRAMP Templates 26](#_Toc389813364)

[Table 5-1 – Preparation Checklist 27](#_Toc389813365)

[Table 5-2 – Information Types for the IaaS Providers 28](#_Toc389813366)

[Table D-1 – Example of Security Control Summary Information 52](#_Toc389813367)

[Table D-2 – Control Origination Definitions 54](#_Toc389813368)

[Table D-3 – Configuration Management Controls 63](#_Toc389813369)

[Table D-4 – Configuration Management Nomenclature 65](#_Toc389813370)

[Table D-5 – Incident Response Controls 67](#_Toc389813371)

[Table D-6 – Agency Points of Contact to Report Incidents 71](#_Toc389813372)

# About this document

This document provides guidance on how to participate in and understand the Federal Risk and Authorization Management Program (FedRAMP).

## Who should use this document?

The target audiences for this document are CSPs, 3PAOs, government employees and contractors working on FedRAMP projects, and any outside organizations that want to make use of the FedRAMP assessment process.

## How this document is organized

This document is divided into eight primary sections and four appendices:

|  |  |
| --- | --- |
| Section 1 | Introduction and overview of FedRAMP. |
| Section 2 | Information on different types of FedRAMP Security Packages. |
| Section 3 | Guidelines for third-party assessment organizations. |
| Section 4 | Guidelines for federal departments and agencies on how to use FedRAMP. |
| Section 5 | Guidelines for Cloud Service Providers on how to achieve an authorization. |
| Section 6 | Instructions for Cloud Service Providers on how to maintain an authorization. |
| Section 7 | General documentation for Cloud Service Providers. |
| Section 8 | Information on how to layer security packages. |
| Appendix A | Acronyms |
| Appendix B | Department of Defense memo from the ECSB Cloud Broker Office. |
| Appendix C | Use cases for various cloud configurations. |
| Appendix D | Guidance on how to interpret specific security controls for FedRAMP. |

## How to contact us

Questions about FedRAMP or this document may be directed to [*info@fedramp.gov*](mailto:info@fedramp.gov)*.*

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

1. FedRAMP Introduction

The Federal Risk and Authorization Management Program (FedRAMP) provides a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

* Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
* A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by Cloud Service Providers (CSPs);
* Authorization packages of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the Department of Homeland Security (DHS), Department of Defense (DOD), and General Services Administration (GSA);
* Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition; and
* A repository of authorization packages for cloud services that can be leveraged government-wide.

FedRAMP processes are designed to assist agencies in meeting FISMA requirements for cloud systems and addresses complexities of cloud systems that create unique challenges for complying with FISMA.

There are three paths to achieving FedRAMP compliance:

1. A Cloud Service Provider can submit the appropriate documentation to the FedRAMP PMO and to the JAB which may grant a Provisional Authorization to Operate (P-ATO)
2. A Cloud Service Provider can submit the appropriate documentation to the FedRAMP PMO and to an agency which may grant an agency “Authorization to Operate” (ATO). Using FedRAMP mechanisms, other agencies can then “leverage” this ATO for use in their agency, decreasing the time for approvals.
3. A Cloud Service Provider can use the “CSP supplied” path by submitting the appropriate documentation to the FedRAMP PMO. While this does not grant the CSP a P-ATO or an agency ATO, it decreases the time for approvals because documentation and testing (by a 3PAO) are complete and available for agency review.
   1. Purpose

This document provides guidance on how cloud service providers can meet FISMA requirements to obtain a FedRAMP authorization. It also provides guidance for third-party independent assessment organizations on how to conduct security assessments for cloud service providers.

Additionally, this document helps U.S. federal agencies, bureaus, and departments understand how to meet federal security requirements for cloud systems.

FedRAMP is designed to speed agencies through the security assessment and authorization process by leveraging FedRAMP authorized cloud systems for use in their own agency. By using cloud systems that have already received a FedRAMP JAB-issued Provisional Authorization or Agency issued Authorization to Operate (ATO), agencies can reap significant financial and time savings to implement new systems quickly.

An agency can issue authorizations (Agency ATO) to cloud providers based on FedRAMP guidelines and templates. The agency’s package is uploaded to the FedRAMP secure repository and available to other agencies for review and use, further supporting ”do-once, use many times”.

* 1. Applicable Laws and Regulations

The following laws and regulations are applicable to FedRAMP:

* Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
* E-Authentication Guidance for Federal Agencies [OMB M-04-04]
* Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
* Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
* Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
* Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
* Internal Control Systems [OMB Circular A-123]
* Management of Federal Information Resources [OMB Circular A-130]
* Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
* Privacy Act of 1974 as amended [5 USC 552a]
* Protection of Sensitive Agency Information [OMB M-06-16]
* Records Management by Federal Agencies [44 USC 31]
* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
* Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]
  1. Applicable Standards and Guidance

The following standards and guidance are applicable to FedRAMP:

* A NIST Definition of Cloud Computing [NIST SP 800-145]
* Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
* Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
* Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
* Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
* Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
* Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
* Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]
* Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
* Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
* Managing Information Security Risk [NIST SP 800-39]
* Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
* Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
* Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
* Risk Management Guide for Information Technology Systems [NIST SP 800-30, Revision 1]
* Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
* Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
* Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
* Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]
  1. FedRAMP Governance

FedRAMP is governed by a Joint Authorization Board (JAB) comprised of the Chief Information Officers from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD). The U.S. Government’s Chief Information Officer Council (CIOC), including its Information Security and Identity Management Committee (ISIMC), endorses FedRAMP. FedRAMP collaborates with the ISIMC as it identifies high-priority security and identity management initiatives and develops recommendations for policies, procedures, and standards to address those initiatives.

* 1. Federal Compliance and Dates

OMB published a memo on December 8, 2011 that states that all low and moderate impact level cloud services leveraged by one or more office or agency must comply with FedRAMP requirements.

FedRAMP commenced Initial Operating Capability (IOC) on June 6, 2012. Cloud systems in the acquisition phase as of June 6, 2012, but not yet implemented, had until June 5, 2014 to become FedRAMP compliant as noted in footnote 10, on page 5 of the FedRAMP policy memo:

*For all currently implemented cloud services or those services currently in the acquisition process prior to FedRAMP being declared operational, security authorizations must meet the FedRAMP security authorization requirement within 2 years of FedRAMP being declared operational.*

A cloud system is compliant with FedRAMP if it meets the following requirements:

* The system security package has been created using the required FedRAMP templates
* The system meets the FedRAMP security control requirements
* The system has been assessed by an independent assessor
* A Provisional Authorization, and/or an Agency ATO, has been granted for the system
* An authorization letter for the system is on file with the FedRAMP Program Management Office (PMO)
  1. Key Stakeholders

FedRAMP streamlines federal agencies’ ability to make use of cloud service provider platforms and offerings. FedRAMP provides three paths for CSPs to obtain compliant authorization after undergoing a third-party independent security assessment. . Figure 1-1 provides an overview of the FedRAMP key stakeholders.

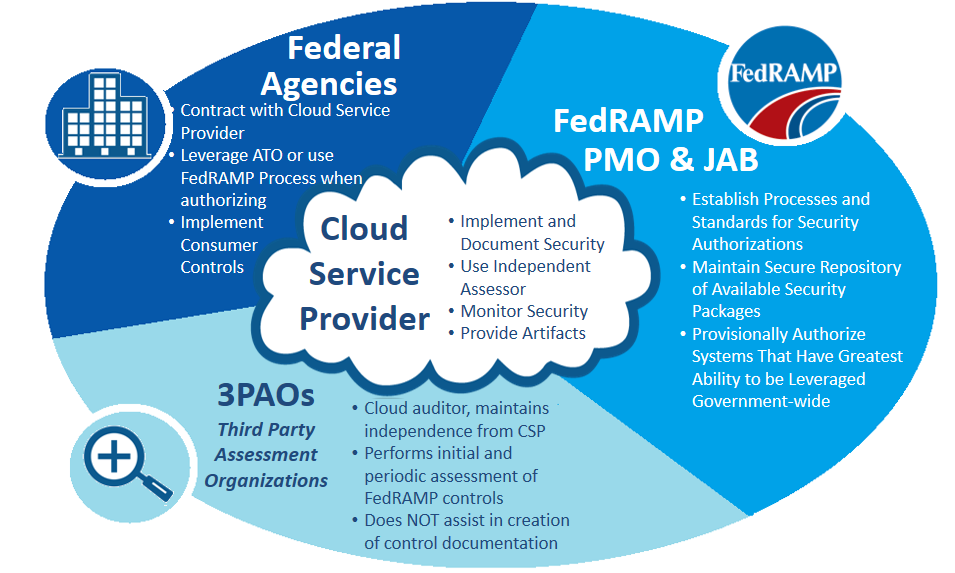


Figure 1-1 – FedRAMP Key Stakeholders

A CSP can be a commercial or government entity that has a cloud offering or service. The CSP is responsible for implementing FedRAMP security controls, hiring an independent third party assessor to perform initial and annual assessments, creating and maintaining its authorization, and complying with continuous monitoring requirements. Commercial CSPs must select an accredited 3PAO.

Agencies are responsible for

* Ensuring all new cloud projects use the FedRAMP baseline controls and templates, as well as reviewing and granting authorizations
* Ensuring existing cloud projects (implemented or in the acquisition process) meet FedRAMP requirements
* Adding or modifying contractual provisions that require CSPs meet FedRAMP requirements
* Updating OMB PortfolioStat data quarterly to identify use of CSPs and plans to meet FedRAMP requirements, and rationalize lack of compliance
* Reviewing CSP documentation and test results prior to leveraging a JAB P-ATO or agency-issued ATO
* Reviewing Plans of Action and Milestones (POAMs) for leveraged CSPs
* Adding any agency-specific controls above the baseline
* Submitting all documents for an agency-issued CSP authorization for leveraging by other agencies

Third Party Assessor Organizations (3PAOs) are independent entities that perform initial and periodic security assessments of cloud systems. 3PAOs assess the CSPs security control implementation, and generate Security Assessment Reports and associated evidence of test results. 3PAOs are hired by CSPs, and can be hired by agencies.

1. FedRAMP Package Categories and Lifecycle

There are three paths for security packages to make their way into the FedRAMP repository. Once a security package is listed in the FedRAMP repository, federal agencies then have the opportunity to review the packages to determine if they would like to use the system described in the package. Some of the packages listed in the repository may already be approved as being FedRAMP compliant while other packages are candidates for approval. Section 3 in this document provides instructions on how agencies can review packages in the FedRAMP repository.

FedRAMP packages are assigned categories (Table 2-1) for easier reference and a discussion of package usage and lifecycle follows. It is possible for a package to move from one level to another. Categories do not necessarily represent the strength of the security controls for the represented cloud system. The biggest difference between the three categories is the level of security package review.

| **Category** | **Review Level Description** | **Authorization** |
| --- | --- | --- |
| CSP | CSP Supplied, not yet reviewed | Candidate for Authorization |
| Agency | Reviewed by agency | Agency ATO |
| JAB | Reviewed by FedRAMP ISSO and JAB | FedRAMP and Agency |

Table 2-1 – FedRAMP Security Package Categories

Figure 1-2 shows the process and notional timeframe to achieve either a JAB Provisional or Agency ATO. The time frame is dependent on CSP readiness and ability to respond to comments throughout each of the stages. Continuous monitoring activities commence once authorization is achieved.

**Authorize**

CSP Addresses JAB Concerns

JAB Review

ISSO & CSP Review SSP

3PAO Creates SAP/ ISSO Reviews SAP

JAB Review

Final JAB Review /

P-ATO Sign Off

3PAO Tests & Creates SAR

**System Security Plan**

**Security Assessment Plan**

**SAR & POA&M Review**

**Testing**

**6 months +**

JAB Review

ISSO / CSP Reviews

SAR

CSP Addresses Jab Concerns Creates POA&M

CSP Addresses JAB Concerns

CSP Addresses Agency Concerns

Agency Review

CSP Implements Control Delta

Agency Review SAP

Address Agency Notes

Final Agency ATO Sign Off

3PAO Tests & Creates SAR

**System Security Plan**

**Security Assessment Plan**

**SAR & POA&M Review**

**Testing**

**4 months +**

**Authorize**

CSP Addresses Concerns

Agency Reviews

SAR

CSP Creates POA&M

***Quality of documentation will determine length of time***

***and possible cycles throughout the entire process***

**JAB**

**P-ATO**

**Agency**

**ATO**

Figure 2-1 – Authorization Timeline

* 1. FedRAMP Category: Agency

Packages in the Agency category were reviewed by at least one agency and determined to be FedRAMP compliant by the reviewing agency resulting in an agency ATO. Agencies reviewing packages must provide their own resources and bear all costs for the review of the package and ongoing use of the system. The agency must arrange for Trusted Internet Connection (TIC) routing for the system, provide continuous monitoring based on FedRAMP requirements, and submit annual assessments to the FedRAMP PMO.

Agencies have the option of using any independent assessor whether the entity is a FedRAMP accredited 3PAO or not. Packages not assessed by a FedRAMP accredited 3PAO are not eligible for review by the JAB and subsequent issuance of a Provisional Authorization. If the independent assessor assesses a CSP system and subsequently applies and receives FedRAMP 3PAO accreditation, the CSP may submit the package to FedRAMP for review by the JAB. For the security package to be acceptable to the JAB, the 3PAO must attest to the fact that the required Quality Management System was in place at the time they completed the system testing.

If the JAB grants a Provisional Authorization to a CSP, the FedRAMP PMO ISSO assumes management of the CSP system from the Agency for the lifecycle of continuous monitoring and annual assessments. The package is re-categorized as a *JAB* package after a FedRAMP Provisional Authorization is granted.

Other agencies can leverage the originating CSP ATO by reviewing the CSP package in the secure repository, and issue an ATO letter based on the originating agency’s work.

* 1. FedRAMP Category: JAB

Packages in the *JAB* category were assessed by an accredited 3PAO and reviewed by both FedRAMP PMO ISSOs and the JAB. JAB packages have undergone rigorous technical reviews for FedRAMP compliance and issued a FedRAMP Provisional Authorization. Systems that have received a FedRAMP Provisional Authorization are assigned a FedRAMP PMO ISSO to manage the complete lifecycle of the Provisional Authorization including continuous monitoring and annual assessments.

The JAB cannot accept risk on behalf of any agency which is why the JAB authorization is titled a “Provisional Authorization.” If an agency decides to use a system with a Provisional Authorization, the agency will need to issue its own ATO letter to indicate that they accept the risk associated with using the system.

A JAB Provisional Authorization may not necessarily be optimal for every system and every CSP. In general, the JAB grants Provisional Authorizations for those systems leveraged government wide. FedRAMP was designed with the objective to authorize a system once and reuse that authorization many times. If a CSP only has one agency customer showing interest in using their system, it is just as efficient for the CSP to obtain an authorization directly through the one agency of interest.

Continuous Monitoring for systems that receive a FedRAMP JAB Authorization are managed by FedRAMP PMO ISSOs. FedRAMP ISSOs ensure that all continuous monitoring artifacts and evidence are submitted on schedule and available for leveraging agencies to review as well as managing Plans of Action and Milestones (POAMs).

CSP systems that receive FedRAMP Provisional Authorizations are listed on the FedRAMP website at [www.fedramp.gov](http://www.fedramp.gov).

* 1. FedRAMP Category: CSP Supplied

CSPs may supply a security package to the FedRAMP secure repository for prospective Agency use. In this case, a CSP decides to work independently instead of through the JAB or through a Federal agency. In this category, a CSP will complete the FedRAMP SAF independently and will not have an authorization at the completion, but will have a FedRAMP-compliant package available for leveraging.

For CSP -supplied packages, CSPs must contract with an accredited 3PAO to independently verify and validate their security implementations and their security assessment package.

Once a CSP completes their security authorization package, the CSP must inform the FedRAMP PMO by sending an email to info@FedRAMP.gov. The PMO then instructs the CSP how to submit the package for PMO review. After reviewing the package to ensure it meets all of the FedRAMP requirements, the FedRAMP PMO will publish the package in the secure repository for other agencies to leverage.

If an Agency decides to issue an ATO to a CSP-supplied package, the status of the package will be changed in the secure repository to indicate that it has evolved to a FedRAMP Agency ATO Package.

1. Third-Party Assessment Organizations Guidelines

Title III, Section 3544, of the E-Government Act of 2002, dated December 17, 2002, requires agencies to conduct periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. The term “system” includes Cloud Service Provider platforms and offerings. Appendix III of Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, specifically requires federal agencies to:

*Review the security controls in each system when significant modifications are made to the system, but at least every three years. §3(a)(3)*

*Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information. §8(a)(1)(g); §8(a)(9)(a)*

*Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time. §8(b)(3)(b)(iv)*

* 1. How to Become A 3PAO

To become an accredited 3PAO under FedRAMP, candidate third party assessors must submit application materials demonstrating that they meet both technical competence in security assessment of cloud systems and management requirements for organizations performing inspections. Prospective 3PAOs must have an operational Quality Management System in place at their organization and must demonstrate knowledge of standard conformity assessment processes.

The 3PAO accreditation program ensures that approved 3PAOs consistently perform security assessments with an appropriate level of rigor and independence. FedRAMP will only review security assessment packages from CSPs that have been assessed by an accredited 3PAO. Furthermore, only CSPs that use an accredited 3PAO are eligible for a Joint Authorization Board (JAB) Provisional Authorization.

FedRAMP approved American Association for Laboratory Accreditation (A2LA) to accredit FedRAMP Third Party Assessment Organizations (3PAOs). Using technical experts as assessors, the A2LA assessment process involves a rigorous evaluation of technical competence of the 3PAOs, as well as an assessment of their compliance to the general requirements of ISO/IEC 17020. More information on working with A2LA and applying to become an accredited FedRAMP 3PAO can be found at <http://a2la.org/fedramp>.

FedRAMP retains governance and oversight of the 3PAO program, and maintains final approval authority for those 3PAO accredited by A2LA.

* 1. Security Testing

It is a goal of FedRAMP for all CSP systems to be assessed equally and according to the same security baseline controls appropriate for the designated sensitivity category. In support of this goal, templates are provided to standardize the assessment process. Templates designed for 3PAOs to complete or use are the *Security Assessment Plan* (SAP), *Security Assessment Test Cases*, and the *Security Assessment Report* (SAR).

* + 1. Security Assessment Plan (SAP)

The purpose of the SAP is to describe the security test plan. The 3PAO must meet with the CSP to discuss the test engagement before developing the SAP, and again prior to finalizing the SAP. If 3PAOs have any questions on security testing, they must contact the FedRAMP PMO ISSO. The 3PAO must submit the final SAP to both the CSP and FedRAMP ISSO for approval prior to starting to test. The ISSO will review the SAP and give the go ahead to start testing after obtaining approval from the JAB. The SAP template is available on [www.fedramp.gov](http://www.fedramp.gov). .

* + 1. Security Test Cases

The *Security Assessment Test Cases* are based on NIST SP 800-53A. There are some FedRAMP test cases modified from NIST SP 800-53A due to the uniqueness of cloud implementations. Therefore, it is important to use the test cases found on [www.fedramp.gov](http://www.fedramp.gov).

For any alternative implementations of controls as described in a CSPs SSP, the 3PAO must create alternative test cases that adequately test the effectiveness of the CSP’s control implementation and any risk associated with that implementation.

* + 1. Security Assessment Report (SAR)

The *Security Assessment Report* is the final report written by the 3PAO to detail the independent security assessment performed on the CSP candidate information system. The FedRAMP PMO provides a *Security Assessment Report* template, and all 3PAOs are required to use this template to report their findings. The SAR template is available on [www.fedramp.gov](http://www.fedramp.gov).

For JAB Provisional ATO’s, the 3PAO is expected to provide a high-level briefing to the FedRAMP PMO and JAB TRs. This brief will highlight findings, mitigations, and operational requirements, as well as identify any problems or areas of concern. The FedRAMP ISSO coordinates with the 3PAO on the briefing.

* + 1. Running Scans

As part of security testing, automated scans are required. On large implementations, a subset of all representative hosts and device types must be scanned using full authentication. The advantage of running scans as fully authenticated privileged users is that the scanner can access the registry, file attributes, installed packages, and patch levels. Account credentials for the authenticated scans must use login IDs and user roles that offer the greatest possible privileges for the scanned system (e.g. root, administrator).

The use of non-authenticated scans can assist in vulnerability severity determinations and to prioritize remediation efforts since non-authenticated scan vulnerabilities are seen from the point of an attacker/intruder. Non-authenticated scans can augment fully authenticated scans if the information from these scans helps to determine the risk exposure. FedRAMP does not require non-authenticated scans.

3PAOs do not need to run source code scans. However, if a CSP develops and uses original source code in their service offering, the CSP is required to perform source code scanning on the installed release and provide the source code analysis report to the 3PAO to satisfy control SA-11(1).

**Tip:** An authenticated scan is sometimes referred to as credentialed scan or a host-based scan.

The 3PAO submits all scan results to the FedRAMP PMO ISSO at the same time the SAR is provided, and the 3PAO must be prepared to brief the results to the FedRAMP PMO and JAB representatives.

A 3PAO scans CSP systems as part of the CSPs annual assessment. The annual scan does not have to be performed by the same 3PAO that performed the previous scan(s).

1. Agency Guidelines

Agencies should be aware of their consumer responsibilities and implement controls in accordance with agency policy or guidance. Agency responsibilities include:

* Management of annual training requirements
* Implementation or integration of two-factor authentication
* Implementation of Trusted Internet Connection (TIC)
* Implementation of incident response capabilities
* Additional mission specific controls to build upon the FedRAMP baseline
  1. Reviewing a FedRAMP Security Package

Before deciding to use a FedRAMP JAB or agency-issued authorized CSP’s system, agencies should review each candidate package to make sure that it meets agency requirements.

* 1. Packages Available for Review

Only U.S. federal agencies may review FedRAMP security packages. These packages are not available for review by the public, nor are they available for review by the private sector. CSP systems that have security packages in the FedRAMP repository are listed on the FedRAMP website at [www.fedramp.gov](http://www.fedramp.gov).

* 1. Obtaining Approvals and Requesting Access

Once an agency reviewer determines which package to review, the next step is to download the *FedRAMP Package Access Request Form* and fill in all of the requisite fields. The form needs to be reviewed and signed internally at the reviewer’s agency by the reviewer’s CISO, before submitting it to the FedRAMP PMO. In the event that the agency has more than one CISO, the signature should come from the CISO that is closest in the line of reporting to the reviewer.

**Note:** The *FedRAMP Package Access Request Form* can be found at: [www.fedramp.gov](http://www.fedramp.gov).

Once the authority within the requesting agency signs the form, prospective package reviewers must scan the signed access request form and email it to [info@fedramp.gov](mailto:info@fedramp.gov). The form will be reviewed for correctness and completeness by the FedRAMP PMO. All information on the form is subject to verification.

There are certain limitations that government contractors face in reviewing FedRAMP security packages. Security packages contain intellectual property of each respective CSP. If the prospective package reviewer is a government contractor, the FedRAMP PMO will contact the CSP system owner to obtain their approval.

The prospective package reviewer will be notified and provided access instructions when the request is approved or denied. A new *FedRAMP Package Access Request Form* must be filled out for each package. A summary of the package access authorization process is found in Figure 4-1.

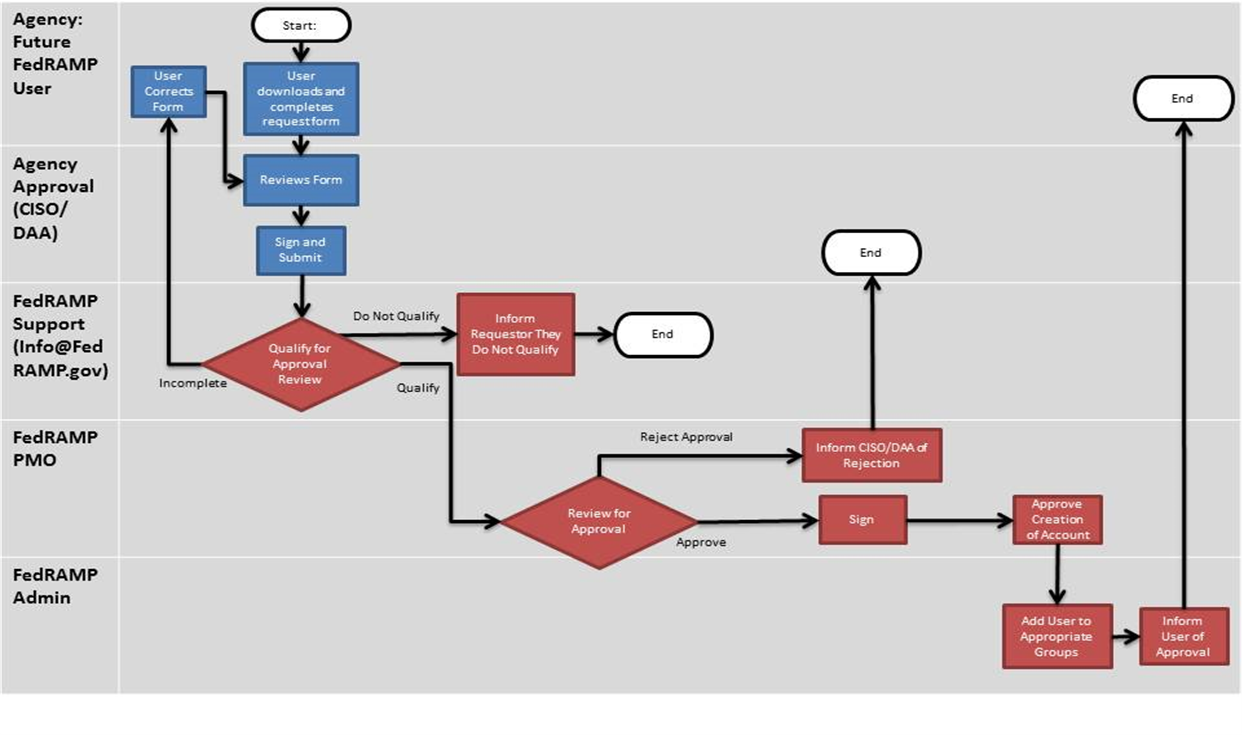


Figure 4-1 – FedRAMP Package Access Process

* 1. Submitting Existing CSP Security Packages to FedRAMP

Agencies are required to submit FedRAMP compliant security packages to the FedRAMP PMO so that other agencies have the opportunity to review the package for possible use.

When an agency is ready to submit a package to the FedRAMP PMO, it should contact the PMO by writing to [info@fedramp.gov](mailto:info@fedramp.gov). A summary of the package submission process is illustrated in Figure 4-1.



Figure 4-1 – Submitting Package to FedRAMP PMO

If at any point an agency revokes an ATO for a package that was submitted to the FedRAMP PMO, the agency should notify the FedRAMP PMO immediately.

* 1. Migrating Existing Systems to FedRAMP

Cloud systems implemented by agencies and CSPs prior to June 6, 2012 must have FedRAMP security controls in place by June 5, 2014. Agencies should perform a gap analysis on their current cloud systems to determine which security controls are missing, and which security control parameters do not meet FedRAMP requirements.

In some situations, an agency may have built their own cloud - either a private cloud or a cloud shared with another agency. If an agency builds an in-house cloud system, the agency must identify and implement missing security controls, and have the system tested by a third-party independent assessor.

If the cloud system was built by an external private sector CSP, the agency should inform the CSP that the system is not FedRAMP compliant, and advise the CSP that FedRAMP requirements should have been met by June 5, 2014. If the CSP is not aware of FedRAMP requirements, the agency should direct the CSP to the FedRAMP website.

* 1. Inventory Cloud Systems

Agencies should create an inventory of its respective cloud systems. Not all agency systems are cloud systems, and agencies should determine which systems are cloud systems and which systems are traditional systems.

FedRAMP recommends that agencies identify a liaison to centrally manage cloud systems and communicate FedRAMP requirements. The liaison should be prepared to respond to agency queries and reporting requirements, and make agency-wide recommendations on FedRAMP. The following information would be useful for the liaison to collect:

* Name of cloud system
* Description of what services the cloud system provides
* Name and contact information of system owner
* Date that the existing authorization was granted
* Status of compliance with FedRAMP
  1. Perform GAP Analysis of Missing Controls

For each cloud system, agencies should review the implemented security controls, and perform a gap analysis using the FedRAMP security control baseline to identify which security controls are missing. FedRAMP security controls are listed on [www.fedramp.gov](http://www.fedramp.gov) in the form of an Excel spreadsheet and are summarized in the System Security Plan template.

**Note:** Do not use NIST 800-53 low or moderate baselines to perform a gap analysis. The FedRAMP baseline contains additional controls that are applicable to cloud environments .

A gap analysis identifies which new security controls must be implemented on the respective cloud system. The gap analysis can serve as an agenda item for meetings with the cloud service provider. Agencies will need to work in concert with their CSPs to implement missing security controls required by the FedRAMP baseline.

* 1. Review CSP Contracts

Agencies should review existing contracts with CSPs and respective Contracting Officers. Existing contracts with CSPs should already require FISMA compliance. Agencies should incorporate explicit FedRAMP compliance in existing and future contracts.

* 1. Obtain Commitment from CSP

Agencies should determine if the CSP plans to submit their security package to FedRAMP for a Provisional Authorization. CSPs actively working either with the FedRAMP PMO to achieve Provisional Authorization, with another agency to achieve ATO, or in queue for authorization are listed on [www.fedramp.gov](http://www.fedramp.gov). Agencies can also contact the FedRAMP PMO to inquire as to the status of CSPs via e-mail at info@fedramp.gov.

CSPs that do not intend to apply for a Provisional Authorization will need to be managed directly by their agency customers. In order to maintain a solid implementation and compliance schedule, agencies should ensure that they have solid milestones for completion. The FedRAMP PMO recommends agencies obtain compliance schedules from CSPs that do not plan on applying for a Provisional Authorization.

* 1. Migrate Security Documents to FedRAMP Templates

Cloud systems that have ATOs are required to migrate existing security package documents to the FedRAMP templates. FedRAMP templates must be used whether the CSP intends to pursue a JAB Provisional Authorization or not. Private clouds must also use FedRAMP templates. Templates for all documents are available on the FedRAMP website. The following FedRAMP supplied templates are mandatory:

* Control Tailoring Workbook (CTW)
* Control Information Summary (CIS)
* System Security Plan (SSP)
* Security Assessment Plan (SAP)
* Security Assessment Report (SAR)

Agencies can use their own templates for the other documents, as long as the agency templates contain the same information as that exists in the FedRAMP templates. A summary of the templates that are available on the FedRAMP website are listed in Table 4-1.

|  |  |  |
| --- | --- | --- |
| **Template Name** | **FedRAMP Template Available?** | **FedRAMP Supplied Template Required?** |
| Control Tailoring Workbook | Yes | Yes |
| Control Information Summary | Yes | Yes |
| FIPS 199 Template | Yes | Yes |
| eAuthentication Template | Yes | No |
| System Security Plan | Yes | Yes |
| Rules of Behavior | Yes | No |
| Configuration Management Plan | No | No |
| Information System Security Policies | No | No |
| IT Contingency Plan | Yes | No |
| Incident Response Plan | No | No |
| Privacy Threshold Assessment / Impact Assessment | Yes | No |
| Security Assessment Plan | Yes | Yes |
| Security Assessment Report | Yes | Yes |
| Plan of Action & Milestones | Yes | No |

Table 4-1 – Required FedRAMP Templates

1. Cloud Service PRovider Guidelines

This section is provided to assist CSPs in understanding how to satisfy requirements for FedRAMP.

* 1. Pre-FedRAMP Initiation

In prior cloud FISMA compliance projects, certain controls proved to be challenging for CSPs to meet. Before a CSP decides to initiate a request to participate in FedRAMP, it must review the checklist in Table 5-1 to ensure ability to meet the requirements. CSPs must consult with legal and technical staff (e.g. systems administrators, database administrators, network engineers) to determine whether appropriate controls are in place and manageable.

| **Checklist** | | **Description** |
| --- | --- | --- |
|  | 1 | Process electronic discovery and litigation holds |
|  | 2 | Clearly define and describe the system boundaries |
|  | 3 | Identify customer responsibilities and what the CSP and agency must do to implement controls |
|  | 4 | System provides identification & 2-factor authentication for network access to privileged accounts |
|  | 5 | System provides identification & 2-factor authentication for network access to non-privileged accounts |
|  | 6 | System provides identification & 2-factor authentication for local access to privileged accounts |
|  | 7 | Perform code analysis scans for code written in-house (non-COTS products) |
|  | 8 | Appropriate boundary protections |
|  | 9 | Remediate high risk issues within 30 days, medium risk within 90 days |
|  | 10 | Provide an inventory and configuration build standards for all devices |
|  | 12 | Cryptographic safeguards preserve confidentiality and integrity of data during transmission |

Table 5-1 – Preparation Checklist

* 1. Initiating the Process

Cloud service providers (CSPs) initiate participation in FedRAMP by submitting a *FedRAMP* *Initiation Request* form. This is a web based form found on the FedRAMP website. This form advises the FedRAMP PMO, and the JAB of the intent to obtain a FedRAMP Provisional Authorization.

On the *FedRAMP* *Initiation Request* form, a CSP provides a categorization of its system and indicate the information types based upon NIST SP 800-60 V2 guidelines. CSPs must use the data type sensitivity categorization to select which control baseline to implement – Low or Moderate. (High sensitivity categorizations are currently not part of the FedRAMP program.) The FedRAMP PMO contacts the CSP to schedule a conference call to discuss CSP readiness to begin the process to achieve Provisional Authorization.

At this time, the CSP must research and hire a 3PAO. FedRAMP accredited 3PAOs are listed on the FedRAMP website.

* 1. After Acceptance into the FedRAMP Program

After acceptance into the FedRAMP JAB Provisional Authorization process, there are certain documents requiring submission. The FedRAMP PMO created templates for documents that the CSP must edit and modify based on the security controls implemented in its system. All templates are available on the FedRAMP website. Guidance on how to fill out the various templates and develop the required documents are described in the sections that follow.

* 1. FIPS 199 Template

The FIPS 199 template exists so that CSPs can categorize and record the sensitivity level of the system. CSPs must use NIST SP 800-60, Revision 1, Volume 2, to select the Information Type for their candidate system. IaaS and PaaS providers must select information types from NIST SP 800-60 Revision 1, Volume 2 Section C.3.5 as noted in Table 5-2. SaaS providers must select information types from the entire list of possible information types.

|  |
| --- |
| **C.3.5 Information and Technology Management** |
| C.3.5.1 System Development Information Type |
| C.3.5.2 Lifecycle/Change Management Information Type |
| C.3.5.3 System Maintenance Information Type |
| C.3.5.4 IT Infrastructure Maintenance Information Type |
| C.3.5.5 Information Security Information Type |
| C.3.5.6 Record Retention Information Type |
| C.3.5.7 Information Management Information Type |
| C.3.5.8 System and Network Monitoring Information Type |
| C.3.5.9 Information Sharing Type |

Table 5-2 – Information Types for the IaaS Providers

Perform FIPS 199 analysis with respect to service provider system data only. Customer agencies will perform a separate FIPS 199 analysis for their customer owned data hosted on the system.

* 1. E-Authentication Template

An e-Authentication template is provided for performing an e-Authentication analysis. The objective of selecting the appropriate e-Authentication level is to ensure that the CSP has used a technical solution that matches the sensitivity of the system and the data it stores and processes. Guidance on selecting the system authentication technology solution is available in *NIST SP 800-63, Revision 1, Electronic Authentication Guidance*.

**Note:** NIST SP 800-63, Revision 1 is located at the following URL: <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

Ensure that the final e-Authentication analysis is consistent with Table 2-5 in the *System Security Plan*.

**Note:** Refer to *OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies* for more information on e-Authentication.

The e-Authentication template is available on [www.fedramp.gov](http://www.fedramp.gov).

* 1. Privacy Threshold Analysis & Privacy Impact Assessment

CSPs are required to fill out a *Privacy Threshold Analysis* (PTA). FedRAMP provides a PTA/PIA template, and the PTA consists of four short questions designed to determine if the system qualifies as a Privacy Sensitive System. If the result of the PTA qualifies the system as a Privacy Sensitive System, then a *Privacy Impact Assessment* (PIA) is also required.

**Note:** In accordance with NIST SP 800-144, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

CSPs must consider whether their security controls (for their own support staff) use PII for any authentication mechanisms (e.g. fingerprint scanners, hand scanners, iris scanners). If the CSP system requires PII from agency customers, for example, to enroll users in authentication mechanisms, then the impending collection of that PII on first use by agency customers should be made known.

When performing the independent security assessment, the 3PAO will review the PTA and/or PIA to make certain determinations and findings that are incorporated into the *Security Assessment Report* (SAR).

A combination PTA and PIA template is available on [www.fedramp.gov](http://www.fedramp.gov).

* 1. CTW Template

The purpose of the *Control Tailoring Workboo*k (CTW) template is to summarize the exception scenarios of the service offering for prospective agency customers. This template is completed after the *System Security Plan* has been completed, and must be consistent with information found in the *System Security Plan*.

In the CTW, as shown in Figure 5-1, in the column “Service Provider Implemented Settings and Exceptions”, CSPs must describe any setting(s) in their service offering that is different from either the stated Control Parameter Requirements or the stated Additional Requirements and Guidance.

* If a parameter or requirement simply does not exist in the candidate service offering, annotate as “not implemented”.
* If the candidate service offering uses an alternative or compensating control, provide a brief explanation of how the alternative control works.
* If a control does not exist but planned for future implementation, provide a brief explanation of how and when the control will be implemented.
* If the CSP system meets all required security controls, settings, and parameters, the CSP must note “Meets” in the right-hand most column for the associated control.

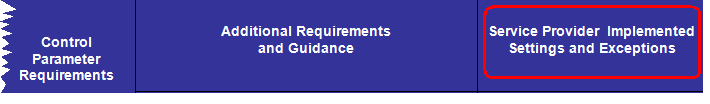


Figure 5-1 – Screenshot from CTW

* 1. CIS Template

Complete the *Control Implementation Summary* (CIS) template to indicate the implementation status of the controls for the system as illustrated in Figure 5-2.

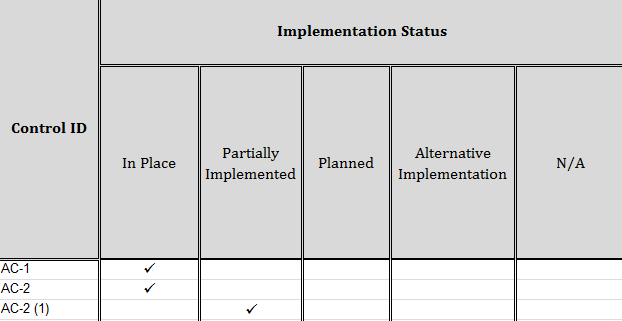


Figure 5-2 – Select the Implementation Status in the CIS

CSPs need to indicate in the CIS the entity responsible to implement and manage the control. In some cases, implementation and management of a control may require joint ownership by the CSP and the customer agency. Figure 5-3 illustrates an example of control origination selections for three different controls.

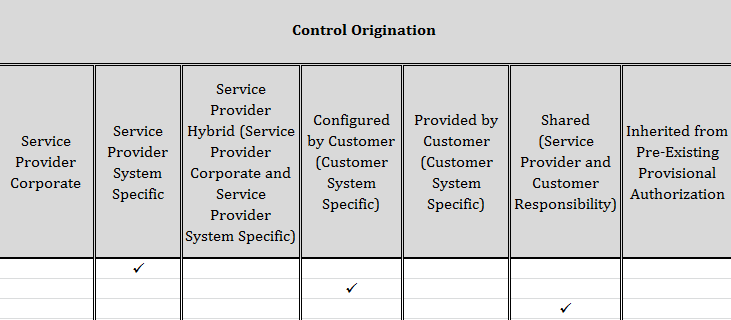


Figure 5-3 – Select the Control Origination Responsibility

The CIS is a living document and updates are expected throughout the development of the *System Security Plan*.

* 1. User Guide

CSPs must provide a User Guide that explains how prospective users (government agencies) will use the system. If the system has a self-service control panel, the User Guide must explain clearly how to use the control panel. Submit the User Guide with the *System Security Plan*.

* 1. Components, Boundaries, and Architecture

The audience for this section is CSPs; however, 3PAOs may want to review this section to better understand CSP requirements. The *System Security Plan* template documents and describes how all required security controls are implemented.

At the start of the FedRAMP JAB P-ATO process, the CSP briefs its system architecture to the FedRAMP ISSO and JAB TRs. This in-depth, technical briefing clearly describes the system boundary, identifies components internal and external to the boundary, and how data flows throughout the system. This briefing provides FedRAMP reviewers an understanding of the system architecture and provides context to the SSP. Agencies may or may not require an architecture briefing.

* + 1. Describing Infromation System Components

The CSP system likely has multiple components. Each component needs to be named and described in Section 9.2 of the *System Security Plan*. Wherever possible, use component names that are already familiar and used within the organization. Components may be described by a unique name (e.g. “Home Base”) or by functionality (e.g. “the Hypervisor”). For example, the system platform might consist of components known as Control Tower, Front Door, Home Base, Builder Box, Holding Vault, App One and Web Wiz as illustrated in Figure 5-4.

When naming and describing the components, ensure consistency throughout the entirety of the *System Security Plan* and all of the FedRAMP documents. Avoid confusion by retaining component names already known within the CSP organization and already described in existing corporate documentation. Inconsistencies create confusion resulting in delays.

Once the FedRAMP security assessment process has started, and if a component name changes for any reason, the Change Control Process (as described in the *Configuration Management Plan*) for the information system must capture and include a recorded history of the name change.



Figure 5-4 – Example of Components Described by Name

Figure 5-4 illustrates software components described by unique names, and Figure 5-5 illustrates software components described by functionality. Regardless of which method is used to describe components, provide a detailed description of the functionality that each component provides to the overall system, and ensure consistency throughout the system documentation.



Figure 5-5 – Example of Components Described by Function

* + 1. Discussing Virtualization

This section includes general guidance on discussing virtualization in *System Security Plans*. CSPs use virtualization techniques that create entire systems (virtual machines or guest hosts) that are embedded inside of a traditional physical host system. There are numerous ways that virtualization can be implemented, and many different virtualization products. The FedRAMP PMO does not make recommendations on virtualization models or products. Whatever virtualization architecture model is used, CSP documentation in all aspects must be clear about which components are parts of the physical host system and which components are parts of virtual abstraction layers.

**Note:** Refer to *NIST SP 800-125, Guide to Security for Full Virtualization Technologies* for information on types of virtualization.

Refer to *NIST SP 800-145, The NIST Definition of Cloud Computing* for information on cloud computing architecture models.

When discussing the functionality of different components, indicate whether the component is a standard host operating system or a guest (virtual) operating system. For each physical host that provides the capability to implement guest systems, discuss whether the virtualization technique is based on hosted virtualization or bare metal virtualization.

Guest operating systems can be deployed in several ways (i) the CSP provides a self-service menu driven control panel where customers can setup and configure their own virtual machines within a controlled environment; (ii) the CSP installs and configures unique virtual machines instances directly for the customer thereby eliminating the need for a self-service portal. When discussing administration, access control, and configuration settings of virtual machines, CSPs need to be clear about whether their service offers a self-serve solution or a CSP administered solution. The roles and authorizations associated with both of these solutions must be detailed in the *System Security Plan* (Table 9-1) User Roles and Privileges.

Network components can also be virtualized. When discussing a network component (or device) that is a virtual component, be clear about the fact that the item discussed is virtual and not physical. Examples of virtual network components and devices are:

* Virtual Local Area Networks (VLANs)
* Virtual Ethernet Modules
* Virtual Firewalls
* Virtual Switches
* Virtual Distributed Switches
* Virtual Security Gateways
* Virtual Routers
* NAT Virtual Interfaces (NVI)
  + 1. Boundaries and inherited controls

When describing the boundaries of the cloud system, it is important to accurately and clearly articulate where the cloud service layers begin and end. If a PaaS service provider is building its service on top of an IaaS service provider, the PaaS provider needs to ensure that their security control boundaries begin where the IaaS security control boundaries end. Alternately, a SaaS provider must understand where the PaaS security control boundaries end. The security controls for an upper layer service needs to begin where the lower layer security controls end as illustrated in Figure 4-16. There are many possible configurations for layering security and FedRAMP does not make recommendations on specific service models.

As outlined in Appendix C, there are multiple ways to layer or stack cloud services. For example, a SaaS CSP can layer or stack on another CSPs IaaS or PaaS. The SaaS CSP inherits controls from a CSPs IaaS or PaaS and must identify those controls as inherited in the SSP. There is a contractual relationship between CSPs, and the sharing CSP(s) must clearly articulate where its boundary ends so that the inheriting CSP is clear on where its boundary begins. If parts of a security control boundary are not clearly articulated, it is possible that there could be gaps resulting in increased risk.

If an agency issues an authorization to a CSP whose system layers on top of a CSP with a JAB P-ATO, the agency must clearly understand the boundary and inherited controls and its responsibilities as related to authorization and continuous monitoring. The agency must also understand the FedRAMP PMO’s continuous monitoring responsibilities for the CSP with the JAB P-ATO.

When discussing boundaries, include information on how different tenants are separated from each other in a multi-tenant environment.

Questions to consider when describing boundaries:

* Will the boundaries leverage any existing Provisional Authorizations?
* What is the definition of a tenant?
* For the service offering, will multiple tenants share the same VLAN(s)?
* Are there controls that prevent VLAN hopping?
* Are virtual machine zones on unique network segments isolated?
* Are separate physical network adapters used to isolate virtual machine zones?
* Is layer-2 isolation performed?
* Is isolation through traffic encapsulation used?
* Do port groups define any boundaries?
* If port groups are used, are they all in the same layer-2 domain or do they span multiple layer-2 domains?
* Are multiple Network Interface Cards (NICs) bonded together?
* How do firewalls provide isolation between tenants?
* How does router ACLs provide isolation between tenants?
* Are IPsec tunnels used to define boundaries?
* Is sharding used?
* Are network filters used that control what packets are sent to or from a virtual machine?
* Are network zones used? If yes, how are zones defined?
* Will U.S. federal agencies be multi-tenanted with non-government entities?
* Are NAT virtual interfaces (NVI) or domain specific NAT configurations used?
* How does NAT play a role in containing network traffic within the boundary?
* What kind of NAT is used? (e.g. static, dynamic, overloading, overlapping)
* Are NAT IP pools used?
* Are geo IP location boundaries used?
* Define the geographic location (City, State) where customer data is stored?
* Will it be possible for agency tenants to know the geographic location (City, State) where their data is stored?
  + - 1. Discussing Live Migrations

Live migrations of virtual machines have the potential to confuse a common understanding of the information system boundaries. Therefore, when describing boundaries, it is important to discuss the live migration strategy for the information system. Live migrations have the ability to move an entire virtual machine to another host or instead, move a virtual machine’s data store (configuration file and virtual disks) to another physical host without actually moving the virtual machine. Complicating this, it is also possible to move and store a virtual machine’s configuration files, and disks in separate locations. The FedRAMP PMO does not make recommendations on live migration strategies. Whatever the live migration strategy is, be clear as to how live migrations are managed. IP addresses declared within the boundary must remain protected by the security controls noted in the *System Security Plan* even if the IP addresses are moved around.

Questions to consider in the discussion of live migration:

* Are live migrations performed manually, or scheduled and automated?
* If live migrations are automated, what are the rules that govern the migration?

FedRAMP is interested in understanding how virtual machines are monitored and how guest systems are migrated one from physical host to another. Consider discussing how virtual machine migration and tracking can be audited through logging and event generation in Section 13.13.2 (AU-2a) of the *System Security Plan*.

* + - 1. Discussing Storage Components

In the description of system components, include information about storage components that are inside the boundary. If using a fiber channel storage array, insert a diagram that shows how the storage connects to the fiber channel fabric and include the switches in the diagram. An example illustration is shown in Figure 5-6.

Questions to consider when describing storage components:

* Does the system use Direct Attached Storage (DAS), Network Attached Storage (NAS), or Storage Area Networks (SANs)?
* If using a SAN, what is used to connect hosts in a cluster (fiber channel or iSCSI)?
* Which fiber channel or iSCSI connections are considered within the boundary?
* Are different types of storage devices used on different network segments?
* Are clusters used?
* How many hosts are on a cluster and which clusters are in the boundary?
* Do the storage devices use a multipath environment?
* Are the storage devices set up to be persistent or non-persistent?

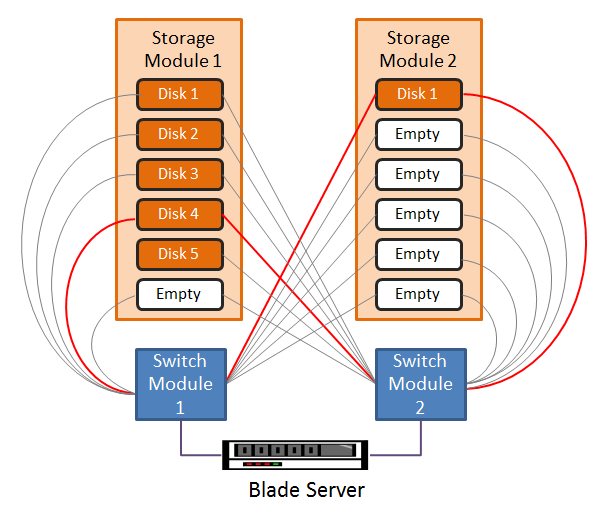
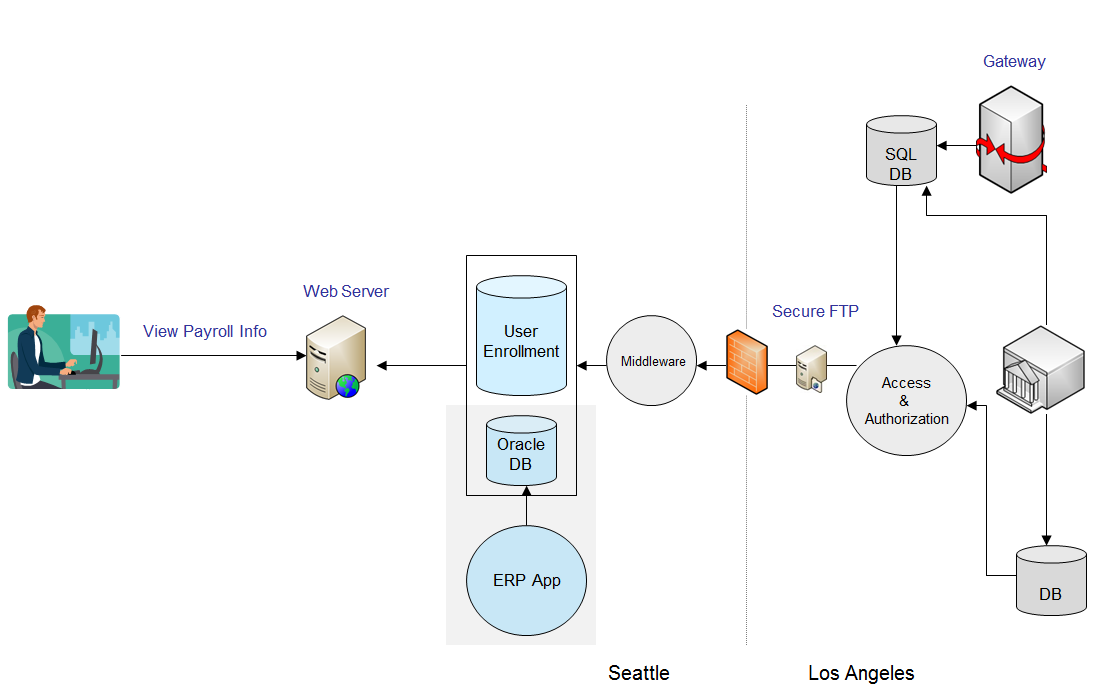


Figure 5-6 – Example of Storage Array Illustration

* + 1. Addressing the Data Flow Diagram

Section 10.1.4 in the System Security Plan template requires a data flow diagram of how network traffic flows through the platform and offering. A data flow diagram focuses more on the direction of the network traffic and less on the actual network topology. However, certain components of the system’s network topology need to be included to illustrate the direction that the network traffic flows through the system. Figure 5-7 shows an example of a data flow diagram.



Source: FISMA Center

Figure 5-7 – Data Flow Diagram Example

1. Maintaining an Authorization

Appendix III of Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, specifically requires federal agencies to:

*Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.§(3)(b)(4)*

All FedRAMP authorizations must be renewed every three years. OMB Circular A-130 Appendix III requires that security controls in information systems be reviewed at least every three years or when there are significant modifications to the system. The scope and frequency of the review must be commensurate with the acceptable level of risk for the system.

**Note:** OMB Circular A-130 Appendix III is available at the following URL: <http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii>

FedRAMP provides a *Continuous Monitoring Strategy & Guide* that contains instructions on the continuous monitoring process. Refer to that guide for more information on continuous monitoring.

1. General Documentation Information for CSPS
   1. Formatting and SEction Numbers

The templates provided by the FedRAMP PMO are intended to standardize the security assessment process and enable CSPs to move through the assessment process as quickly as possible. Modifications to the templates are acceptable, provided that required sections are not removed. Templates are designed to capture FedRAMP requirements. It is acceptable to add new sections to better describe the system. If new sections are added, the section numbering may impact references to sections and guidance in this document.

* 1. Sensitivity Markings

Ensure that all documents have sensitivity markings on at least the cover page and the footer of each document. Sensitivity marking on any template may be adapted to match official company sensitivity nomenclature if it is different from what is on the template. Optionally, sensitivity markings may be placed on the headers or any other sections of any document. Any documents that do not have sensitivity markings on them could possibly be subject to a Freedom of Information Act (FOIA) request.

* 1. Items That Are Not Applicable

If a particular control requirement is not applicable to the system, do not leave the section in the template blank and do not delete that section. Simply write “Not Applicable” in that section and justify why any requirement is not applicable.

1. Layering One Package on top of Another

FedRAMP was architected with the concept that agencies can layer one cloud service on top of another. Appendix C offers various use case illustrations and descriptions for layering cloud services. Agencies can add their own security control requirements on top of the standard FedRAMP security baseline controls.

Agencies should think of an IaaS Security Package as providing similar capabilities that General Support Systems (GSS) provide for traditional (non-cloud) systems. Once an IaaS package is in place, agencies can layer on a different cloud service platform that was built internally at the agency or by an external cloud service provider.

System owners of cloud layers built on top of a lower layer of the stack must ensure that the lower layer has a FedRAMP authorization. For a SaaS or a PaaS to obtain a FedRAMP JAB Authorization, the IaaS layer must have a FedRAMP JAB Authorization as well.

It is recommended that agencies use cloud solutions that are modular so that any given layer of the cloud stack could be migrated to a different CSP if necessary. Using layers that are transportable from CSP to CSP enables agencies to negotiate more competitive pricing and eliminates the constraint of being locked into one CSP.

**Unique Instructions for Department of Defense (DoD)**

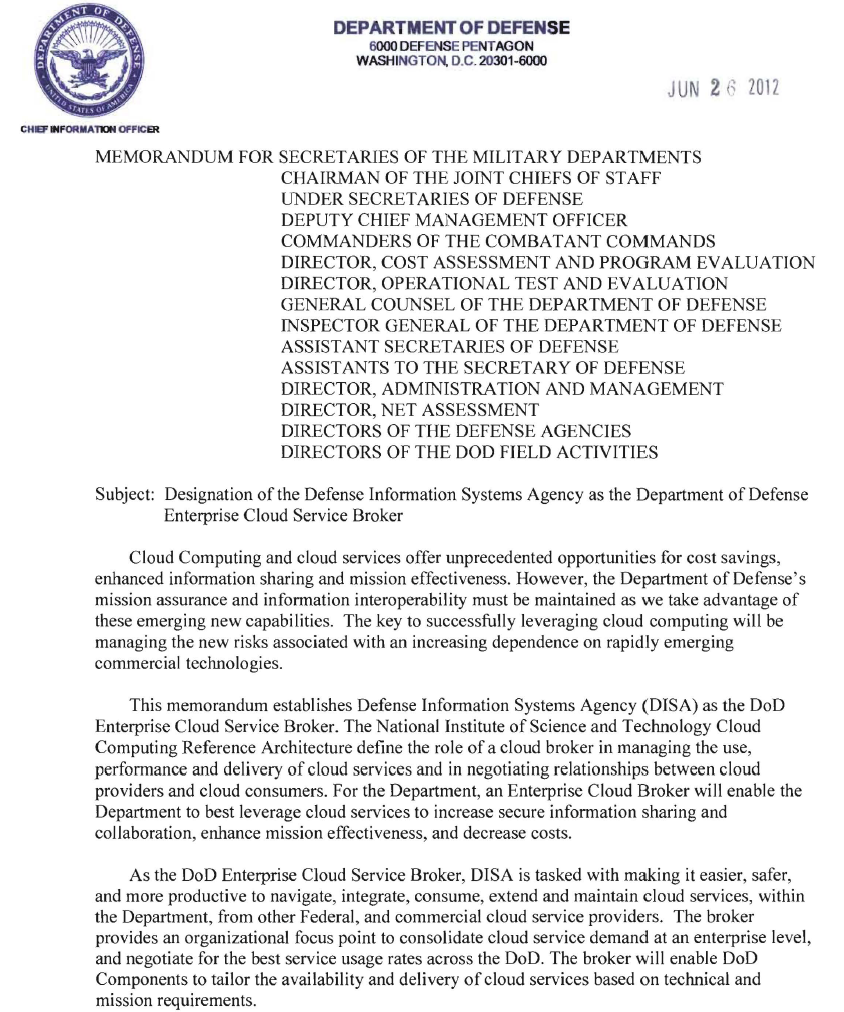
DoD organizations seeking to acquire cloud computing service should go through the DISA Enterprise Cloud Service Broker (ECSB). DoD issued a Cloud Broker Policy on June 26, 2012. The DISA ECSB is building a service catalog that includes FedRAMP authorized cloud services, including internal cloud services already available in the DoD. The general Email box for DoD's Enterprise Cloud Service Broker is: [disa.meade.cae.mbx.cloud-broker@mail.mil](mailto:disa.meade.cae.mbx.cloud-broker@mail.mil). The website for the DoD Enterprise Cloud Service broker is <http://www.disa.mil/Services/DoD-Cloud-Broker>. See the DoD memo found in Appendix B for more information.

The DoD CIO, who is responsible for the DoD Cloud Broker is a member of the JAB. Therefore CSPs that have obtained a JAB P-ATO will greatly reduce the time needed to obtain a DoD ATO (Although there still may be agency-specific controls).

Appendix A – Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| 3PAO | Third Party Assessment Organization |
| CIS | Control Information Summary |
| CSP | Cloud Service Provider |
| CTW | Control Tailoring Workbook |
| DoD | Department of Defense |
| FedRAMP | Federal Risk and Authorization Management Program |
| FISMA | Federal Information Security Management Act |
| IaaS | Infrastructure as a Service |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |
| SAP | Security Assessment Plan |
| SAR | Security Assessment Report |
| SSP | System Security Plan |

Appendix B – Department of Defense Memo



Appendix C – Use Cases

There are multiple types of cloud configurations. The FedRAMP PMO does not endorse or prescribe any particular type of cloud configuration. However, to assist CSPs in describing the scenario that their cloud configuration represents, various use case scenarios are illustrated in the sections that follow. The uses cases presented do not constitute all possible use cases.

**Note:** For more information on cloud use cases, consult NIST SP

500-293, U.S. Government Cloud Computing Technology Roadmap, Volume II (Draft).

Case 1: Simple IaaS

An agency may want to use one IaaS provider with the intention of having the top layer controls (platform and application) provided by the agency. In this scenario, one FedRAMP Provisional Authorization is applicable as illustrated in Figure C-1.

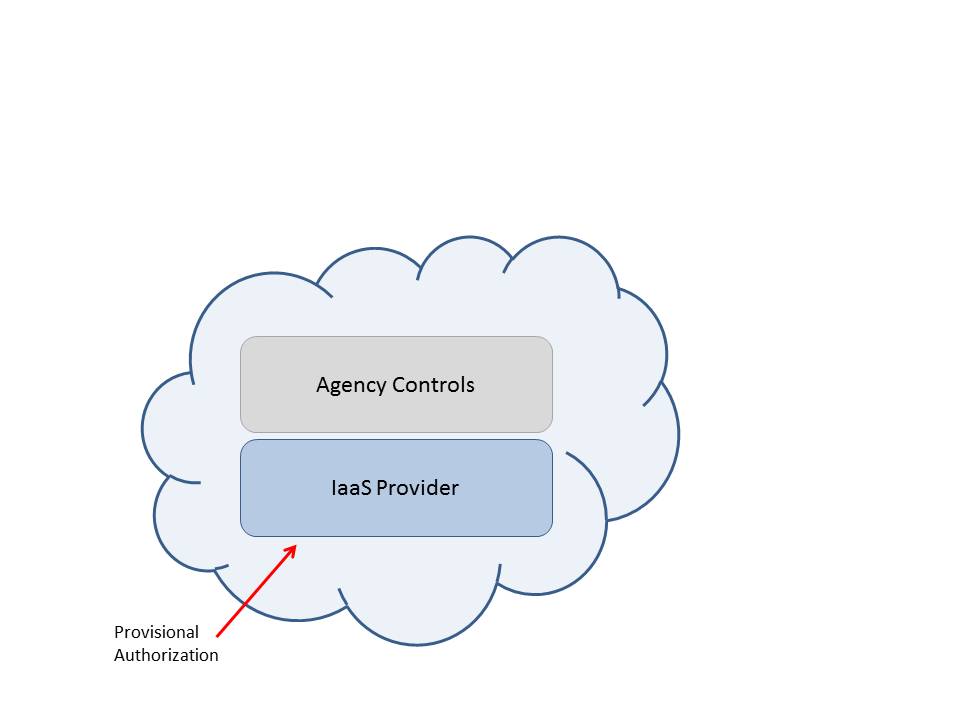


Figure C-1 – One IaaS Provider

Case 2: Simple PaaS

An agency may want to use one CSP for both the IaaS and PaaS layers, with the intention of having the top layer controls (application) provided by the agency. In this scenario, one FedRAMP Provisional Authorization is applicable as illustrated in Figure C-2.

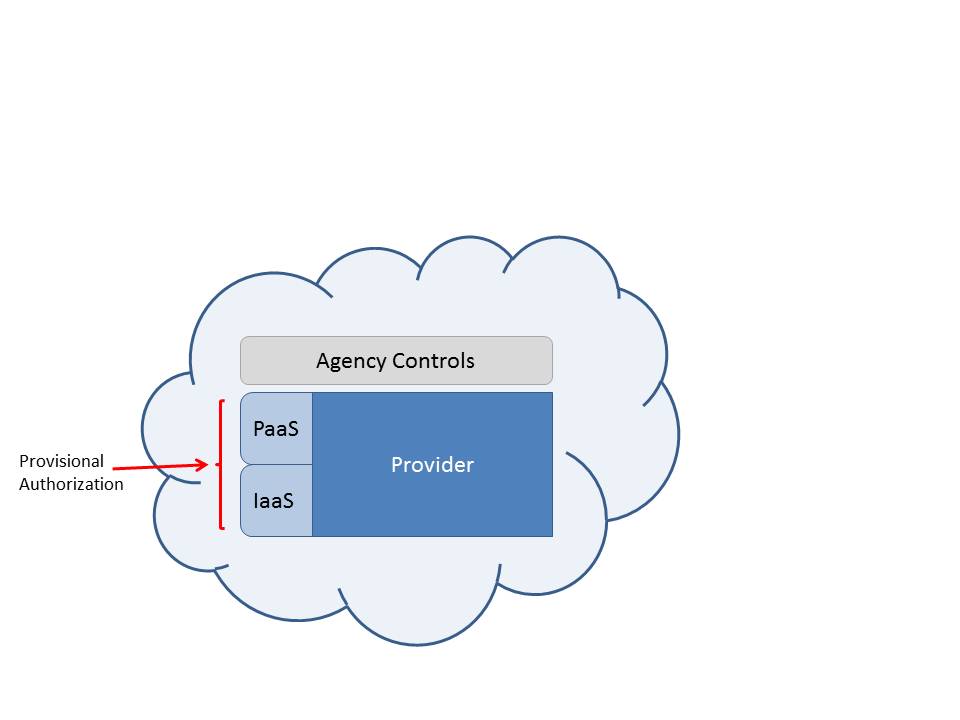


Figure C-2 – One Provider for Iaas and PaaS

Case 3: Simple SaaS

An agency may want to use one provider that provides the IaaS, PaaS, and SaaS layers. In this scenario, one FedRAMP Provisional Authorization is applicable as illustrated in Figure C-3.

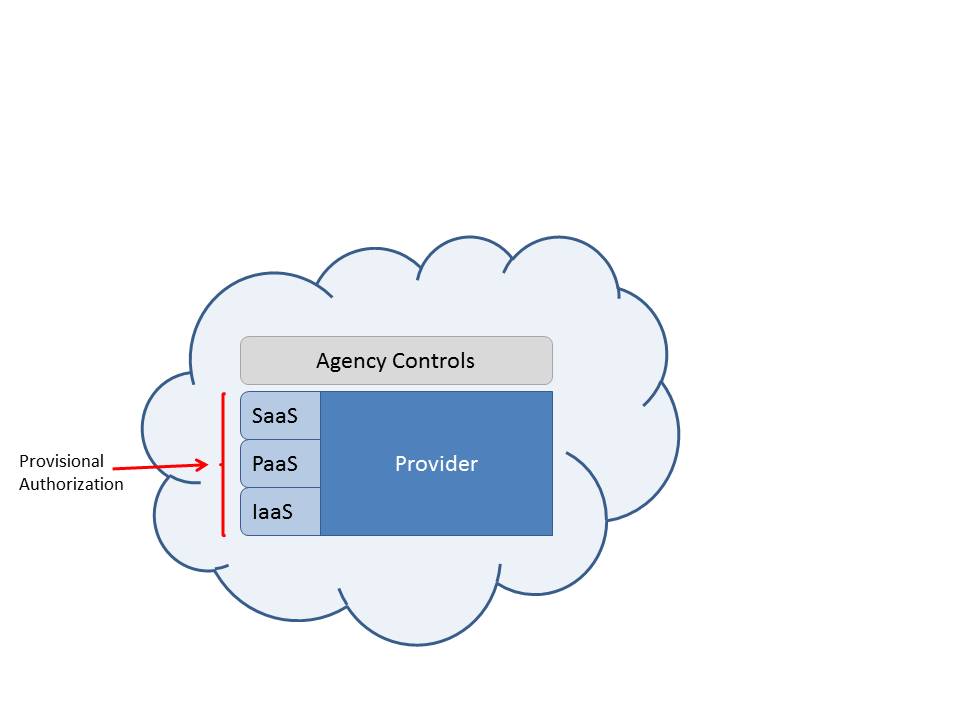


Figure C-3 – One Provider, IaaS, Paas, Saas

Case 4: One Provider, Just Saas

A cloud service provider may build a SaaS application that encompasses the entire stack of security controls, but does not differentiate between the PaaS and IaaS layers as illustrated in Figure C-4. NIST SP 500-293, Volume II (Draft) states:

*SaaS applications can be built on top of PaaS components, and PaaS components can be built on top of IaaS components.*

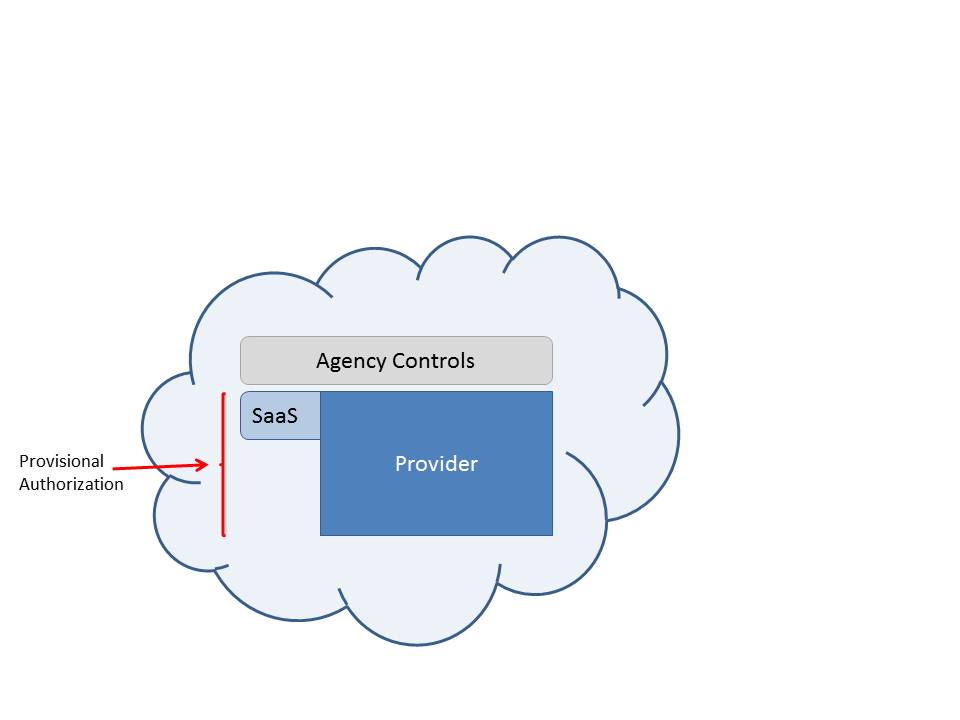


Figure C-4 – One Provider, Just SaaS

Case 5: Two Cloud Providers, Iaas and Paas (or SaaS)

An agency may want to use one CSP for IaaS and a different CSP for the PaaS or SaaS layer. In this scenario, the PaaS provider is dependent on leveraging a pre-existing Provisional Authorization – from the IaaS provider. If the agency decides to make use of this integrated package, two different FedRAMP Provisional Authorizations are applicable as illustrated in Figure C-5.

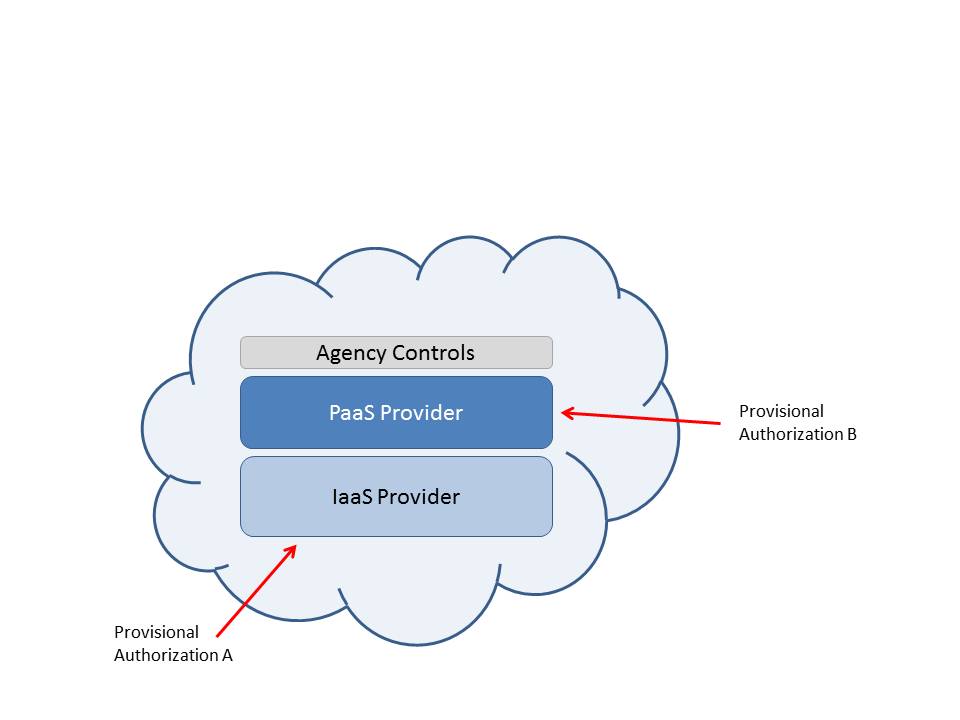


Figure C-5 – Two Providers, One IaaS and One PaaS (or Saas)

Case 6: Three Cloud Providers, IaaS, PaaS, and SaaS

An agency may want to use three providers that each provide a different layer. In this scenario, the PaaS provider is dependent on leveraging a pre-existing Provisional Authorizations from the IaaS provider and the SaaS provider is dependent on leveraging a pre-existing Provisional Authorization from the PaaS provider (and indirectly the IaaS provider). If the agency decides to make use of this integrated package, three different FedRAMP Provisional Authorizations are applicable as illustrated in Figure C-6.

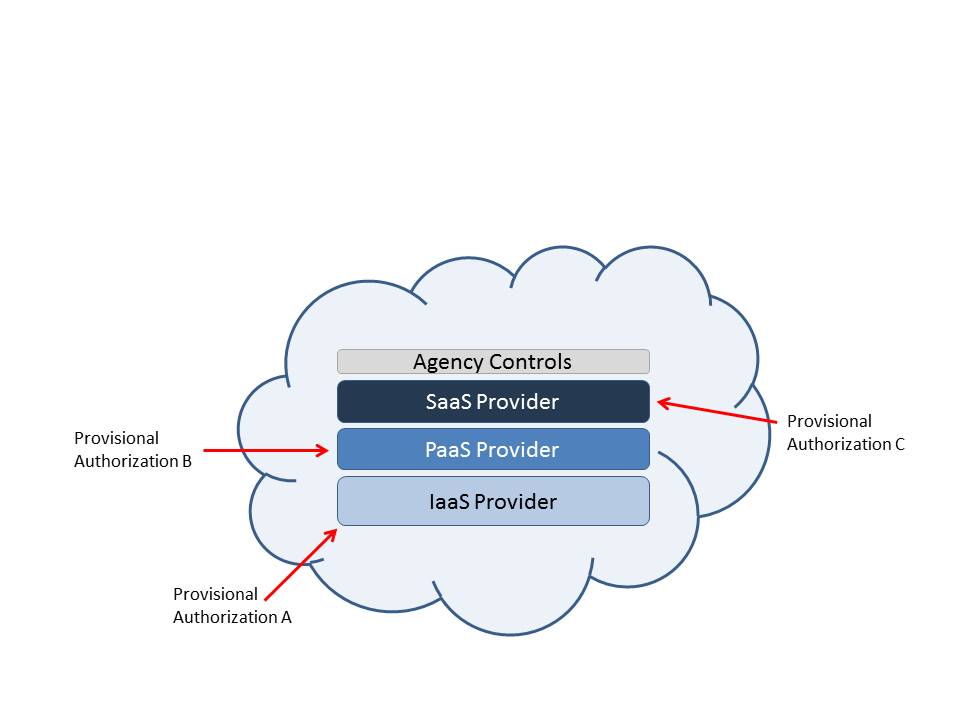


Figure C-6 – Three Providers, One IaaS, One PaaS, and One SaaS

Case 7: Two Cloud IaaS Provders

It is possible that an agency may want to make use of two separate IaaS providers with the intention of having the top layer controls (platform and application) provided completely by the agency. In this scenario, two different FedRAMP Provisional Authorizations are applicable as illustrated in Figure C-7.

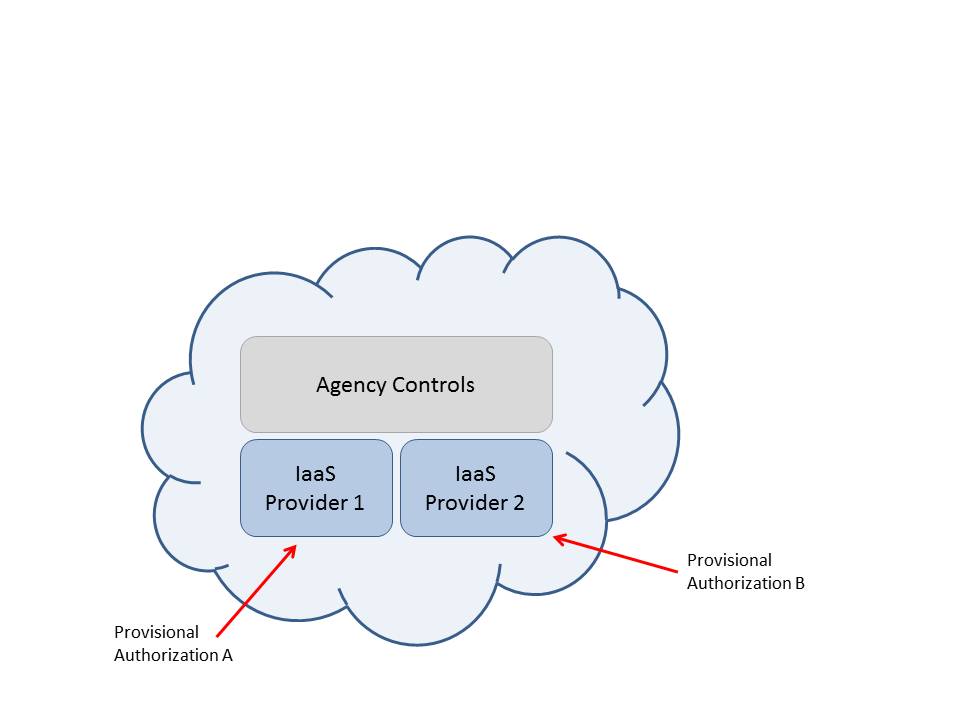


Figure C-7 – Two IaaS Providers

Case 8: Two Cloud IaaS Providers and a PaaS Provider

It is possible that a cloud implementation could make use of two separate IaaS providers and a third separate PaaS provider. In this scenario, the Paas provider is dependent on leveraging two pre-existing Provisional Authorizations – one from each of the IaaS providers. In this scenario, if the agency decides to make use of this integrated package, three different FedRAMP Provisional Authorizations are applicable as illustrated in C-8.

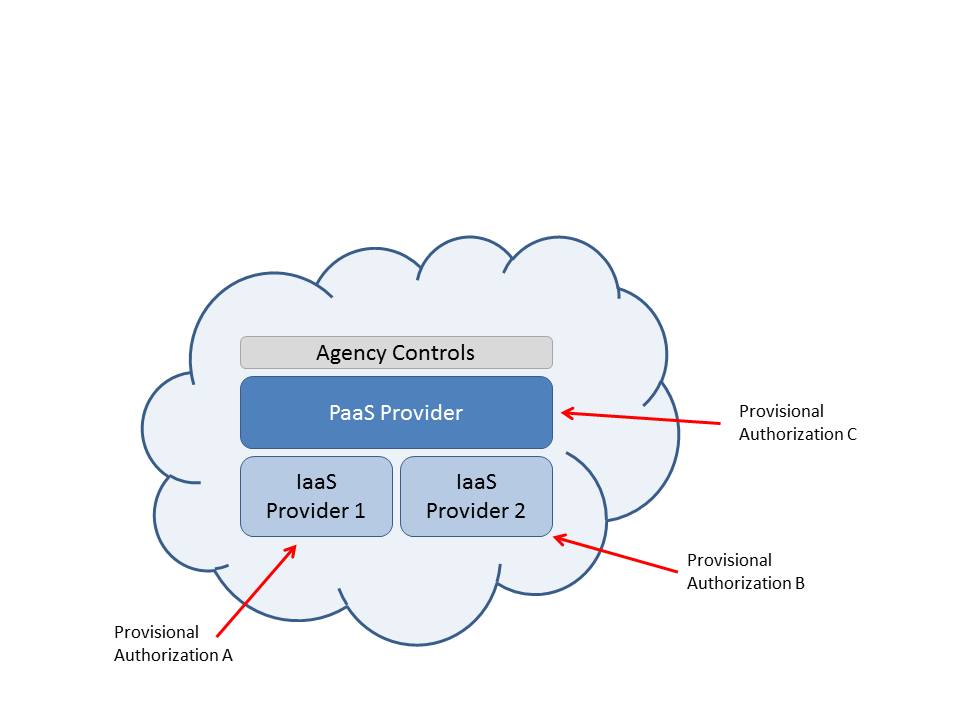


Figure C-8 – Two IaaS and One PaaS Provider

When IaaS Provider 1 writes their *System Security Plan*, they will not indicate that they are leveraging any other Provisional Authorization. The same holds true for IaaS Provider 2. However, when the PaaS provider writes their *System Security Plan*, in Section 8.2 of the *System Security Plan*, they must indicate that they are leveraging the Provisional Authorization of both IaaS Provider 1 and IaaS Provider 2. It is anticipated that the PaaS provider will inherit controls from both IaaS providers.

Case 9: Three Cloud Providers, One IaaS and Two PaaS

It is possible that a cloud implementation could make use of one IaaS provider and two PaaS providers. In this scenario, both PaaS providers are dependent on leveraging the pre-existing Provisional Authorizations from the IaaS providers. In this scenario, if the agency decides to make use of this integrated package, three different FedRAMP Provisional Authorizations are applicable as illustrated in Figure C-9.

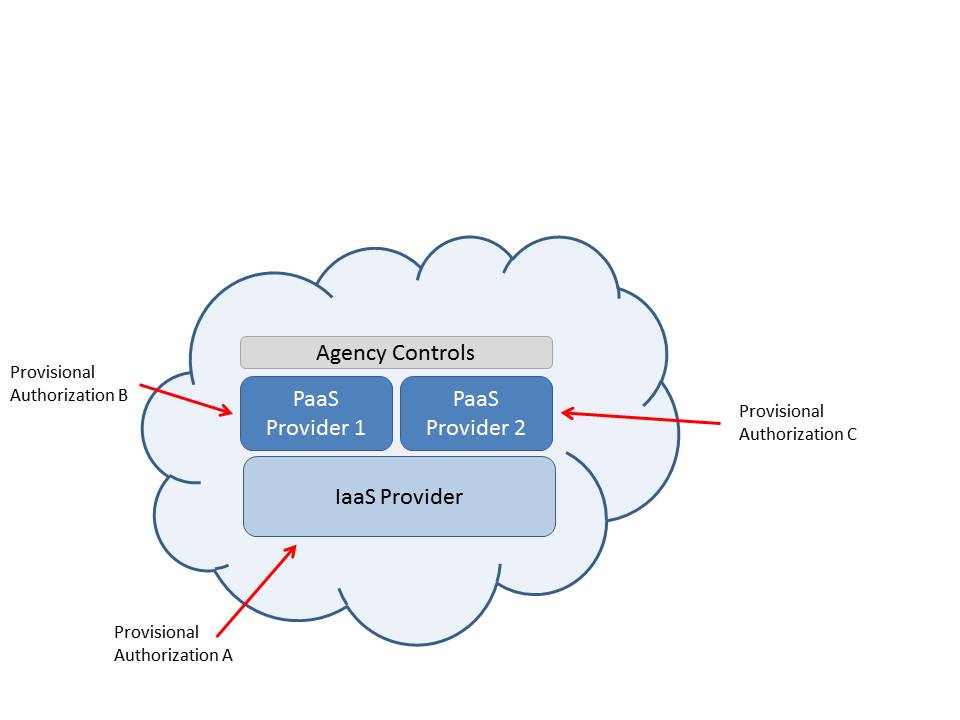


Figure C-9 – Three Providers, One IaaS and Two PaaS

Appendix D – FedRAMP Security Control Guidance

Security Control Summary Information

Each security control includes a table called Security Control Summary Information as illustrated in Table D-1. Security control enhancements also require security control summary information. Definitions for Control Origination are in Table 5-2. For any of the “-1” controls that describe Policies and Procedures (e.g. AC-1, SC-1 etc.) it is not possible to select Configured by Customer, Provided by Customer, Shared, or Inherited from pre-existing Provisional Authorization. This is by design since CSPs have their own set(s) of Policies and Procedures.

| Control ID | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter: | |
| Implementation Status (check all that apply):  In place  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authorization (PA) for <**Information System Name**>, <**Date of PA**> | |

Table D-1 – Example of Security Control Summary Information

In the field described as Responsible Role, indicate what staff role within the organization is responsible for maintaining and implementing that particular security control. Examples of the types of role names may differ from CSP to CSP but could include role names such as:

* System Administrator
* Database Administrator
* Network Operations Analyst
* Network Engineer
* Configuration Management Team Lead
* IT Director
* Firewall Engineer

All controls originate from a system or from a business process. It is important to describe from where the control originates so that it is clear whose responsibility it is to implement and manage the control. In some cases, the responsibility is shared by the CSP and the customer. Since each service offering is unique, the FedRAMP PMO cannot provide guidance on which controls should or should not be defined according to the Control Origination definitions in Table D-2.

| **Control Origination** | **Definition** | **Example** |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the CSP corporate network. | DNS from the corporate network provides address resolution services for the information system and the service offering. |
| Service Provider System Specific | A control specific to a particular system at the CSP and the control is not part of the standard corporate controls. | A unique host based intrusion detection system (HIDs) is available on the service offering platform but is not available on the corporate network. |
| Service Provider Hybrid | A control that makes use of both corporate controls and additional controls specific to a particular system at the CSP. | There are scans of the corporate network infrastructure. Scans of databases and web based application are system specific. |
| Configured by Customer | A control where the customer must apply a configuration to meet the control requirement. | User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http or https, etc.), entering an IP range specific to their organization are configurable by the customer. |
| Provided by Customer | A control where the customer needs to provide additional hardware or software in order to meet the control requirement. | The customer provides a SAML SSO solution, adding in SAML assertions, to implement two-factor authentication. |
| Shared | A control that is managed and implemented partially by the CSP and partially by the customer. | Both the service provider and the customer require two-factor authentication for both privileged and non-privileged users for network access. |

Table D-2 – Control Origination Definitions

As of this edition, guidance has been provided for a subset of the security controls. This document may be updated in the future to include guidance on other security controls.

Security Control AC-7

Section 13.1.7(a) in the *System Security Plan* template requires a description of how the system handles unsuccessful logins and that it permits 3 or fewer unsuccessful logins within a 15 minute period.

Questions to consider in the discussion are:

* Is the unsuccessful login parameter configured on a central policy server? What server?
* Is the unsuccessful login parameter configured manually on a server by server basis?
* What tool/function is used to configure unsuccessful logins?
* Are policy templates or a policy manager used to configure this parameter?
* Is the unsuccessful login parameter configured the same for all groups and roles of users?
* Is the unsuccessful login parameter configured using different techniques on application servers, databases, firewalls, routers, and all other components?
* Is a single sign-on application that controls unsuccessful login parameters used?
* Are unsuccessful login parameters configured through a GUI or a CLI?
* Are any COTS authentication/access control products used to configure the unsuccessful login parameter?
* Provide any screenshots that show the configuration of the unsuccessful login parameter is configured.
* When using multiple operating systems is the unsuccessful logon parameter set using different techniques for the different operating systems?

Section 13.1.7(b) in the *System Security Plan* template requires details as to how account lockouts occur when a user has more than 3 unsuccessful login attempts within a 15 minute period.

Questions to consider include:

* Are account lockouts configured on all systems that are within the boundary?
* Are account lockouts configured on any customer control panel login mechanisms?
* If a user is locked out, how will he/she know who to call to have the account reset?
* Will VPNs made available to customers through self-service control panel’s lockout via the physical system lockout parameters? Or do customers need to configure their own VPN lockouts separately?

Security Control IA-5(3)

Section 13.7.5.1.3 in the *System Security Plan* template requires a description of how HSPD12 card registrations are performed in person. If smart cards are used for two-factor authentication, they must be HSPD12 and registration must take place in person. This control does not mean that using HSPD12 cards is a requirement for two-factor authentication. If the system does not use HSPD12 cards, this control is not applicable to the system and is not implemented.

Security Control PE-2(A)(B)(C)

Section 13.11.2 in the *System Security Plan* template requires a description of the implementation of physical access authorizations.

Questions to consider include:

* Is there a list of who has access to the data center?
* Who authorizes access to data center?
* Are there different authorization levels for different physical areas? (e.g. chillers, electrical substation room, UPS/battery room, generator area)
* Are there different types of authorization credentials? If yes, what are they?
* Are the data center access list and authorization credentials reviewed at least once annually?

Security Control PE-3(A)(B)(C)(D)(E)(F)(G)

Section 13.11.3 in the *System Security Plan* template requires a discussion of the enforcement of physical access authorizations?

Questions to consider include:

* What is used to control access to the data center? (e.g. hand scanner, card key)
* Are there separate access control devices for the electrical substation room, battery room, chillers, and generators?
* What is the make/model of the access control devices?
* If PINs or passwords are used, do they meet the password change requirement frequency?
* How does the access control device verify an individual’s identity?
* Are cages/racks locked?
* Are there guards at the data center entrance?
* Are areas considered publicly accessible areas controlled?
* On what date were physical access control devices were last inventoried?
* On what date were keys and combination locks last changed?

Security Control PE-4

Section 13.11.4 in the *System Security Plan* template requires a description of how access control for transmission media is implemented.

Questions to consider include:

* Do wiring closets and patch panels have locks? Who has access?
* Are there exposed telecomm jacks that are not locked?
* Where does telecomm circuit/Internet connectivity enter the data center?
* Are cables and wires below the floor?
* Are cables and wires in inaccessible (locked) ceiling trays?

Security Control PE-6(A)(B)(C)

Section 13.11.6 in the *System Security Plan* template requires that a discussion of how monitoring of physical access is implemented.

Questions to consider include:

* Are guards located at data center entrances? Are they armed?
* Are balusters outside the data center building near entrance areas?
* Are cameras pointed at data center entrances? What kind of cameras are being used?
* If cameras are being used, how long is recorded media kept for?
* Are hand scanners used to at data center entrances? What make and model are they?
* Are access logs to hand scanners reviewed? If yes, who reviews them?
* Are sign in sheets required at data center entrances? Who reviews these sheets?
* Are card keys required at data center entrances?
* Are access logs to card keys reviewed? If yes, who reviews them?

Security Contorl PE-6(1)

Section 13.11.6.1.1 in the *System Security Plan* template requires that a description of how monitoring of real-time physical intrusion alarms and surveillance equipment is monitored.

Questions to consider include:

* Is there an alarm system installed at the data center?
* What events will set off the alarm system?
* Does an outside service provider maintain and manage the alarm system?
* When was the alarm system last tested or inspected?
* Are cameras located inside the data center?
* Does an outside service provider maintain and manage the surveillance cameras?
* When were the cameras last tested or inspected?

Security Conrol PE-13(1)(2)(3)

Section 13.11.13 in the System Security Plan template requires the description of fire suppression security controls. Indicate whether or not the fire suppression system complies with NFPA 75[[1]](#footnote-2). Indicate if local fire marshals have performed a recent inspection and the date of the last inspection.

Questions to consider include:

* Is there a fire alarm system?
* Are fire alarms sent to a remote monitoring center?
* How are alarms activated? (e.g. smoke, heat)
* Where are fire detection devices located?
* Where are fire suppression devices located?
* Is the monitoring and maintenance of the system outsourced to a service provider?
* Are there maintenance records for the fire suppression system?
* Are wet pipe, dry pipe, pre-action, or deluge sprinklers in use?
* Is an inert agent fire suppression system in use?
* Are there fire extinguishers in the data center?
* Where are fire extinguishers located?
* When are fire extinguishers inspected?
* What fire suppression agent do the fire extinguishers use?

Security Control PL-4

Section 13.12.3 in the *System Security Plan* template requires that CSPs provide Rules of Behavior to their users. FedRAMP developed a template for Rules of Behavior which is available on the FedRAMP website. The template includes two sample sets of Rules of Behavior – one for Internal Users and one for External Users. Internal Users are company employees or company contractors. External Users are customers who will use the service provider platform.

Before a CSP gives customers access to the service provider platform, the CSP must require their customers to sign the External Rules of Behavior. If the CSP provisions one account to one customer user (a customer account administrator), who in turn provisions accounts for the all the other customer users, the CSP only needs to obtain a signed External Rules of Behavior for that one customer user (the customer account administration). That one customer user who provisions accounts for other customer users inside their respective agency is then responsible for ensuring that Rules of Behavior for his/her agency are signed for the system. The agency customer account administrator must then determine the appropriate Rules of Behavior for the agency users to sign – but must take into consideration the rules listed on External Rules of Behavior that was signed and provided to the CSP.

The general rule of thumb is that if an account is assigned to an individual, the person who provisions the account is responsible for obtaining signed Rules of Behavior. In some cases, the person provisioning the account might be the CSP and in other cases the person provisioning the account might be an agency employee.

The rules provided in the FedRAMP template are samples. CSPs must consider what rules apply to the candidate system and edit the template to describe the rules that are actually required. CSPs can use any of the sample rules, or replace them completely with other rules. Signed records of the Rules of Behavior are retained by the entity that provisions the account. It is acceptable to implement the Rules of Behavior electronically or on paper, however, agreement to the Rules of Behavior and sign-off must obtained before users are granted access to new accounts.

Security Control SA-11(1)

Section 13.15.11.1.1 in the *System Security Plan* template is a control for original source code development. If the CSP service offering has been developed using original source code, the CSP must provide a code analysis report that shows that the latest release was scanned with a code analysis scanner. Indicate what scanner was used and insert the report into the *System Security Plan* for this control. All code analysis reports must be made available to the 3PAO that performs the testing on the CSP system. If the CSP is not writing any original code, then this control is not applicable and must be indicated as such in the *System Security Plan*.

Security Control SC-7(1)

Section 13.16.6.1.1 in the *System Security Plan* template and SC-7(1) references the Trusted Internet Connection (TIC) initiative. The TIC initiative is mandated by OMB in Memo M-08-05[[2]](#footnote-3). The purpose of the Trusted Internet Connections (TIC) is to reduce and consolidate connections to the federal government, including connections to the Internet. Additionally, data must pass through the TIC to obtain monitoring services from US-CERT.

There are two categories of TICs as defined and approved by the DHS Federal Network Services:

* Federal agencies that are approved TIC Access Providers (referred to as TICAPs)
* Networx Managed Trusted IP Service providers with qualified and approved capabilities (referred to as MTIPS).

For a commercial cloud service provider to comply with SC-7(1), the CSP must demonstrate an architecture that allows an agency to provide effective separation of network traffic to meet the following objectives:

1. All government data shall be capable of routing through a dedicated logical or physical network connection.
2. The service shall be capable of excluding co-tenant data, or any other third party data, not intended for the government from being transmitted through a government network connection.
3. The service shall be capable of excluding data intended solely for government use from being routed through an external (non-dedicated) network connection.

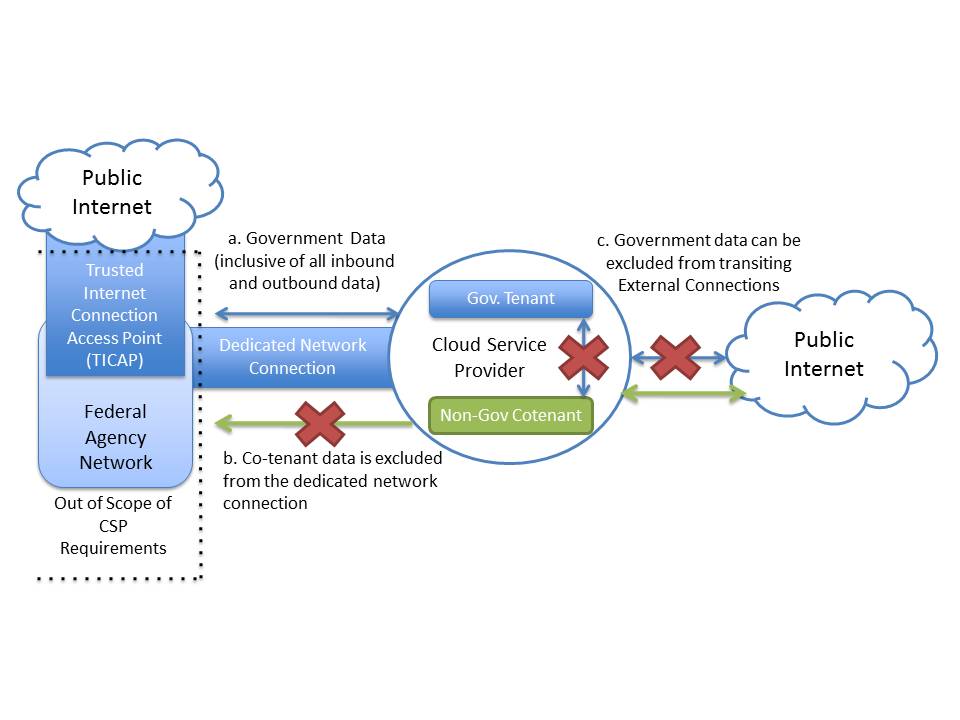


Figure D-1 – TIC Compliant Architecture

To accomplish the TIC objectives, there are multiple architectures that CSPs may propose with an example illustrated in Figure D-1. Federal Network Services approved the following architectures:

1. CSP routes all Government traffic via VPN back to an agency network.
2. CSP routes all government traffic through an agency sponsored MTIPS, no government traffic is allowed over the public Internet.
3. CSP routes all government traffic through dedicated network connections to an agency network, no government traffic is allowed over the public Internet.
4. CSP routes by all government traffic through government endpoints, not allowing any data to traverse any other end-points than agency IP address ranges (effectively all inbound/outbound traffic routes through government network by proxy or other rules).

It is not possible for a CSP to connect directly to a TICAP. Connection to an MTIPS Provider is available through the Networx contract but this contract vehicle can only be used by agencies. An agency should sponsor the CSP that it wants to use, and then use the Networx contract vehicle to assist the CSP in connecting to the MTIPS Provider. More information about the Networx contract can be found at the following URL:

<http://www.gsa.gov/portal/content/104870> . More information on the TIC is available at the following URL: <http://www.dhs.gov/files/programs/gc_1268754123028.shtm>. The TIC Program Office can be contacted at [dhs@tic.gov](mailto:dhs@tic.gov).

Security Control SC-13

Section 13.16.12 in the *System Security Plan* template and SC-13 requires that description of where cryptographic protections are implemented. Cryptographic protections can be used in a multitude of places on an information system. Describe what components or devices use cryptographic protections and how they are implemented.

Questions to consider include:

* Are data partitions encrypted?
* Are swap partitions encrypted?
* Are temporary file systems encrypted?
* Are file systems encrypted?
* Are files encrypted? All files or just some files?
* Are storage devices encrypted?
* Are log files encrypted?
* Are databases encrypted?
* Are hardware encryption modules used?
* Are encrypted logical volumes used?
* Do virtual machines that are not running have their images/templates encrypted?
* Are commercial off-the-shelf encryption products being used? Which ones?

Cryptographic protections are used to protect data in transmission. Describe the control implementation for Transmission Confidentiality SC-9, in Section 13.16.8 in the *System Security Plan*.

Security Control SC-13(1)

Section 13.16.12.1.1 in the *System Security Plan* template and SC-13(1) requires the use of FIPS 140-2 cryptography to protect unclassified information. Specific products that use cryptography on the system can be validated by looking for a validation certificate for that product on the Cryptographic Module Validation Program (CMVP) website. Click on *Module Validation Lists* as shown in Figure D-2 to search for products.

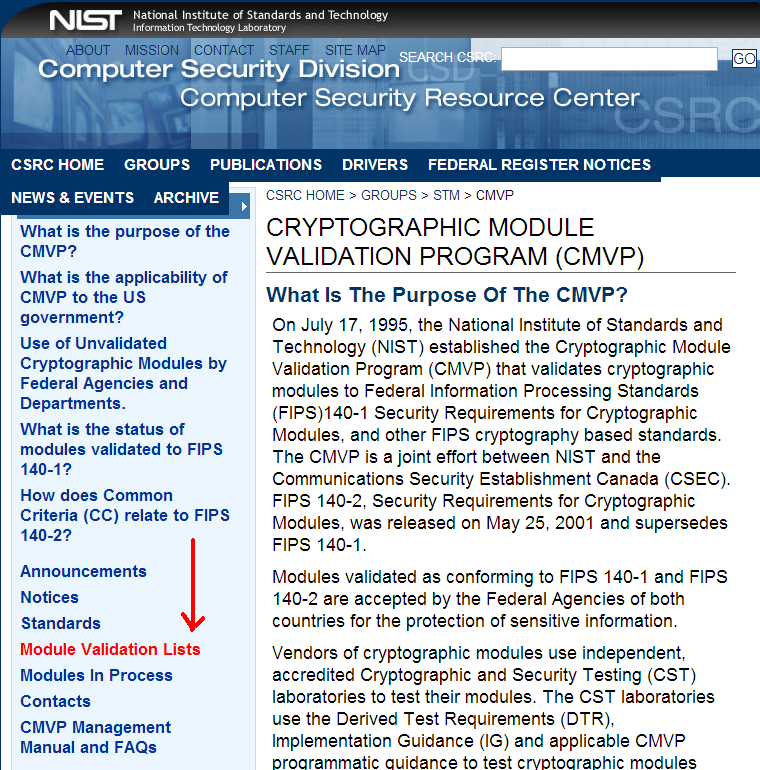


Figure D-2 – Module Validation Lists

Validation certifications always apply to a specific product version number. If a product is patched, the patch disqualifies the FIPS 140-2 validation (even if it makes the product more secure). If the patch is non-security related, CMVP IG G.8 defines a path for a validation update that is timely and cost effective (1SUB). CMVP IG G.8 also addresses how such changes can be re-validated. Refer to the FIPS 140-2 standards for more information.

**Note:** FIPS 140-2 Standards can be found at the following URL: <http://csrc.nist.gov/groups/STM/cmvp/standards.html#02>.

Some hardware appliances use a Hardware Security Module (HSM) where the encryption is performed entirely on the HSM. The validation certificate is listed in the name of the HSM vendor, and not in the name of the appliance vendor.

Validation certificates must be documented in the *System Security Plan*, but may be shown in any of the following ways:

* A URL of the certificate
* A screenshot of the certificate
* The PDF download of the certificate (.pdf file)

Security Control SI-5

Section 15.7.5 in the System Security Plan requires that the CSP discuss how information system security alerts, advisories, and directives are received from designated external organizations. One of these external organizations must be US-CERT. FedRAMP recommends receipt of advisories from all vendors used (e.g. operating system, database, router etc.).

It is often easiest to send all advisories to one internal list such as [advisories@cspname.com](mailto:advisories@cspname.com) or [security@cspname.com](mailto:security@cspname.com). Then lists must be maintained as needed. This control must be auditable. Therefore, an auditor will need to see that advisories are in fact coming in and a list of people receiving advisories.

Security Control CP-2

FedRAMP provides an *IT Contingency Plan (ITCP)* template that is available on the FedRAMP website. Refer to NIST SP 800-34, Revision 1 for assistance in writing the IT Contingency Plan <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>.

Security Control CM-9

The FedRAMP PMO does not provide a template for a Configuration Management Plan. However, each CSP is required to submit a Configuration Management Plan which must describe how its organizational controls change for the information system. The Configuration Management Plan needs to stand alone since it is likely that the staff that uses the Configuration Management Plan does not have access to the System Security Plan. The Configuration Management Plan needs to address the Configuration Management (CM) family of security controls as indicated in the System Security Plan template. A summary of the CM controls can be found in the Table D-3.

| **Control No** | **Control Name** | **Low** | **Moderate** |
| --- | --- | --- | --- |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | CM-2 (1) (3) (7) |
| CM-3 | Configuration Change Control | Not Selected | CM-3 (2) |
| CM-4 | Security Impact Analysis | CM-4 | CM-4 |
| CM-5 | Access Restrictions for Change | Not Selected | CM-5 |
| CM-6 | Configuration Settings | CM-6 | CM-6 |
| CM-7 | Least Functionality | CM-7 | CM-7 (1) (2) (4) |
| CM-8 | Information System Component Inventory | CM-8 | CM-8 (1) (3) (5) |
| CM-9 | Configuration Management Plan | Not Selected | CM-9 |

Table D-3 – Configuration Management Controls

Configuration management nomenclature must be defined in the *Configuration Management Plan* as it is used at the CSP. Suggested configuration management nomenclature that is worth taking into consideration can be found in Table D-4. FedRAMP allows for flexibility of development and release nomenclature, and the definitions in Table 5-4 may not match the terminology that CSPs are accustomed to using. Modify the definitions in Table 5-4 to match the nomenclature used by the CSP. If terminology is changed, ensure that it is consistent across all documentation, including any supporting documentation.

| **Nomenclature** | **Definition** |
| --- | --- |
| Alpha Release | The Alpha phase of the release cycle is the first phase to begin software testing. Alpha releases can potentially contain stability issues and are not made available to customers. |
| Beta Release | The Beta phase of the release cycle is a secondary phase to begin software testing after all features of the code are complete and after bugs found during the Alpha Release have been fixed. |
| Baseline | (1) A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. (2) A document or a set of such documents formally designated and fixed at a specific time during the life cycle of a configuration item. (3) Any agreement or result designated and fixed at a given time, from which changes require justification and approval. (IEEE Std. 610-12-1990). A baseline is configuration identification formally designated and applicable at a specific point in the life cycle of a configuration item. |
| Build | An operational version of a system or component that incorporates a specified subset of the capabilities that the final product will provide. (IEEE Std. 610-12-1990) |
| Configuration (or Change) Control Board (CCB) | A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes. (IEEE Std. 610-12-1990) |
| Change Request | A request from either an internal or an external customer to make a change to a baseline configuration. Change requests can be related to either software releases or to network components such as server or workstation configurations or to any other network infrastructure component. |
| Configuration Control | An element of CM, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. (IEEE Std. 610-12-1990) |
| Configuration Item | An identifiable part of a system that is a discrete target of configuration control processes. (NIST SP 800-128) |
| Configuration Management | A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. (IEEE Std. 610-12-1990) |
| Release | A software build that has been thoroughly tested and made available to customers. |
| Hardware Baseline | A current and comprehensive baseline inventory of all hardware (HW) to include manufacturer, type, model, physical location and network topology or architecture) required to support <Information System Name> operations is maintained by the Configuration Control Board (CCB) and is part of the Hardware and Software Inventory. A backup copy of the inventory is stored in a fire-rated container located or otherwise not collocated with the original. |
| Software Baseline | A current and comprehensive baseline inventory of all software that includes manufacturer, type, and version and installation manuals and procedures. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. |
| Version | Each software build is assigned a version number. The version number is used as a mechanism for differentiating one build from another. Version numbers are used regardless of whether or not a build is ultimately released. |

Table D-4 – Configuration Management Nomenclature

**Note:** NIST SP 800-128, *Guide for Security-Focused Configuration*

*Management of Information Systems* can be found at the following URL: <http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf>

When there is a significant change to a system, the SSP and other documents must be updated, and new security testing may be required on all or some controls. If there is a plan for a significant change to a system, notify the FedRAMP ISSO in advance of the change giving as much advanced notice as possible. The FedRAMP ISSO will convey final determination if the change is significant and affects the risk posture. Nomenclature such as that found in Table 5-4 must be taken into consideration during implementation.

A Configuration Management Plan, is required to describe the change management process that is used to implement changes (CM-3). The change management process must indicate if the change is a significant change, a standard change, or an emergency change (CM-3a). Other change types may be added according to organizational needs.

A signficant change includes (but is not limited to):

* Changing the authentication or access control implementation
* Changing the storage implementation
* Implementing a new code release s
* Changing the backup mechanisms and process
* Changing the IaaS provider
* Adding new interconnections to outside service providers
* Changing an alternate (or compensating) control
* Removing security controls
* An addition or change to functionality or services
* A change in the system boundary definition (e.g. adding new data center
* A change to the account provisioning process

The following types of changes must always be handled through the standard Configuration Management change control process:

* Changing a COTS product implemented in the system to another vendor or product
* Changing a product that delivers like functionality (e.g. a scanner, a firewall)
* Any change related to patch management
* A configuration change
* Adding or changing a firewall rule or a router ACL
* Emergency change

Security Control IR-8

Item 13.8.8 in the *System Security Plan* template requires an *Incident Response Plan*. FedRAMP does not provide a template for an *Incident Response Plan*. Nonetheless, each CSP is required to submit an *Incident Response Plan* that describes how security incidents are managed for a system. The Incident Response Plan addresses the Incident Response (IR) family of security controls as indicated in the *System Security Plan* template. A summary of the IR controls is found in Table D-5. The *Incident Response Plan* (IR-8) for the system must include information that provides descriptions of how IR-1 through IR-7 are implemented.

In the event of a security incident, CSPs are required to notify the FedRAMP PMO and US-CERT. This is described in more detail in the FedRAMP Incident Communications Procedure, which is available at [www.fedramp.gov](http://www.fedramp.gov).

| **Control No** | **Control Name** | **Low** | **Moderate** |
| --- | --- | --- | --- |
| IR-1 | Incident Response Policy and Procedures | IR-1 | IR-1 |
| IR-2 | Incident Response Training | IR-2 | IR-2 |
| IR-3 | Incident Response Testing & Exercises | Not Selected | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | IR-4 (1) |
| IR-5 | Incident Monitoring | IR-5 | IR-5 |
| IR-6 | Incident Reporting | IR-6 | IR-6 (1) |
| IR-7 | Incident Response Assistance | IR-7 | IR-7 (1) |
| IR-8 | Incident Response Plan | IR-8 | IR-8 |

Table D-5 – Incident Response Controls

The purpose of the *Incident Response Plan* is to have a fully documented plan with clearly defined roles and responsibilities used as a reference in the event of a security or privacy incident, or any other incident that may affect operations of the system (e.g. incidents related to power outages, natural disasters). The staff that may need to use the Incident Response Plan may not have access to the System Security Plan. Therefore, the Incident Response Plan must be able to stand alone.

Questions to consider include:

* Are incident roles and responsibilities defined?
* Who is responsible for incident response planning?
* Are there clear lines of reporting related to incidents?
* Are incident types defined?
* When was the Incident Response Plan last reviewed and who approved it?
* How does incident response fit into the overall Information Security Program?
* Are the number of incidents each month/year tracked?
* Are the type and prevalence of incidents tracked?
* Is the average time to close an incident tracked?

Questions to consider include:

* To whom has the Incident Response Plan been distributed?
* Does the Incident Response Plan indicate designated FedRAMP personnel must be included in the distribution?

Questions to consider include:

* How often is the Incident Response Plan reviewed?
* When was the Incident Response Plan last reviewed?

Questions to consider include:

* Does the Incident Response Plan include a document history to record changes?
* Who is responsible for updating the plan with revisions?
* Were any revisions made after the last testing exercise?

Questions to consider include:

* If there is a change to incident response procedures or policies who is notified?
* Is there an organizational contact list included for the incident response team members?
* Are role names listed for the individuals identified in the contact list?

Additional FedRAMP requirements for IR-8(b) and IR-8(e) require that FedRAMP PMO points of contact are included in the incident response plan. Obtain FedRAMP PMO points of contact from the designated FedRAMP ISSO.

When contracting with customer agencies, obtain and document notification points of contact from each customer agency in the event of a security incident. One of the points of contact must be the agency CSIRC[[3]](#footnote-4). The points of contact must be listed in the order in the agency has specified. The *Incident Response Plan* must be updated not less than annually. At the time of the annual update, contact the customer agency and validate phone numbers and POCs.

Security Control IR-2

Section 13.8.2 in the *System Security Plan* requires a description of how personnel are trained in incident response for the system.

Questions to consider include:

* What roles are trained? (e.g. database administrator, systems administrator)
* On what date did the last training occur?
* When will the next training take place?
* Where did the training take place and was it online or in person?
* Is there a participant/attendance list of who participated in the last training?
* Who is responsible for ensuring the training takes place?

Security Control IR-3

Section 13.8.3 in the *System Security Plan* requires that CSPs perform an annual incident response test/exercise.

Questions to consider include:

* What roles participate in the incident response test/exercise?
* On what date did the last test/exercise occur?
* When will the next test/exercise occur?
* Where did the test/exercise occur?
* Is there a participant list of who participated in the last text/exercise?
* Who is responsible for leading the test exercise?
* Who is responsible for writing the test plan that must be submitted to FedRAMP annually?

Security Control IR-4

Section 13.8.4 in the *System Security Plan* requires that a description of incident handling capability.

Questions to consider for part (a) include:

* How does the CSP prepare for incidents?
* Who must agency customers call if they suspect an incident?
* Is there an incident hotline or phone number published where customers can see it?
* What capability does the CSP have to detect incidents?
* If the CSP suspects that an incident has taken place, what steps are taken to verify that it really is an incident?
* What methods and tools are used to analyze confirmed incidents?
* What methods and tools are used to contain incidents?
* What methods and tools are used to eradicate incidents?
* What is the process for determining that the system has recovered from the incident?

Questions to consider for part (b) include:

* Which incident handling activities are coordinated with contingency planning activities?
* How does the coordination take place?
* Which incident handling activities are coordinated with contingency planning activities?

Questions to consider for part (c) include:

* Who maintains archives of lessons learned regarding incidents?
* How do the CSP determine which incidents require a lessons learned report?
* How soon after an incident is closed will the lessons learned report be published?
* Who is responsible for integrating lessons learned into procedures, training, and test/exercises?

Questions to consider for the additional FedRAMP requirements and guidance for IR-4 include:

* What personnel security requirements are required of individuals who perform incident handling?

Security Control IR-4(1)

Section 13.8.4.1.1 in the *System Security Plan* template requires a description of the automated mechanisms for incident handling?

Questions to consider include:

* Is there any sort of online workflow tool used for managing incidents?
* Are there any automated alerts related to incidents?
* Are there any automated programs, scripts, or applications that look for incidents or suspicious activities?

Security Control IR-5

Section 13.8.5 in the *System Security Plan* template requires that a description of how security incidents are tracked and documented.

Questions to consider include:

* What mechanism is used to record and track information about incidents?
* Is there an incident reporting and tracking form?
* Is the incident reporting form online on the intranet? Where?
* Is the incident reporting form a .pdf file?
* Can the CSP insert a blank copy of the incident reporting form in the template?
* Is there a place on the incident reporting form to indicate whether Personally Identifiable Information (PII) has been compromised?
* Who is responsible for ensuring that incidents are documented internally?
* Who will be the FedRAMP point of contact for incidents?
* Who will be the point of contact for customer agencies?
* Is there a flow chart to show how decisions about incident escalation are made?

Security Control IR-6

Section 13.8.6 in the *System Security Plan* template requires a description of incident reporting capabilities.

Questions to consider for part (a) include:

* What notification timeframes are built into the incident reporting process?
* Do reporting timeframes line up with Table J-1 in NIST SP 800-61, Revision 1?

Questions to consider for part (b) include:

* Who will ensure that incident reporting timeframes are adhered to?
* Who at the CSP determines whether law enforcement must be notified?
* What decisions need to be made or steps need to be taken before law enforcement is notified?
* Does the CSP have contact information for all agency customers?

Table D-6 must be inserted in the section related to incident reporting (IR-6). As CSPs contract with new customers, agency contact information must be recorded in this table. In the event of a security incident, the CSP must contact all agency customers using their system as well as the FedRAMP ISSO.

| Agency Name | Point of Contact | Phone | Email |
| --- | --- | --- | --- |
| <Agency Name> | 1. | 1. Primary: 2. Alternate: |  |
| 2. | 1. Primary: 2. Alternate: |  |
| 3. CSIRC |  |  |
| <Agency Name> | 1. | 1. Primary: 2. Alternate: |  |
| 2. | 1.Primary: 2. Alternate: |  |
| 3. CSIRC |  |  |

Table D-6 – Agency Points of Contact to Report Incidents

Security Control IR-6(1)

Section 13.8.6.1.1 in the *System Security Plan* template requires a description of automated mechanisms to assist in the reporting of security incidents.

Questions to consider include:

* Is there an online Incident Reporting Form that is available to staff?
* Is there an online Incident Reporting Form that is available to customers?
* Are there any apps for Incident Reporting?

Security Control IR-7

Section 13.8.7 in the *System Security Plan* template requires that CSPs provide incident response assistance and resources for users.

Questions to consider include:

* Who are the identified incident response experts within the CSP?
* Is there an internal Intranet page or wiki that includes helpful information for users about security incidents and reporting?

Security Control IR-7(1)

Section 13.8.7.1.1 in the *System Security Plan* template requires that a description of mechanisms to increase the availability of incident response related information and support.

Questions to consider include:

* Is an incident reporting phone number available 24 x 7 x 365?
* Is there an internal web page or wiki with incident reporting information that has high-availability mechanisms built into it?
* Has contact information been provided for at least one outside vendor that specializes in incident response?
* Does the CSP have contracts with outside vendors to provide incident response?

Security Control IR-7(2)

Section 13.8.7.1.2 in the *System Security Plan* template requires ta description of incident response capabilities that extend beyond the CSP’s organization.

Part (a) requires that the CSP establishes a direct, cooperative relationship between their incident response personnel and external providers of information system protection.

Questions to consider in the discussion for part (a) include:

* Has the process been documented on how to contact vendors if there is a suspected security vulnerability in a COTS product?
* Does the organization receive patch update information from all vendors? Who receives information on the latest patches?
* Does the organization receive advisories from US-CERT? Who receives the advisories?

Part (b) requires that internal incident contact information to external providers.

Questions to consider for part (b) include:

* What are the incident points of contact available to agency customers?
* Do Internet providers have contact information for internal points of contact for incidents?
* Do telecom providers have contact information for internal points of contact for incidents?
* If the CSP uses an external IaaS or PaaS vendor, does that vendor have contact information for internal incident response POCs?

Business Impact Analysis (BIA)

The *Business Impact Analysis* is an Appendix of the *IT Contingency Plan*. At this time, FedRAMP does not provide a template for the BIA. Refer to NIST SP 800-34, Revision 1 for more information on developing a *Business Impact Analysis*.

POA&M Template

CSPs must leverage the *Security Assessment Report* to put together a *Plan of Action & Milestones* (POA&M) for mitigating security weaknesses. FedRAMP provides a POA&M template for CSPs which is available on the FedRAMP website. All High and Moderate findings from the *Security Assessment Re*port must be mapped into the POA&M. High impact vulnerabilities must be mitigated within 30 days, and Moderate impact vulnerabilities must be mitigated within 90 days.

1. National Fire Protection Association (NFPA) Standard for the Protection of Information Technology Equipment 75 [↑](#footnote-ref-2)
2. <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf> [↑](#footnote-ref-3)
3. Computer Security Incident Response Center [↑](#footnote-ref-4)