Indian Health Service

FedRAMP - A Guide to Selecting FedRAMP Products

ANTHONY HARRIS
HQ LEAD ISSO
AUGUST 2023



 The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security authorizations for Cloud Service Offerings

FedRAMP

 The Federal Risk and Authorization Management Program (FedRAMP) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information.

FedRAMP Marketplace

The FedRAMP Marketplace is a searchable and sortable database of CSOs that have achieved a FedRAMP designation, a list of federal agencies using FedRAMP Authorized CSOs, and FedRAMP recognized assessors/auditors (3PAOs) that can perform a FedRAMP assessment.



Agencies and Cloud Service Providers (CSPs) are encouraged to use the Marketplace as a resource to:

- Research cloud services that have achieved a FedRAMP Marketplace designation
- •Research agencies partnering with CSPs for a FedRAMP Authorization, or identify agencies that are using FedRAMP Authorized CSOs
- Review FedRAMP's community of recognized 3PAOs

Private Cloud Deployments

The FedRAMP Marketplace is intended to enable the reuse of security package documentation, therefore private cloud deployments are not listed on the Marketplace.



- Once a Cloud Service Provider has confirmed partnership for authorization with their federal agency partner, and testing has been confirmed to occur within 6 months, an In Process Request may be submitted to the FedRAMP PMO
- FedRAMP PMO at info@FedRAMP.gov
- The In Process request may be submitted via email or as an attachment.

Marketplace Designations

The FedRAMP PMO defines three official designations for CSOs:

FedRAMP Ready

A designation provided to CSPs that indicates that a FedRAMP-recognized Third Party Assessment Organization (3PAO) attests to a CSO's security capabilities, and that a Readiness Assessment Report (RAR) has been reviewed and deemed acceptable by the FedRAMP PMO.

FedRAMP In Process

A designation provided to CSPs that are actively working toward a FedRAMP Authorization with either the Joint Authorization Board (JAB) or a federal agency.

FedRAMP Authorized

A designation provided to CSPs that have successfully completed the FedRAMP Authorization process with the JAB or a federal agency.



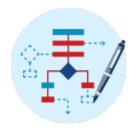
Highlights of FedRAMP Ready:

- Only available for CSOs at the Moderate and High impact levels*
- •Valid for one calendar year from the date of designation by the FedRAMP PMO
- •CSPs do not need an agency partner to submit a RAR to achieve a FedRAMP Ready designation
- * Impact levels for federal information systems, including CSOs, are defined in NIST FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems.



FedRAMP In Process

FedRAMP In Process indicates a CSP is actively working towards FedRAMP Authorization through the JAB or Agency Authorization processes. All FedRAMP In Process CSOs are listed on the FedRAMP Marketplace.



* AA Ring MD - IHS Sponsored Video Telehealth Solution



FedRAMP Authorized

Once a P-ATO letter is provided to a CSP, the Marketplace listing for the service offering will be updated to reflect its FedRAMP Authorized designation and the date of authorization.

Agency Authorization

- ✓ An agency grants an ATO for the CSO
- ✓ The CSP and 3PAO upload all required security package materials to their secure FedRAMP repository (MAX.gov for packages Authorized below the High baseline, their own repository for packages Authorized at the High baseline)
- √ The FedRAMP PMO reviews the package and releases an Agency Authorization Review Report



Phase 0 Initiation

- Introduction Meeting
- Critical Mass Determination
- Kick off Meeting
- · IHS

FedRAMP PMO

Duration: 3 Days

CSP Prepares Documents

- · CSP Documents all system information
- CSP Develops: · System Security Plan
- FIPS Pub 199
- · e-Authentication (Digital Identity Worksheet)
- Information System Security Practices & Procedures
- · Configuration Management Plan (CM)
- Control Implementation Summary (CIS) Worksheet
- · Information System Contingency Plan (ISCP) and ISCP Test Report
- · Incident Response Plan
- Privacy Threshold Analysis (PTA) / Privacy Impact Assessment (PIA) (SSP)
- · User Guide Roles of Behavior (ROB)

CSP Duration: Determined by

Phase 1 Initial **Security Review**

- CST Reviews Package Documentation
- Hold Phase 1 Meeting
- · CSP
- IHS Provides Comments on SSP
- CSP gets approval for Testing from CST

Duration: 11 Days

CSP Duration: Determined by

CSP Updates Phase 2 Final **Documents and**

- CSP Updates SSP and other documents per IHS' request
- CSP engages with 3PAO to conduct testing of system

Tests

 CSP resolves 3PAO findings if possible

Security Review

- CST Reviews Package Documentation with SAR and SSP
- Hold Phase 2 Meeting
- · CSP 3PAO
- · IHS Determines if CSP will obtain an ATO
- CSP and IHS meet Monthly to conduct Continuous Monitoring Meeting

IHS issues ATO

Phase 2 Submission

& Authorization

 CSP, IHS, 3PAO meet Annually to conduct Annual Assessment Meeting

Duration: 11 Days

Duration: 23 Days

CSP Duration:



https://www.fedramp.gov/

https://marketplace.fedramp.gov/products

Filter Marketplace by List Type:

PRODUCTS**AGENCIES**ASSESSORS





Questions Please





