FedRAMP Authorization Data Sharing Standard

- **Release:** 25.08A
- **Published:** 2025-08-24
- **Designator:** ADS
- **Description:** Initial release of the Authorization Data Sharing Standard

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-09-01** for **20x**.
  - These requirements apply to all participants in the FedRAMP 20x Phase One pilot.
  - 20xP1 participants do not need to fully align with this policy to receive pilot authorization.
  - Participants in the 20xP1 pilot who receive pilot authorizations must demonstrate progress towards the adoption of this policy and be in full alignment by the expiration date of their pilot authorization.
- **FedRAMP Rev5**:
  - This release is effective **2025-09-01** for **R5.ADS.B1** *(tentatively)*.
  - This release is effective 2025-09-01 for R5.ADS.B1 for FedRAMP Rev5 Authorized or In Process services.
  - These requirements will be initially tested and evaluated for Rev5 in the ADS Closed Beta (B1).
  - Providers MUST participate in a Balance Improvement Test to transition to the Authorization Data Sharing Standard process prior to wide release of this process for Rev5. Providers should participate in the FedRAMP Rev5 Community Working Group at https://www.fedramp.gov/community/ to follow this process.
  - Providers MUST NOT adopt changes to meet these requirements unless they inform the FedRAMP PMO and participate in a Balance Improvement Test.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

- 44 USC § 3609 (a)(8) The FedRAMP Authorization Act directs the Administrator of the General Services Administration to "provide a secure mechanism for storing and sharing necessary data, including FedRAMP authorization packages, to enable better reuse of such packages across agencies, including making available any information and data necessary for agencies..."
- OMB Memorandum M-24-15 on Modernizing FedRAMP Section 6 states that "In general, to encourage both security and agility, Federal agencies should use the same infrastructure relied on by the rest of CSPs' commercial customer base."

Purpose

Modern cloud services store and share security and compliance information in convenient repositories that allow customers to rapidly review security information and gain access to additional information as needed. These services often include automated integration with cloud service infrastructure to remove manual burden and ensure information is accurate and up to date.

This security and compliance information (including FedRAMP authorization data) is the intellectual property of the cloud service provider and is not federal information in most cases.* The federal government benefits when the same security information is shared among all customers and even the public to ensure maximum transparency and accountability of cloud service providers.

The FedRAMP Authorization Data Sharing Standard provides a process or mechanism for cloud service providers to store and share authorization data on their preferred platform of choice if it meets certain FedRAMP requirements.

At the initial release of this standard there will not be many platforms that directly support the requirements in this standard. FedRAMP anticipates this will change rapidly in response to market demand as platforms work to provide innovative solutions to these requirements.

** Providers with questions about this should consult with a lawyer who specializes in procurement law. Typically a contract with the government granting ownership of information is required to transfer ownership to the government.*

Expected Outcomes

- Cloud service providers will be able to manage authorization data in the same platforms used for commercial customers, reusing data as appropriate
- Federal agencies will be able to access necessary authorization data via API or other automated mechanisms integrated into agency authorization systems to simplify the burden of review and continuous monitoring
- Trust center providers and GRC automation tool providers will develop innovative solutions and improvements to ensure standardized automated data sharing and validation within the FedRAMP ecosystem

---

Requirements

FRR-ADS

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-ADS-01

> *Providers MUST publicly share up-to-date information about the cloud service offering in both human-readable and machine-readable formats, including at least:*
>
> 1. *Direct link to the FedRAMP Marketplace for the offering*
> 2. *Service Model*
> 3. *Deployment Model*
> 4. *Business Category*
> 5. *UEI Number*
> 6. *Contact Information*
> 7. *Overall Service Description*

> 8. *Detailed list of specific services and their impact levels (see FRR-ADS-03)*
> 9. *Summary of customer responsibilities and secure configuration guidance*
> 10. *Process for accessing information in the trust center (if applicable)*
> 11. *Availability status and recent disruptions for the trust center (if applicable)*
> 12. *Customer support information for the trust center (if applicable)*

FRR-ADS-02

> *Providers MUST use automation to ensure information remains consistent between human-readable and machine-readable formats when authorization data is provided in both formats; Providers SHOULD generate human-readable and machine-readable data from the same source at the same time OR generate human-readable formats directly from machine-readable data.*

FRR-ADS-03

> *Providers MUST share a detailed list of specific services and their impact levels that are included in the cloud service offering using clear feature or service names that align with standard public marketing materials; this list MUST be complete enough for a potential customer to determine which services are and are not included in the FedRAMP authorization without requesting access to underlying authorization data.*

FRR-ADS-04

> *Providers MUST share authorization data with all necessary parties without interruption, including at least FedRAMP, CISA, and agency customers.*

FRR-ADS-05

> *Providers MUST provide sufficient information in authorization data to support authorization decisions but SHOULD NOT include sensitive information that would likely enable a threat actor to gain unauthorized access, cause harm, disrupt operations, or otherwise have a negative adverse impact on the cloud service offering.*

FRR-ADS-06

> *Providers of FedRAMP Rev5 Authorized cloud service offerings MUST share authorization data via the USDA Connect Community Portal UNLESS they use a FedRAMP-compatible trust center.*

FRR-ADS-07

> *Providers of FedRAMP 20x Authorized cloud service offerings MUST use a FedRAMP-compatible trust center to store and share authorization data with all necessary parties.*

FRR-ADS-08

> *Providers MUST notify all necessary parties when migrating to a trust center and MUST provide information in their existing USDA Connect Community Portal secure folders explaining how to use the trust center to obtain authorization data.*

FRR-ADS-09

> *Providers MUST make historical versions of authorization data available for three years to all necessary parties UNLESS otherwise specified by applicable FedRAMP requirements; deltas between versions MAY be consolidated quarterly.*

FRR-ADS-10

> *Providers SHOULD follow FedRAMP's best practices and technical assistance for sharing authorization data where applicable.*

FRR-ADS-AC

These requirements for managing access apply to cloud service providers who establish FedRAMP-compatible *trust centers* for storing and sharing *authorization data*.

FRR-ADS-AC-01

> *Providers MUST publicly provide plain-language policies and guidance for all necessary parties that explains how they can obtain and manage access to authorization data stored in the trust center.*

FRR-ADS-AC-02

> *Providers SHOULD share at least the authorization package with prospective agency customers upon request and MUST notify FedRAMP within five business days if a prospective agency customer request is denied.*

FRR-ADS-TC

These requirements apply to FedRAMP-compatible *trust centers* used to store and share *authorization data*.

FRR-ADS-TC-01

> *Trust centers MUST be included as an information resource included in the cloud service offering for assessment if FRR-MAS-01 applies.*

FRR-ADS-TC-02

> *Trust centers SHOULD make authorization data available to view and download in both human-readable and machine-readable formats*

FRR-ADS-TC-03

> *Trust centers MUST provide documented programmatic access to all authorization data, including programmatic access to human-readable materials.*

FRR-ADS-TC-04

> *Trust centers SHOULD include features that encourage all necessary parties to provision and manage access to authorization data for their users and services directly.*

FRR-ADS-TC-05

> *Trust centers MUST maintain an inventory and history of federal agency users or systems with access to authorization data and MUST make this information available to FedRAMP without interruption.*

FRR-ADS-TC-06

> *Trust centers MUST log access to authorization data and store summaries of access for at least six months; such information, as it pertains to specific parties, SHOULD be made available upon request by those parties.*

FRR-ADS-TC-07

> *Trust centers SHOULD deliver responsive performance during normal operating conditions and minimize service disruptions.*

FRR-ADS-EX

These exceptions MAY override some or all of the FedRAMP requirements for this standard.

FRR-ADS-EX-01

> *Providers of FedRAMP Rev5 Authorized cloud service offerings at FedRAMP High using a legacy self-managed repository for authorization data MAY ignore the requirements in this standard until future notice.*

Technical assistance

FRA-ADS

Purpose: This Technical Assistance helps stakeholders understand the intent behind the requirements in the FedRAMP *authorization data* Sharing Standard.

Disclaimer: Every cloud service provider is different, every architecture is different, and every environment is different. Best practices and technical assistance MUST NOT be used as a checklist. All examples are for discussion purposes ONLY.

FRA-ADS-04

"Without interruption" means that parties should not have to request manual approval each time they need to access *authorization data* or go through a complicated process. The preferred way of ensuring access without interruption is to use on-demand just-in-time access provisioning.

FRA-ADS-05

This is not a license to exclude accurate risk information, but specifics that would *likely* lead to compromise should be abstracted. A breach of confidentiality with *authorization data* should be anticipated by a secure cloud service provider.

Examples of unnecessary sensitive information in *authorization data*

Key Tests:

- Passwords, API keys, access credentials, etc.
- Excessive detail about methodology that exposes weaknesses
- Personally identifiable information about employees

Examples:

- DON'T: "In an emergency, an administrator with physical access to a system can log in using "secretadmin" with the password "pleasewutno"" DO: "In an emergency, administrators with physical access can log in directly."
- DON'T: "All backup MFA credentials are stored in a SuperSafe Series 9000 safe in the CEOs office." DO: "All backup MFA credentials are stored in a UL Class 350 safe in a secure location with limited access."

- DON'T: "During an incident, the incident response team lead by Jim Smith (555-0505) will open a channel at the conference line (555-0101 #97808 passcode 99731)..." DO: "During an incident, the incident response team will coordinate over secure channels."
