FedRAMP Minimum Assessment Standard

- **Release:** 25.10A
- **Published:** 2025-10-17
- **Designator:** MAS
- **Description:** minor updates to improve clarity; switch from federal information to federal customer data; add impact level metadata; no substantive changes.

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-06-17** for **20x Phase One Pilot**.
  - These requirements apply to all participants in the FedRAMP 20x Phase One pilot.
- **FedRAMP Rev5**:
  - This release is effective **2025-07-30** for **Rev5 Closed Beta**.
  - These requirements will be initially tested and evaluated for Rev5 in the MAS Closed Beta.
  - Providers MUST participate in the MAS Closed Beta to transition from the Rev 5 legacy boundary until a final transition path is announced. Providers should participate in the FedRAMP Rev5 Community Working Group at https://www.fedramp.gov/community/ to follow this process.

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

- OMB Circular A-130: Managing Information as a Strategic Resource Section 10 states that an "Authorization boundary" includes "all components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected." and further adds in footnote 64 that "Agencies have significant flexibility in determining what constitutes an information system and its associated boundary."
- NIST SP 800-37 Rev. 2 Chapter 2.4 footnote 36 similarly states that "the term authorization boundary is now used exclusively to refer to the set of system elements comprising the system to be authorized for operation or authorized for use by an authorizing official (i.e., the scope of the authorization)."
- FedRAMP Authorization Act (44 USC § 3609 (a) (4)) Requires the General Services Administration to "establish and update guidance on the boundaries of FedRAMP authorization packages to enhance the security and protection of Federal information and promote transparency for agencies and users as to which services are included in the scope of a FedRAMP authorization."

Purpose

Application boundaries that are defined too broadly complicate the assessment process by introducing components that are unlikely to have an impact on the confidentiality, integrity or accessibility of the offering. The Minimum Assessment

Standard provides guidance for cloud service providers to narrowly define information resource boundaries while still including all necessary components.

Expected Outcomes

- Boundaries will include the minimum number of components to make authorization and assessment easier
- Cloud service providers will define clear boundaries for security and assessment of offerings based on the direct risk to federal customer data
- Third-party independent assessors will have a simple well documented approach to assess security and implementation decisions
- Federal agencies will be able to easily, quickly, and effectively review and consume security information about the service to make informed risk-based Authorization to Operate decisions based on their planned use case

---

Requirements

FRR-MAS

These requirements apply ALWAYS to ALL FedRAMP authorizations based on the Effective Date(s) and Overall Applicability.

FRR-MAS-01

Applies to: Low, Moderate, High

> Providers MUST identify a set of *information resources* to assess for FedRAMP authorization that includes all *information resources* that are *likely* to *handle federal customer data* or *likely* to impact the confidentiality, integrity, or availability of *federal customer data handled* by the *cloud service offering*.

FRR-MAS-02

Applies to: Low, Moderate, High

> Providers MUST include the configuration and usage of *third-party information resources*, ONLY IF *FRR-MAS-01* APPLIES.

FRR-MAS-03

Applies to: Low, Moderate, High

> Providers MUST clearly identify and document the justification, mitigation measures, compensating controls, and potential impact to *federal customer data* from the configuration and usage of non-FedRAMP authorized *third-party information resources*, ONLY IF *FRR-MAS-01* APPLIES.

FRR-MAS-04

Applies to: Low, Moderate, High

> Providers MUST include metadata (including metadata about *federal customer data*), ONLY IF *FRR-MAS-01* APPLIES.

FRR-MAS-05

Applies to: Low, Moderate, High

> Providers MUST clearly identify, document, and explain information flows and impact levels for ALL *information resources*, ONLY IF *FRR-MAS-01* APPLIES.

FRR-MAS-EX

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

FRR-MAS-EX-01

Applies to: Low, Moderate, High

> Providers MAY include documentation of *information resources* beyond the *cloud service offering*, or even entirely outside the scope of FedRAMP, in a FedRAMP assessment and *authorization package* supplement; these resources will not be FedRAMP authorized and MUST be clearly marked and separated from the *cloud service offering*.

FRR-MAS-AY

These rules provide general guidance on the application of this standard.

FRR-MAS-AY-01

Applies to: Low, Moderate, High

> Certain categories of cloud computing products and services are specified as entirely outside the scope of FedRAMP by the Director of the Office of Management and Budget. All such products and services are therefore not included in the *cloud service offering* for FedRAMP. For more, see fedramp.gov/scope.

FRR-MAS-AY-02

Applies to: Low, Moderate, High

> Software produced by cloud service providers that is delivered separately for installation on agency systems and not operated in a shared responsibility model (typically including agents, application clients, mobile applications, etc. that are not fully managed by the cloud service provider) is not a cloud computing product or service and is entirely outside the scope of FedRAMP under the FedRAMP Authorization Act. All such software is therefore not included in the *cloud service offering* for FedRAMP. For more, see fedramp.gov/scope.

FRR-MAS-AY-03

Applies to: Low, Moderate, High

> *Information resources* (including *third-party information resources*) that do not meet the conditions in FRR-MAS-01 are not included in the *cloud service offering* for FedRAMP (*FRR-MAS-02*).

FRR-MAS-AY-04

Applies to: Low, Moderate, High

> *Information resources* (including *third-party information resources*) MAY vary by impact level as appropriate to the level of information *handled* or impacted by the information resource (*FRR-MAS-05*).

FRR-MAS-AY-05

Applies to: Low, Moderate, High

> All parties SHOULD review best practices and technical assistance provided separately by FedRAMP for help with applying the Minimum Assessment Standard as needed.

FRR-MAS-AY-06

Applies to: Low, Moderate, High

> All aspects of the *cloud service offering* are determined and maintained by the cloud service provider in accordance with related FedRAMP authorization requirements and documented by the cloud service provider in their assessment and authorization materials.
