FedRAMP™

FedRAMP Boundary Policy

Working DRAFT

January 2025

APPLICABILITY

This policy defines requirements and recommendations related to FedRAMP boundaries for the following parties:

- **Cloud service providers (CSPs)** who participate or want to participate in the FedRAMP marketplace
- **Independent assessors (IAs)** who perform third-party cybersecurity assessments for cloud service offerings (CSOs) through their FedRAMP packages. IAs conduct both initial and periodic evaluations of CSOs to ensure they comply with federal security requirements. IAs are also known as *third-party assessment organizations (3PAOs)*.
- **Package reviewers from *FedRAMP designated leads*,** who are federal agencies responsible for sponsoring CSPs for FedRAMP authorization. A designated lead can be:
    - An authorizing official at a federal agency; or
    - The FedRAMP Director at GSA in the case of a program-sponsored authorization.

The purpose of this guidance is to establish greater consistency and a shared interpretation of which systems and data fall within a FedRAMP authorized boundary, and which do not, across all FedRAMP authorization pathways.

This guidance is normative and applies to **all** FedRAMP authorizations, and is required to be followed by **all** cloud service providers (CSPs) and **all** federal sponsors of FedRAMP authorizations (individual agencies, multi-agency constructs, and FedRAMP itself in the case of program authorizations).

CSPs and IAs must adhere to this version of the policy by MONTH DD, 2025. Package reviewers from FedRAMP designated leads must adhere to this version of the policy starting on MONTH DD, 2025.

FEEDBACK

Suggestions for improving the policy are welcome anytime through the feedback form at https://www.fedramp.gov/documents-templates/.

TABLE OF CONTENTS

1. Policy Overview

The FedRAMP boundary defines the scope of a Cloud Service Offering (CSO) that must be assessed for FedRAMP authorization.

The ***FedRAMP boundary*** includes all aspects of the CSO, including external services, that:

1. handle[1] federal information; and/or
2. directly impact the confidentiality, integrity, or availability of federal information

This includes all services to be consumed by tenants/customers and the underlying components, infrastructure, and services (including external services), that handle federal information as part of the CSO and the related organizational users operating the service. It also includes privileged security tooling, authentication systems, management/orchestration, and keying material and secrets.

Cloud Service Providers (CSPs) and Independent Assessors (IAs) are encouraged to engage FedRAMP when navigating complex scenarios about when services should be inside the boundary or not. FedRAMP will create and maintain a knowledge base of examples with specific guidance where appropriate to help CSPs and IAs navigate this.

1.1 Reuse of FedRAMP Authorized Cloud Service Offerings

CSPs can leverage existing FedRAMP authorized cloud service offerings as part of their CSO to streamline their engineering and authorization process. Reusing a FedRAMP authorized cloud service offering will allow the CSO to inherit the existing implementation, assessment, and testing of services from those cloud service offerings without including the entirety of those offerings inside the FedRAMP boundary.

The relevant inherited controls from leveraged FedRAMP authorized cloud service providers should be reviewed during reuse or agency assessment for an Authorization to Operate but should not be duplicated in the FedRAMP boundary or assessment for the CSO. Documentation and assessment of leveraged FedRAMP authorized cloud service offerings used by the CSO should be limited to the configuration of leveraged services following guidelines in the leveraged service's Customer Responsibility Matrix (CRM) and remaining in compliance with CISA BOD 25-01: Implementation Guidance for Implementing Secure Practices for Cloud Services.

1.2 Operations Outside the FedRAMP Boundary

Ancillary services that support the CSP or CSO but pose negligible[2] or no direct risk to federal information should remain outside the FedRAMP boundary. These systems may be documented in the SSP front matter and other diagrams as appropriate to demonstrate operations of the CSO. Interactions with such systems

[1] inclusive of any possible use of information, including creation, collection, processing, storing, transmitting, accessing, disposing, etc.

[2] so small that it is not worth considering; any foreseeable risk would be merely an inconvenience

will be reviewed by the IA to affirm that they pose the low level of risk as documented, but systems that pose this low risk will not be tested by the IA.

Examples of ancillary services that *may* be outside the FedRAMP boundary include corporate email services, development environments, and customer service systems where a loss of confidentiality, integrity, or availability is not likely to directly affect federal information within the CSO.

2. Requirements and Recommendations

This section defines requirements and recommendations related to FedRAMP boundaries for three types of stakeholders: CSPs, IAs, and package reviewers from FedRAMP designated leads.

Each requirement and recommendation has an identifier that is unique across FedRAMP policies. This identification approach enables referencing specific requirements and recommendations in this and other resources.

2.1 Cloud Service Providers

CSPs are responsible for defining the FedRAMP boundary for each of their CSOs, protecting information and components within each boundary, and safeguarding the environments of operation. The following requirements and recommendations apply to all FedRAMP authorized CSOs unless otherwise stated.

2.1.1 FedRAMP Boundary Definition

- **FRR201:** CSPs **shall** include all CSO services and their underlying components, infrastructure, and services (including external services) that:
    - handle federal information; and/or
    - directly impact the confidentiality, integrity, or availability of federal information.
- **FRR202**: CSPs **shall** include any components required to be installed or run on a tenant system in order to use the CSO and may include additional optional components if they are included in the SSP.
- **FRR203:** CSPs **shall** document all components, their relationships, data flows, types, encryption employed, access and policy enforcement points, security components, and ports/protocols/services used in the SSP.
- **FRR204:** CSPs **shall** address only the customer responsibilities for any FedRAMP authorized cloud service offerings that they wish to inherit controls from. Configurations must comply with CISA BOD 25-01: Implementation Guidance for Implementing Secure Practices for Cloud Services.
- **FRR205:** CSPs **shall** update boundary documentation as architectures evolve and as protections or data flows change. CSPs **shall** reflect such updates promptly in SSPs, continuous monitoring reports, and in the POA&M where they deviate from these requirements.

2.1.2 FedRAMP Boundary Protection of Information

- **FRR206:** CSPs **shall** designate a System Owner for the CSO who has sufficient organizational authority to enforce all policies, procedures, and control implementations which affect the FedRAMP boundary, including contractual obligations with third parties.
- **FRR207:** CSPs **shall not** reuse federal information for shared purposes unless the government tenant specifically opts in to such sharing or grants access to the information. CSPs **shall** ensure that external services that handle federal information are configured to meet this requirement. This requirement applies to machine learning models trained on federal information.
- **FRR208:** CSPs **shall** ensure that security and administrative configuration, secrets, key material, and agents are managed within the FedRAMP boundary and are documented within the SSP.
- **FRR209:** CSPs **shall** document and maintain information exchange agreements for all external systems within the FedRAMP boundary. This **shall** include the information types, encryption employed, ports/protocols/services used, access levels, and the requirement to meet FedRAMP security requirements.
- **FRR210:** CSPs **shall** ensure that federal information sent to public or commercial services used to support the function of a CSO is limited to information approved by the owner of the federal information.

2.1.3 FedRAMP Boundary Restrictions on Inbound and Outbound Connections

- **FRR211:** CSPs **shall not** permit any systems outside the FedRAMP boundary to directly access federal information or to make changes to the security of the FedRAMP boundary except when approved by the owners of the federal information.
- **FRR212:** CSPs **shall** document all connections established between the FedRAMP boundary and systems in the environment of operations, including the data types, encryption employed, ports/protocols/services used, the level of access, and the service or component involved.

2.2 Independent Assessors (IAs)

- **FRR216:** IAs **shall** test all components within the FedRAMP boundary and **shall** review and evaluate connections to systems outside the FedRAMP boundary as documented by the CSP following FRR201-212**.**
- **FRR217:** IAs **shall** review data flows between the FedRAMP boundary and the environment of operations, and **shall** validate the impact categorization of the data in those services, the presence of appropriate certifications, and ensure they have no direct security impact or privileged access to the federal information.
- **FRR219:** IAs **shall** document deviations from this guidance within the SAR, POA&M, and other materials.