FedRAMP

FedRAMP Authorization Boundary Guidance

Version 2.0

07/13/2021

GSA

Info@FedRAMP.gov

FedRAMP.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
5/10/2018	1.0	All	Document published	FedRAMP PMO
7/13/2021	2.0	All	Document updated to provide clarity of the boundary requirements	FedRAMP PMO

TABLE OF CONTENTS

Purpose

The purpose of this document is to provide Cloud Service Providers (CSPs) guidance for developing the authorization boundary associated with their Cloud Service Offering (CSO) to support their FedRAMP Authorization package. An authorization boundary provides a diagrammatic illustration of a CSP's internal services, components, and other devices along with connections to external services and systems. An authorization boundary encompasses all technologies, external and internal services, and leveraged systems and accounts for all federal information, data, and metadata that a CSO is responsible for. The authorization boundary is a critical component associated with the federal National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems and Office of Management* and Budget (OMB) circular A-130, *Managing Information as a Strategic Resource*.

This document serves as a living document, evolving with changes to cloud computing technology and federal information security policy relevant to FedRAMP.

The information found in this document pertains to CSPs that are pursuing and maintaining a FedRAMP Authorization.

Key Federal Definitions and Requirements

The concepts below provide an overview of various terms and definitions outlined in NIST SP 800-37, SP 800-53, and OMB A-130 and provide guidance from the FedRAMP Program Management Office (PMO) and Joint Authorization Board (JAB).

1. Defining Your Authorization Boundary in the Cloud

Federal Definition: NIST SP 800-37 defines an authorization boundary as "all components of an information system to be authorized for operation by an Authorizing Official (AO) and excludes separately authorized systems to which the information system is connected."

FedRAMP Guidance: An authorization boundary for cloud technologies should describe a cloud system's internal components and connections to external services and systems that will process federal data or federal metadata. All external services that process, store, or transmit federal data or sensitive federal metadata must either be included in the authorization boundary or reside in a FedRAMP authorized system

at the same FIPS-199 impact level. Some sensitive federal metadata can be authorized to reside in corporate systems that are wholly owned by the CSO. Authorized systems that are controlled and managed by the customer are excluded from the CSO boundary. Components that are provided by the CSO and run in the customer environment (i.e. agents, applications, specialized hardware) may be included in the assessment, and therefore in the boundary.

When describing the authorization boundary in security documentation or diagrams, all data types and flow of data within the boundary and to external systems that will process, transmit, or store federal data and federal metadata on behalf of the system must be described.

Non-sensitive and corporate metadata can reside in corporate systems and commercial cloud systems procured by the CSP. When determining the sensitivity of the data being stored in CSO systems, the CSP must work with the Authorizing Official or delegates to determine if the data can be stored in a non FedRAMP authorized system.

The types of data and metadata, determination of potential impact and of inclusion within the boundary will be made by the Authorizing Official in cooperation and consultation with the CSP.

2. Federal Data in the Cloud

Federal Definition: OMB A-130 describes federal information as "information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form."

FedRAMP Guidance: CSPs should account for, and include within an authorization boundary, all federal data populated or generated by a federal customer within the CSO, including metadata. Any information that the system processes or stores that originates from or is produced for a federal government entity is considered federal data.

Some examples include:

- Federal HR/personnel information
- Federal resource management
- Taxpayer/citizen information
- Federal acquisition information
- Federal law enforcement data
- Federal Court information

These are a few examples of federal data, not a comprehensive list. A more exhaustive list of types of federal data can be found in NIST SP 800-60 and can be determined with each individual agency or federal government entity authorizing a CSO. This includes information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments or 5 U.S.C. 552a, Privacy Act.

3. Federal Metadata in the Cloud

Federal Definition: NIST SP 800-53 describes metadata as "information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels)."

FedRAMP Guidance: There are two types of metadata that each have their own security considerations and requirements:

1. Federal metadata:

Data that, if compromised, could impact the confidentiality, availability, or integrity of the systems supporting the processing, storage, or transmission of federal data.

For example:

- Configuration data (hostnames, IPs, system running configuration, patching level, etc.)
- Scan data (Raw scan data, POA&M, Deviation Requests, etc.)
- Security Documentation
- Incident Response Data (Active incident response data and investigation communications)
- Ticketing information with systems specific information

This is not an exhaustive list and only provides a guideline for determining the impact level of the metadata. If there is a question about the categorization of the metadata in a CSO, the CSP must validate with the AO the nature of the metadata. Within the federal metadata category there are two subcategories.

Federal metadata with a direct potential impact on mission, organizations or individuals should there be a loss of confidentiality, integrity, or availability. This includes security metadata revealing the current security posture of the system; vulnerability information; active incident response information and communications; and active threat assessment, penetration test or security investigation information and communications. This type of federal metadata must reside within the authorization boundary or within the boundary of another federal information system authorized by the AO at the same or greater FIPS-199 impact level. The types of metadata, determination of potential impact and of inclusion within the boundary shall be made by the AO in cooperation and consultation with the CSP.

Note: *JAB systems that are using external systems for the processing, storage or transmission of this type of federal metadata must utilize a system with a JAB authorization at the same or greater FIPS-199 impact level.*

Federal metadata with an indirect potential impact on mission, organizations or individuals should there be a loss of confidentiality, integrity, or availability. This includes data revealing system infrastructure, facilities, and design; applications name, version, and release; application, system, and network configuration information; interconnections and access methods; systems inventories; architecture models, diagrams, and details; system security plans, contingency plans, risk management plans, security impact

analysis, plans, and roadmaps; personnel security information; information that could be sold for profit; and historical federal metadata the previously was considered to have a direct potential impact. This type of federal metadata may be authorized to reside in a system that is fully owned, maintained and operated by the CSP where established contractual vehicles or other agreements provide for and where the CSP shall demonstrate or attest to meeting and maintaining satisfactory performance of security requirements commensurate with NIST SP 800-171.

Note: *For JAB systems, this type of federal metadata must reside in a cloud that is JAB authorized to the same level or greater as the CSO or in a system that is fully owned, maintained and operated by the CSP and meets the JAB requirements commensurate with NIST SP 800-171. This type of metadata cannot be stored in another entity's cloud or corporate system. The CSP must be able to provide attestation that the corporate system meets JAB security requirements that are commensurate with NIST SP 800-171.*

2. Corporate metadata:

Data about processes within the authorization boundary or federal customers that does not contain security sensitive information and/or information that if compromised could be a threat to the systems supporting the processing and storage of federal or federal metadata or federal personnel data.

For Example:

- Sales data
- IT utilization and performance data
- Project planning information
- Marketing materials
- Pricing data

Corporate metadata should be accounted for, adequately protected, and documented by the CSP within applicable FedRAMP deliverables. External systems processing or storing corporate metadata can maintain an active connection with the authorization boundary, but all connections must be examined and the type of information transmitted in the connection must be validated by the 3PAO during initial authorization and at annual assessment.

4. Interconnections in the Cloud

Federal Definition: Per NIST SP 800-47, an interconnection is defined as “the direct connection of two or more IT systems for the purpose of sharing data and other information resources.”

FedRAMP Guidance: Interconnections must be reviewed by Authorizing Officials (AOs) to ensure that all federal data and metadata residing within or leaving the system is adequately protected. Cloud technologies that utilize interconnections, Application Programming Interfaces (APIs), and other synchronous/asynchronous connections that potentially transmit federal data or metadata, must document, test and monitor the connections in accordance with FedRAMP and federal guidelines.

5. External Services in the Cloud

Federal Definition: NIST SP 800-53 defines external services as "a system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security and privacy controls or the assessment of security and privacy control effectiveness."

FedRAMP Guidance: Cloud technologies can augment or support their functionality by utilizing systems, components, and services from external services that are not directly controlled by the CSP pursuing a FedRAMP authorization. The CSP must clearly document these external services including the flow of the data, specific ports, the security and encryption used in all the connections and the extent to which federal information (data) can be impacted by the use of these services. The use of external services that carry federal data and metadata must be depicted as part of the CSO's authorization boundary and must meet the data requirements for the different data categories. CSPs should make sure their FedRAMP Authorization Package (e.g., System Security Plan [SSP], Security Assessment Plan [SAP], Security Assessment Report [SAR], etc.) reflects this information. As part of issuing the Authority to Operate, the AO must review and approve the use of the external systems as part of the CSP's authorization boundary.

Item of Note: *External services may or may not have a pre-existing FedRAMP Authorization unless they are processing federal data or metadata. External services that impact the Confidentiality, Integrity, or Availability (CIA) of federal information must be included within the CSO's authorization boundary, or another authorized boundary.*

6. Leveraging External Services with a FedRAMP Authorization

Federal Definition: If a CSO is leveraging an underlying IaaS, PaaS, or SaaS it must have a FedRAMP Authorization, and the leveraged CSP must demonstrate compliance with all FedRAMP security and privacy requirements. CSPs must reflect this relationship within the FedRAMP Authorization Package (e.g., SSP, Control Implementation Summary [CIS], etc.), and they must ensure that they are meeting all the customer requirements outlined in the leveraged customer responsibility matrix.

Item of Note: *Leveraged services are a subcategory of external services, see above, and must have a pre-existing FedRAMP Authorization at the same or greater FIPS-199 impact level.* For JAB Authorizations all external and leveraged services must have a JAB Authorization at the same or greater FIPS-199 impact level as the CSO.

7. Corporate Services

FedRAMP Guidance: Corporate services are services used by a CSP to support their daily business operations and exist outside of the CSO authorization boundary. These services must not contain any federal data or unauthorized metadata. Any corporate services that contain federal metadata must meet the security requirements outlined above. If a corporate system is being utilized to process or store federal metadata, the CSP must own and operate the system and attest that the system meets the security requirements outlined in NIST SP 800-171 or be in a CSO at the same security level.

Data Requirements

Federal Data: Federal data that is processed, stored, or transmitted by or for the federal government, in any medium or form must be included in the authorization boundary and must be in a system authorized to the same level as the CSO being authorized.

JAB Specific Requirement: All JAB systems must only leverage JAB systems of the same FIPS-199 impact level to process, store or transmit Federal Data.

Federal Metadata (Direct Impact): Federal metadata that can directly impact the CIA of an information system that stores, processes or transmists Federal Data for the Federal Government, in any medium or form must be included within the authorization boundary or must be in a system authorized to the same level as the CSO being authorized.

JAB Specific Requirement: All JAB systems must only leverage JAB Authorized systems of the same FIPS-199 impact level to process, store or transmit dynamic federal metadata.

Federal Metadata (Indirect Impact): Federal metadata that can indirectly impact the CIA of an information system that stores, processes or transmits federal data for the federal government, in any medium or form, must be included within the authorization boundary or must be in a system authorized to the same level as the CSO being authorized or must be authorized to be in a corporate system that is wholly owned and operated by the CSO.

JAB-Specific Requirement: All JAB systems must only leverage JAB systems of the same FIPS-199 impact level or corporate information systems that are wholly owned and operated by the CSO to process, store or transmit static authorized federal metadata.

Corporate Meta: Data about processes within the authorization boundary or federal customers that does not contain security sensitive personal information and/or information that if compromised could be a threat to the systems supporting the processing and storage of federal or federal metadata or federal personnel data.

Additional Agency-Specific Security Requirements

FedRAMP provides a baseline from which CSPs and Agencies can define their desired security posture according to Federal Information Security Modernization Act (FISMA) requirements and NIST security categorizations. While FedRAMP considers its baseline to be comprehensive per impact levels, federal agencies may define additional security requirements in service of the agency's mission and desired security posture. CSPs should account for requirements variances on a customer-by-customer basis.

FedRAMP strongly recommends CSPs engage their customers early and often to identify additional requirements for federal data types and understand the impact on a system's cloud authorization boundary. Where possible, the FedRAMP PMO provides support to align CSPs and agencies on additional security requirements.

Examples of agency-specific requirements that could impact the authorization boundary include privacy controls, controls associated with foreign nationals, etc.

Appendix A: Guidance on Developing Authorization Boundary, Network and Data Flows Diagrams

The following section provides guidance on how to develop authorization boundary, network, and data flow diagrams that align with FedRAMP's expectations.

Authorization Boundary Diagram (ABD)

Before implementing and documenting security controls, CSPs must clearly define the authorization boundary for the CSO. The authorization boundary is the foundation on which the remainder of a SSP is built. The authorization boundary is validated against the inventory during the 3PAO assessment.

The Authorization Boundary Diagram (ABD) is a visual representation of the components that make up the authorization boundary. The ABD provides the Authorizing Official (AO) and/or the Joint Authorization Board (JAB) with a clear understanding of what, exactly, is being secured, tested, and then authorized.

To help AOs/JAB understand areas that may require risk-acceptance or areas where the agency has responsibility (that is, everything *excluded* from the authorization boundary), the ABD should also depict:

- External systems/services that provide functionality to the CSO or are used to manage and operate the CSO. This includes underlying IaaS/PaaS/SaaS offerings, system interconnections, APIs, external cloud services, and corporate shared services.
- System components, services, or devices that reside in the customer's environment may be in boundary, or out.
    - For example, many CSPs require customers to authenticate via an agency-provided IdP. This should be depicted as out-of-boundary on the ABD.
    - On the other hand, often CSPs provide components as part of the offering that run in the customer's environment, such as data collectors, clients or agents. These components should be included in scope for 3PAO testing and included in-boundary.

In short, every tool, service, or component that is mentioned in the SSP should appear on the ABD, and all components provided by the CSP should be tested by the 3PAO and shown as in-boundary.

AOs should **carefully review** the authorization boundary for the CSO to understand areas that require risk-acceptance and areas where the agency is responsible for implementing, managing and monitoring security controls.

The following checklist represents FedRAMP's requirements for the ABD and should be used by CSPs when developing the ABD:

- Provide an easy-to-read diagram that includes a legend. The ABD should be readable without having to enlarge it.
    - It is acceptable to provide the ABD as a separate attachment
- Include a prominent **RED** border drawn around all components in the authorization boundary
- Depict all ingress / egress points
- Depict services leveraged from the underlying IaaS/PaaS/SaaS and identify any services that are not FedRAMP authorized
    - How this is done is up to the CSP.. Some CSPs use color-coding with a corresponding legend. Others have included a call-out box that lists all services that are not FedRAMP authorized.
- Depict all interconnected systems and external services, including corporate shared services, and identify any systems/services that are not FedRAMP authorized. Again, how this is done is up to the CSP.
- Depict every tool, service, or component that is mentioned in the SSP narrative and controls
    - This includes services used to manage and operate the system (e.g., SIEM, Vulnerability Scanning, System Health Monitoring, Ticketing)
    - Identify all depicted tools, services, or components as either external or internal to the boundary
- Depict how CSP admins and agency customers access the cloud service (i.e., authentication used to access service). While this will cover these in detail in the data flow diagrams, FedRAMP requires this information on the boundary diagram.
- If applicable, depict components provided by the CSP, and installed on customer devices, as inside the authorization boundary

    - These components are required to be in the boundary if they materially affect the CIA of the CSO (e.g., data collectors in customer data centers and mobile applications)
- Show connections between components within the boundary and to/from external services as well as the separation and security in-place between the boundary and external services and access.
    - For example, include connections from load balancers to the servers they support. Similar flows can be combined or noted (e.g., bastion server access to all hosts, all devices forward logs to log server, etc.)
- Depict dev/test environment, alternate processing site, and location of backups including the connections and security mechanisms associated with the connections and services.
    - The dev/test environment must be included within the boundary if federal data is used and/or if federal government personnel have access to the environment for any reason, including training and user acceptance testing
- Show update services (e.g., malware signatures and OS updates) outside the boundary

Network Diagram

The Network Diagram should address all components reflected in the ABD, and:

- Depict subnetting
- Depict location of DNS servers including:
    - External authoritative servers used by customers to access the CSO
    - Internal recursive servers used to access domains outside the boundary
    - Note: Both of these should support DNSSEC

Data Flow Diagrams (DFD)

The Data Flow Diagrams should address all components reflected in the ABD. At a minimum, SSPs should include diagrams for the following logical data flows:

- Customer User and Customer Admin Authentication, including type of Multifactor Authentication (MFA)
- CSP Administrative and Support Personnel Authentication, including type of MFA
- System Application Data Flow within the Authorization Boundary
- System Application Data Flow to/from:
    - External Services, including corporate shared services
    - Interconnected Systems
    - Alternate Processing Sites and Backup Storage
    - Dev/Test environment

Each DFD should explicitly identify:

- Everywhere (internal & external) federal data and metadata **at rest** and **in transit** is not protected through encryption,
- Everywhere data is protected through encryption, and
- Whether or not the encryption using FIPS-validated cryptographic modules.
    - NOTE: FIPS validation applies to cryptographic modules, not protocols (e.g., TLS). The cryptographic module that sets up the TLS tunnel must be FIPS validated.

Security control SC-28 requires the use of cryptographic mechanisms to protect data at rest.
Security control SC-8(1) requires the use of cryptographic mechanisms to protect data in transit.
Security control SC-13 requires the use of FIPS-validated cryptography.

Common quality issues for data flow diagrams include:

- Does not depict all access by all parties (e.g., CSP admins, Agency customers, IaaS/PaaS portal)
- Does not indicate MFA tool and protocol (OTP, push, etc.) employed for administrative/support personnel and customers
- Lacks port and protocol information
- Does not indicate encryption of data in transit and data at rest
- Does not indicate use of FIPS-validated cryptography
- Fails to include internal flows such as to data stores, or within a microservices environment
- Fails to address address replication of data to alternate processing site, or to backup storage
- Does not include a legend

Appendix B: Frequently Asked Questions

What is an authorization boundary and why is it important?

The authorization boundary is the foundation on which the remainder of a system security plan is built.

Historically, NIST has used the terms authorization boundary and system boundary interchangeably. In the interest of clarity, accuracy, and use of standardized terminology, 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)." *(NIST SP 800-37r2 p15)*

Before implementing and documenting security controls, CSPs must clearly define the authorization boundary for the CSO. The Authorization Boundary Diagram (ABD) is a visual representation of the components that make up the system services, and devices of the CSO. The ABD provides the Authorizing Official (AO) and/or the Joint Authorization Board (JAB) with a clear understanding of what, exactly, is being secured, tested, and then authorized.

To help AOs/JAB understand areas that may require risk-acceptance or areas where the agency has responsibility (that is, everything excluded from the authorization boundary), the ABD should also depict:

External systems/services that provide functionality to the CSO or are used to manage and operate the CSO. This includes underlying IaaS/PaaS offerings, system interconnections, APIs, external cloud services, and corporate shared services that process federal data or direct federal metadata. If laptops do not take advantage of jump hosts and will process or store federal data or metadata they must be included in the boundary.

System components, services, or devices that reside in the customer's environment may be in boundary, or out.

For example, many CSPs require customers to authenticate via an agency-provided IdP. This should be depicted as out-of-boundary on the ABD.

On the other hand, often CSPs provide components as part of the offering that run in the customer's environment, such as data collectors, clients or agents. These components should be included in scope for 3PAO testing and included in-boundary.

In short, every tool, service, or component that is mentioned in the system security plan should appear on the ABD, and all components provided by the CSP should be tested by the 3PAO and shown in the boundary diagram.

AOs should carefully review the authorization boundary for the CSO to understand areas that require risk-acceptance and areas where the agency is responsible for implementing, managing, and monitoring security controls.

At a minimum, authorization boundary diagrams should:

- Include a clearly defined authorization boundary,
- Include system interconnections used to operate and support the intended mission/business functions,
- Depict every tool, service, or component that is mentioned in the SSP narrative, and controls,
- Identify those depicted tools, services, or components as either external or internal to the boundary,
- Identify all interconnected systems, and whether they are FedRAMP authorized (or not),

- Depict how CSP and Customer/Agency access the service (e.g., authentication used to access service),
- Depict all major software/virtual components (or groups of) within the boundary,
- Be validated against the inventory,
- Show alternate processing site, and
- Show pulling of updates from external services, such as OS, and antivirus updates.

Does a system that stores or processes federal data/metadata or sensitive system data, but is not directly connected to the boundary, need to be identified as an external system and/or service?

Yes. The authorization boundary diagram and description must include any external system or service that contains federal data/metadata or sensitive data about the CSO). In addition, every tool, service, or component that is mentioned in the system security plan and excluded from testing should be evaluated as an external service. For example, an external ticketing system that is used to capture and track system vulnerabilities may not be directly connected to the CSO, but still contains sensitive data that could impact the CIA of the CSO. These types of external systems and services must be disclosed to the Authorizing Official. They must be depicted on the authorization boundary diagram and described in the authorization package deliverables (SSP, SAP, SAR) or Readiness Assessment Report (for CSPs pursuing a FedRAMP Ready designation).

Agencies play a critical role in working with CSPs to define the authorization boundary. There could be cases where there are shared components or Agencies responsible for correctly configuring and security end-point components, etc. FedRAMP strongly advises that all agencies understand:

1. The risk accepted security posture by prior agencies that have authorized a given cloud product
2. Authorization boundary (components that are within the boundary and excluded from the boundary)
3. Data flows/traffic flows and associated federal information - internal, external, and crossing the boundary
4. Third party external services
5. Testing status of components in the CSP's corporate environment
6. CSP-provided components that are installed in the customer environment

How does FedRAMP define "corporate" services?

Corporate services are a subset of external services. Corporate services are operated and managed by the CSP and are used to support daily business operations. Cloud services used to support the Corporate environment are not considered “Corporate services,” since they are not under the full control of the CSP; such services are external cloud services. Corporate services exist outside of the CSO authorization boundary and do not contain any information that would impact the CIA of the CSO or federal data.

Corporate services that support a FedRAMP boundary environment must be depicted on authorization boundary and data flow diagrams and described in the SSP as external systems or services, and risks associated with connections to corporate systems or services should likewise be described in 3PAO assessment results (SAR or RAR).

What should 3PAOs keep in mind when assessing external services?

Generally, JAB systems can only leverage external services that are also FedRAMP Authorized at the same (or higher) security baseline as the leveraging service. High Baseline systems should only leverage other FedRAMP JAB systems authorized at the High Baseline. Moderate JAB systems should only leverage Moderate or High Baseline JAB external systems. There may be flexibility with FedRAMP agency systems, though. The agency authorization official (AO) may be willing to accept the risk associated with permitting external systems that are not yet FedRAMP Authorized which is why it is crucial that they are documented correctly.

3PAOs should confirm that the CSP has properly identified every tool, service, or component that is mentioned in the system security plan, and excluded from testing as an external service.

3PAOs should identify the external systems that are leveraged, but not authorized, as a finding and list it among “Remaining Risks” for the system.

Appendix C: Data Type Use Cases

The table below provides a list of data types and how they are categorized. This is a representative list and should not be considered fully comprehensive.

Data Type	Inside FedRAMP Authorization Boundary	Corporate Environment (repository & ticketing system)	External non-FedRAMP authorized Services
Vulnerability Scan Data	X	X	
POA&Ms	X	X	
Documentation (e.g. SSP, IRP, etc.)	X	X	
System Logs (e.g. Security logs, etc.)	X		
Configuration data	X		
Service tickets	X	X	
Incident response tickets	X	X	
Change Control tickets	X	X	
Access & Identity Management data	X		
IP addresses data	X		
MAC Addresses data	X		
Host/Server Names data	X		
Protocol use data	X		
Port use data	X		
Firewall rules data	X		
Billing data	X	X	X
Health and monitoring	X	X	X
DNS data	X		
Key management data	X		

Corporate account provisioning data		X	X
Corporate identity proofing data		X	X
FedRAMP MFA data	X	X	
Corporate MFA data		X	
RTM Technical data	X		
Operating System and software version information	X		
Software inventory list	X	X	
Hardware inventory list	X	X	
MFA Pin Generator	X	X	
High Repositories	X	X	X