A FEDRAMP AUTHORIZATION BOUNDARY

PURPOSE: The purpose of this document is to provide Cloud Service Providers (CSPs) further 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 accounts for all federal information, data, and metadata that flows through a CSO. 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 will act as a "living document," evolving with changes to cloud computing technology and federal information security policy relevant to FedRAMP.

KEY CONCEPTS

The concepts below provide an overview of various terms and definitions outlined in NIST SP 800-37 and OMB A-130 and provide guidance from the FedRAMP PMO.

1 Defining Your Authorization Boundary in the Cloud

Federal Definition: OMB A-130 defines an authorization boundary as "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."

FedRAMP Guidance: An authorization boundary for cloud technologies should describe a cloud system's internal components and connections to external services and systems. The authorization boundary accounts for the flow of all federal information and metadata through the system. A cloud authorization boundary illustrates a CSP's scope of control over the system as well as any system components or services that are leveraged from external services or controlled by the customer.

2 Federal Information (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 *(see Key Concept #3)*.

3 Metadata Associated with 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: Metadata associated with cloud environments typically fall into two buckets:

1. Data that describes or gives information about data populated by a federal customer that is associated with customer tenant activity logs and xml/script files, derived from customer data inputs
2. Information that could impact the system's confidentiality, integrity, or availability (CIA) included in logs, audit trails, and vulnerability reports

Metadata should be accounted for, adequately protected, and documented by the CSP within applicable FedRAMP deliverables.

4 Interconnections in the Cloud

Federal Definition: Per NIST SP 800-47 Rev 1, an interconnection is defined as "the direct connection of two or more IT systems for the purpose of sharing data and other information resources."

Update: NIST is in the process of updating this definition to include information exchange. The release date is tentatively scheduled for summer 2018.

FedRAMP Guidance: Interconnections are heavily reviewed by Agency Authorizing Officials (AOs) to ensure that wherever federal data and metadata may reside in the system, it is adequately protected. Cloud technologies utilize interconnections, Application Programming Interfaces (APIs), and other synchronous/asynchronous connections that potentially transmit federal data and metadata. It is imperative that these connections, and any potential risk to federal information, are disclosed to the AO via the FedRAMP deliverables.

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 leveraging systems, components, and services from external services that are not directly controlled by the vendor pursuing a FedRAMP authorization. The CSP must clearly communicate these external services to the AO and the extent to which federal information (data) can be impacted by the use of these services. CSPs should make sure their FedRAMP Authorization Package (System Security Plan [SSP], Security Assessment Plan [SAP], Security Assessment Report [SAR], etc.) reflects this information.

Item of Note: External services may or may not have a pre-existing FedRAMP Authorization.

Item of Note: External services that impact the CIA of federal information must be included within the CSO's authorization boundary.

6 Leveraging External Services with a FedRAMP Authorization

Federal Definition: Taking the concept of external services one step further, if a CSO is utilizing an external service that has a FedRAMP Authorization, the CSP may demonstrate compliance with various FedRAMP/NIST SP 800-53 control requirements by leveraging these capabilities from another provider. CSPs must reflect this relationship within the FedRAMP Authorization Package (SSP, Control Implementation Summary [CIS], etc.).

Item of Note: Leveraged services are a subcategory of external services, see above, and have a pre-existing FedRAMP Authorization.

7 Corporate Services

FedRAMP Guidance: Corporate services are a subset of external services. Corporate services are services used by a CSP to support their daily business operations and exist outside of the CSO authorization boundary. These services also do not contain any information that would impact the CIA of the CSO.

GUIDING PRINCIPLES

The authorization boundary is one of the most critical concepts to grasp and document. CSPs should review this information for additional clarity.

An authorization boundary is integral to a CSP's SSP and must describe components of an information system that process, store, or transmit federal information, and it must be illustrated accurately.

IN BOUNDARY

The following are "Rules of Thumb" associated with the system components that are **included within an authorization boundary**:

RULE OF THUMB #1: Federal information that is processed, stored, or transmitted by or for the Federal Government, in any medium or form

CSPs are expected to conduct their own due diligence when defining their FedRAMP authorization boundary to identify any other contexts where they store, process, or transmit federal information on behalf of a federal customer outside of the concept of "customer-populated data" or "tenant data."

The authorization boundary should clearly delineate between internal and external services within the CSP's scope of control over the CSO, services that are leveraged from an external provider, and the scope of control of anticipated customer authorization boundaries within the CSO. The CSP must make the authorization boundary transparent to the Third Party Assessment Organization (3PAO) and the AO. The FedRAMP requirements (documentation, testing, continuous monitoring, etc.) apply to all system components that are outlined within the authorization boundary.

RULE OF THUMB #2: External services that impact the CIA of federal information

Any external service that contains federal information or metadata that affects the CIA of federal information within a CSO must be depicted within the boundary. The CIA impact level of a CSO is commensurate with a federal customer's required impact level of the data being placed within the CSO as defined by FIPS 199.

All external services must be made transparent to the AO as well as the potential impacts to federal information. If the CIA of federal information is impacted by the use of external services, the services must be included within the CSO authorization boundary. These external services (if they don't have a standalone FedRAMP ATO) must have an appropriate scope of assessment as determined by the AO's risk tolerance.

Examples of external services that could impact the CIA of the cloud system security posture:

- An IaaS that a PaaS or SaaS resides upon
- An API that calls data from an external source
- A system that provides functionality such as audit logging, vulnerability scanning, or ticketing systems

Data elements such as vulnerability data, incident management reporting, customer intellectual property, or customer system descriptors all impact the CIA of a system and would fall under this rule of thumb. The impact level of these data elements might be at the same level as the CSO offering itself, or may be lower depending on the FIPS 199 analysis of the data.

As a note, historically, some CSPs have described many services that provide additional functionality for a system (such as those previously mentioned) as corporate services and external to the authorization boundary. This is ***not*** correct and those services would fall under this rule of thumb.

OUT OF BOUNDARY

The following are "Rules of Thumb" associated with the system components that are typically **outside of an authorization boundary**:

RULE OF THUMB #3: Corporate services that do not affect the CIA of federal information

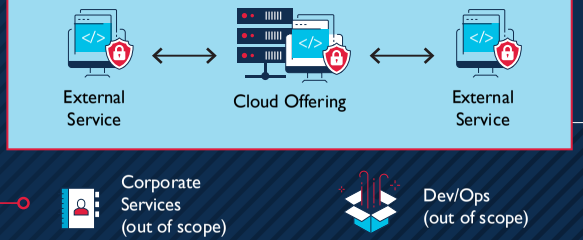
A CSP may utilize corporate services *(see Key Concept #7)*, such as customer relationship, ticketing, billing systems, etc. as part of normal business operations. If data that is being transmitted to these corporate services does not affect the CIA of federal information *(see Key Concept #2)*, these services may be excluded from the authorization boundary. Corporate services do not provide any functionality to the CSO.

An example of corporate services outside the authorization boundary is a Customer Relationship Management (CRM) system that includes data pertaining to customer relationships only (e.g., that potential or current customer meetings occurred, customer preferences, etc.).

CSPs must be careful ***how*** they use corporate services. For example, if a CSP's employee relays vulnerability information via corporate email, then that email system would then have metadata that could impact the CIA of CSO. This would mean the CSP's corporate email would fall within *Rule of Thumb #2* and need to be within the authorization boundary.

RULE OF THUMB #4: Development environments that do not process, store, or transmit federal information

A CSP may utilize "development environments" that are used to design, develop, test, and deliver software/code to end users. Development environments may be considered outside the authorization boundary if there is no federal information within this environment *(see Key Concept #2)*. If interconnections *(see Key Concept #4)* exist between the development environment and the CSO's authorization boundary, they must be transparent and provided to the AO for review and risk acceptance. Depending on the federal information exchange between the development environment and CSO authorization boundary, an AO could request the development environment be included within the authorization boundary and the scope of FedRAMP requirements would apply.



ADDITIONAL CONSIDERATIONS

Agency-Specific Security Requirements

FedRAMP provides a baseline from which CSPs and Agencies can define their desired security posture according to FISMA requirements and NIST security categorizations. While the FedRAMP PMO considers its baseline to be comprehensive per impact levels, Federal Agencies can 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.

The FedRAMP PMO 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 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.

HOW TO GET STARTED: Define and describe all system data flows and interconnections

The FedRAMP PMO has seen CSPs better illustrate their system boundary after depicting the various data flows through the system. As a best practice, CSPs should consider diagramming the following:

- Federal Customer User Authentication Logical Data Flow
- Administrative and Support Personnel User Authentication Logical Data Flow
- System Application Data Flow within the Proposed Cloud Authorization Boundary
- System Application Data Flow to All Leveraged and Interconnected Systems

Any questions or comments can be directed to info@fedramp.gov