FedRAMP FedRAMP Definitions

- **Release:** 25.11A
- **Published:** 2025-11-08
- **Designator:** FRD
- **Description:** Added FRD-ALL-40 (definition of incident) to support the 20x Incident Communications Procedures.

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-06-01** for **20x Phase One Pilot**.
  - These definitions apply to all FedRAMP 20x documents, standards, requirements, and other materials.
- **FedRAMP Rev5**:
  - This release is effective **2025-06-01** for **Rev5 Balance Improvement Releases**.
  - These definitions apply to all FedRAMP Rev5 documents, standard, requirements, and other materials that have been included in updates to Rev5 in a Balance Improvement Release.

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

- FedRAMP Authorization Act (44 USC § 3608) requires that the Administrator of the General Services Administration shall "establish a Government- wide program that provides a standardized, reusable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies"

Purpose

This document consolidates formal FedRAMP definitions for terms used in FedRAMP standards.

Expected Outcomes

- All stakeholders will have a common understanding of key terms used in FedRAMP standards.

Definitions

FRD-ALL-01

> **Federal Customer Data**: All electronic information, content, and materials that an *agency* or its authorized users upload, store, or otherwise provide to a cloud service for processing or storage. This does NOT include account information, service metadata, analytics, telemetry, or other similar metadata generated by the cloud service provider.
>
> *Note: In the context of FedRAMP authorization, "federal customer data" ONLY ever refers to data owned by federal agency customers. Agreements and contracts with specific _agencies* may require providers to protect additional data or even transfer ownshership of telemetry or usage data to the *agency*; always consult a lawyer that is familiar with company agreements and contracts when determining the scope of federal customer data._

FRD-ALL-02

> **Information Resource**: Has the meaning from 44 USC § 3502 (6): "information and related resources, such as personnel, equipment, funds, and information technology."
>
> *Note: This applies to any aspect of the _cloud service offering*, both technical and managerial, including everything that makes up the business of the offering from organizational policies and procedures to hardware, software, and code._
>
> *Reference: 44 USC § 3502 (6)*

FRD-ALL-03

> **Handle**: Has the plain language meaning inclusive of any possible action taken with information, such as access, collect, control, create, display, disclose, disseminate, dispose, maintain, manipulate, process, receive, review, store, transmit, use... etc.

FRD-ALL-04

> **Likely**: A reasonable degree of probability based on context.

FRD-ALL-05

> **Third-party Information Resource**: Any *information resource* that is not entirely included in the assessment for the *cloud service offering* seeking authorization.

FRD-ALL-06

> **Cloud Service Offering**: A specific, packaged cloud computing product or service provided by a cloud service provider that can be used by a customer. FedRAMP assessment and authorization of the cloud computing product or service is based on the Minimum Assessment Standard.

FRD-ALL-07

> **Regularly**: Performing the activity on a consistent, predictable, and repeated basis, at set intervals, automatically if possible, following a documented plan. These intervals may vary as appropriate between different requirements.

FRD-ALL-08

> **Significant change**: Has the meaning given in NIST SP 800-37 Rev. 2 which is "a change that is *likely* to substantively affect the security or privacy posture of a system."
>
> *Reference: NIST SP 800-37 Rev. 2*

FRD-ALL-09

> **Routine Recurring**: The type of *significant change* that *regularly* and routinely recurs as part of ongoing operations, vulnerability mitigation, or vulnerability remediation.

FRD-ALL-10

> **Adaptive**: The type of *significant change* that does not routinely recur but does not introduce substantive potential security risks that need to be assessed in depth.
>
> *Note: Adaptive changes typically require careful planning that focuses on engineering execution instead of customer adoption, can be verified with minor changes to existing automated validation procedures, and do not require large changes to operational procedures, deployment plans, or documentation.*

FRD-ALL-11

> **Transformative**: The type of *significant change* that introduces substantive potential security risks that are *likely* to affect existing risk determinations and must be assessed in depth.
>
> *Note: Transformative changes typically introduce major features or capabilities that may change how a customer uses the service (in whole or in part) and require extensive updates to security assessments, operational procedures, deployment plans, and documentation.*

FRD-ALL-12

> **Impact Categorization**: The type of *significant change* that is *likely* to increase or decrease the impact level categorization for the entire cloud service offering (e.g. from low to moderate or from high to moderate).

FRD-ALL-13

> **Interim Requirement**: A temporary requirement included as part of a FedRAMP Pilot or Beta Test that will *likely* be replaced, updated, or removed prior to the formal wide release of the requirement.

FRD-ALL-14

> **Authorization Package**: Has meaning from 44 USC § 3607 (b)(8) which is "the essential information that can be used by an agency to determine whether to authorize the operation of an information system or the use of a designated set of common controls for all cloud computing products and services authorized by FedRAMP."
>
> *Note: In FedRAMP documentation, _authorization package* always refers to a FedRAMP *authorization package* unless otherwise specified._
>
> *Reference: 44 USC § 3607 (b)(8)*

FRD-ALL-15

> **Authorization data**: The collective information required by FedRAMP for initial and ongoing assessment and authorization of a *cloud service offering*, including the *authorization package*.
>
> *Note: In FedRAMP documentation, _authorization data* always refers to FedRAMP *authorization data* unless otherwise specified._

FRD-ALL-16

> **Trust Center**: A secure repository or service used by cloud service providers to store and share *authorization data*. *Trust centers* are the complete and definitive source for *authorization data* and must meet the requirements outlined in the FedRAMP *authorization data* Sharing Standard to be FedRAMP-compatible.

> *Note: In FedRAMP documentation, all references to _trust centers* indicate FedRAMP-compatible *trust centers* unless otherwise specified._

FRD-ALL-17

> **Machine-Readable**: Has the meaning from 44 U.S. Code § 3502 (18) which is "the term "*machine-readable*", when used with respect to data, means data in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost"
>
> *Reference: 44 U.S. Code § 3502 (18)*

FRD-ALL-18

> **All Necessary Parties**: All entities whose interests are affected directly by activity related to a specific *cloud service offering* in the context of a FedRAMP authorization. This always includes FedRAMP and any *agency* customer who is operating the *cloud service offering*, but may include additional parties depending on agreements made by the cloud service provider (such as consultants or third-party assessors). Potential *agency* customers or third-party cloud service providers should also be included in most cases but this is not a mandatory requirement under FedRAMP as ultimately the cloud service provider may choose who they wish to do business with.

FRD-ALL-19

> **Agency**: Has the meaning given in 44 U.S. Code § 3502 (1), which is "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include—(A) the Government Accountability Office; (B) Federal Election Commission; (C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities."
>
> *Reference: 44 U.S. Code § 3502 (1)*

FRD-ALL-20

> **Vulnerability**: Has the meaning given to "security vulnerability" in 6 USC § 650 (25), which is "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of [...] management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information." This includes gaps in Rev5 controls and 20x Key Security Indicators, software vulnerabilities, misconfigurations, exposures, weak credentials, insecure services, and all other such potential weaknesses in protection (intentional or unintentional).
>
> *Reference: 6 USC § 650 (25)*

FRD-ALL-21

> **Vulnerability Detection**: The systematic process of discovering and identifying security vulnerabilities in *information resources* through assessment, scanning, threat intelligence, vulnerability disclosure mechanisms, bug bounties, supply chain monitoring, and other capabilities. This process includes the initial discovery of a *vulnerability's* existence and the determination of affected *information resources* within a *cloud service offering*.
>
> *Note: This definition applies to other forms such as "detect vulnerabilities" or simply "detection" / "detected" used in FedRAMP materials.*

FRD-ALL-22

> **Vulnerability Response**: The systematic process of tracking, evaluating, mitigating, monitoring, remediating, assessing exploitation, reporting, and otherwise managing *detected vulnerabilities*.

> *Note: This definition applies to other forms such as "respond to vulnerabilities" or simply "response" / "responded" used in FedRAMP materials.*

FRD-ALL-23

> **Likely Exploitable Vulnerability (LEV)**: A vulnerability that is not *fully mitigated*, AND is reachable by a *likely* threat actor, AND a *likely* threat actor with knowledge of the *vulnerability* would likely be able to gain unauthorized access, cause harm, disrupt operations, or otherwise have an undesired adverse impact within the *cloud service offering* by exploiting the *vulnerability*.
>
> *Notes:*
>
> - *The opposite of this is a "Not Likely Exploitable Vulnerability" (NLEV).*
> - *At the absolute minimum, any _vulnerability* that an automated unauthenticated system can exploit over the internet is a *likely exploitable vulnerability._*

FRD-ALL-24

> **Internet-Reachable Vulnerability (IRV)**: A *vulnerability* in a machine-based *information resource* that might be exploited or otherwise triggered by a payload originating from a source on the public internet; this includes machine-based *information resources* that have no direct route to/from the internet but receive payloads or otherwise take action triggered by internet activity.
>
> *Notes:*
>
> - *The opposite of this is a "Not Internet-reachable Vulnerability" (NIRV).*
> - *Internet-reachability applies only to the specific vulnerable machine-based _information resources* processing the payload; please review the relevant FedRAMP technical assistance on *internet-reachable vulnerabilities* for examples._

FRD-ALL-25

> **Known Exploited Vulnerability (KEV)**: Has the meaning given in CISA Binding Operational Directive 22-01, which is any *vulnerability* identified in CISA's Known Exploited Vulnerabilities catalog.
>
> *Reference: CISA BOD 22-01*

FRD-ALL-26

> **Remediated Vulnerability**: A *vulnerability* that has been neutralized or eliminated and is no longer *detected*.

FRD-ALL-27

> **Partially Mitigated Vulnerability**: A *vulnerability* where the likelihood or *potential adverse impact* of exploitation has been reduced from the original evaluation but the risk of exploitation still exists and the *vulnerability* is still *detected*.

FRD-ALL-28

> **Fully Mitigated Vulnerability**: A *vulnerability* where the likelihood of exploitation or *potential adverse impact* of exploitation has been reduced from the original evaluation until either are negligible, but the *vulnerability* is still *detected*.

FRD-ALL-29

> **False Positive Vulnerability**: A *detected vulnerability* that is not actually present in an exploitable state in the *information resource*; this includes situations where vulnerable software or code exist on an machine-based *information resource* but are not loaded, running, or otherwise in an operating state required for exploitation.

> *Note: This only applies if the _vulnerability* is not and was not present; a *remediated vulnerability* or a *fully mitigated vulnerability* cannot also be a *false positive vulnerability*._

FRD-ALL-30

> **Overdue Vulnerability**: A *vulnerability* that the provider intends to *fully mitigate* or *remediate* but has not or will not do so within the time frames recommended or required by FedRAMP.

FRD-ALL-31

> **Accepted Vulnerability**: A *vulnerability* that the provider does not intend to *fully mitigate* or *remediate*, OR that has not or will not be *fully mitigated* or *remediated* within the maximum overdue period recommended or required by FedRAMP.

FRD-ALL-32

> **Catastrophic Adverse Effect**: A severe negative impact on an organization caused by the loss of confidentiality, integrity, or availability of its information. At a minimum, this includes effects that would *likely*: (i) result in a severe degradation in the availability or performance of services within the *cloud service offering* for 24+ hours; OR (ii) directly or indirectly result in unauthorized access, disclosure, or modification of a majority of the *federal customer data* stored within the *cloud service offering*.

FRD-ALL-33

> **Serious Adverse Effect**: A significant negative impact on an organization caused by the loss of confidentiality, integrity, or availability of its information. At a minimum, this includes effects that would likely: (i) result in intermittent or ongoing degradation in the availability or performance of services within the *cloud service offering*, causing unpredictable interruptions to operations for 12+ hours; OR (ii) directly or indirectly result in unauthorized access, disclosure, or modification of a minority of the *federal customer data* stored within the *cloud service offering*.

FRD-ALL-34

> **Limited Adverse Effect**: A minor negative impact on an organization caused by the loss of confidentiality, integrity, or availability of its information. At a minimum, this includes effects that would likely: (i) result in degradation of the availability or performance of services within the *cloud service offering* for a minority of relevant users; OR (ii) directly or indirectly result in unauthorized access, disclosure, or modification of a small amount of the *federal customer data* stored within the *cloud service offering* by only a few relevant users.

FRD-ALL-35

> **Negligible Adverse Effect**: A small negative impact on an organization caused by the loss of confidentiality, integrity, or availability of its information. At a minimum, this includes effects that would likely: (i) result in minor inconvenience when accessing or using services within the *cloud service offering*; OR (ii) result in degradation of the availability or performance of services within the *cloud service offering* for only a few relevant users.

FRD-ALL-36

> **Potential Adverse Impact (of vulnerability exploitation)**: The estimated cumulative effect of unauthorized access, disruption, harm, or other adverse impact to agencies that *likely* could result if a threat actor exploits a *vulnerability* in the *cloud service offering*; as estimated following FedRAMP recommendations and requirements.

FRD-ALL-37

> **Promptly**: Without Unnecessary Delay.
>
> *Note: The use of _promptly* in FedRAMP materials frames conveys a need for urgent action where the expected time frame will vary by circumstance but earlier action is more likely to improve security outcomes and increase the

> security posture of a *cloud service offering*._

FRD-ALL-38

> **Persistently**: Occurring in a firm, steady way that is repeated over a long period of time in spite of obstacles or difficulties. Persistent activities may vary between actors, may occur irregularly, and may include interruptions or waiting periods between cycles. These attributes of persistent activities should be intentional, understood, and documented; the status of persistent activities will always be known.
>
> *Note: The use of _persistently* indicates a process that may not always occur continuously (without interruption or gaps) or regularly (on a consistent, predictable basis) but will repeat frequently in cycles. It aligns generally with historical misuse of "continuous" in federal information security policies._

FRD-ALL-39

> **Drift**: Changes to *information resources* that cause deviations from the intended and assessed state; common forms of drift include changes to configurations, deployed software, privileges, running processes, and availability.