FedRAMP FedRAMP 20x All Impact Requirements

- **Release:** Untracked
- **Published:** 2025-10-20
- **Designator:** FRMR-ALL
- **Description:** FedRAMP 20x All Impact Requirements

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.

Requirements

FRR-ADS

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-ADS-01

Applies to: Low, Moderate, High

> Providers MUST publicly share up-to-date information about the *cloud service offering* in both human-readable and *machine-readable* formats, including at least:
>
> 1. Direct link to the FedRAMP Marketplace for the offering
> 2. Service Model
> 3. Deployment Model
> 4. Business Category

5. UEI Number
6. Contact Information
7. Overall Service Description
8. Detailed list of specific services and their impact levels (see FRR-ADS-03)
9. Summary of customer responsibilities and secure configuration guidance
10. Process for accessing information in the *trust center* (if applicable)
11. Availability status and recent disruptions for the *trust center* (if applicable)
12. Customer support information for the *trust center* (if applicable)

FRR-ADS-02

Applies to: Low, Moderate, High

> Providers MUST use automation to ensure information remains consistent between human-readable and *machine-readable* formats when *authorization data* is provided in both formats; Providers SHOULD generate human-readable and *machine-readable* data from the same source at the same time OR generate human-readable formats directly from *machine-readable* data.

FRR-ADS-03

Applies to: Low, Moderate, High

> Providers MUST share a detailed list of specific services and their impact levels that are included in the *cloud service offering* using clear feature or service names that align with standard public marketing materials; this list MUST be complete enough for a potential customer to determine which services are and are not included in the FedRAMP authorization without requesting access to underlying *authorization data*.

FRR-ADS-04

Applies to: Low, Moderate, High

> Providers MUST share *authorization data* with all necessary parties without interruption, including at least FedRAMP, CISA, and agency customers.

FRR-ADS-05

Applies to: Low, Moderate, High

> Providers MUST provide sufficient information in *authorization data* to support authorization decisions but SHOULD NOT include sensitive information that would *likely* enable a threat actor to gain unauthorized access, cause harm, disrupt operations, or otherwise have a negative adverse impact on the *cloud service offering*.

FRR-ADS-06

Applies to: Low, Moderate, High

> Providers of FedRAMP Rev5 Authorized *cloud service offerings* MUST share *authorization data* via the USDA Connect Community Portal UNLESS they use a FedRAMP-compatible *trust center*.

FRR-ADS-07

Applies to: Low, Moderate, High

> Providers of FedRAMP 20x Authorized *cloud service offerings* MUST use a FedRAMP-compatible *trust center* to store and share *authorization data* with all necessary parties.

FRR-ADS-08

Applies to: Low, Moderate, High

> Providers MUST notify all necessary parties when migrating to a *trust center* and MUST provide information in their existing USDA Connect Community Portal secure folders explaining how to use the *trust center* to obtain *authorization data*.

FRR-ADS-09

Applies to: Low, Moderate, High

> Providers MUST make historical versions of *authorization data* available for three years to all necessary parties UNLESS otherwise specified by applicable FedRAMP requirements; deltas between versions MAY be consolidated quarterly.

FRR-ADS-10

Applies to: Low, Moderate, High

> Providers SHOULD follow FedRAMP's best practices and technical assistance for sharing *authorization data* where applicable.

FRR-ADS-AC

These requirements for managing access apply to cloud service providers who establish FedRAMP-compatible *trust centers* for storing and sharing *authorization data*.

FRR-ADS-AC-01

Applies to: Low, Moderate, High

> Providers MUST publicly provide plain-language policies and guidance for all necessary parties that explains how they can obtain and manage access to *authorization data* stored in the *trust center*.

FRR-ADS-AC-02

Applies to: Low, Moderate, High

> Providers SHOULD share at least the *authorization package* with prospective agency customers upon request and MUST notify FedRAMP within five business days if a prospective agency customer request is denied.

FRR-ADS-TC

These requirements apply to FedRAMP-compatible *trust centers* used to store and share *authorization data*.

FRR-ADS-TC-01

Applies to: Low, Moderate, High

> *Trust centers* MUST be included as an *information resource* included in the *cloud service offering* for assessment if FRR-MAS-01 applies.

FRR-ADS-TC-02

Applies to: Low, Moderate, High

> *Trust centers* SHOULD make *authorization data* available to view and download in both human-readable and *machine-readable* formats

FRR-ADS-TC-03

Applies to: Low, Moderate, High

> *Trust centers* MUST provide documented programmatic access to all *authorization data*, including programmatic access to human-readable materials.

FRR-ADS-TC-04

Applies to: Low, Moderate, High

> *Trust centers* SHOULD include features that encourage all necessary parties to provision and manage access to *authorization data* for their users and services directly.

FRR-ADS-TC-05

Applies to: Low, Moderate, High

> *Trust centers* MUST maintain an inventory and history of federal agency users or systems with access to *authorization data* and MUST make this information available to FedRAMP without interruption.

FRR-ADS-TC-06

Applies to: Low, Moderate, High

> *Trust centers* MUST log access to *authorization data* and store summaries of access for at least six months; such information, as it pertains to specific parties, SHOULD be made available upon request by those parties.

FRR-ADS-TC-07

Applies to: Low, Moderate, High

> *Trust centers* SHOULD deliver responsive performance during normal operating conditions and minimize service disruptions.

FRR-ADS-EX

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

FRR-ADS-EX-01

Applies to: Low, Moderate, High

> Providers of FedRAMP Rev5 Authorized *cloud service offerings* at FedRAMP High using a legacy self-managed repository for *authorization data* MAY ignore the requirements in this standard until future notice.

FRR-SCN

These requirements apply ALWAYS to ALL *significant changes* based on current Effective Date(s) and Overall Applicability

FRR-SCN-01

Applies to: Low, Moderate, High

> Providers MUST notify all necessary parties when Significant Change Notifications are required, including at least FedRAMP and all agency customers. Providers MAY share Significant Change Notifications publicly or with other parties.

FRR-SCN-02

Applies to: Low, Moderate, High

> Providers MUST follow the procedures documented in their security plan to plan, evaluate, test, perform, assess, and document changes.

FRR-SCN-03

Applies to: Low, Moderate, High

> Providers MUST evaluate and type label all *significant changes*, then follow FedRAMP requirements for the type.

FRR-SCN-04

Applies to: Low, Moderate, High

> Providers MUST maintain auditable records of these activities and make them available to all necessary parties.

FRR-SCN-05

Applies to: Low, Moderate, High

> Providers MUST keep historical Significant Change Notifications available to all necessary parties at least until the service completes its next annual assessment.

FRR-SCN-06

Applies to: Low, Moderate, High

> All parties SHOULD follow FedRAMP's best practices and technical assistance on *significant change* assessment and notification where applicable.

FRR-SCN-07

Applies to: Low, Moderate, High

> Providers MAY notify necessary parties in a variety of ways as long as the mechanism for notification is clearly documented and easily accessible.

FRR-SCN-08

Applies to: Low, Moderate, High

> Providers MUST make ALL Significant Change Notifications and related audit records available in similar human-readable and compatible *machine-readable* formats.

FRR-SCN-09

Applies to: Low, Moderate, High

> Providers MUST include at least the following information in Significant Change Notifications:
>
> 1. Service Offering FedRAMP ID
> 2. 3PAO Name (if applicable)
> 3. Related POA&M (if applicable)
> 4. Significant Change type and explanation of categorization
> 5. Short description of change
> 6. Reason for change
> 7. Summary of customer impact, including changes to services and customer configuration responsibilities
> 8. Plan and timeline for the change, including for the verification, assessment, and/or validation of impacted Key Security Indicators or controls
> 9. Copy of the business or security impact analysis
> 10. Name and title of approver

FRR-SCN-10

Applies to: Low, Moderate, High

> Providers MAY include additional relevant information in Significant Change Notifications.

FRR-SCN-EX

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

FRR-SCN-EX-01

Applies to: Low, Moderate, High

> Providers MAY be required to delay *significant changes* beyond the standard Significant Change Notification period and/or submit *significant changes* for approval in advance as a condition of a formal FedRAMP Corrective Action Plan or other agreement.

FRR-SCN-EX-02

Applies to: Low, Moderate, High

> Providers MAY execute *significant changes* (including *transformative* changes) during an emergency or incident without meeting Significant Change Notification requirements in advance ONLY if absolutely necessary. In such emergencies, providers MUST follow all relevant procedures, notify all necessary parties, retroactively provide all Significant Change Notification materials, and complete appropriate assessment after the incident.

FRR-SCN-RR

These requirements apply ONLY to *significant changes* of type *routine recurring*.

FRR-SCN-RR-01

Applies to: Low, Moderate, High

> Providers SHOULD NOT make formal Significant Change Notifications for *routine recurring* changes; this type of change is exempted from the notification requirements of this standard.

FRR-SCN-AD

These requirements apply ONLY to *significant changes* of type *adaptive*.

FRR-SCN-AD-01

Applies to: Low, Moderate, High

> Providers MUST notify all necessary parties within ten business days after finishing *adaptive* changes, also including the following information:
>
> 1. Summary of any new risks identified and/or POA&Ms resulting from the change (if applicable)

FRR-SCN-TF

These requirements apply ONLY to *significant changes* of type *transformative*.

FRR-SCN-TF-01

Applies to: Low, Moderate, High

> Providers SHOULD engage a third-party assessor to review the scope and impact of the planned change before starting *transformative* changes if human validation is necessary. This review SHOULD be limited to security decisions that require human validation. Providers MUST document this decision and justification.

FRR-SCN-TF-02

Applies to: Low, Moderate, High

> Providers MUST notify all necessary parties of initial plans for *transformative* changes at least 30 business days before starting *transformative* changes.

FRR-SCN-TF-03

Applies to: Low, Moderate, High

> Providers MUST notify all necessary parties of final plans for *transformative* changes at least 10 business days before starting *transformative* changes.

FRR-SCN-TF-04

Applies to: Low, Moderate, High

> Providers MUST notify all necessary parties within 5 business days after finishing *transformative* changes, also including the following information:
>
> 1. Updates to all previously sent information

FRR-SCN-TF-05

Applies to: Low, Moderate, High

> Providers MUST notify all necessary parties within 5 business days after completing the verification, assessment, and/or validation of *transformative* changes, also including the following information:
>
> 1. Updates to all previously sent information
> 2. Summary of any new risks identified and/or POA&Ms resulting from the change (if applicable)
> 3. Copy of the security assessment report (if applicable)

FRR-SCN-TF-06

Applies to: Low, Moderate, High

> Providers MUST publish updated service documentation and other materials to reflect *transformative* changes within 30 business days after finishing *transformative* changes.

FRR-SCN-TF-07

Applies to: Low, Moderate, High

> Providers MUST allow agency customers to OPT OUT of *transformative* changes whenever feasible.

FRR-SCN-IM

These requirements apply ONLY to *significant changes* of type *impact categorization*.

FRR-SCN-IM-01

Applies to: Low, Moderate, High

> Providers MUST follow the legacy Significant Change Request process or full re-authorization for *impact categorization* changes, with advance approval from an identified lead agency, until further notice.

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.

FRR-VDR

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-VDR-01

Applies to: Low, Moderate, High

> Providers MUST systematically, *persistently*, and *promptly* discover and identify *vulnerabilities* within their *cloud service offering* using appropriate techniques such as assessment, scanning, threat intelligence, vulnerability disclosure mechanisms, bug bounties, supply chain monitoring, and other relevant capabilities; this process is called *vulnerability detection*.

FRR-VDR-02

Applies to: Low, Moderate, High

> Providers MUST systematically, *persistently*, and *promptly* track, evaluate, monitor, *mitigate*, *remediate*, assess exploitation of, report, and otherwise manage all detected vulnerabilities within their *cloud service offering*; this

> process is called *vulnerability response*.

FRR-VDR-03

Applies to: Low, Moderate, High

> Providers MUST follow the requirements and recommendations outlined in FRR-VDR-TF regarding timeframes for *vulnerability detection* and *response*.
>
> *Note: Providers are strongly encouraged to build programs that consistently exceed these thresholds. Performance will be measured by FedRAMP for comparison between providers and scoring within the FedRAMP Marketplace.*

FRR-VDR-04

Applies to: Low, Moderate, High

> Providers MAY sample effectively identical *information resources*, especially machine-based *information resources*, when performing *vulnerability detection* UNLESS doing so would decrease the efficiency or effectiveness of *vulnerability detection*.

FRR-VDR-05

Applies to: Low, Moderate, High

> Providers SHOULD evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to identify logical groupings of affected *information resources* that may improve the efficiency and effectiveness of *vulnerability response* by consolidating further activity; requirements and recommendations in this standard are then applied to these consolidated groupings of *vulnerabilities* instead of each individual detected instance.

FRR-VDR-06

Applies to: Low, Moderate, High

> Providers SHOULD evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to determine if they are *false positive vulnerabilities*.

FRR-VDR-07

Applies to: Low, Moderate, High

> Providers MUST evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to determine if they are *likely exploitable vulnerabilities*.

FRR-VDR-08

Applies to: Low, Moderate, High

> Providers MUST evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to determine if they are *internet-reachable vulnerabilities*.

FRR-VDR-09

Applies to: Low, Moderate, High

> Providers MUST evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to estimate the *potential adverse impact* of exploitation on government customers AND assign one of the following *potential adverse impact* ratings:

> - **N1**: Exploitation could be expected to have *negligible adverse effects* on one or more *agencies* that use the *cloud service offering*.
> - **N2**: Exploitation could be expected to have *limited adverse effects* on one or more *agencies* that use the *cloud service offering*.
> - **N3**: Exploitation could be expected to have a *serious adverse effect* on one *agency* that uses the *cloud service offering*.
> - **N4**: Exploitation could be expected to have a *catastrophic adverse effect* on one *agency* that uses the *cloud service offering* OR a *serious adverse effect* on more than one federal agency that uses the *cloud service offering*.
> - **N5**: Exploitation could be expected to have a *catastrophic adverse effect* on more than one *agency* that uses the *cloud service offering*.

FRR-VDR-10

Applies to: Low, Moderate, High

> Providers SHOULD consider at least the following factors when considering the context of the *cloud service offering* to evaluate *detected vulnerabilities*:
>
> 1. **Criticality**: How important are the systems or information that might be impacted by the *vulnerability*?
> 2. **Reachability**: How might a threat actor reach the *vulnerability* and how *likely* is that?
> 3. **Exploitability**: How easy is it for a threat actor to exploit the *vulnerability* and how *likely* is that?
> 4. **Detectability**: How easy is it for a threat actor to become aware of the *vulnerability* and how *likely* is that?
> 5. **Prevalence**: How much of the *cloud service offering* is affected by the *vulnerability*?
> 6. **Privilege**: How much privileged authority or access is granted or can be gained from exploiting the *vulnerability*?
> 7. **Proximate Vulnerabilities**: How does this *vulnerability* interact with previously *detected vulnerabilities*, especially *partially* or *fully mitigated vulnerabilities?*
> 8. **Known Threats**: How might already known threats leverage the *vulnerability* and how *likely* is that?

FRR-VDR-11

Applies to: Low, Moderate, High

> Providers MUST document the reason and resulting implications for their customers when choosing not to meet FedRAMP recommendations in this standard; this documentation MUST be included in the *authorization data* for the *cloud service offering*.

FRR-VDR-AY

This section provides guidance on the application of this standard, including recommendations for implementing high quality *vulnerability detection* and *response* programs; providers who follow some or all of these will be better positioned to meet future FedRAMP authorization requirements.

FRR-VDR-AY-01

Applies to: Low, Moderate, High

> If it is not possible to *fully mitigate* or *remediate detected vulnerabilities*, providers SHOULD instead *partially mitigate vulnerabilities promptly*, progressively, and *persistently*.

FRR-VDR-AY-02

Applies to: Low, Moderate, High

> Providers SHOULD make design and architecture decisions for their *cloud service offering* that mitigate the risk of *vulnerabilities* by default AND decrease the risk and complexity of *vulnerability detection* and *response*.

FRR-VDR-AY-03

Applies to: Low, Moderate, High

> Providers SHOULD use automated services to improve and streamline *vulnerability detection* and *response*.

FRR-VDR-AY-04

Applies to: Low, Moderate, High

> Providers SHOULD automatically perform *vulnerability detection* on representative samples of new or *significantly changed information resources*.

FRR-VDR-AY-05

Applies to: Low, Moderate, High

> Providers SHOULD NOT weaken the security of *information resources* to facilitate vulnerability scanning or assessment activities.

FRR-VDR-AY-06

Applies to: Low, Moderate, High

> Providers SHOULD NOT deploy or otherwise activate new machine-based *information resources* with *Known Exploited Vulnerabilities*.

FRR-VDR-RP

This section identifies FedRAMP-specific reporting requirements and recommendations for *vulnerabilities*.

FRR-VDR-RP-01

Applies to: Low, Moderate, High

> Providers MUST report *vulnerability detection* and *response* activity to all necessary parties *persistently*, summarizing ALL activity since the previous report; these reports are *authorization data* and are subject to the FedRAMP Authorization Data Sharing (ADS) standard.

FRR-VDR-RP-02

Applies to: Low, Moderate, High

> Providers SHOULD include high-level overviews of ALL *vulnerability detection* and *response* activities conducted during this period for the *cloud service offering;* this includes vulnerability disclosure programs, bug bounty programs, penetration testing, assessments, etc.

FRR-VDR-RP-03

Applies to: Low, Moderate, High

> Providers MUST NOT irresponsibly disclose specific sensitive information about *vulnerabilities* that would *likely* lead to exploitation, but MUST disclose sufficient information for informed risk-based decision-making to all necessary parties.
>
> *Note: See FRR-VDR-EX for exceptions to this requirement.*

FRR-VDR-RP-04

Applies to: Low, Moderate, High

> Providers MAY responsibly disclose *vulnerabilities* publicly or with other parties if the provider determines doing so will NOT *likely* lead to exploitation.

FRR-VDR-RP-05

Applies to: Low, Moderate, High

> Providers MUST include the following information (if applicable) on *detected vulnerabilities* when reporting on *vulnerability detection* and *response* activity, UNLESS it is an *accepted vulnerability*:
>
> 1. Provider's internally assigned tracking identifier
> 2. Time and source of the detection
> 3. Time of completed evaluation
> 4. Is it an *internet-reachable vulnerability* or not?
> 5. Is it a *likely exploitable vulnerability* or not?
> 6. Historically and currently estimated *potential adverse impact* of exploitation
> 7. Time and level of each completed and evaluated reduction in *potential adverse impact*
> 8. Estimated time and target level of next reduction in *potential adverse impact*
> 9. Is it currently or is it likely to become an *overdue vulnerability* or not? If so, explain.
> 10. Any supplementary information the provider responsibly determines will help federal agencies assess or mitigate the risk to their *federal customer data* within the *cloud service offering* resulting from the *vulnerability*
> 11. Final disposition of the *vulnerability*

FRR-VDR-RP-06

Applies to: Low, Moderate, High

> Providers MUST include the following information on *accepted vulnerabilities* when reporting on *vulnerability detection* and *response* activity:
>
> 1. Provider's internally assigned tracking identifier
> 2. Time and source of the detection
> 3. Time of completed evaluation
> 4. Is it an *internet-reachable vulnerability* or not?
> 5. Is it a *likely exploitable vulnerability* or not?
> 6. Currently estimated *potential adverse impact* of exploitation
> 7. Explanation of why this is an *accepted vulnerability*
> 8. Any supplementary information the provider determines will responsibly help federal agencies assess or mitigate the risk to their *federal customer data* within the *cloud service offering* resulting from the *accepted vulnerability*

FRR-VDR-EX

These exceptions MAY override some or all of the FedRAMP requirements and recommendations in this standard.

FRR-VDR-EX-01

Applies to: Low, Moderate, High

> Providers MAY be required to share additional *vulnerability* information, alternative reports, or to report at an alternative frequency as a condition of a FedRAMP Corrective Action Plan or other agreements with federal agencies.

FRR-VDR-EX-02

Applies to: Low, Moderate, High

> Providers MAY be required to provide additional information or details about *vulnerabilities*, including sensitive information that would *likely* lead to exploitation, as part of review, response or investigation by necessary parties.

FRR-VDR-EX-03

Applies to: Low, Moderate, High

> Providers MUST NOT use this standard to reject requests for additional information from necessary parties which also include law enforcement, Congress, and Inspectors General.

FRR-VDR-TF

This section provides guidance on timeframes that apply to all impact levels of FedRAMP authorization for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-VDR-TF-01

Applies to: Low, Moderate, High

> Providers MUST report *vulnerability detection* and *response* activity to all necessary parties in a consistent format that is human readable at least monthly.

FRR-VDR-TF-02

Applies to: Low, Moderate, High

> Providers SHOULD *remediate Known Exploited Vulnerabilities* according to the due dates in the CISA Known Exploited Vulnerabilities Catalog (even if the vulnerability has been *fully mitigated*) as required by CISA Binding Operational Directive (BOD) 22-01 or any successor guidance from CISA.

FRR-VDR-TF-03

Applies to: Low, Moderate, High

> Providers MUST categorize any vulnerability that is not or will not be *fully mitigated* or *remediated* within 192 days of evaluation as an *accepted vulnerability*.

FRR-VDR-TF-LO

This section provides guidance on timeframes that apply specifically to FedRAMP Low authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently

strive to exceed by significant margins.

FRR-VDR-TF-LO-01

Applies to: Low

> Providers SHOULD make all recent historical *vulnerability detection* and *response* activity available in a *machine-readable* format for automated retrieval by all necessary parties (e.g. using an API service or similar); this information SHOULD be updated *persistently*, at least once every month.

FRR-VDR-TF-LO-02

Applies to: Low

> Providers SHOULD *persistently* perform *vulnerability detection* on representative samples of similar machine-based *information resources*, at least once every week.

FRR-VDR-TF-LO-03

Applies to: Low

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are *likely* to *drift*, at least once every month.

FRR-VDR-TF-LO-04

Applies to: Low

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are NOT *likely* to *drift*, at least once every six months.

FRR-VDR-TF-LO-05

Applies to: Low

> Providers SHOULD evaluate ALL *vulnerabilities* as required by FRR-VDR-07, FRR-VDR-08, and FRR-VDR-09 within 7 days of *detection*.

FRR-VDR-TF-LO-06

Applies to: Low

> Providers SHOULD *partially mitigate, fully mitigate,* or *remediate vulnerabilities* to a lower *potential adverse impact* within the timeframes from evaluation shown below (in days), factoring for the current *potential adverse impact*, *internet reachability,* and *likely exploitability*:

Potential Adverse Impact	LEV + IRV	LEV + NIRV	NLEV
N5	4	8	32
N4	8	32	64
N3	32	64	192
N2	96	160	192

FRR-VDR-TF-LO-07

Applies to: Low

> Providers SHOULD *mitigate* or *remediate* remaining *vulnerabilities* during routine operations as determined necessary by the provider.

FRR-VDR-TF-MO

This section provides guidance on timeframes that apply specifically to FedRAMP Moderate authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-VDR-TF-MO-01

Applies to: Moderate

> Providers SHOULD make all recent historical *vulnerability detection* and *response* activity available in a *machine-readable* format for automated retrieval by all necessary parties (e.g. using an API service or similar); this information SHOULD be updated *persistently*, at least once every 14 days.

FRR-VDR-TF-MO-02

Applies to: Moderate

> Providers SHOULD *persistently* perform *vulnerability detection* on representative samples of similar machine-based *information resources*, at least once every 3 days.

FRR-VDR-TF-MO-03

Applies to: Moderate

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are *likely* to *drift*, at least once every 14 days.

FRR-VDR-TF-MO-04

Applies to: Moderate

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are NOT *likely* to *drift*, at least once per month.

FRR-VDR-TF-MO-05

Applies to: Moderate

> Providers SHOULD evaluate ALL *vulnerabilities* as required by FRR-VDR-07, FRR-VDR-08, and FRR-VDR-09 within 5 days of *detection*.

FRR-VDR-TF-MO-06

Applies to: Moderate

> Providers SHOULD treat *internet-reachable likely exploitable vulnerabilities* with a *potential adverse impact* of N4 or N5 as a security incident until they are *partially mitigated* to N3 or below.

FRR-VDR-TF-MO-07

Applies to: Moderate

> Providers SHOULD *partially mitigate, fully mitigate,* or *remediate vulnerabilities* to a lower *potential adverse impact* within the timeframes from evaluation shown below, factoring for the current *potential adverse impact*, *internet reachability,* and *likely exploitability*:

Potential Adverse Impact	LEV + IRV	LEV + NIRV	NLEV
N5	2	4	16
N4	4	8	64
N3	16	32	128
N2	48	128	192

FRR-VDR-TF-MO-08

Applies to: Moderate

> Providers SHOULD *mitigate* or *remediate* remaining *vulnerabilities* during routine operations as determined necessary by the provider.

FRR-VDR-TF-HI

This section provides guidance on timeframes that apply specifically to FedRAMP High authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-VDR-TF-HI-01

Applies to: High

> Providers SHOULD make all recent historical *vulnerability detection* and *response* activity available in a *machine-readable* format for automated retrieval by all necessary parties (e.g. using an API service or similar); this information SHOULD be updated *persistently*, at least once every 7 days.

FRR-VDR-TF-HI-02

Applies to: High

> Providers SHOULD *persistently* perform *vulnerability detection* on representative samples of similar machine-based *information resources*, at least once per day.

FRR-VDR-TF-HI-03

Applies to: High

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are *likely* to *drift*, at least once every 7 days.

FRR-VDR-TF-HI-04

Applies to: High

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are NOT *likely* to *drift*, at least once every month.

FRR-VDR-TF-HI-05

Applies to: High

> Providers SHOULD evaluate ALL *vulnerabilities* as required by FRR-VDR-07, FRR-VDR-08, and FRR-VDR-09 within 2 days of *detection*.

FRR-VDR-TF-HI-06

Applies to: High

> Providers SHOULD treat *internet-reachable likely exploitable vulnerabilities* with a *potential adverse impact* of N4 or N5 as a security incident until they are *partially mitigated* to N3 or below.

FRR-VDR-TF-HI-07

Applies to: High

> Providers SHOULD treat *likely exploitable vulnerabilities* that are NOT *internet-reachable* with a *potential adverse impact* of N5 as a security incident until they are partially mitigated to N4 or below.

FRR-VDR-TF-HI-08

Applies to: High

> Providers SHOULD *partially mitigate vulnerabilities* to a lower *potential adverse impact* within the maximum time-frames from evaluation shown below, factoring for the current *potential adverse impact*, *internet reachability,* and *likely exploitability*:

Potential Adverse Impact	LEV + IRV	LEV + NIRV	NLEV
N5	.5	1	8
N4	2	8	32
N3	8	16	64
N2	24	96	192

FRR-VDR-TF-HI-09

Applies to: High

> Providers SHOULD *mitigate* or *remediate* remaining *vulnerabilities* during routine operations as determined necessary by the provider.

FRR-VDR-AG

The section provides guidance for agencies that apply under 44 USC § 3613 (e) which states that the assessment and materials within a FedRAMP authorization package "shall be presumed adequate for use in an agency authorization to operate cloud computing products and services."

FRR-VDR-AG-01

Applies to: Low, Moderate, High

> Agencies SHOULD review the information provided in vulnerability reports at appropriate and reasonable intervals commensurate with the expectations and risk posture indicated by their Authorization to Operate, and SHOULD use automated processing and filtering of machine readable information from cloud service providers.
>
> *Note: FedRAMP recommends that agencies only review _overdue* and *accepted vulnerabilities* with a *potential adverse impact* of N3 or higher unless the cloud service provider recommends mitigations or the service is included in a higher risk federal information system. Furthermore, *accepted vulnerabilities* generally only need to be reviewed when they are added or during an updated risk assessment due to changes in the agency's use or authorization._

FRR-VDR-AG-02

Applies to: Low, Moderate, High

> Agencies SHOULD use *vulnerability* information reported by the Provider to maintain Plans of Action & Milestones for agency security programs when relevant according to agency security policies (such as if the agency takes action to mitigate the risk of exploitation or authorized the continued use of a cloud service with *accepted vulnerabilities* that put agency information systems at risk).

FRR-VDR-AG-03

Applies to: Low, Moderate, High

> Agencies SHOULD NOT request additional information from cloud service providers that is not required by this FedRAMP standard UNLESS the head of the agency or an authorized delegate makes a determination that there is a demonstrable need for such.
>
> *Note: This is related to the Presumption of Adequacy directed by 44 USC § 3613 (e).*

FRR-VDR-AG-04

Applies to: Low, Moderate, High

> Agencies MUST inform FedRAMP after requesting any additional *vulnerability* information or materials from a cloud service provider beyond those required by this policy by sending a notification to info@fedramp.gov.
>
> *Note: This is an OMB policy; agencies are required to notify FedRAMP in OMB Memorandum M-24-15 section IV (a).*

FRR-KSI

These requirements apply ALWAYS to ALL FedRAMP 20x authorizations based on the Effective Date(s) and Overall Applicability.

FRR-KSI-01

Applies to: Low, Moderate, High

> Cloud service providers MUST apply ALL Key Security Indicators to ALL aspects of their *cloud service offering* that are within the FedRAMP Minimum Assessment Scope.

FRR-KSI-02

Applies to: Low, Moderate, High

> All parties SHOULD follow FedRAMP's best practices and technical assistance on assessing Key Security Indicators where applicable.

FRR-KSI-03

Applies to: Low, Moderate, High

> All parties SHOULD continuously monitor and review materials in the FedRAMP 20x Phase One (20xP1) pilot requirements and the 20x Community Working Group. Additional details, interim best practices and technical assistance, answers to common questions, and more will be provided asynchronously during 20xP1.

Key Security Indicators

KSI-CED: Cybersecurity Education

A secure cloud service provider will continuously educate their employees on cybersecurity measures, testing them *regularly* to ensure their knowledge is satisfactory.

KSI-CED-01

> Ensure all employees receive security awareness training.

KSI-CED-02

> Require role-specific training for high risk roles, including at least roles with privileged access.

KSI-CMT: Change Management

A secure cloud service provider will ensure that all system changes are properly documented and configuration baselines are updated accordingly.

KSI-CMT-01

> Log and monitor system modifications.

KSI-CMT-02

> Execute changes though redeployment of version controlled immutable resources rather than direct modification wherever possible.

KSI-CMT-03

> Implement automated testing and validation of changes prior to deployment.

KSI-CMT-04

> Have a documented change management procedure.

KSI-CMT-05

> Evaluate the risk and potential impact of any change.

KSI-CNA: Cloud Native Architecture

A secure *cloud service offering* will use cloud native architecture and design principles to enforce and enhance the Confidentiality, Integrity and Availability of the system.

KSI-CNA-01

> Configure ALL *information resources* to limit inbound and outbound traffic.

KSI-CNA-02

> Design systems to minimize the attack surface and minimize lateral movement if compromised.

KSI-CNA-03

> Use logical networking and related capabilities to enforce traffic flow controls.

KSI-CNA-04

> Use immutable infrastructure with strictly defined functionality and privileges by default.

KSI-CNA-05

> Have denial of service protection.

KSI-CNA-06

> Design systems for high availability and rapid recovery.

KSI-CNA-07

> Ensure cloud-native *information resources* are implemented based on host provider's best practices and documented guidance.

KSI-IAM: Identity and Access Management

A secure *cloud service offering* will protect user data, control access, and apply zero trust principles.

KSI-IAM-01

> Enforce multi-factor authentication (MFA) using methods that are difficult to intercept or impersonate (phishing-resistant MFA) for all user authentication.

KSI-IAM-02

> Use secure passwordless methods for user authentication and authorization when feasible, otherwise enforce strong passwords with MFA.

KSI-IAM-03

> Enforce appropriately secure authentication methods for non-user accounts and services.

KSI-IAM-04

> Use a least-privileged, role and attribute-based, and just-in-time security authorization model for all user and non-user accounts and services.

KSI-IAM-05

> Apply zero trust design principles.

KSI-IAM-06

> Automatically disable or otherwise secure accounts with privileged access in response to suspicious activity.

KSI-INR: Incident Reporting

A secure *cloud service offering* will document, report, and analyze security incidents to ensure regulatory compliance and continuous security improvement.

KSI-INR-01

> Report incidents according to FedRAMP requirements and cloud service provider policies.

KSI-INR-02

> Maintain a log of incidents and periodically review past incidents for patterns or vulnerabilities.

KSI-INR-03

> Generate after action reports and *regularly* incorporate lessons learned into operations.

KSI-MLA: Monitoring, Logging, and Auditing

A secure *cloud service offering* will monitor, log, and audit all important events, activity, and changes.

KSI-MLA-01

> Operate a Security Information and Event Management (SIEM) or similar system(s) for centralized, tamper-resistent logging of events, activities, and changes.

KSI-MLA-02

> *Regularly* review and audit logs.

KSI-MLA-03

> Rapidly detect and remediate or mitigate vulnerabilities.

KSI-MLA-04

> Perform authenticated vulnerability scanning on *information resources*.

KSI-MLA-05

> Perform Infrastructure as Code and configuration evaluation and testing.

KSI-MLA-06

> Centrally track and prioritize the mitigation and/or remediation of identified vulnerabilities.

KSI-PIY: Policy and Inventory

A secure *cloud service offering* will have intentional, organized, universal guidance for how every *information resource*, including personnel, is secured.

KSI-PIY-01

> Have an up-to-date *information resource* inventory or code defining all deployed assets, software, and services.

KSI-PIY-02

> Have policies outlining the security objectives of all *information resources*.

KSI-PIY-03

> Maintain a vulnerability disclosure program.

KSI-PIY-04

> Build security considerations into the Software Development Lifecycle and align with CISA Secure By Design principles.

KSI-PIY-05

> Document methods used to evaluate *information resource* implementations.

KSI-PIY-06

> Have a dedicated staff and budget for security with executive support, commensurate with the size, complexity, scope, and risk of the service offering.

KSI-PIY-07

> Document risk management decisions for software supply chain security.

KSI-RPL: Recovery Planning

A secure *cloud service offering* will define, maintain, and test incident response plan(s) and recovery capabilities to ensure minimal service disruption and data loss during incidents and contingencies.

KSI-RPL-01

> Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

KSI-RPL-02

> Develop and maintain a recovery plan that aligns with the defined recovery objectives.

KSI-RPL-03

> Perform system backups aligned with recovery objectives.

KSI-RPL-04

> *Regularly* test the capability to recover from incidents and contingencies.

KSI-SVC: Service Configuration

A secure *cloud service offering* will follow FedRAMP encryption policies, continuously verify *information resource* integrity, and restrict access to *third-party information resources*.

KSI-SVC-01

> Harden and review network and system configurations.

KSI-SVC-02

> Encrypt or otherwise secure network traffic.

KSI-SVC-03

> Encrypt all federal and sensitive information at rest.

KSI-SVC-04

> Manage configuration centrally.

KSI-SVC-05

> Enforce system and *information resource* integrity through cryptographic means.

KSI-SVC-06

> Use automated key management systems to manage, protect, and *regularly* rotate digital keys and certificates.

KSI-SVC-07

> Use a consistent, risk-informed approach for applying security patches.

KSI-TPR: Third-Party Information Resources

A secure *cloud service offering* will understand, monitor, and manage supply chain risks from *third-party information resources*.

KSI-TPR-01

> Identify all *third-party information resources*.

KSI-TPR-02

> *Regularly* confirm that services handling *federal customer data* or are likely to impact the confidentiality, integrity, or availability of *federal customer data* are FedRAMP authorized and securely configured.

KSI-TPR-03

> Identify and prioritize mitigation of potential supply chain risks.

KSI-TPR-04

> Monitor third party software information resources for upstream vulnerabilities, with contractual notification requirements or active monitoring services.

Technical assistance

FRA-ADS

Purpose: This Technical Assistance helps stakeholders understand the intent behind the requirements in the FedRAMP *authorization data* Sharing Standard.

Disclaimer: Every cloud service provider is different, every architecture is different, and every environment is different. Best practices and technical assistance MUST NOT be used as a checklist. All examples are for discussion purposes ONLY.

FRA-ADS-04

"Without interruption" means that parties should not have to request manual approval each time they need to access *authorization data* or go through a complicated process. The preferred way of ensuring access without interruption is to use on-demand just-in-time access provisioning.

FRA-ADS-05

This is not a license to exclude accurate risk information, but specifics that would *likely* lead to compromise should be abstracted. A breach of confidentiality with *authorization data* should be anticipated by a secure cloud service provider.

Examples of unnecessary sensitive information in *authorization data*

Key Tests:

- Passwords, API keys, access credentials, etc.
- Excessive detail about methodology that exposes weaknesses
- Personally identifiable information about employees

Examples:

- DON'T: "In an emergency, an administrator with physical access to a system can log in using "secretadmin" with the password "pleasewutno"" DO: "In an emergency, administrators with physical access can log in directly."
- DON'T: "All backup MFA credentials are stored in a SuperSafe Series 9000 safe in the CEOs office." DO: "All backup MFA credentials are stored in a UL Class 350 safe in a secure location with limited access."
- DON'T: "During an incident, the incident response team lead by Jim Smith (555-0505) will open a channel at the conference line (555-0101 #97808 passcode 99731)..." DO: "During an incident, the incident response team will coordinate over secure channels."

FRA-SCN

Purpose: This Technical Assistance helps stakeholders evaluate and label *significant changes* by type as required by *FRR-SCN-03*. This assistance is designed for the 20x Phase One Pilot and Rev5 Closed Beta Balance Improvement Test. The Significant Change Notification Requirements will be tested, evaluated, and improved in partnership with stakeholders based on real-world experience.

Disclaimer: Every cloud service provider is different, every architecture is different, and every environment is different. Best practices and technical assistance MUST NOT be used as a checklist. All examples are for discussion purposes ONLY.

FRA-SCN-03

Once a change has been identified as a *significant change* in general, FedRAMP recommends next determining if a change is of the type *routine recurring*. If it is not, work down from the highest impact to lowest to identify the type of change.

1. Is it a *significant change*?
2. If it is, is it a *routine recurring* change?
3. If it is not, is it an *impact categorization* change?
4. If it is not, is it a *transformative* change?
5. If it is not, then it is an *adaptive* change.

FRA-SCN-RR

Activities that match the *routine recurring significant change* type are performed *regularly* and routinely by cloud service providers to address flaws or vulnerabilities, address incidents, and generally perform the typical maintenance and service delivery changes expected during day-to-day operations.

These changes leverage mature processes and capabilities to identify, mitigate, and remediate risks as part of the change. They are often entirely automated and may occur without human intervention, even though they have an impact on security of the service.

If the activity does not occur *regularly* and routinely then it cannot be a *significant change* of this type (e.g., replacing all physical firewalls to remediate a vulnerability is obviously not regular or routine).

Ongoing operations

Key Tests:

- Routine care and feeding by staff during normal duties
- No major impact to service availability
- Does not require executive approval

Examples:

- Provisioning or deprovisioning capacity to support service elasticity
- Changing or tuning performance configurations for instances or services
- Updating and maintaining operational handling of information flows and protection across physical and logical networks (e.g., updating firewall rules)
- Generating or refreshing API or access tokens

Vulnerability Management

Key Tests:

- Minor, incremental patching or updates
- Significant refactoring or migration process NOT required
- No breaking changes

Examples:

- Updating security service or endpoint signatures
- Routine patching of devices, operating systems, software or libraries
- Updating and deploying code that applies normal fixes and improvements as part of a regular development cycle
- Vulnerability remediation activity that simply replaces a known-bad component(s) with a better version of the exact same thing, running in the exact same way with no changes to processes

---

FRA-SCN-TF

Activities that match the *transformative significant change* type are rare for a cloud service offering, adjusted for the size, scale, and complexity of the service. Small cloud service offerings may go years without *transformative* changes, while hyperscale providers may release multiple *transformative* changes per year.

Transformative changes

Key Tests:

- Alters the service risk profile or require new or significantly different actions to address customer responsibilities
- Requires significant new design, development and testing with discrete associated project planning, budget, marketing, etc.
- Requires extensive updates to security assessments, documentation, and how a large number of security requirements are met and validated

Examples:

- The addition, removal, or replacement of a critical third party service that handles a significant portion of information (e.g., IaaS change)
- Increasing the security categorization of a service within the offering that actively handles *federal customer data* (does NOT include impact change of entire offering - see impact categorization change)
- Replacement of underlying management planes or paradigm shift in workload orchestration (e.g., bare-metal servers or virtual machines to containers, migration to kubernetes)
- Datacenter migration where large amounts of *federal customer data* is moved across boundaries different from normal day-to-day operations
- Adding a new AI-based capability that impacts *federal customer data* in a different way than existing services or capabilities (such as integrating a new third-party service or training on *federal customer data*)

FRA-SCN-AD

Activities that match the *adaptive significant change* type are a frequent and normal part of iteratively improving a service by deploying new functionality or modifying existing functionality in a way that is typically transparent to customers and does not introduce significant new security risks.

In general, most changes that do not happen *regularly* will be *adaptive* changes. This change type deliberately covers a wide range of activities in a way that requires assessment and consideration.

Service adjustments

Key Tests:

- Requires minimal changes to security plans or procedures
- Requires some careful planning and project management to implement, but does not rise to the level of planning required for transformative changes
- Requires verification of existing functionality and secure configuration after implementation

Examples:

- Updates to operating systems, containers, virtual machines, software or libraries with known breaking changes, complex steps, or service disruption
- Deploying larger than normal incremental feature improvements in code or libraries that are the work of multiple weeks of development efforts but are not considered a major new service
- Changing cryptographic modules where the new module meets the same standards and characteristics of the former
- Replacing a like-for-like component where some security plan or procedure adjustments are required (e.g., scanning tool or managed database swap)
- Adding models to existing approved AI services without exposing *federal customer data* to new services

---

FRA-VDR

Purpose: This Technical Assistance provides additional context behind the intent and goals of certain aspects of this standard that have caused significant confusion or requests for clarification during public comment. This assistance is initially designed for 20x Phase Two/Three and the Rev5 Closed Beta Balance Improvement Test.

Disclaimer: Every cloud service provider is different, every architecture is different, and every environment is different. Best practices and technical assistance MUST NOT be used as a checklist. All examples are for discussion purposes ONLY.

FRA-VDR-01

FedRAMP focuses on internet-reachable (rather than internet-accessible) to ensure that any service that might receive a payload from the internet is prioritized if that service has a vulnerability that can be triggered by processing the data in the payload. The simplest way to prevent exploitation of internet-reachable vulnerabilities is to intercept, inspect, filter, sanitize, reject, or otherwise deflect triggering payloads before they are processed by the vulnerable resource; once this prevention is in place the vulnerability should no longer be considered an internet-reachable vulnerability.

A classic example of an internet-reachable vulnerability on systems that are not typically internet-accessible is SQL injection (https://en.wikipedia.org/wiki/SQL_injection), where an application stack behind a load balancer and firewall with no ability to route traffic to or from the internet can receive a payload indirectly from the internet that triggers the manipulation or compromise of data in a database that can only be accessed by an authorized connection from the application server on a private network.

Another simple example is the infamous Log4Shell (https://en.wikipedia.org/wiki/Log4Shell) vulnerability from 2021, where exploitation was possible via vulnerable internet-reachable resources deep in the application stack that were often not internet-accessible themselves.

FRA-VDR-02

The simple reality is that most traditional vulnerabilities discovered by scanners or during assessment are not likely to be exploitable; exploitation typically requires an unrealistic set of circumstances that will not occur during normal operation. The likelihood of exploitation will vary depending on so many factors that FedRAMP will not recommend a specific framework for approaching this beyond the recommendations and requirements in this document.

The proof, ultimately, is in the pudding - providers who regularly evaluate vulnerabilities as not likely exploitable without careful consideration are more likely to suffer from an adverse impact where the root cause was an exploited vulnerability that was improperly evaluated. If done recklessly or deliberately, such actions will have a potential adverse impact on a provider's FedRAMP authorization.
