FedRAMP FedRAMP 20x Combined Requirements

- **Release:** 25.08A
- **Published:** 2025-08-24
- **Designator:** FRMR-LOW
- **Description:** Combined FedRAMP 20x Low Requirements

Definitions

FRD-ALL-01

> ***Federal Information***: *Has the meaning from OMB Circular A-130 and any successor documents. As of Apr 2025, this means "information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the federal government, in any medium or form."*
>
> *Note: This typically does not include information that a cloud service provider produces outside of a government contract or agreement. Review FedRAMP's Technical Assistance and consult qualified legal experts for additional assistance identifying federal information.*
>
> *Reference: OMB Circular A-130*

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)*

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

> *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

> *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

> *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

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

FRR-ADS-05

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

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

FRR-ADS-TC-03

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

FRR-ADS-TC-04

> *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

> *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

> *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

> *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

> *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

> *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

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

FRR-SCN-03

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

FRR-SCN-04

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

FRR-SCN-05

> *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

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

FRR-SCN-07

> *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

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

FRR-SCN-09

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *Providers MUST identify a set of information resources to assess for FedRAMP authorization that includes all information resources that are likely to handle federal information or likely to impact the confidentiality, integrity, or availability of federal information handled by the cloud service offering.*

FRR-MAS-02

> *Providers MUST include the configuration and usage of third-party information resources, ONLY IF FRR-MAS-01 APPLIES.*

FRR-MAS-03

> *Providers MUST clearly identify and document the justification, mitigation measures, compensating controls, and potential impact to federal information from the configuration and usage of non-FedRAMP authorized third-party information resources, ONLY IF FRR-MAS-01 APPLIES.*

FRR-MAS-04

> *Providers MUST include metadata (including metadata about federal information), ONLY IF FRR-MAS-01 APPLIES.*

FRR-MAS-05

> *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

> *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

> *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

> *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

> *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

> *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

> *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

> *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-KSI

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

FRR-KSI-01

> *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

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

FRR-KSI-03

> *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 information or are likely to impact the confidentiality, integrity, or availability of federal information 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 information (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 information is moved across boundaries different from normal day-to-day operations
- Adding a new AI-based capability that impacts federal information in a different way than existing services or capabilities (such as integrating a new third-party service or training on federal information)

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 information to new services

---