FedRAMP Key Security Indicators

- **Release:** 25.05D
- **Published:** 2025-08-24
- **Designator:** KSI
- **Description:** Minor non-breaking updates to align term definitions and highlighted terms across updated materials (no changes to KSIs, definitions are now in FRD-ALL).

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-06-01** for **20xP1**.
  - These requirements apply to all participants in the FedRAMP 20x Phase One pilot.
  - For FedRAMP 20x Low authorizations for cloud service offerings deployed on an existing FedRAMP authorized cloud service offering, using primarily cloud-native services, and only using FedRAMP authorized *third-party information resources*.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

- OMB Circular A-130 Appendix I states "Agencies may also develop overlays for specific types of information or communities of interest (e.g., all web-based applications, all health care-related systems) as part of the security control selection process. Overlays provide a specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information as part of the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay may be more stringent or less stringent than the original security control baseline and can be applied to multiple information systems."
- NIST SP 800-53B Section 2.5 states "As the number of controls in [SP 800-53] grows in response to an increasingly sophisticated threat space, it is important for organizations to have the ability to describe key capabilities needed to protect organizational missions and business functions, and to subsequently select controls that—if properly designed, developed, and implemented—produce such capabilities. The use of capabilities simplifies how the protection problem is viewed conceptually. Using the construct of a capability provides a method of grouping controls that are employed for a common purpose or to achieve a common objective." This section later states "Ultimately, authorization decisions (i.e., risk acceptance decisions) are made based on the degree to which the desired capabilities have been effectively achieved."
- NIST SP 800-53A Section 3.5 states "When organizations employ the concept of capabilities, automated and manual assessments account for all security and privacy controls that comprise the security and privacy capabilities. Assessors are aware of how the controls work together to provide such capabilities."

- FedRAMP Authorization Act (44 USC § 3609 (a) (1)) requires that the Administrator of the General Services Administration shall "in consultation with the [DHS] Secretary, develop, coordinate, and implement a process to support agency review, reuse, and standardization, where appropriate, of security assessments of cloud computing products and services..." 44 USC § 3609 (c) (2) further states that "the [GSA] Administrator shall establish a means for the automation of security assessments and reviews."

Purpose

Modern cloud services use automated or code-driven configuration management and control planes to ensure predictable, repeatable, reliable, and secure outcomes during deployment and operation. The majority of a service security assessment can take place continuously via automated validation for simple cloud-native services if the need for a traditional control-by-control narrative approach is removed.

Expected Outcomes

- Cloud service providers following commercial security best practices will be able to meet and validate FedRAMP security requirements with the application of simple changes and automated capabilities
- Third-party independent assessors will have a simpler framework to assess security and implementation decisions based on engineering decisions in context
- Federal agencies will be able to easily, quickly, and effectively review and consume security information about the service to make informed risk-based authorization to operate decisions based on their planned use case

---

Requirements

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.*