FedRAMP Key Security Indicators

- **Release:** 25.11A DRAFT
- **Published:** 2025-00-00
- **Designator:** KSI
- **Description:** THIS IS A DRAFT AND IS NOT FINALIZED, USE AT YOUR OWN RISK. Initial DRAFT release of the Phase Two Key Security Indicators (KSI) after public comment.

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-00-00** for **20x**.
  - These Key Security Indicators apply to all FedRAMP 20x authorizations.
  - Phase One Pilot participants have one year from authorization to fully address these Key Security Indicators but must demonstrate continuous quarterly progress.
  - Phase Two Pilot participants must address all of these Key Security Indicators prior to submission for authorization review.

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 and Recommendations

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

> 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

> 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

> 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-AFR: Authorization by FedRAMP

A secure cloud service provider seeking FedRAMP authorization will address all FedRAMP 20x requirements and recommendations, including government-specific requirements for maintaining a secure system and reporting on

activities to government customers.

KSI-AFR-01

Applies to: Low, Moderate

> Apply the FedRAMP Minimum Assessment Standard (MAS) to identify and document the scope of the cloud service offering to be assessed for FedRAMP authorization and persistently address all related requirements and recommendations..

KSI-AFR-02

Applies to: Low, Moderate

> Set security goals for the cloud service offering based on FedRAMP 20x Phase Two Key Security Indicators (KSIs - you are here), develop automated validation of status and progress to the greatest extent possible, and persistently address all related requirements and recommendations..

KSI-AFR-03

Applies to: Low, Moderate

> Determine how authorization data will be shared with all necessary parties in alignment with the FedRAMP Authorization Data Sharing (ADS) standard and persistently address all related requirements and recommendations..

KSI-AFR-04

Applies to: Low, Moderate

> Document the vulnerability detection and vulnerability response methodology used within the cloud service offering in alignment with the FedRAMP Vulnerability Detection and Response (VDR) standard and persistently address all related requirements and recommendations..

KSI-AFR-05

Applies to: Low, Moderate

> Determine how significant changes will be tracked and how all necessary parties will be notified in alignment with the FedRAMP Significant Change Notification (SCN) standard and persistently address all related requirements and recommendations..

KSI-AFR-06

Applies to: Low, Moderate

> Maintain a plan and process for providing Ongoing Authorization Reports and Quarterly Reviews for all necessary parties in alignment with the FedRAMP Collaborative Continuous Monitoring (CCM) standard and persistently address all related requirements and recommendations..

KSI-AFR-07

Applies to: Low, Moderate

> Develop secure by default configurations and provide guidance for secure configuration of the cloud service offering to customers in alignment with the FedRAMP Recommended Secure Configuration (RSC) standard and persistently address all related requirements and recommendations..

KSI-AFR-08

Applies to: Low, Moderate

> Operate a secure inbox to receive critical communication from FedRAMP and other government entities in alignment with FedRAMP Security Inbox Requirements (SIR) and persistently address all related requirements and recommendations..

KSI-AFR-09

Applies to: Low, Moderate

> Persistently validate, assess, and report on the effectiveness and status of security decisions and policies that are implemented within the cloud service offering in alignment with the FedRAMP 20x Persistent Validation and Assessment (PVA) standard, and persistently address all related requirements and recommendations..

KSI-AFR-10

Applies to: Low, Moderate

> Integrate FedRAMP's Incident Communications Procedures (ICP) into incident response procedures and persistently address all related requirements and recommendations..

KSI-AFR-11

Applies to: Low, Moderate

> Ensure that cryptographic modules used to protect potentially sensitive federal customer data are selected and used in alignment with the FedRAMP 20x Use of Cryptographic Modules policy and persistently address all related requirements and recommendations..

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

Applies to: Low, Moderate

> Require and monitor the effectiveness of training given to all employees on policies, procedures, and security-related topics..

KSI-CED-02

Applies to: Low, Moderate

> Require and monitor the effectiveness of role-specific training for high risk roles, including at least roles with privileged access..

KSI-CED-03

Applies to: Low, Moderate

> Require and monitor the effectiveness of role-specific training provided to development and engineering staff that covers best practices for delivering secure software..

KSI-CED-04

Applies to: Low, Moderate

> Require and monitor the effectiveness of role-specific training to staff involved with incident response or disaster recovery..

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

Applies to: Low, Moderate

> Log and monitor modifications to the cloud service offering..

KSI-CMT-02

Applies to: Low, Moderate

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

KSI-CMT-03

Applies to: Low, Moderate

> Automate persistent testing and validation of changes throughout deployment..

KSI-CMT-04

Applies to: Low, Moderate

> Always follow a documented change management procedure..

KSI-CMT-05

Applies to: Low, Moderate

> Superseded by KSI-AFR-05 (SCN).

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

Applies to: Low, Moderate

> Configure all machine-based information resources to limit inbound and outbound network traffic..

KSI-CNA-02

Applies to: Low, Moderate

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

KSI-CNA-03

Applies to: Low, Moderate

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

KSI-CNA-04

Applies to: Low, Moderate

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

KSI-CNA-05

Applies to: Low, Moderate

> Protect against denial of service attacks and other unwanted activity..

KSI-CNA-06

Applies to: Low, Moderate

> Design systems for high availability and rapid recovery.

KSI-CNA-07

Applies to: Low, Moderate

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

KSI-CNA-08

Applies to: Moderate

> Use automated services to persistently assess the security posture of all machine-based information resources and automatically enforce their intended operational state..

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

Applies to: Low, Moderate

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

KSI-IAM-02

Applies to: Low, Moderate

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

KSI-IAM-03

Applies to: Low, Moderate

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

KSI-IAM-04

Applies to: Low, Moderate

> 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

Applies to: Low, Moderate

> Configure identity and access management with measures that always verify each user or device can only access the resources they need..

KSI-IAM-06

Applies to: Low, Moderate

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

KSI-IAM-07

Applies to: Low, Moderate

> Securely manage the lifecycle and privileges of all accounts, roles, and groups, using automation..

KSI-INR: Incident Response

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

KSI-INR-01

Applies to: Low, Moderate

> Always follow a documented incident response procedure..

KSI-INR-02

Applies to: Low, Moderate

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

KSI-INR-03

Applies to: Low, Moderate

> 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

Applies to: Low, Moderate

> 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

Applies to: Low, Moderate

> *Regularly* review and audit logs.

KSI-MLA-03

Applies to: Low, Moderate

> Superseded by KSI-AFR-04 (VDR).

KSI-MLA-04

Applies to: Low, Moderate

> Superseded by KSI-AFR-04 (VDR).

KSI-MLA-05

Applies to: Low, Moderate

> Perform Infrastructure as Code and configuration evaluation and testing.

KSI-MLA-06

Applies to: Low, Moderate

> Superseded by KSI-AFR-04 (VDR).

KSI-MLA-07

Applies to: Low, Moderate

> Maintain a list of information resources and event types that will be monitored, logged, and audited, then do so..

KSI-MLA-08

Applies to: Moderate

> Use a least-privileged, role and attribute-based, and just-in-time access authorization model for access to log data based on organizationally defined data sensitivity..

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

Applies to: Low, Moderate

> Use authoritative sources to automatically maintain real-time inventories of all information resources.

KSI-PIY-02

Applies to: Low, Moderate

> Document the security objectives and requirements for each information resource or set of information resources..

KSI-PIY-03

Applies to: Low, Moderate

> Maintain a vulnerability disclosure program.

KSI-PIY-04

Applies to: Low, Moderate

> Monitor the effectiveness of building security and privacy considerations into the Software Development Lifecycle and aligning with CISA Secure By Design principles..

KSI-PIY-05

Applies to: Low, Moderate

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

KSI-PIY-06

Applies to: Low, Moderate

> Monitor the effectiveness of the organization’s investments in achieving security objectives..

KSI-PIY-07

Applies to: Low, Moderate

> Document risk management decisions for software supply chain security.

KSI-PIY-08

Applies to: Low, Moderate

> Regularly measure executive support for achieving the organization’s security objectives..

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

Applies to: Low, Moderate

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

KSI-RPL-02

Applies to: Low, Moderate

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

KSI-RPL-03

Applies to: Low, Moderate

> Perform system backups aligned with recovery objectives.

KSI-RPL-04

Applies to: Low, Moderate

> *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

Applies to: Low, Moderate

> Implement improvements based on persistent evaluation of information resources for opportunities to improve security..

KSI-SVC-02

Applies to: Low, Moderate

> Encrypt or otherwise secure network traffic.

KSI-SVC-03

Applies to: Low, Moderate

> Superseded by KSI-AFR-11 (UCM).

KSI-SVC-04

Applies to: Low, Moderate

> Manage configuration of machine-based information resources using automation..

KSI-SVC-05

Applies to: Low, Moderate

> Use cryptographic methods to validate the integrity of machine-based information resources..

KSI-SVC-06

Applies to: Low, Moderate

> Automate management, protection, and regular rotation of digital keys, certificates, and other secrets..

KSI-SVC-07

Applies to: Low, Moderate

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

KSI-SVC-08

Applies to: Moderate

> Do not introduce or leave behind residual elements that could negatively affect confidentiality, integrity, or availability of federal customer data during operations..

KSI-SVC-09

Applies to: Moderate

> Persistently validate the authenticity and integrity of communications between machine-based information resources using automation..

KSI-SVC-10

Applies to: Moderate

> Remove unwanted federal customer data promptly when requested by an agency in alignment with customer agreements, including from backups if appropriate; this typically applies when a customer spills information or when a customer seeks to remove information from a service due to a change in usage..

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

Applies to: Low, Moderate

> Superseded by KSI-AFR-01 (MAS).

KSI-TPR-02

Applies to: Low, Moderate

> Superseded by KSI-AFR-01 (MAS).

KSI-TPR-03

Applies to: Low, Moderate

> Identify and prioritize mitigation of potential supply chain risks.

KSI-TPR-04

Applies to: Low, Moderate

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