FedRAMP Key Security Indicators

- **Release:** 25.05A
- **Published:** 2025-05-30
- **Designator:** KSI
- **Description:** Initial release of Key Security Indicators

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.

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."

  (*These responsibilities are delegated to the FedRAMP Director*)

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

---

Definitions

FRD-KSI-01

> ***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.*

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-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-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-IAM: Identity and Access Management

A secure cloud service offering will use modern identity management principles to control access to information resources.

KSI-IAM-01

> *Use centrally managed authentication and authorization.*

KSI-IAM-02

> *Control access based on roles and cloud-native functions.*

KSI-IAM-03

> *Enforce minimum password and authentication requirements.*

KSI-IAM-04

> *Manage and protect privileged accounts.*

KSI-IAM-05

> *Regularly review and validate access.*

KSI-AUD: Audit Logging

A secure cloud service offering will maintain detailed audit logs of system and user activity.

KSI-AUD-01

> *Enable and configure detailed audit logging.*

KSI-AUD-02

> *Protect audit logs from tampering and deletion.*

KSI-AUD-03

> *Monitor audit logs for suspicious activity.*

KSI-AUD-04

> *Retain audit logs according to requirements.*

KSI-CMT: Configuration Management

A secure cloud service offering will use configuration management best practices to maintain system security.

KSI-CMT-01

> *Use infrastructure-as-code to deploy and manage infrastructure.*

KSI-CMT-02

> *Track and document configuration changes.*

KSI-CMT-03

> *Review and validate configuration changes.*

KSI-CMT-04

> *Use configuration management for all system components.*

KSI-MON: Continuous Monitoring

A secure cloud service offering will continuously monitor system health and security.

KSI-MON-01

> *Monitor system performance and availability.*

KSI-MON-02

> *Monitor security events and alerts.*

KSI-MON-03

> *Use automated monitoring tools.*

KSI-MON-04

> *Regularly review monitoring data.*

KSI-VLN: Vulnerability Management

A secure cloud service offering will actively manage and remediate vulnerabilities.

KSI-VLN-01

> *Regularly scan for vulnerabilities.*

KSI-VLN-02

> *Track and remediate identified vulnerabilities.*

KSI-VLN-03

> *Use automated vulnerability scanning tools.*

KSI-VLN-04

> *Maintain vulnerability management program.*

KSI-INC: Incident Reporting

A secure cloud service offering will have procedures in place to report and respond to security incidents.

KSI-INC-01

> *Maintain incident response procedures.*

KSI-INC-02

> *Report security incidents promptly.*

KSI-INC-03

> *Document and track incident responses.*

KSI-INC-04

> *Review and update incident response procedures.*