FedRAMP 20x Key Security Indicators

Effective Date(s) & Overall Applicability

This standard applies as follows:

- **FedRAMP 20x:** Effective Friday, May 30, 2025 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.

  Providers **MUST** participate in the FedRAMP 20xP1 pilot to qualify for FedRAMP 20x authorization until a final transition path is announced; this pilot is currently active and open to the public at https://www.fedramp.gov/20x/phase-one/.

This standard does not apply to FedRAMP Rev 5 authorizations.

Background & Authority

OMB Circular A-130: Managing Information as a Strategic Resource 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: Control Baselines for Information Systems and Organizations 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: Assessing Security and Privacy Controls in Information Systems and Organizations 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."*

The 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.

Introduction

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 from the application of Key Security Indicators include:

- 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

The following definitions apply to all FedRAMP materials:

> **FRD-KSI-01:** "**Regularly**" means 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.

Key Security Indicators

FedRAMP Key Security Indicators (KSIs) summarize the capabilities that satisfy FedRAMP security requirements aligned to NIST SP 800-53. Each Key Security Indicator includes critical security capabilities that must be met and validated. These capabilities are designed to provide a concrete approach to evaluating cloud security risks that can often be derived automatically from technical configurations.

The following rules ALWAYS apply to ALL FedRAMP 20x authorizations:

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.

The following rules provide general guidance on the application of Key Security Indicators:

FRR-KSI-AY-01: All parties SHOULD follow FedRAMP's best practices and technical assistance on assessing Key Security Indicators where applicable.

FRR-KSI-AY-02: (INTERIM RULE) 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.

FedRAMP Low, Cloud Native

Cloud Native Architecture

KSI-CNA: 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.

Validation

To report KSI-CNA as True, cloud service providers MUST:

01: Configure ALL information resources to limit inbound and outbound traffic

02: Design systems to minimize the attack surface and minimize lateral movement if compromised

03: Use logical networking and related capabilities to enforce traffic flow controls

04: Use immutable infrastructure with strictly defined functionality and privileges by default

05: Have denial of service protection

06: Design systems for high availability and rapid recovery

07: Ensure cloud-native information resources are implemented based on host provider's best practices and documented guidance

Service Configuration

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

Validation

To report KSI-SVC as True, cloud service providers MUST:

01: Harden and review network and system configurations

02: Encrypt or otherwise secure network traffic

03: Encrypt all federal and sensitive information at rest

04: Manage configuration centrally

05: Enforce system and information resource integrity through cryptographic means

06: Use automated key management systems to manage, protect, and regularly rotate digital keys and certificates

07: Use a consistent, risk-informed approach for applying security patches

Identity and Access Management

KSI-IAM: A secure cloud service offering will protect user data, control access, and apply zero trust principles.

Validation

To report KSI-IAM as True, cloud service providers MUST:

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

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

03: Enforce appropriately secure authentication methods for non-user accounts and services

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

05: Apply zero trust design principles

06: Automatically disable or otherwise secure accounts with privileged access in response to suspicious activity

Monitoring, Logging, and Auditing

KSI-MLA: A secure cloud service offering will monitor, log, and audit all important events, activity, and changes.

Validation

To report KSI-MLA as True, cloud service providers MUST:

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

02: Regularly review and audit logs

03: Rapidly detect and remediate or mitigate vulnerabilities

04: Perform authenticated vulnerability scanning on information resources

05: Perform Infrastructure as Code and configuration evaluation and testing

06: Centrally track and prioritize the mitigation and/or remediation of identified vulnerabilities

Change Management

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

Validation

To report KSI-CMT as True, cloud service providers MUST:

01: Log and monitor system modifications

02: Execute changes though redeployment of version controlled immutable resources rather than direct modification wherever possible

03: Implement automated testing and validation of changes prior to deployment

04: Have a documented change management procedure

05: Evaluate the risk and potential impact of any change

Policy and Inventory

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

Validation

To report KSI-PIY as True, cloud service providers MUST:

01: Have an up-to-date information resource inventory or code defining all deployed assets, software, and services

02: Have policies outlining the security objectives of all information resources

03: Maintain a vulnerability disclosure program

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

05: Document methods used to evaluate information resource implementations

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

07: Document risk management decisions for software supply chain security

Third-Party Information Resources

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

Validation

To report KSI-TPR as True, cloud service providers MUST:

01: Identify all third-party information resources

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

03: Identify and prioritize mitigation of potential supply chain risks

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

Cybersecurity Education

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

Validation

To report KSI-CED as True, cloud service providers MUST:

01: Ensure all employees receive security awareness training

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

Recovery Planning

KSI-RPL: 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.

Validation

To report KSI-RPL as True, cloud service providers MUST:

01: Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

02: Develop and maintain a recovery plan that aligns with the defined recovery objectives

03: Perform system backups aligned with recovery objectives

04: Regularly test the capability to recover from incidents and contingencies

Incident Reporting

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

Validation

To report KSI-INR as True, cloud service providers MUST:

01: Report incidents according to FedRAMP requirements and cloud service provider policies

02: Maintain a log of incidents and periodically review past incidents for patterns or vulnerabilities

03: Generate after action reports and regularly incorporate lessons learned into operations