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.*

Controls

- at-2 Literacy Training and Awareness
- at-2.2 Insider Threat
- at-2.3 Social Engineering and Mining
- at-4 Training Records

KSI-CED-02

> *Require role-specific training for high risk roles, including at least roles with privileged access.*

Controls

- at-2 Literacy Training and Awareness
- at-3 Role-based Training
- sr-11.1 Anti-counterfeit Training

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.*

Controls

- au-2 Event Logging
- cm-3 Configuration Change Control
- cm-4.2 Verification of Controls
- cm-6 Configuration Settings
- ma-2 Controlled Maintenance

KSI-CMT-02

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

Controls

- cm-2 Baseline Configuration
- cm-3 Configuration Change Control
- cm-5 Access Restrictions for Change
- cm-6 Configuration Settings
- cm-7 Least Functionality
- cm-8.1 Updates During Installation and Removal
- si-3 Malicious Code Protection

KSI-CMT-03

> *Implement automated testing and validation of changes prior to deployment.*

Controls

- cm-3 Configuration Change Control
- cm-3.2 Testing, Validation, and Documentation of Changes
- si-2 Flaw Remediation

KSI-CMT-04

> *Have a documented change management procedure.*

Controls

- cm-3 Configuration Change Control
- cm-3.4 Security and Privacy Representatives
- cm-5 Access Restrictions for Change
- cm-7.1 Periodic Review
- cm-9 Configuration Management Plan

KSI-CMT-05

> *Evaluate the risk and potential impact of any change.*

Controls

- ca-7.4 Risk Monitoring
- cm-3.4 Security and Privacy Representatives
- cm-4 Impact Analyses
- si-2 Flaw Remediation

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.*

Controls

- ac-17.3 Managed Access Control Points
- ca-9 Internal System Connections

KSI-CNA-02

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

Controls

- ac-17.3 Managed Access Control Points
- ca-9 Internal System Connections

KSI-CNA-03

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

Controls

- ac-17.3 Managed Access Control Points
- ca-9 Internal System Connections
- sc-7 Boundary Protection

KSI-CNA-04

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

Controls

- cm-2 Baseline Configuration
- si-3 Malicious Code Protection

KSI-CNA-05

> *Have denial of service protection.*

Controls

- sc-5 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.*

Controls

- ac-17.3 Managed Access Control Points
- cm-2 Baseline Configuration
- pl-10 Baseline Selection

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.*

Controls

- ac-2 Account Management
- ia-2 Identification and Authentication (Organizational Users)
- ia-2.1 Multi-factor Authentication to Privileged Accounts
- ia-2.2 Multi-factor Authentication to Non-privileged Accounts
- ia-2.8 Access to Accounts — Replay Resistant
- ia-8 Identification and Authentication (Non-organizational Users)

KSI-IAM-02

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

Controls

- ac-2 Account Management
- ac-3 Access Enforcement
- ia-2.1 Multi-factor Authentication to Privileged Accounts
- ia-2.2 Multi-factor Authentication to Non-privileged Accounts
- ia-2.8 Access to Accounts Replay Resistant
- ia-5.1 Password-based Authentication
- ia-5.2 Public Key-based Authentication
- ia-5.6 Protection of Authenticators

- ia-6 Authentication Feedback

KSI-IAM-03

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

Controls

- ac-2 Account Management
- ac-4 Information Flow Enforcement
- ia-3 Device Identification and Authentication
- ia-5.2 Public Key-based Authentication

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.*

Controls

- ac-2 Account Management
- ac-2.2 Automated Temporary and Emergency Account Management
- ac-2.3 Disable Accounts
- ac-2.4 Automated Audit Actions
- ac-2.6 Dynamic Privilege Management
- ac-3 Access Enforcement
- ac-4 Information Flow Enforcement
- ac-5 Separation of Duties
- ac-6 Least Privilege
- ac-6.1 Authorize Access to Security Functions
- ac-6.2 Non-privileged Access for Nonsecurity Functions
- ac-6.5 Privileged Accounts
- ac-6.7 Review of User Privileges
- ac-6.9 Log Use of Privileged Functions
- ac-6.10 Prohibit Non-privileged Users from Executing Privileged Functions
- ac-7 Unsuccessful Logon Attempts
- ac-17 Remote Access
- au-9.4 Access by Subset of Privileged Users
- cm-5 Access Restrictions for Change
- cm-7 Least Functionality
- cm-9 Configuration Management Plan
- ia-4 Identifier Management
- ia-4.4 Identify User Status
- ia-7 Cryptographic Module Authentication
- ps-2 Position Risk Designation
- ps-3 Personnel Screening
- ps-4 Personnel Termination
- ps-5 Personnel Transfer
- ps-6 Access Agreements
- ps-9 Position Descriptions
- sc-39 Process Isolation

KSI-IAM-05

> *Apply zero trust design principles.*

Controls

- ac-2.5 Inactivity Logout
- ac-2.6 Dynamic Privilege Management
- ac-3 Access Enforcement
- ac-4 Information Flow Enforcement
- ac-6 Least Privilege
- ac-12 Session Termination
- ac-14 Permitted Actions Without Identification or Authentication
- ac-17 Remote Access
- ac-17.1 Monitoring and Control
- ac-17.2 Protection of Confidentiality and Integrity Using Encryption
- ac-17.3 Managed Access Control Points
- ac-20 Use of External Systems
- ac-20.1 Limits on Authorized Use
- cm-9 Configuration Management Plan
- ia-2 Identification and Authentication (Organizational Users)
- ia-3 Device Identification and Authentication
- ia-4 Identifier Management
- ia-4.4 Identify User Status
- ia-5.2 Public Key-based Authentication
- ia-11 Re-authentication
- ps-2 Position Risk Designation
- ps-3 Personnel Screening
- ps-4 Personnel Termination
- ps-5 Personnel Transfer
- ps-6 Access Agreements
- sc-20 Secure Name/Address Resolution Service (Authoritative Source)
- sc-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)
- sc-22 Architecture and Provisioning for Name/Address Resolution Service
- sc-39 Process Isolation
- si-3 Malicious Code Protection

KSI-IAM-06

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

Controls

- ac-2 Account Management
- ac-2.1 Automated System Account Management
- ac-2.3 Disable Accounts
- ac-2.13 Disable Accounts for High-risk Individuals
- ac-7 Unsuccessful Logon Attempts
- ps-4 Personnel Termination
- ps-8 Personnel Sanctions

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.*

Controls

- ir-4 Incident Handling
- ir-4.1 Automated Incident Handling Processes
- ir-6 Incident Reporting
- ir-6.1 Automated Reporting
- ir-7 Incident Response Assistance
- ir-7.1 Automation Support for Availability of Information and Support
- ir-8 Incident Response Plan

KSI-INR-02

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

Controls

- ir-3 Incident Response Testing
- ir-4 Incident Handling
- ir-4.1 Automated Incident Handling Processes
- ir-5 Incident Monitoring
- ir-8 Incident Response Plan

KSI-INR-03

> *Generate after action reports and regularly incorporate lessons learned into operations.*

Controls

- ir-3 Incident Response Testing
- ir-4 Incident Handling
- ir-4.1 Automated Incident Handling Processes
- ir-8 Incident Response Plan

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.*

Controls

- au-2 Event Logging
- au-3 Content of Audit Records
- au-3.1 Additional Audit Information
- au-4 Audit Log Storage Capacity
- au-5 Response to Audit Logging Process Failures
- au-6.1 Automated Process Integration
- au-6.3 Correlate Audit Record Repositories
- au-7 Audit Record Reduction and Report Generation
- au-7.1 Automatic Processing
- au-8 Time Stamps
- au-9 Protection of Audit Information
- au-11 Audit Record Retention

KSI-MLA-02

> *Regularly review and audit logs.*

Controls

- ac-2.4 Automated Audit Actions
- ac-6.9 Log Use of Privileged Functions
- au-2 Event Logging
- au-6 Audit Record Review, Analysis, and Reporting
- si-4 System Monitoring

KSI-MLA-03

> *Rapidly detect and remediate or mitigate vulnerabilities.*

Controls

- au-5 Response to Audit Logging Process Failures
- ca-7 Continuous Monitoring
- ra-5 Vulnerability Monitoring and Scanning
- ra-5.2 Update Vulnerabilities to Be Scanned
- sa-22 Unsupported System Components
- si-2 Flaw Remediation
- si-5 Security Alerts, Advisories, and Directives

KSI-MLA-04

> *Perform authenticated vulnerability scanning on information resources.*

Controls

- ca-7 Continuous Monitoring
- ra-5 Vulnerability Monitoring and Scanning
- si-3 Malicious Code Protection

KSI-MLA-05

> *Perform Infrastructure as Code and configuration evaluation and testing.*

Controls

- ca-7 Continuous Monitoring
- cm-2 Baseline Configuration
- cm-6 Configuration Settings

KSI-MLA-06

> *Centrally track and prioritize the mitigation and/or remediation of identified vulnerabilities.*

Controls

- ca-5 Plan of Action and Milestones

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.*

Controls

- cm-7.5 Authorized Software Allow-by-exception
- cm-8 System Component Inventory
- cm-8.1 Updates During Installation and Removal
- cm-12 Information Location
- cm-12.1 Automated Tools to Support Information Location
- cp-2.8 Identify Critical Assets

KSI-PIY-02

> *Have policies outlining the security objectives of all information resources.*

Controls

- ac-1 Policy and Procedures
- at-1 Policy and Procedures
- au-1 Policy and Procedures
- ca-1 Policy and Procedures
- cm-1 Policy and Procedures
- cp-1 Policy and Procedures
- cp-2.1 Coordinate with Related Plans
- cp-4.1 Coordinate with Related Plans
- ia-1 Policy and Procedures
- ir-1 Policy and Procedures
- ma-1 Policy and Procedures
- mp-1 Policy and Procedures
- pe-1 Policy and Procedures
- pl-1 Policy and Procedures
- pl-2 System Security and Privacy Plans
- pl-4 Rules of Behavior
- pl-4.1 Social Media and External Site/Application Usage Restrictions
- ps-1 Policy and Procedures
- ra-1 Policy and Procedures
- sa-1 Policy and Procedures
- sc-1 Policy and Procedures
- si-1 Policy and Procedures
- sr-1 Policy and Procedures
- sr-2 Supply Chain Risk Management Plan
- sr-3 Supply Chain Controls and Processes
- sr-11 Component Authenticity

KSI-PIY-03

> *Maintain a vulnerability disclosure program.*

Controls

- ra-5.11 Public Disclosure Program

KSI-PIY-04

> *Build security considerations into the Software Development Lifecycle and align with CISA Secure By Design principles.*

Controls

- ac-5 Separation of Duties

- sa-3 System Development Life Cycle

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.*

Controls

- ac-5 Separation of Duties
- cp-2.1 Coordinate with Related Plans
- cp-4.1 Coordinate with Related Plans
- ir-3.2 Coordination with Related Plans
- sa-2 Allocation of Resources
- sa-3 System Development Life Cycle
- sr-2.1 Establish SCRM Team

KSI-PIY-07

> *Document risk management decisions for software supply chain security.*

Controls

- ca-7.4 Risk Monitoring

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).*

Controls

- cp-2.3 Resume Mission and Business Functions
- cp-10 System Recovery and Reconstitution

KSI-RPL-02

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

Controls

- cp-2 Contingency Plan
- cp-2.3 Resume Mission and Business Functions
- cp-6 Alternate Storage Site
- cp-10 System Recovery and Reconstitution

KSI-RPL-03

> *Perform system backups aligned with recovery objectives.*

Controls

- cm-2.3 Retention of Previous Configurations
- cp-6 Alternate Storage Site
- cp-9 System Backup

- cp-10 System Recovery and Reconstitution
- cp-10.2 Transaction Recovery
- si-12 Information Management and Retention

KSI-RPL-04

> *Regularly test the capability to recover from incidents and contingencies.*

Controls

- cp-4 Contingency Plan Testing
- cp-6 Alternate Storage Site
- cp-9.1 Testing for Reliability and Integrity
- cp-10 System Recovery and Reconstitution
- ir-3 Incident Response Testing

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.*

Controls

- ma-2 Controlled Maintenance
- sc-7 Boundary Protection
- sc-39 Process Isolation
- si-4 System Monitoring
- sr-10 Inspection of Systems or Components

KSI-SVC-02

> *Encrypt or otherwise secure network traffic.*

Controls

- ac-1 Policy and Procedures
- ac-17.2 Protection of Confidentiality and Integrity Using Encryption
- cp-9.8 Cryptographic Protection
- sc-13 Cryptographic Protection
- sc-20 Secure Name/Address Resolution Service (Authoritative Source)
- sc-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)
- sc-22 Architecture and Provisioning for Name/Address Resolution Service

KSI-SVC-03

> *Encrypt all federal and sensitive information at rest.*

Controls

- ac-20.2 Portable Storage Devices — Restricted Use
- cm-12 Information Location
- cp-9.8 Cryptographic Protection
- sc-13 Cryptographic Protection

KSI-SVC-04

> *Manage configuration centrally.*

Controls

- ac-2.4 Automated Audit Actions
- cm-2 Baseline Configuration
- cm-2.2 Automation Support for Accuracy and Currency
- cm-2.3 Retention of Previous Configurations
- cm-6 Configuration Settings
- pl-10 Baseline Selection
- sa-5 System Documentation
- si-5 Security Alerts, Advisories, and Directives
- sr-10 Inspection of Systems or Components

KSI-SVC-05

> *Enforce system and information resource integrity through cryptographic means.*

Controls

- cm-2.2 Automation Support for Accuracy and Currency
- cm-8.3 Automated Unauthorized Component Detection
- sc-13 Cryptographic Protection
- sr-10 Inspection of Systems or Components

KSI-SVC-06

> *Use automated key management systems to manage, protect, and regularly rotate digital keys and certificates.*

Controls

- ac-17.2 Protection of Confidentiality and Integrity Using Encryption
- ia-5.2 Public Key-based Authentication
- ia-5.6 Protection of Authenticators
- sc-12 Cryptographic Key Establishment and Management

KSI-SVC-07

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

Controls

- ca-7.4 Risk Monitoring
- ra-5 Vulnerability Monitoring and Scanning
- ra-7 Risk Response

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.*

Controls

- ca-3 Information Exchange
- cm-10 Software Usage Restrictions
- ps-7 External Personnel Security

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.*

Controls

- ac-21 Information Sharing
- ca-3 Information Exchange
- cm-12 Information Location
- ps-7 External Personnel Security
- sa-2 Allocation of Resources
- sa-4 Acquisition Process
- sa-9 External System Services

KSI-TPR-03

> *Identify and prioritize mitigation of potential supply chain risks.*

Controls

- ac-20 Use of External Systems
- ra-3.1 Supply Chain Risk Assessment
- sa-9 External System Services
- sa-22 Unsupported System Components
- sr-5 Acquisition Strategies, Tools, and Methods

KSI-TPR-04

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

Controls

- ac-20 Use of External Systems
- ca-3 Information Exchange
- ir-6.3 Supply Chain Coordination
- ps-7 External Personnel Security
- ra-5 Vulnerability Monitoring and Scanning
- sa-9 External System Services
- si-5 Security Alerts, Advisories, and Directives
- sr-5 Acquisition Strategies, Tools, and Methods
- sr-8 Notification Agreements