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..

Controls

- ac-3 Access Enforcement
- ac-4 Information Flow Enforcement
- au-2 Event Logging
- au-3 Content of Audit Records
- au-6 Audit Record Review, Analysis, and Reporting
- ca-2 Control Assessments
- ir-4 Incident Handling
- ra-5 Vulnerability Monitoring and Scanning
- sc-8 Transmission Confidentiality and Integrity

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..

Controls

- ca-2 Control Assessments
- ca-7 Continuous Monitoring
- ca-7.6 Automation Support for Monitoring
- ir-1 Policy and Procedures
- ir-4 Incident Handling
- ir-4.1 Automated Incident Handling Processes
- ir-5 Incident Monitoring
- ir-5.1 Automated Tracking, Data Collection, and Analysis

- ir-6 Incident Reporting
- ir-6.1 Automated Reporting
- ir-6.2 Vulnerabilities Related to Incidents
- pm-3 Information Security and Privacy Resources
- pm-5 System Inventory
- pm-31 Continuous Monitoring Strategy
- ra-2 Security Categorization
- ra-2.1 Impact-level Prioritization
- ra-3 Risk Assessment
- ra-3.3 Dynamic Threat Awareness
- ra-5 Vulnerability Monitoring and Scanning
- ra-5.2 Update Vulnerabilities to Be Scanned
- ra-5.3 Breadth and Depth of Coverage
- ra-5.4 Discoverable Information
- ra-5.5 Privileged Access
- ra-5.6 Automated Trend Analyses
- ra-5.7 Automated Detection and Notification of Unauthorized Components
- ra-5.11 Public Disclosure Program
- ra-9 Criticality Analysis
- ra-10 Threat Hunting
- si-2 Flaw Remediation
- si-2.1 Central Management
- si-2.2 Automated Flaw Remediation Status
- si-2.4 Automated Patch Management Tools
- si-2.5 Automatic Software and Firmware Updates
- si-3 Malicious Code Protection
- si-3.1 Central Management
- si-3.2 Automatic Updates
- si-4 System Monitoring
- si-4.2 Automated Tools and Mechanisms for Real-time Analysis
- si-4.3 Automated Tool and Mechanism Integration
- si-4.7 Automated Response to Suspicious Events

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..

Controls

- at-2 Literacy Training and Awareness
- at-2.2 Insider Threat
- at-2.3 Social Engineering and Mining
- at-3.5 Processing Personally Identifiable Information
- at-4 Training Records
- ir-2.3 Breach

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..

Controls

- at-2 Literacy Training and Awareness
- at-2.3 Social Engineering and Mining
- at-3 Role-based Training
- sr-11.1 Anti-counterfeit Training

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..

Controls

- cp-3 Contingency Training
- ir-2 Incident Response Training
- ps-6 Access Agreements

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..

Controls

- au-2 Event Logging
- cm-3 Configuration Change Control
- cm-3.2 Testing, Validation, and Documentation of Changes
- cm-4.2 Verification of Controls
- cm-6 Configuration Settings
- cm-8.3 Automated Unauthorized Component Detection
- ma-2 Controlled Maintenance

KSI-CMT-02

Applies to: Low, Moderate

> 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

Applies to: Low, Moderate

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

Controls

- cm-3 Configuration Change Control
- cm-3.2 Testing, Validation, and Documentation of Changes
- cm-4.2 Verification of Controls
- si-2 Flaw Remediation

KSI-CMT-04

Applies to: Low, Moderate

> Always follow a documented change management procedure..

Controls

- cm-3 Configuration Change Control
- cm-3.2 Testing, Validation, and Documentation of Changes
- 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

Applies to: Low, Moderate

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

Controls

- ca-7.4 Risk Monitoring
- cm-3.4 Security and Privacy Representatives

- cm-4 Impact Analyses
- cm-7.1 Periodic Review
- 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

Applies to: Low, Moderate

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

Controls

- ac-17.3 Managed Access Control Points
- ca-9 Internal System Connections
- cm-7.1 Periodic Review
- sc-7.5 Deny by Default — Allow by Exception
- si-8 Spam Protection

KSI-CNA-02

Applies to: Low, Moderate

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

Controls

- ac-17.3 Managed Access Control Points
- ac-18.1 Authentication and Encryption
- ac-18.3 Disable Wireless Networking
- ac-20.1 Limits on Authorized Use
- ca-9 Internal System Connections
- sc-7.3 Access Points
- sc-7.4 External Telecommunications Services
- sc-7.5 Deny by Default — Allow by Exception
- sc-7.8 Route Traffic to Authenticated Proxy Servers
- sc-8 Transmission Confidentiality and Integrity
- sc-10 Network Disconnect
- si-10 Information Input Validation
- si-11 Error Handling
- si-16 Memory Protection

KSI-CNA-03

Applies to: Low, Moderate

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

Controls

- ac-12 Session Termination
- ac-17.3 Managed Access Control Points
- ca-9 Internal System Connections
- sc-4 Information in Shared System Resources
- sc-7 Boundary Protection
- sc-7.7 Split Tunneling for Remote Devices
- sc-8 Transmission Confidentiality and Integrity
- sc-10 Network Disconnect

KSI-CNA-04

Applies to: Low, Moderate

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

Controls

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

KSI-CNA-05

Applies to: Low, Moderate

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

Controls

- sc-5 Denial-of-service Protection
- si-8 Spam Protection
- si-8.2 Automatic Updates

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.

Controls

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

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..

Controls

- ca-2.1 Independent Assessors
- ca-7.1 Independent Assessment

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.

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-5 Authenticator Management
- ia-8 Identification and Authentication (Non-organizational Users)
- sc-23 Session Authenticity

KSI-IAM-02

Applies to: Low, Moderate

> 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
- sc-23 Session Authenticity

KSI-IAM-03

Applies to: Low, Moderate

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

Controls

- ac-2 Account Management
- ac-2.2 Automated Temporary and Emergency Account Management
- ac-4 Information Flow Enforcement
- ac-6.5 Privileged Accounts
- ia-3 Device Identification and Authentication
- ia-5.2 Public Key-based Authentication
- ra-5.5 Privileged Access

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.

Controls

- ac-2 Account Management
- ac-2.1 Automated System 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
- ac-17.4 Privileged Commands and Access
- ac-20.1 Limits on Authorized Use
- au-9.4 Access by Subset of Privileged Users
- cm-5 Access Restrictions for Change
- cm-7 Least Functionality
- cm-7.2 Prevent Program Execution
- cm-7.5 Authorized Software — Allow-by-exception
- 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
- ra-5.5 Privileged Access
- sc-2 Separation of System and User Functionality
- sc-23 Session Authenticity
- sc-39 Process Isolation

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..

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-2.7 Configure Systems and Components for High-risk Areas
- 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-5.6 Protection of Authenticators
- 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-4 Information in Shared System Resources
- 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-23 Session Authenticity
- sc-39 Process Isolation
- si-3 Malicious Code Protection

KSI-IAM-06

Applies to: Low, Moderate

> 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-IAM-07

Applies to: Low, Moderate

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

Controls

- ac-2.2 Automated Temporary and Emergency Account Management
- ac-2.3 Disable Accounts
- ac-2.13 Disable Accounts for High-risk Individuals
- ac-6.7 Review of User Privileges
- ia-4.4 Identify User Status
- ia-12 Identity Proofing
- ia-12.2 Identity Evidence
- ia-12.3 Identity Evidence Validation and Verification
- ia-12.5 Address Confirmation

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..

Controls

- ir-4 Incident Handling
- ir-4.1 Automated Incident Handling Processes

- ir-6 Incident Reporting
- ir-6.1 Automated Reporting
- ir-6.3 Supply Chain Coordination
- ir-7 Incident Response Assistance
- ir-7.1 Automation Support for Availability of Information and Support
- ir-8 Incident Response Plan
- ir-8.1 Breaches
- si-4.5 System-generated Alerts

KSI-INR-02

Applies to: Low, Moderate

> 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

Applies to: Low, Moderate

> 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

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.

Controls

- ac-17.1 Monitoring and Control
- ac-20.1 Limits on Authorized Use
- 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
- ir-4.1 Automated Incident Handling Processes
- si-4.2 Automated Tools and Mechanisms for Real-time Analysis
- si-4.4 Inbound and Outbound Communications Traffic
- si-7.7 Integration of Detection and Response

KSI-MLA-02

Applies to: Low, Moderate

> *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
- au-6.1 Automated Process Integration
- si-4 System Monitoring
- si-4.4 Inbound and Outbound Communications Traffic

KSI-MLA-03

Applies to: Low, Moderate

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

Controls

- au-5 Response to Audit Logging Process Failures
- ca-5 Plan of Action and Milestones
- 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-2.2 Automated Flaw Remediation Status
- si-3 Malicious Code Protection
- si-5 Security Alerts, Advisories, and Directives
- si-7.7 Integration of Detection and Response
- si-10 Information Input Validation
- si-11 Error Handling

KSI-MLA-04

Applies to: Low, Moderate

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

Controls

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

KSI-MLA-05

Applies to: Low, Moderate

> Perform Infrastructure as Code and configuration evaluation and testing.

Controls

- ca-7 Continuous Monitoring
- cm-2 Baseline Configuration
- cm-6 Configuration Settings
- si-7.7 Integration of Detection and Response

KSI-MLA-06

Applies to: Low, Moderate

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

Controls

- ca-5 Plan of Action and Milestones

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..

Controls

- ac-2.4 Automated Audit Actions
- ac-6.9 Log Use of Privileged Functions
- ac-17.1 Monitoring and Control
- ac-20.1 Limits on Authorized Use
- au-2 Event Logging
- au-7.1 Automatic Processing
- au-12 Audit Record Generation
- si-4.4 Inbound and Outbound Communications Traffic
- si-4.5 System-generated Alerts
- si-7.7 Integration of Detection and Response

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..

Controls

- si-11 Error Handling

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.

Controls

- cm-2.2 Automation Support for Accuracy and Currency
- 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

Applies to: Low, Moderate

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

Controls

- ac-1 Policy and Procedures
- ac-21 Information Sharing
- at-1 Policy and Procedures
- au-1 Policy and Procedures
- ca-1 Policy and Procedures
- ca-2 Control Assessments
- cm-1 Policy and Procedures
- cp-1 Policy and Procedures
- cp-2.1 Coordinate with Related Plans
- cp-2.8 Identify Critical Assets
- 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
- ra-9 Criticality Analysis
- 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

Applies to: Low, Moderate

> Maintain a vulnerability disclosure program.

Controls

- ra-5.11 Public 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..

Controls

- ac-5 Separation of Duties
- au-3.3 Limit Personally Identifiable Information Elements
- cm-3.4 Security and Privacy Representatives
- pl-8 Security and Privacy Architectures
- pm-7 Enterprise Architecture
- sa-3 System Development Life Cycle
- sa-8 Security and Privacy Engineering Principles
- sc-4 Information in Shared System Resources
- sc-18 Mobile Code
- si-10 Information Input Validation
- si-11 Error Handling
- si-16 Memory Protection

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..

Controls

- ac-5 Separation of Duties
- ca-2 Control Assessments
- cp-2.1 Coordinate with Related Plans
- cp-4.1 Coordinate with Related Plans
- ir-3.2 Coordination with Related Plans
- pm-3 Information Security and Privacy Resources
- sa-2 Allocation of Resources
- sa-3 System Development Life Cycle
- sr-2.1 Establish SCRM Team

KSI-PIY-07

Applies to: Low, Moderate

> Document risk management decisions for software supply chain security.

Controls

- ca-7.4 Risk Monitoring
- sc-18 Mobile Code

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).

Controls

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

KSI-RPL-02

Applies to: Low, Moderate

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

Controls

- cp-2 Contingency Plan
- cp-2.1 Coordinate with Related Plans
- cp-2.3 Resume Mission and Business Functions
- cp-4.1 Coordinate with Related Plans
- cp-6 Alternate Storage Site
- cp-6.1 Separation from Primary Site
- cp-6.3 Accessibility
- cp-7 Alternate Processing Site
- cp-7.1 Separation from Primary Site
- cp-7.2 Accessibility
- cp-7.3 Priority of Service
- cp-8 Telecommunications Services
- cp-8.1 Priority of Service Provisions
- cp-8.2 Single Points of Failure
- cp-10 System Recovery and Reconstitution
- cp-10.2 Transaction Recovery

KSI-RPL-03

Applies to: Low, Moderate

> 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

Applies to: Low, Moderate

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

Controls

- cp-2.1 Coordinate with Related Plans
- cp-2.3 Resume Mission and Business Functions
- cp-4 Contingency Plan Testing
- cp-4.1 Coordinate with Related Plans
- cp-6 Alternate Storage Site
- cp-6.1 Separation from Primary Site

- cp-9.1 Testing for Reliability and Integrity
- cp-10 System Recovery and Reconstitution
- ir-3 Incident Response Testing
- ir-3.2 Coordination with Related Plans

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..

Controls

- cm-7.1 Periodic Review
- cm-12.1 Automated Tools to Support Information Location
- ma-2 Controlled Maintenance
- pl-8 Security and Privacy Architectures
- sc-7 Boundary Protection
- sc-39 Process Isolation
- si-2.2 Automated Flaw Remediation Status
- si-4 System Monitoring
- sr-10 Inspection of Systems or Components

KSI-SVC-02

Applies to: Low, Moderate

> 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-8 Transmission Confidentiality and Integrity
- sc-8.1 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
- sc-23 Session Authenticity

KSI-SVC-03

Applies to: Low, Moderate

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

Controls

- ac-19.5 Full Device or Container-based Encryption
- ac-20.2 Portable Storage Devices — Restricted Use
- ac-21 Information Sharing
- cm-12 Information Location
- cp-9.8 Cryptographic Protection
- sc-13 Cryptographic Protection
- sc-28 Protection of Information at Rest
- sc-28.1 Cryptographic Protection

KSI-SVC-04

Applies to: Low, Moderate

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

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
- cm-7.1 Periodic Review
- pl-9 Central Management
- 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

Applies to: Low, Moderate

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

Controls

- cm-2.2 Automation Support for Accuracy and Currency
- cm-8.3 Automated Unauthorized Component Detection
- sc-13 Cryptographic Protection
- sc-23 Session Authenticity
- si-7 Software, Firmware, and Information Integrity
- si-7.1 Integrity Checks
- sr-10 Inspection of Systems or Components

KSI-SVC-06

Applies to: Low, Moderate

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

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
- sc-17 Public Key Infrastructure Certificates

KSI-SVC-07

Applies to: Low, Moderate

> 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-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..

Controls

- sc-4 Information in Shared System Resources

KSI-SVC-09

Applies to: Moderate

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

Controls

- sc-23 Session Authenticity
- si-7.1 Integrity Checks

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..

Controls

- si-12.3 Information Disposal
- si-18.4 Individual Requests

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).

Controls

- ca-3 Information Exchange
- cm-10 Software Usage Restrictions
- ps-7 External Personnel Security
- sa-4.9 Functions, Ports, Protocols, and Services in Use

KSI-TPR-02

Applies to: Low, Moderate

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

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-4.1 Functional Properties of Controls
- sa-4.2 Design and Implementation Information for Controls
- sa-4.9 Functions, Ports, Protocols, and Services in Use
- sa-9 External System Services
- sa-9.2 Identification of Functions, Ports, Protocols, and Services
- sa-10 Developer Configuration Management
- sa-11 Developer Testing and Evaluation
- sa-15 Development Process, Standards, and Tools

KSI-TPR-03

Applies to: Low, Moderate

> 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-10 Developer Configuration Management
- sa-11 Developer Testing and Evaluation

- sa-15.3 Criticality Analysis
- sa-22 Unsupported System Components
- si-7.1 Integrity Checks
- sr-5 Acquisition Strategies, Tools, and Methods
- sr-6 Supplier Assessments and Reviews

KSI-TPR-04

Applies to: Low, Moderate

> 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-6 Supplier Assessments and Reviews
- sr-8 Notification Agreements