RFC-0006 20x Key Security Indicators

Thursday, April 24, 2025

Background

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 often use automated or code-driven configuration management and control planes to ensure predictable, repeatable, reliable, and secure outcomes during deployment and operation.

Consequently, FedRAMP asserts that 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.

The FedRAMP 20x Phase One Pilot will test this assertion for a subset of low impact systems by granting conditional FedRAMP Low authorization to services that meet the full Phase One eligibility requirements and qualifications. To qualify for this authorization, cloud services must at minimum provide a machine readable package that demonstrates a continuous, automated validation approach for a significant portion of the FedRAMP Key Security Indicators (KSIs) outlined in this standard.

The resulting packages and validation approaches will inform Phase Two and other formal standards for FedRAMP 20x. Services that receive FedRAMP 20x Low authorizations during Phase One will be prioritized for the FedRAMP 20x Moderate pilot in Phase Two.

Key Security Indicators

FedRAMP Key Security Indicators summarize the capabilities that satisfy FedRAMP security requirements aligned to NIST SP 800-53 controls, providing an abstraction layer that is simpler to approach and assess. 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 automatically derived from technical configurations and resolved to true or false.

Key Security Indicators are engineered to address critical limitations in existing security assessment approaches:

- Simplified capabilities: Reduce lengthy and complex security compliance to clear, actionable, capability-based standards
- Automation-Friendly: Eliminate reliance on narrative to create a foundation for future automated security assessment processes
- Flexible Implementation: Enable private innovation to design different methods for validation

Although Key Security Indicators are designed to produce final validations that are true or false, the minimum expectations for validation and assessment will require cloud service providers and third party assessment organizations to provide reasonable evidence supporting the final validation.

To maximize innovation, this standard does not propose validation, evidence, or assessment expectations for Key Security Indicators. Instead, minimum expectations for validation, evidence, and assessment will be determined during active FedRAMP 20x pilots in collaboration with cloud service providers, third party assessment organizations, and federal agencies.

All FedRAMP 20x packages submitted for assessment based on these standards must be in a machine-readable format that can be regenerated on demand.

Key Security Indicators (FedRAMP Low, Cloud Native)

This release includes the Key Security Indicators that must be addressed to meet security requirements for FedRAMP Low authorization for cloud service offerings that meet the following eligibility criteria:

1. Deployed on an existing FedRAMP authorized cloud service offering
    a. Using primarily cloud-native services from the host provider
    b. Using only FedRAMP authorized external services
2. Service is provided only via the public internet (browser and/or APIs)
3. Has completed a SOC 2 Type 2 audit or federal agency ATO process within the last 12 months

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

Cloud service providers MUST:

1. Have denial of service (DoS) protection
2. Configure firewalls/proxy servers to limit inbound and outbound traffic
3. Use immutable containers and serverless functions with strictly defined functionality and privileges
4. Design systems as logically segmented micro-services to minimize the attack surface and lateral movement if compromised
5. Use cloud native virtual networks and related capabilities to enforce logical traffic flow controls
6. Execute continuous scanning of cloud native system components
7. Use high availability design principles to maximize uptime

Related NIST SP 800-53 Controls: SC-5, SC-7, SC-12, SC-39, SR-12

Service Configuration

KSI-SC: A secure cloud service offering will enforce the use of approved cryptography, continuously verify component integrity, and restrict access to external services.

Validation

Cloud service providers MUST:

1. Harden and review network and system configurations
2. Encrypt all network traffic
3. Encrypt all federal and sensitive information at rest
4. Manage configuration centrally
5. Enforce system and component integrity through cryptographic means
6. Use a key management capability to execute regular rotation of digital keys
7. Use a consistent, risk-informed approach for applying security patches

Related NIST SP 800-53 Controls: CM-2, CM-4, CM-8, IA-7, RA-7, SC-8, SC-8 (1), SC-13, SC-28, SC-28 (1), SI-3, SI-4

Identity and Access Management

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

Validation

Cloud service providers MUST:

1. Enforce phishing-resistant multi-factor authentication (MFA)
2. Enforce strong passwords
3. Use secure API authentication methods via industry standard protocols

4. Use a least-privileged, role-based, and just-in-time security model

Related NIST SP 800-53 Controls: AC-2, AC-3, AU-9, AC-14, IA-2, IA-2 (1), IA-2 (2), IA-2 (8), IA-2 (12), IA-4, IA-5, IA-5 (1), IA-6, IA-8, IA-8 (1) ,IA-8 (2), IA-8 (4), IA-11, PS-2, PS-3, PS-4, PS-5, PS-7, PS-9

Monitoring, Logging, and Auditing

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

Validation

Cloud service providers MUST:

1. Operate a Security Information and Event Management (SIEM) system for centralized, tamper-resistent event, activity, and change logging
2. Regularly review and audit logs
3. Rapidly detect and remediate or mitigate vulnerabilities
4. Perform authenticated vulnerability scanning on publicly accessible components
5. Perform Infrastructure as Code (IaC) and configuration scanning
6. Centrally track and prioritize the remediation of identified vulnerabilities

Related NIST SP 800-53 Controls: AC-7, AU-11, AU-2, AU-3, AU-4, AU-8, AU-12, RA-5, SI-2

Change Management

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

Validation

Cloud service providers MUST:

1. Log and monitor system modifications
2. Execute changes though redeployment of version controlled immutable resources rather than direct modification wherever possible
3. Implement automated testing and validation of changes prior to deployment
4. Have a documented change management procedure
5. Evaluate the risk and potential impact of any change

Related NIST SP 800-53 Controls: CM-6, CM-7, CM-10, CM-11

Policy and Inventory

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

Validation

Cloud service providers MUST:

1. Have an up-to-date asset inventory or code defining all deployed assets
2. Have policies outlining their security objectives
3. Maintain a vulnerability disclosure program
4. Build security considerations into the Software Development Lifecycle (SDLC) and aligning with Secure By Design principles
5. Document methods used to automatically evaluate implementations
6. Have a dedicated staff and budget for security

Related NIST SP 800-53 Controls: AC-1, AU-1, CA-1, CM-1, CM-8, CP-1, IA-1, IR-1, PL-1, PL-2, PS-1, RA-1, SA-1, SA-2, SA-3, SA-5, SA-8, SC-1, SI-1, SR-1

Third Party Information Resources

KSI-3IR: A secure cloud service offering will understand, monitor, and manage supply chain risks from third party services or components.

Validation

Cloud service providers MUST:

1. Regularly confirm that services storing Federal information are all FedRAMP authorized and securely configured
2. Identify and prioritize potential supply chain risks
3. Obtain a Software Bill of Materials (SBOM) for third party commercial software components
4. Confirm that third party information resources have a Secure Software Development Attestation with CISA
5. Implement zero trust design principles

Related NIST SP 800-53 Controls: AC-2, AC-20, AC-23, CA-3, CA-9, RA-3 (1), SA-4, SA-9, SA-22, SI-5, SR-2, SR-2 (1), SR-3, SR-5, SR-8, SR-10, SR-11, SR-11 (2)

Cybersecurity Education

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

Validation

Cloud service providers MUST:

1. Ensure all employees receive security awareness training
2. Require role-specific training for high risk roles

Related NIST SP 800-53 Controls: AT-2, AT-3, AT-6

Incident Response

KSI-IR: A secure cloud service offering will maintain, test, and execute effective Incident Response Plans for routine incidents such as vulnerability discovery, abnormal activity detection, and exfiltration of data.

Validation

Cloud service providers MUST:

1. Define Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
2. Perform system backups aligned with the RTO and RPO
3. Test the capability to recover from incidents and contingencies
4. Report incidents according to federal requirements
5. Maintain a log of incidents and periodically review past incidents for patterns or vulnerabilities
6. Measure Mean Time To Detect (MTTD) and Mean Time To Resolution (MTTR) for incidents

Related NIST SP 800-53 Controls: CP-2, CP-4, CP-9, CP-10, IR-4, IR-5, IR-6, IR-7, IR-8, PS-8, RA-3, RA-5 (2), RA-5 (11)