SunStone Secure

FedRAMP 20x KSIs

May 15

2025

SunStone

Secure By Design

FedRAMP 20x KSIs

- KSI-CNA: Cloud Native Architecture
- KSI-SC: Service Configuration
- KSI-SC: Identity and Access Management
- KSI-MLA: Monitoring, Logging, and Auditing
- KSI-CM: Change Management
- KSI-PI: Policy and Inventory
- KSI-3IR: Third Party Information Resources
- KSI-CE: Cybersecurity Education
- KSI-IR: Incident Response

KSI-CNA

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

KSI-SC

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

KSI-IAM

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

KSI-MLA

Cloud service providers MUST:

1. **Operate a Security Information and Event Management (SIEM) system for centralized, tamper-resistant 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-2, AU-3, AU-4, AU-8, AU-11, AU-12, RA-5, SI-2

KSI-CM

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

KSI-PI

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

KSI-3IR

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)

KSI-CE

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

KSI-IR

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)

Idea 1

New Catalog or Profile

Idea 2

Group Components into supporting Capabilities

Idea 3

Use the mapping model

Idea 4

Keep it in the Assessment Results

Question: Where do metrics go?

Idea 1: New Catalog or Profile

KSIs define what is “expected of a cloud-native service offering to meet FedRAMP Low authorization requirements. These indicators *align* to NIST SP 800-53 controls and form a **baseline equivalent**.”

Pros: Simple fit for existing tooling, existing 1.1.x models

Cons: KSIs are not really controls. They are measures or metrics (like KPIs) - meant to be boolean true/false.

Violates DRY

EASY

Idea 2: Component Definition Capabilities

“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.”

Pros: Fits the definition and intent - automation technology provides security - not only “controls”

Cons: Capabilities in the CDef model are just groups of controls. No link back from SSP/AP/AR

Both: You can’t really define your KSIs without your component defs.

Idea 3: Use the Mapping Prototype

"Key Security Indicators creates an **abstraction layer** to summarize the security capabilities expected of a cloud-native service offering to meet FedRAMP Low authorization requirements. These indicators *align* to NIST SP 800-53 controls and form a **baseline equivalent**."

Pros: Most DRY solution - can simply map new KSI "dummy" controls to existing frameworks

Cons:Prototype model - well supported? (We'll find out today!)

Seems extra toil to have extra catalogs.

Idea 4: Assessment Plan and Results - objectives

Pros: Most of the complexity hidden until the Assessment

Reuse of existing catalog(s)

Overloading objectives with a “MEASURE”

Cons:you need controls (control-id) to define assessment-objectives.

Not native - need “plugin”

OPEN MIC

New Idea

????

New Idea

????

New Idea

????