Working Group: Advancing Cloud Security

May 9, 2025

GovRAMP

Agenda

1. Introductions
2. Pilot, Open Request for Comments & Working Group Highlights
3. Member Feedback
4. Next Steps

Note: Due to the number of participants, please use the chat feature to post comments and questions. We will be recording the meeting and make it available to participants following the call.

Facilitators

Leah McGrath
Executive
Director
GovRAMP
leah@stateramp.org

Fred Brittain
Executive Advisor to
GovRAMP PMO
GovRAMP PMO
fred@stateramp.org

David Resler
GovRAMP PMO
Director
GovRAMP PMO
david@stateramp.org

FedRAMP Pilot, Open *Request for Comment* & Discussion

FedRAMP posted updates to a pilot, significant changes, boundary guidance and KSI’s for 20x Pilot.

GovRAMP

FedRAMP Open Request for Comments (RFC)

FedRAMP Open Request for Comments on 4/25 -- Due 5/25/2025

Description	Opened
Significant Change Notification Standard	FedRAMP intends to replace the previous Significant Change Request process with an updated Significant Change Notification standard. The process asserts authorizations granted to cloud service providers include the authority to make changes that are in the best interest of agency customers without asking permission from an authorizing official in advance, in most cases.
20x Phase One Key Security Indicators	In FedRAMP 20x, Key Security Indicators summarize the security capabilities expected of cloud-native service offerings to meet FedRAMP Low authorization requirements.
Minimum Assessment Scope	The FedRAMP Minimum Assessment Scope Standard is an updated approach to determining what is included in a FedRAMP assessment and authorization. The approach avoids the unnecessary detail to support FedRAMP's ongoing shift from compliance-based to security-based decision making and assessment.

RFC: Significant Change Notification Standard

High level summary of proposed Significant Change Notification Standard

Further defines significant change:

Adaptive Change: Adjusts existing components or functionality; least impactful.

- Does not require 3PAO
- Notification to FedRAMP and Agency *after and within 14 days of* making change and at next monthly meeting

Transformative Change: Adds, replaces, or removes major components and functionality.

- Requires 3PAO
- Notification to FedRAMP and Agency *before (minimum 14 days)* making change and at next monthly meeting

Impact Categorization Change: Likely to change the impact level rating; most impactful.

- Not allowed. Requires re-authorization at new impact level.

Describes exception process and notification requirements.

RFC: Minimum Assessment Scope Standard

Excerpts

FedRAMP asserts that tying FedRAMP authorizations to an "authorization boundary" creates confusion because the boundary specified in an agency's authorization to operate a cloud service will always include additional resources… Agencies must follow OMB and NIST guidance to establish an appropriate authorization boundary for agency information systems that use FedRAMP authorized or certified cloud services.

This updated standard creates a standardized FedRAMP Minimum Assessment Scope that rescinds and replaces ALL previous guidance related to the boundaries.

The Minimum Assessment Scope includes all information resources managed by a cloud service provider and their cloud service offering that:

1. *Handle federal information; and/or*
2. *Likely impact confidentiality, integrity, or availability of federal information*

RFC: 20x Phase 1 Key Security Indicator’s (KSI)

High level summary of FedRAMP Phase 1 20x pilot eligibility for Low Impact SaaS Providers

Eligibility criteria for FedRAMP Low authorization for cloud service offerings:

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

RFC: 20x Phase 1 Key Security Indicator's (KSI)

Example:

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*

RFC: 20x Phase 1 Key Security Indicator's (KSI)

High level summary of KSI's for Phase 1 Pilot

Category	Description	Related NIST SP 800-53 Controls
Cloud Native Architecture	Uses cloud native architecture and design principles to enhance Confidentiality, Integrity, and Availability.	SC-5, SC-7, SC-12, SC-39, SR-12
Service Configuration	Enforces approved cryptography, verifies component integrity, and restricts access to external services.	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	Protects user data, controls access, and implements zero trust practices.	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	Monitors, logs, and audits all important events, activity, and changes.	AC-7, AU-2, AU-3, AU-4, AU-8, AU-11, AU-12, RA-5, SI-2
Change Management	Ensures all system changes are documented and configuration baselines are updated.	CM-6, CM-7, CM-10, CM-11
Policy and Inventory	Provides organized guidance for securing every asset, including personnel.	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	Manages supply chain risks from third party services or components.	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	Continuously educates employees on cybersecurity measures and tests their knowledge.	AT-2, AT-3, AT-6
Incident Response	Maintains, tests, and executes effective Incident Response Plans for routine incidents.	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)

FedRAMP Working Group Discussion

Most of the recent discussion is around the FedRAMP 20x Pilot scenario:

- *FedRAMP 20x Pilot scenario: I am a CSP with an existing SOC2 Type 2 report - what KSIs can't be validated and why?*
- *Open thread for questions related to FedRAMP 20x Pilot*

Ask Me Anything with Pete Waterman

April 30 Automating Assessments Working Group Call

Video available at: https://www.youtube.com/watch?v=IIRoPUykBRo

Key Takeaways:

- When asked what Plan B was if 20x fails, Pete indicated **20x is Plan B…Traditional Assessments are Plan A**.
- **KSI could change** over time & with community input, but the focus will be on the KSIs in the RFC.
- The emphasis is on providing **Machine Readable** data to the FedRAMP PMO. Albeit there is not yet an established standard for this interchange of data.
  - "Do your best to establish machine readable formats. That's the goal of this. The expectation is not 100% coverage.“
  - The Machine Readable format **does not have to be OSCAL** (Open Security Controls Assessment Language).
- If the pilot is successful, the intent is to do a pilot for Moderate Impact and also entertain other frameworks like ISO27001

Thoughts?

GovRAMP

Next GovRAMP Working Session

Submit an Idea + Register for
GovRAMP Working Session #3:

Friday, June 20 at 2 pm ET

https://govramp.org/working-group/

Thank you!

It is an honor to serve you. For questions, please email info@stateramp.org.

GovRAMP