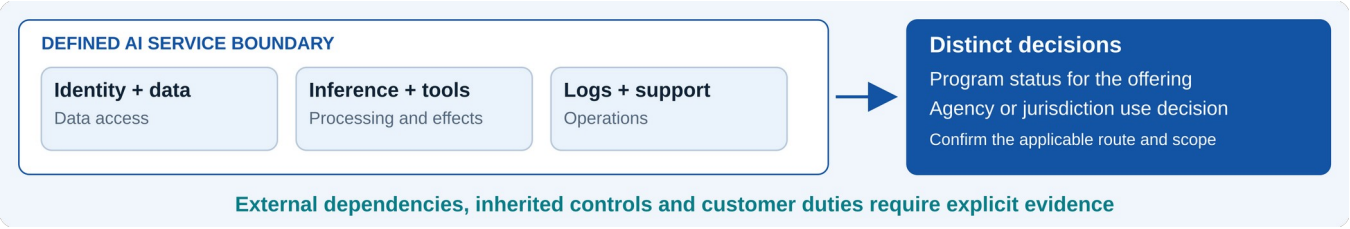
FedRAMP 20x and GovRAMP for AI services

Choosing the right boundary and producing credible security evidence

Anwesh Rath, Founder and CTO, AI Standards Inc.



Conceptual service boundary. Program status and the government use decision remain distinct.

Executive summary

An AI service needs a defined operating boundary and evidence for the controls it claims. Running on a certified cloud, using a particular model provider or storing data on customer hardware does not by itself establish government approval. Start with the offering, the division of responsibilities and the intended government use.

This paper connects FedRAMP and GovRAMP requirements to AI architecture decisions: data flows, inherited controls, evidence collection and changes to models or tools. The practical objective is an assessable service whose security assertions can be tested. The offering's formal program status and the agency's decision to use it remain distinct decisions.

Use the current program types and paths

FedRAMP's Consolidated Rules for 2026 distinguish certification type, class and path. The types are 20x and Rev5. A 20x offering follows Program Certification; Rev5 generally follows Agency Certification, with limited temporary exceptions [1].

Cloud-native services built on FedRAMP-certified infrastructure or platforms generally fit 20x. Under current guidance, services operating their own infrastructure or requiring Class D use Rev5. Formal 20x Class D availability is planned for 2027. Confirm eligibility and the required class before committing to a route. Certification classes do not map directly to agency impact levels [1].

The published timetable opened applications for 20x Class B and C on 31 August 2026. It sets 1 January 2027 for mandatory adoption of the consolidated rules, subject to applicable transition provisions, and 11 June 2027 as the final date for applications for new Rev5 certifications [2].

FedRAMP certification does not remove the agency's responsibility to assess integration and authorize operation of its information system [3]. Identify the decision-maker and evidence needed for both the offering and its intended agency use.

GovRAMP is the public brand of StateRAMP, which remains the legal entity [4]. Its Authorized and Provisional verification routes involve independent assessment and government sponsorship or Approvals Committee review [5]. Confirm the purchasing jurisdiction's requirements; GovRAMP status is not interchangeable with federal agency authorization.

Define the AI service and its responsibilities

Map identity, retrieval, inference, tools, storage, management access, telemetry and support. Show where government information enters, where it is processed and which parties can access it. Include external model calls, logs and backups. Distinguish resources inside the assessment scope from third-party dependencies, and record the basis for that treatment under the applicable boundary rules [6].

For an on-premises deployment, first determine whether the offering and intended use are within FedRAMP's scope. Identify who operates the service, its external cloud dependencies, and the agency authorization and procurement requirements that apply. Record the determination for the actual deployment.

Create a responsibility record for each control outcome. Identify what the provider implements, what is inherited and what the customer must configure or operate. Substantiate inheritance with the exact offering, package and conditions of use. Infrastructure status alone does not establish coverage for retrieval permissions, tool access or support processes.

Design evidence around the offering

For 20x, build evidence collection into operations. Identify the measured resources, collection method, acceptable age and failure conditions. A privileged-access check, for example, should identify the account population, approved scopes, observed grants, collector version and observation time. Retain exclusions and collection failures with the result, and separate collection credentials from workload credentials.

Engineering preparation checklist

Map these preparation areas to the selected profile or GovRAMP package. For each applicable requirement, record its version, owner, implementation, evidence and unresolved exceptions.

Preparation area	Technical and operating control	Evidence to retain
Define the boundary	Inventory data flows, dependencies and administrative paths.	Versioned scope, asset inventory and responsibility record.
Restrict consequential access	Enforce authorization at the service or tool boundary; define required approvals.	Identity and scope records, denial tests and approval-to-execution records.
Substantiate inheritance	Review the exact external service and conditions of use.	Relevant package, dependency review and customer control requirements.
Assess AI changes	Evaluate model, retrieval, tool and supplier changes before release.	Change decision, evaluation results and deployment history.
Maintain current assurance	Own evidence collection, exceptions and required monitoring.	Dated observations, remediation records and assessment results.

Make evidence failures visible

A collector can fail while the AI application continues to answer requests. For each evidence source, name an owner, define its maximum acceptable age and test the response to missing or incomplete observations. Decide whether the failure blocks a consequential operation, creates an incident or requires another documented response. Follow the applicable requirement and the consequence of losing the evidence.

Separate observation time from collection or submission time. Preserve the assessed configuration and reconcile the observed population to the inventory. Protect records against alteration, control access and apply an approved retention policy. For the FedRAMP Security Decision Record, maintain implementation rationale, customer risk, assessment findings and supporting artifacts as the service changes [7].

Move from architecture to an assessable service

Confirm the government use case, information sensitivity and program requirements with the agency and applicable program participants. Engage the independent assessor early to agree on scope and evidence expectations. Close gaps in support access, dependencies, recovery and the service's behavior when a control or supplier is unavailable.

Exercise the deployed configuration with representative data, permissions and failure conditions. Retain acceptance tests and observed results, then resolve findings through accountable remediation. Maintain the monitoring and change processes required after formal status is obtained. GovRAMP Fast Track permits reuse of federal assessment materials subject to PMO review; it does not remove the separate verification decision [5].

Illustrative model service change

This is an invented scenario, not a government deployment. A provider operates an AI document service within a defined cloud boundary. A team proposes routing difficult requests to an external model API. The application interface stays the same, but the data flow, dependency and operating responsibilities change.

Before enabling the route, identify whether prompts, retrieved passages, outputs, identifiers or telemetry leave the approved environment. Check the exact supplier service, retention and reuse terms, support access and effect on inherited controls. Determine whether assessment, notification or a new decision is required under the applicable program and agency process. Preserve that decision and update the system description [8].

A later proposal moves inference onto customer hardware. Assess that configuration separately, including management access, updates, backups, telemetry and recovery. Local placement can change responsibilities and data movement; the relevant result is a documented treatment of the service and evidence for the controls that apply.



Conceptual evidence lifecycle. Collection failure remains visible and has an accountable owner.

AI Standards engineering approach

AI Standards focuses on client-controlled AI infrastructure: defining where workloads run, who can authorize consequential actions and what information may cross a boundary. These priorities connect directly to the evidence a government buyer needs to understand the offering and its operating responsibilities.

Filed provisional patent applications associated with this work address client-controlled deployment, workload boundaries and selective disclosure. They reflect an engineering focus on keeping control with the customer while making governance decisions and permitted information sharing accountable. The applications are not granted patents and do not establish government program status.

For a deployment-specific review, evaluate scoped operator permissions, server-side approval enforcement, controlled inference configuration and records linking requests to decisions and outcomes. Test the response to expired permissions, failed record writes, retries and alternate execution paths. Define exactly when an operation is considered complete. A local hash alone does not establish record completeness or independent attestation.

A scoped AIS architecture and evidence review should produce a versioned boundary, a responsibility record and a prioritized plan for closing evidence gaps with the buyer and applicable assessor. Validate the actual configuration and its operation before asserting readiness. No FedRAMP certification, GovRAMP authorization or government deployment is claimed for AIS in this paper.

References

Public sources checked 5 November 2026. Reconfirm operative rules before an application or procurement decision.

[1] FedRAMP, certification paths, types and classes. Choose a Path; Choose a Type; Choose a Class

[2] FedRAMP, Consolidated Rules for 2026. Important Dates

[3] FedRAMP, Consolidated Rules for 2026. Agency Responsibilities

[4] StateRAMP, 14 February 2025. GovRAMP rebrand announcement

[5] GovRAMP. Authorized and Provisional Verification

[6] FedRAMP. The 20x FedRAMP Boundary; Provider eligibility

[7] FedRAMP. Definitions including Security Decision Record

[8] FedRAMP. 20x Assurance Rulesets

About the author Anwesh Rath, Founder and CTO, AI Standards Inc.

Disclaimer Informational, not legal advice. Applicability depends on the offering, jurisdiction and intended use. Obtain qualified advice and validate controls for the deployment. Examples are illustrative; no certification, compliance or performance guarantee is offered.