FedRAMP Standard

- **Release:** 25.00A DRAFT
- **Published:** 2025-00-00
- **Designator:** CCM
- **Description:** THIS IS A DRAFT AND IS NOT FINALIZED, USE AT YOUR OWN RISK. Initial DRAFT release of the Collaborative Continuous Monitoring Standard (CCM) after public comment.

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-00-00** for **20x**.
  - This policy applies to all FedRAMP 20x authorizations.
  - Phase One Pilot participants have one year from authorization to fully implement this standard but must demonstrate continuous quarterly progress.
  - Phase Two Pilot participants must demonstrate significant progress towards implementing this standard prior to submission for authorization review.
- **FedRAMP Rev5**:
  - This release is effective **2025-00-00** for **Rev5 Closed Beta**.
  - Rev5 Authorized providers MUST NOT adopt this standard without participating in a formal beta process with FedRAMP.
  - Rev5 providers MUST first align with the Significant Change Notification Standard and the Vulnerability Detection and Response Standard.

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: Managing Information as a Strategic Resource section 4 (c) states that agencies SHALL "conduct and document security and privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and the agency risk tolerance"
- The FedRAMP Authorization Act (44 USC § 3609 (a)(1)) directs the Administrator of the General Services Administration to "develop, coordinate, and implement a process … including, as appropriate, oversight of continuous monitoring of cloud computing products and services"

Purpose

Agencies are required to continuously monitor all of their information systems following a documented process integrated into their Information Security Continuous Monitoring (ISCM) strategy. These strategies are specific to each agency and

may even vary at the bureau, component, or information system levels.

The concept behind collaborative continuous monitoring is unique to government customers and creates a burden for commercial cloud service providers. This standard attempts to minimize this burden by encouraging the use of automated monitoring and review of authorization data required by other FedRAMP standards and limiting the expected human interaction costs for cloud service providers and agencies. Agencies are expected to use information from the cloud service provider collaboratively in accordance with their agency ISCM strategy without blocking other agencies from making their own risk-based decisions about ongoing authorization.

Expected Outcomes

- Cloud service providers will operate their services and share additional information with agency customers to ensure they can meet their responsibilities and obligations for safely and securely operating the service
- Federal agencies will have streamlined access to the information they actually need to make ongoing security and authorization decisions while having support from government-wide policies that demonstrate the different responsibilities and obligations for operating cloud services

---

Requirements and Recommendations

FRR-CCM

These requirements and recommendations apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-CCM-01

Applies to: Low, Moderate, High

> Providers MUST make an *Ongoing Authorization Report* available to *all necessary parties* every 3 months, in a consistent format that is human readable, covering the entire period since the previous summary; this report MUST include high-level summaries of at least the following information:
>
> 1. Changes to *authorization data*
> 2. Planned changes to *authorization data* during at least the next 3 months
> 3. _Accepted vulnerabilities
> 4. *Transformative* changes
> 5. Updated recommendations or best practices for security, configuration, usage, or similar aspects of the *cloud service offering*

FRR-CCM-02

Applies to: Low, Moderate, High

> Providers SHOULD establish a regular 3 month cycle for *Ongoing Authorization Reports* that is spread out from the beginning, middle, or end of each quarter.
>
> *Note: This recommendation is intended to discourage hundreds of cloud service providers from releasing their _Ongoing Authorization Reports* during the first or last week of each quarter because that is the easiest way for a single provider to track this deliverable; the result would overwhelm agencies with many cloud services. Widely used cloud service providers are encouraged to work with their customers to identify ideal timeframes for this cycle._

FRR-CCM-03

Applies to: Low, Moderate, High

> Providers MUST publicly include the target date for their next *Ongoing Authorization Report* with the *authorization data* required by FRR-ADS-01.

FRR-CCM-04

Applies to: Low, Moderate, High

> Providers MUST establish and share an asynchronous mechanism for *all necessary parties* to provide feedback or ask questions about each *Ongoing Authorization Report*.

FRR-CCM-05

Applies to: Low, Moderate, High

> Providers MUST maintain an anonymized and desensitized summary of the feedback, questions, and answers about each *Ongoing Authorization Report* as an addendum to the *Ongoing Authorization Report*.
>
> *Note: This is intended to encourage sharing of information and decrease the burden on the cloud service provider - providing this summary will reduce duplicate questions from _agencies* and ensure FedRAMP has access to this information. It is generally in the provider's interest to update this addendum frequently throughout the quarter._

FRR-CCM-06

Applies to: Low, Moderate, High

> Providers MUST NOT irresponsibly disclose sensitive information in an *Ongoing Authorization Report* that would *likely* have an adverse effect on the *cloud service offering*.

FRR-CCM-07

Applies to: Low, Moderate, High

> Providers MAY responsibly share some or all of the information an *Ongoing Authorization Report* publicly or with other parties if the provider determines doing so will NOT *likely* have an adverse effect on the *cloud service offering*.

FRR-CCM-QR

These requirements and recommendations apply to providers hosting synchronous *Quarterly Reviews* with all agencies.

FRR-CCM-QR-01

Applies to: Low

> Providers SHOULD host a synchronous *Quarterly Review* every 3 months, open to *all necessary parties*, to review aspects of the most recent *Ongoing Authorization Reports* that the provider determines are of the most relevance to *agencies*; providers who do not host *Quarterly Reviews* MUST clearly state this and explain this decision in the *authorization data* available to all *necessary parties* required by FRR-ADS-06 and FRR-ADS-07

FRR-CCM-QR-02

Applies to: Moderate, High

> Providers MUST host a synchronous *Quarterly Review* every 3 months, open to *all necessary parties*, to review aspects of the most recent *Ongoing Authorization Reports* that the provider determines are of the most relevance to *agencies*.

FRR-CCM-QR-03

Applies to: Low, Moderate, High

> Providers SHOULD regularly schedule *Quarterly Reviews* to occur at least 3 business days after releasing an *Ongoing Authorization Report* AND within 10 business days of such release.

FRR-CCM-QR-04

Applies to: Low, Moderate, High

> Providers MUST NOT irresponsibly disclose sensitive information in a *Quarterly Review* that would *likely* have an adverse effect on the *cloud service offering*.

FRR-CCM-QR-05

Applies to: Low, Moderate, High

> Providers MUST include either a registration link or a downloadable calendar file with meeting information for *Quarterly Reviews* in the *authorization data* available to all *necessary parties* required by FRR-ADS-06 and FRR-ADS-07.

FRR-CCM-QR-06

Applies to: Low, Moderate, High

> Providers MUST publicly include the target date for their next *Quarterly Review* with the *authorization data* required by FRR-ADS-01.

FRR-CCM-QR-07

Applies to: Low, Moderate, High

> Providers SHOULD include additional information in *Quarterly Reviews* that the provider determines are of interest, use, or otherwise relevant to *agencies*.

FRR-CCM-QR-08

Applies to: Low, Moderate, High

> Providers MUST NOT invite third parties to attend *Quarterly Reviews* intended for *agencies* unless it is of specific relevance.
>
> *Note: This is because _agencies* are less likely to actively participate in meetings with third parties; the cloud service provider's independent assessor should be considered relevant by default._

FRR-CCM-QR-09

Applies to: Low, Moderate, High

> Providers SHOULD record or transcribe *Quarterly Reviews* and make such available to *all necessary parties* with other *authorization data* required by FRR-ADS-06 and FRR-ADS07.

FRR-CCM-QR-10

Applies to: Low, Moderate, High

> Providers MAY responsibly share recordings or transcriptions of *Quarterly Reviews* with the public or other parties ONLY if the provider removes all *agency* information (comments, questions, names, etc.) AND determines sharing will NOT *likely* have an adverse effect on the *cloud service offering*.

FRR-CCM-QR-11

Applies to: Low, Moderate, High

> Providers MAY responsibly share content prepared for a *Quarterly Review* with the public or other parties if the provider determines doing so will NOT *likely* have an adverse effect on the *cloud service offering*.

FRR-CCM-AG

This section includes requirements and recommendations for *agencies* who are using FedRAMP Authorized cloud services based on statute and policy directives from OMB that apply to *agencies*.

FRR-CCM-AG-01

Applies to: Low, Moderate, High

> Agencies MUST review each *Ongoing Authorization Report* to understand how changes to the *cloud service offering* may impact the previously agreed-upon risk tolerance documented in the *agency's* Authorization to Operate of a federal information system that includes the *cloud service offering* in its boundary.
>
> *Note: This is required by 44 USC § 35, OMB A-130, FIPS-200, and M-24-15.*

FRR-CCM-AG-02

Applies to: Low, Moderate, High

> Agencies SHOULD consider the Security Category noted in their Authorization to Operate of the federal information system that includes the *cloud service offering* in its boundary and assign appropriate information security resources for reviewing *Ongoing Authorization Reports*, attending *Quarterly Reviews*, and other ongoing *authorization data*.

FRR-CCM-AG-03

Applies to: High

> Agencies SHOULD designate a senior information security official to review *Ongoing Authorization Reports* and represent the agency at *Quarterly Reviews* for *cloud service offerings* included in agency information systems with a Security Category of High.

FRR-CCM-AG-04

Applies to: Low, Moderate, High

> Agencies SHOULD formally notify the provider if the information presented in an *Ongoing Authorization Report*, *Quarterly Review*, or other ongoing *authorization data* causes significant concerns that may lead the *agency* to remove

> the *cloud service offering* from operation.

FRR-CCM-AG-05

Applies to: Low, Moderate, High

> Agencies MUST notify FedRAMP by sending a notification to info@fedramp.gov if the information presented in an *Ongoing Authorization Report*, *Quarterly Review*, or other ongoing *authorization data* causes significant concerns that may lead the *agency* to stop operation of the *cloud service offering*.
>
> *Note: Agencies are required to notify FedRAMP by OMB Memorandum M-24-15 section IV (a).*

FRR-CCM-AG-06

Applies to: Low, Moderate, High

> Agencies MUST NOT place additional security requirements on cloud service providers beyond those required by FedRAMP UNLESS the head of the agency or an authorized delegate makes a determination that there is a demonstrable need for such; this does not apply to seeking clarification or asking general questions about *authorization data*.
>
> *Note: This is a statory requirement in 44 USC § 3613 (e) related to the Presumption of Adequacy for a FedRAMP authorization.*

FRR-CCM-AG-07

Applies to: Low, Moderate, High

> Agencies MUST inform FedRAMP after requesting any additional information or materials from a cloud service provider beyond those required in this policy by sending a notification to info@fedramp.gov.
>
> *Note: Agencies are required to notify FedRAMP by OMB Memorandum M-24-15 section IV (a).*
