FedRAMP Roadmap 2024-2025

March 2024

info@fedramp.gov

fedramp.gov

GSA

We are making a roadmap to:

- Respond to stakeholder feedback that the program’s growth is not enough to **meet the needs of the market.**
- Clearly define **GSA’s and FedRAMP’s strategic goals**, and make sure the program’s resources are prioritized around them.
- Communicate publicly that **FedRAMP is committed to modernizing**, with enough key details to show how and why.

Read our **blog post to learn more** about FedRAMP’s Roadmap and why it matters

Our Commitment to Our Customers

FedRAMP will **make it safe and easy** for the U.S. government to **take full advantage of cloud services** to meet its mission.

The Benefits of What We Do

FedRAMP applies a unified security standard for all cloud products and services

Do Once, Use Many Times

Providing a common security framework improves the government's security posture and allows agencies and cloud providers to reuse work and eliminate duplicative efforts

A Brand That Goes Beyond The Federal Space

FedRAMP is recognized government-wide, internationally, commercially, in higher education, and within state and local government as the leader in security frameworks

Security Guidance And Support

FedRAMP provides training, guidance and advisory support to cloud providers and agencies, helping them navigate the FedRAMP process and understand the requirements

Our Key Stakeholders

200+

Federal Agencies

400+

Cloud Service Providers (CSPs)

** Including 60+ small businesses*

40+

Third Party Assessment Organizations (3PAOs)

We are driving towards a future with...

Improved Customer Experience

- Growth of a trusted marketplace of cloud services available for federal agencies
- Engagement with a larger, more technical PMO staff

Stronger Security and Risk Management

- Increased visibility into the security posture of CSPs through centralized continuous monitoring
- More clear and consistent security expectations with supporting guidance

Reduced Time and Cost

- Less manual and time intensive to create and share authorization packages
- Reduced time and cost to review and assess authorization packages
- Reduced manual effort and time to complete continuous monitoring

Strategic Goals - Our Focus for 2024-2025

1 Orient FedRAMP around the **customer experience.**

2 Position the program as a **leader in cybersecurity** and risk management.

3 Significantly **scale** the size and scope of a **trusted FedRAMP marketplace.**

4 Increase **program effectiveness** through automation and technology-forward operations.

1

Orient FedRAMP around the customer experience

Challenge

Cloud service providers have found it difficult to navigate a process that takes too long and costs too much to achieve a FedRAMP authorization and implement new features.

What We Will Deliver First

- **Enable agile software delivery** by piloting a replacement “significant change request” process that does not block on advance approval.
- **Tackle known key policy obstacles** that inhibit larger security goals in the authorization process (e.g., cryptography requirements, how cloud providers integrate with other cloud providers).
- **Increase clarity on how to successfully navigate FedRAMP** by creating a living knowledge base of guidance, training, and real-world examples.
- **Incentivize CSPs to provide secure configuration profiles** and guidance on the use of their services, in collaboration with CISA.

2

Position the program as a leader in cybersecurity and risk management

Challenge

FedRAMP is a security and risk management program and people expect that authorized services meet a certain security bar.

What We Will Deliver First

- **Bring more technical capacity and expertise** into the FedRAMP program (at GSA) and ecosystem (agency partners).
- **Define the core security expectations** for all FedRAMP authorizations in support of a government-wide presumption of adequacy.
- **Define initial approach for reciprocity between FedRAMP and external frameworks**, starting with low-impact SaaS.

3

Significantly scale the size and scope of a trusted FedRAMP marketplace

Challenge

Despite its growth over the years, the FedRAMP marketplace has not kept pace with agency demand for new and innovative services.

What We Will Deliver First

- **Implement low-review process with trusted authorizing partners.** Pursuing a pilot with the Department of Defense.
- **Form initial joint authorization groups** to reduce extra reviews and delays in FedRAMP authorization.
- **Centralize and automate continuous monitoring** to reduce burden and improve visibility into the cybersecurity posture of cloud service providers.

4

Increase program effectiveness through automation and technology-forward operations

Challenge

FedRAMP processes are too manual and take too long, and its performance metrics should drive program outcomes that more fully address customer needs.

What We Will Deliver First

- **Publish new key performance metrics aligned with the lived customer experience**, including their time and cost outcomes.
- **Establish a new FedRAMP technology platform** that will facilitate a data-first, api-first foundation for agencies and cloud providers to send and receive security information from FedRAMP.
- **Support machine-readable “digital authorization packages”** to support automation. Piloting with commercial cloud providers, and agency partners.

Benefits We Will Deliver to Our Customers

Cloud Service Providers

- Can see how to deploy significant changes without blocking on federal approval
- Can use and contribute to a growing public knowledge base
- Can confidently build, validate and submit a digital authorization package
- Are seeing the program's metrics reflect their own experience

Authorization Teams (Agencies and PMO)

- All authorizers should have a platform that eases the authorization and review process
- Pilot partners should see reduced PMO review of their packages based on their mature processes
- Are led and engaged by a larger, more technical PMO staff

Agencies

- Have a centralized repository that accommodates all authorization packages
- Have the tools to review digital authorization packages

HIGH-LEVEL ROADMAP

	FY24 (Q3-Q4)	FY25 (Q1-Q2)	FY25 (Q3-Q4)
Customer Experience	• Pilot a new agile significant change process • Begin publishing a knowledge base of guidance and examples to help navigate FedRAMP	• Enhance knowledge base of guidance, training, and examples based on feedback and survey • Incorporate CISA SCuBA guidance into secure configuration profiles	• Incorporate secure configuration profiles into FedRAMP marketplace and platform
Cybersecurity Leadership	• Bring more technical capacity and expertise into the program • Release updated guidance on FIPS 140 • Release updated guidance on integrations with external services	• Define initial approach for reciprocity between external frameworks and low baseline • Define core security expectations across FedRAMP authorizations, and a threat-based approach to updating them regularly • Partner with CISA on red teaming and specialized reviews	• Release crosswalk between external frameworks and FedRAMP low baseline • Release draft Expert Risk Assessment Framework (“red teaming”)
Scaling the Trusted Market	• Implement low-review process with trusted authorizing partners • Form initial joint authorization groups • Release approach for centralized continuous monitoring	• Publish low-review FedRAMP authorization criteria • Publish initial program authorization criteria	• Move to low-review FedRAMP authorization process for more agencies • Centralize and automate continuous monitoring • Establish program authorization path
Program Effectiveness	• Pilot machine-readable “digital authorization packages” with cloud service providers and agencies • Propose new key performance metrics	• Migrate to new FedRAMP technology platform • Pilot user workflows within the FedRAMP platform • Pilot threat sharing between FedRAMP platform and CISA CDM	• Publish new key performance metrics • DHS CDM Dashboard integration

These timelines are estimates, and are expected to be revised over time based on current priorities.

Help Shape FedRAMP’s Future

Participate in a partnership or pilot

A number of items in this roadmap will require pilots with agencies and CSPs, let FedRAMP know if you are interested in participating.

Provide public comment on future guidance

We will be doing frequent public comments - major items that impact our stakeholders will have public comment periods.

Engage in upcoming public forums

Join us on Thursday, April 11 for the first public forum on the FedRAMP Roadmap.