GOVDATAHOSTING
POWERED BY IT-CNP, INC.
FEDRAMP HIGH (CLASS D) CERTIFIED CLOUD PLATFORM

FEDRAMP CERTIFICATION PLAYBOOK

Your Step-by-Step Guide to Federal Government Cloud Certification Success

2026 EDITION • **UPDATED FOR FEDRAMP 20x & CR26**

INSIDE THIS PLAYBOOK

FedRAMP fundamentals • FedRAMP 20x & Certification Classes • 5-phase methodology • Control inheritance • Timeline planning • Cost optimization • Ready-to-use checklists

DESIGNED FOR

Federal Agency IT Leaders • Government Contractors • Cloud Architects

GovDataHosting

FedRAMP High (Class D) Certified • NIST 800-53 High • DoD IL2

www.govdatahosting.com | 800-967-1004

What's Inside

Executive Summary

Achieving FedRAMP Certification is no longer optional for organizations serving the federal government—it's a strategic imperative. FedRAMP provides a standardized approach to the security assessment, certification, and continuous monitoring of cloud products and services used by federal agencies.

This playbook provides a proven, repeatable methodology for planning and executing a successful FedRAMP Certification effort. Whether you're pursuing certification for a cloud service or leveraging FedRAMP-certified infrastructure to accelerate your path, this guide will help you navigate the process efficiently.

EXPECTED TIME INVESTMENT

A typical FedRAMP certification takes 6–18 months depending on system complexity and impact level. Organizations that leverage existing FedRAMP-certified infrastructure can reduce this timeline by 40% or more through control inheritance.

Key Benefits of FedRAMP Certification

- **Standardized security** — Consistent baseline across all cloud deployments
- **Reduced certification burden** — Reuse existing assessments through control inheritance
- **Accelerated procurement** — Pre-certified solutions streamline acquisition
- **Cost optimization** — Shared responsibility model reduces compliance overhead
- **Continuous compliance** — Built-in monitoring replaces point-in-time assessments
- **Market access** — FedRAMP Certification opens doors to federal opportunities

Understanding FedRAMP

What is FedRAMP?

FedRAMP is a government-wide program that provides a standardized approach to security assessment, certification, and continuous monitoring for cloud products and services. Established in 2011 and codified into law by the 2022 FedRAMP statute, the program ensures consistent security across federal cloud deployments.

FedRAMP Impact Levels

FedRAMP defines its security baselines using FIPS 199 security categorization. Under the Consolidated Rules for 2026 (CR26), the familiar Low / Moderate / High labels are being renamed to Certification Classes B / C / D—the baselines map closely, and the new names are covered in the next section.

Factor	LOW	MODERATE	HIGH
Data Types	Public data, non-sensitive	CUI, PII, PHI, financial	Law enforcement, critical infrastructure
Controls (Rev5)	~156	~325	~421
Timeline	3–6 months	6–12 months	12–18 months
% of Systems	~15%	~80%	~5%
CR26 Class	**Class B**	**Class C**	**Class D**

KEY INSIGHT

Approximately 80% of federal systems require FedRAMP Moderate (Class C). If you're unsure of your impact level, Moderate is likely the right baseline. Agencies handling law enforcement or critical infrastructure data typically require High (Class D).

FedRAMP 20x & Certification Classes

FedRAMP is undergoing the most significant modernization in its history. Anchored in the 2022 FedRAMP statute and OMB Memorandum M-24-15, the initiative known as FedRAMP 20x is changing how cloud services are assessed and certified—shifting away from a document-centric review of hundreds of NIST 800-53 control narratives toward automated, machine-readable validation built around Key Security Indicators (KSIs) and experimenting with Open Security Controls Assessment Language (OSCAL). The goal is a faster, more repeatable, and more scalable path to federal cloud adoption.

The Move to Certification Classes (CR26)

One of the most visible changes arrives with the Consolidated Rules for 2026 (CR26). CR26 retires the long-standing FIPS 199 impact-level labels—Low, Moderate, and High—and replaces them with lettered Certification Classes (A through D). The change is largely terminology: the underlying security baselines map closely and existing certifications carry over. A primary driver was to end years of confusion between FedRAMP impact levels and the Department of Defense Impact Levels (IL2–IL6).

Class	Replaces	Typical Scope	Controls (Rev5)	Path
Class A	Pilot / Ready (new tier)	Transitional entry via external frameworks (e.g., SOC 2 Type II); time-limited	KSI-based	Program only
Class B	Low / Li-SaaS	Non-sensitive federal data; limited impact if breached	~156	Program or Agency
Class C	Moderate	CUI and non-public federal data; ~80% of services	~323–325	Program, Agency or 20x
Class D	High	Mission-critical data—law enforcement, critical infrastructure	~410–421	Agency only

Class C (formerly Moderate)

Class C is the workhorse of the program—roughly 80% of certified cloud services operate at this tier. It covers Controlled Unclassified Information (CUI) and other non-public federal data where a breach would cause serious but not catastrophic harm, and requires approximately 323–325 controls under the Rev5 baseline. Class C is the primary target for most providers entering the federal market and is supported by the FedRAMP 20x automated path.

Class D (formerly High)

Class D is the most demanding tier, reserved for mission-critical systems—law enforcement, emergency services, national security, and critical infrastructure—where a breach could be severe or catastrophic. It requires approximately 410–421 controls. Importantly, as the program stands today, Class D must go through the agency-sponsored path; there is no FedRAMP 20x path for Class D, and a dedicated Class D (High) pilot is not expected until FY27.

ONE OFFICIAL DESIGNATION

Under CR26, every FedRAMP assessment—whether completed under Rev5 or 20x—carries a single official label: FedRAMP Certified (a FedRAMP Certification). The separate "FedRAMP Validated" designation has been dropped to avoid procurement confusion.

Rev5 vs. FedRAMP 20x at a Glance

FedRAMP Rev5 (traditional)	FedRAMP 20x
Document-centric SSP; control-by-control narratives	Automation-first; Key Security Indicators (KSIs)
3PAO assessment cycles often spanning 12–18 months	Continuous, machine-readable validation; far faster in pilots
PDF / Word certification packages	Machine-readable packages
Supports all classes (A–D)	Classes A–C today; Class D pilot targeted for FY27

Transition Timeline

FedRAMP describes the dates below as goals that may shift as the program learns from pilot feedback. Treat them as planning guidance, not firm commitments.

Milestone	Target (estimated)
CR26 final publication	End of June 2026
20x submission pipeline opens (Class A, B, C)	FY26 Q4 (Jul–Sep 2026)
"FedRAMP Ready" retired (transitions to Class A)	July 28, 2026
New Rev5 submissions must be OSCAL	Sep 30, 2026
CR26 enforced	January 2027
FedRAMP stops accepting new Rev5 Certifications	June 11, 2027
Class D (High) pilot	FY27 Q1–Q2
CR26 in effect through	December 2028

WHAT THIS MEANS FOR YOU

GovDataHosting operates a FedRAMP High (Class D) certified cloud platform. Whether you plan around today's Rev5 baselines or tomorrow's Certification Classes, building on GovDataHosting lets you inherit the platform-layer controls and focus your assessment on the application layer—regardless of how the labels evolve.

IMPORTANT NUANCE

A FedRAMP Certification reflects the assessment baseline; it is not, by itself, an agency's acceptance of risk at a given FIPS 199 security category. Agencies make that determination under the Risk Management Framework, using the FedRAMP package as the foundation.

FedRAMP Certification Paths

Cloud service providers reach a FedRAMP Certification through one of two primary routes: an agency-sponsored path or the FedRAMP Program path (including FedRAMP 20x). The agency-sponsored route remains the dominant traditional option today. Understanding which applies to your situation is critical for planning.

AGENCY PATH	FEDRAMP PROGRAM / 20x
Best for: CSPs with an agency sponsor	**Best for:** CSPs seeking broad, sponsor-free adoption
Timeline: 6–12 months (Rev5)	**Timeline:** Weeks–months in 20x pilots (automation-based)
Cost: Lower (shared with sponsor)	**Cost:** Varies; continuous-monitoring tooling required

For Agencies: Leveraging Existing Certifications

Federal agencies don't need to assess cloud services from scratch. The FedRAMP Marketplace contains hundreds of pre-certified services:

1. Search the FedRAMP Marketplace for certified services
2. Review the CSP's certification package and security documentation
3. Conduct an agency-specific risk assessment for your use case
4. Issue an Agency ATO leveraging the existing FedRAMP Certification
5. Establish a continuous monitoring and reporting relationship

> **ACCELERATOR STRATEGY**
>
> Agencies can reduce certification timelines by 40–60% by selecting FedRAMP-certified infrastructure and inheriting controls. Instead of assessing 400+ controls, you focus only on application-layer controls.

The 5-Phase Certification Methodology

Our proven methodology breaks FedRAMP certification into five distinct phases, each with clear objectives, deliverables, and success criteria.

Phase 1: Discovery & Assessment (Weeks 1–4)

Objective: Understand current state, define target architecture, and establish project foundation.

- Inventory existing systems, applications, and data flows
- Conduct FIPS 199 security categorization
- Define system boundary and scope
- Evaluate FedRAMP-certified infrastructure options
- Develop project plan, budget, and resource requirements

Deliverables: System inventory, categorization documentation, gap analysis, project plan

Phase 2: Architecture & Planning (Weeks 5–10)

Objective: Design a compliant architecture and develop comprehensive documentation.

- Design target cloud architecture aligned with FedRAMP requirements
- Map control inheritance from FedRAMP-certified infrastructure
- Begin System Security Plan (SSP) development
- Develop network diagrams and data flow documentation
- Create deployment runbooks and test plans

Deliverables: Architecture design, control responsibility matrix, draft SSP, deployment runbook

Phase 3: Build & Implement (Weeks 11–20)

Objective: Deploy infrastructure, implement controls, and bring systems online.

- Provision FedRAMP-certified cloud infrastructure
- Configure security controls per SSP documentation
- Deploy monitoring, logging, and alerting systems
- Deploy applications and data per runbook
- Complete SSP with implementation details

Deliverables: Deployed infrastructure, implemented controls, completed SSP, test results

Phase 4: Assessment & Certification (Weeks 21–28)

Objective: Complete the security assessment, remediate findings, and achieve certification.

- Conduct vulnerability scanning and penetration testing
- Engage a Third-Party Assessment Organization (3PAO)
- Remediate identified vulnerabilities and control gaps
- Develop the Security Assessment Report (SAR) and POA&M
- Submit the certification package to the Authorizing Official

Deliverables: Scan results, SAR, POA&M, certification package, ATO letter

Phase 5: Operations & Continuous Monitoring (Ongoing)

Objective: Maintain certification through continuous monitoring and compliance.

- Implement a continuous monitoring (ConMon) program
- Conduct monthly vulnerability scans
- Update the POA&M and track remediation progress
- Conduct annual security assessments (one-third of controls)
- Manage significant changes through change control

Deliverables: ConMon reports, updated POA&M, annual assessment results, recertification package

Control Inheritance Strategy

Control inheritance is the key to accelerating FedRAMP certification. By leveraging FedRAMP-certified infrastructure, you can inherit hundreds of pre-assessed controls instead of implementing them yourself.

The Shared Responsibility Model

CSP RESPONSIBILITY	SHARED	CUSTOMER
• Physical security • Hypervisor security • Network infrastructure • Platform patching	• Identity management • Encryption key management • Security monitoring • Incident response	• Application security • Data classification • User access control • Security training

BOTTOM LINE

By deploying on GovDataHosting's FedRAMP High (Class D) certified infrastructure, you can inherit over 300 controls—reducing your documentation burden by up to 70% and your assessment scope proportionally. This translates to months of saved time and hundreds of thousands of dollars in reduced costs.

FedRAMP Certification Checklist

Use this checklist to track your certification progress and ensure no critical steps are missed.

Phase 1: Discovery & Assessment

- ☐ Complete system inventory and data flow mapping
- ☐ Conduct FIPS 199 security categorization
- ☐ Define system boundary
- ☐ Evaluate FedRAMP-certified infrastructure options
- ☐ Complete security gap analysis
- ☐ Secure budget and resource commitments

Phase 2: Architecture & Planning

- ☐ Design target cloud architecture
- ☐ Create control responsibility matrix
- ☐ Begin System Security Plan (SSP) development
- ☐ Develop network and data flow diagrams
- ☐ Create deployment runbooks

Phase 3: Build & Implement

- ☐ Provision cloud infrastructure
- ☐ Configure security controls
- ☐ Deploy monitoring and logging
- ☐ Deploy applications per runbook
- ☐ Complete SSP with implementation details

Phase 4: Assessment & Certification

- ☐ Conduct vulnerability scanning
- ☐ Perform penetration testing
- ☐ Engage 3PAO for independent assessment
- ☐ Remediate critical findings
- ☐ Compile certification package
- ☐ Obtain signed ATO letter

How GovDataHosting Accelerates Your Certification

GovDataHosting provides a FedRAMP High (Class D) certified cloud platform specifically designed to simplify and accelerate the path to FedRAMP Certification for federal agencies and government contractors. Continuous monitoring is run around the clock by our 24/7 U.S.-based Security Operations Center (SOC)—vulnerability scanning, POA&M management, and monthly ConMon reporting.

Why Organizations Choose GovDataHosting

- **40% faster ATO timelines** through control inheritance and documentation support
- **300+ inherited controls** reducing documentation burden by hundreds of hours
- **10–40% cost savings** compared to multi-vendor approaches
- **Single-source accountability** — one vendor for infrastructure, security, 24/7 SOC-run monitoring, and support
- **100% client retention** demonstrating long-term partnership value

FREE CERTIFICATION ASSESSMENT

Schedule a complimentary 30-minute consultation to assess your current infrastructure, identify the optimal certification path, and develop a customized project plan.

800-967-1004

www.govdatahosting.com/contact-us • **info@govdatahosting.com**

GOVDATAHOSTING POWERED BY IT-CNP, INC.

A Division of IT-CNP, Inc. • Founded 2001

FedRAMP High (Class D) Certified • NIST 800-53 High • DoD IL2 • SOC 2 Type II

© 2026 IT-CNP, Inc. All rights reserved.

DISCLAIMER

The information in this playbook is accurate as of the date of publication. FedRAMP policy, certification classes, control baselines, and timelines—particularly those associated with FedRAMP 20x and the Consolidated Rules for 2026 (CR26)—are evolving rapidly and are subject to change. Always verify the latest requirements at fedramp.gov before making compliance decisions.