The FedRAMP Playbook

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, ITES-SW2, NASPO ValuePoint and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with stackArmor, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit **carahsoft.com**

Explore More Resources:
carah.io/stackarmorresources

Join Events & Webinars:
carah.io/stackarmor

Discover Technology Solutions:
carah.io/stackarmor

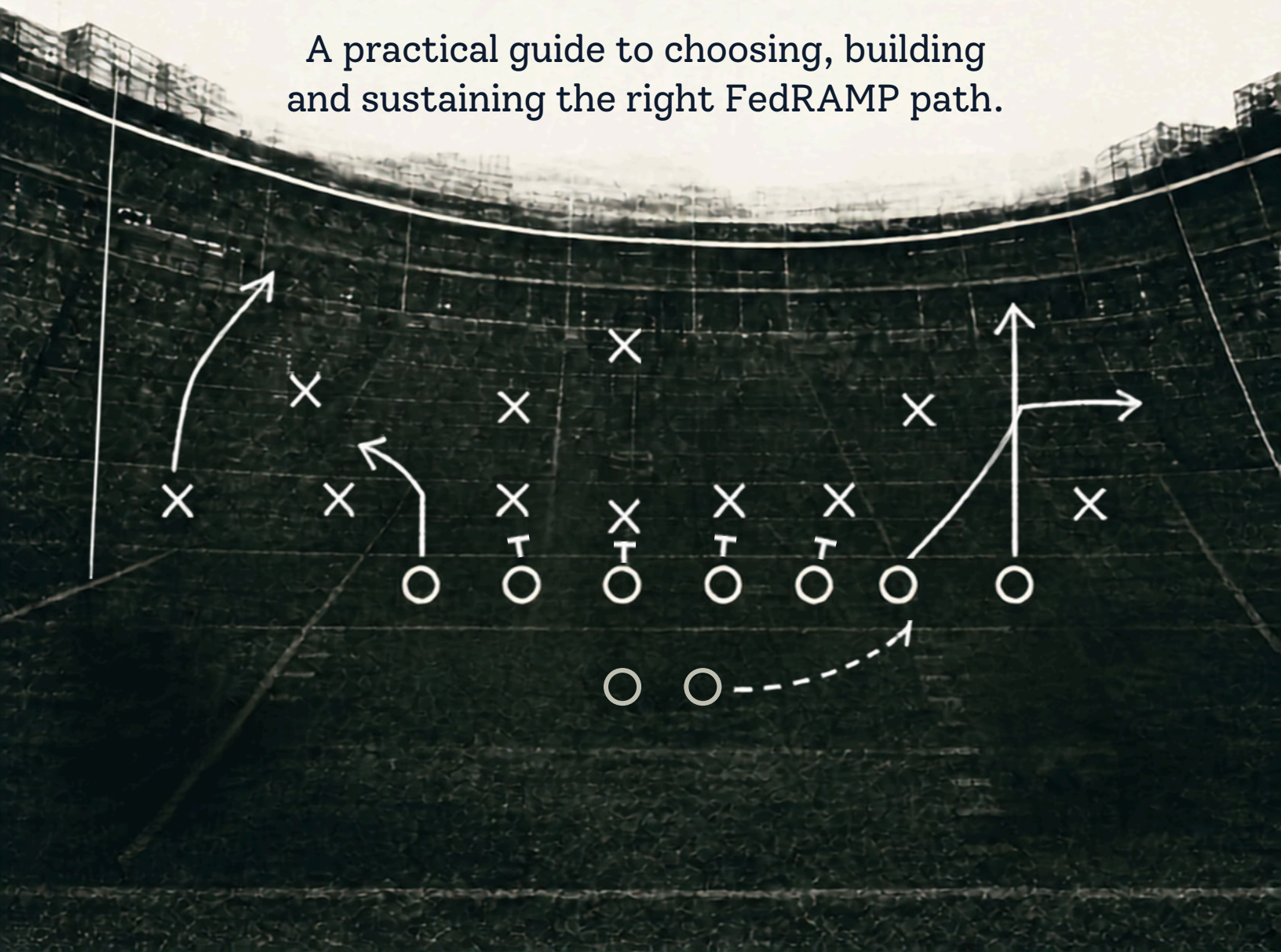
Learn About Procurement:
carah.io/stackarmorcontracts

Connect With Our Team:
stackarmor@carahsoft.com
571-662-4440

stackArmor

THE FEDRAMP PLAYBOOK

A practical guide to choosing, building and sustaining the right FedRAMP path.



1

PREGAME

KNOW WHAT YOU'RE ACTUALLY SIGNING UP FOR

FedRAMP is a journey, not a checkbox.

FedRAMP is not just about getting authorized quickly. It is about building a secure, resilient, and sustainable foundation for your business in the federal market. Before you commit to a path, understand what the work really involves, what the long-term operating model will require, and what success should look like after the ATO.

WHO THIS IS FOR

Commercial software vendors	Cybersecurity and SaaS providers	AI and cloud-native companies	Federal market entrants

An ATO gets you in the game. Staying in the game requires continuous compliance, operational discipline, and long-term ownership!

CLARITY TODAY PREVENTS COSTLY DETOURS TOMORROW.

2

THE LANDSCAPE

ABOVE THE NOISE. CALL THE RIGHT PLAY.

The federal cloud security landscape is evolving. Understanding where it's been — and where it's going — helps you make the right investments today and stay aligned for tomorrow.

FedRAMP Rev 5 →

TODAY

- Stronger security requirements
- Greater accountability
- Focus on continuous monitoring
- Foundation for what's next

FedRAMP 20x →

EMERGING

- Streamlined processes
- Increased automation
- Broader industry participation
- Faster time to value

Broader Federal Alignment

TOMORROW

- Greater cross-agency consistency
- Alignment with DoD, CISA and OMB
- Expanded use cases
- A more unified federal cloud ecosystem

THE DIRECTION IS CLEAR

FedRAMP is moving toward a more streamlined, automated, and interoperable model for federal cloud adoption. The organizations that prepare for that shift now will be better positioned to reduce friction, adapt to new requirements, and expand into future agency opportunities.



STREAMLINE



INTEROPERATE



SCALE

3

CHOOSE YOUR FORMATION

TWO PATHS. ONE MISSION.

Most FedRAMP providers sell you a path. stackArmor helps you choose the path. We support both a Hosted solution through the Armory and a Managed In-Boundary approach — because there is no one-size-fits-all architecture. Your mission, your requirements, and your long-term goals determine the right formation.

HOSTED THROUGH THE ARMORY

BUILT-IN STRENGTH.

Greater control inheritance
Leverage the Armory's authorized environment and controls.

Reduced compliance infrastructure
Less hardware, tooling, and operational overhead to stand up.

Lower implementation lift
Get to authorization faster with proven, repeatable processes.

Managed authorization environment
Our team helps operate, maintain, and support the authorized environment.

MANAGED IN-BOUNDARY

MAXIMUM FLEXIBILITY.

You own your environment
You operate your own environment and security boundary.

Greater ownership and portability
You retain your SSP, supporting evidence, and program flexibility.

Support long-term control
Build internal expertise and retain operational control over time.

Ideal for future requirements
Provides long-term flexibility as agency needs evolve.

4

KNOW WHAT YOU OWN

IT MATTERS LATER.

What you own affects your flexibility, your long-term costs, portability, and your ability to adapt. Before you choose a provider, understand what you're getting — and what you'll own when the process is complete.

KEY QUESTIONS

1

Who owns the boundary?
Understand whether you or your provider owns the dedicated environment and security boundary.

2

Who owns the documentation?
Will you own the SSP, POA&Ms, and supporting evidence, or will the provider retain control?

3

What happens if you change providers?
Can you take your authorization, evidence, and configurations with you, or will you be locked in?

4

What are you responsible for?
Understand what you inherit, and what your team must operate, maintain, and update as the customer.

WHAT OWNERSHIP AFFECTS



Documentation and evidence
Your ability to retain the SSP, POA&Ms, and evidence set.



Portability and flexibility
Your ability to move environments or adapt the program as needs change.



Ongoing operations and monitoring
Who maintains controls, updates, and continuous compliance.



Ability to adapt to future requirements
Whether the model supports changing customer, agency, or mission needs.

5 READ THE DEFENSE
THE RIGHT QUESTIONS LEAD TO A BETTER OUTCOME.

Before you choose a provider, ask the right questions. Understanding their architecture, ownership model, assessment burden, and long-term operating responsibilities will help you avoid costly surprises and set your mission up for success.

FIVE QUESTIONS TO ASK ANY FEDRAMP PROVIDER

1. Are they helping you choose the right architecture, or selling you the one they already have?
2. What will you inherit — and what will you own?
3. Can you change providers without starting over?
4. How do they handle continuous monitoring?
5. What is their experience with your agency or mission area?

Not all providers operate the same way

SCOUTING REPORT
WHAT TO LOOK FOR.

CLEAR OWNERSHIP MODEL
Understand what the provider owns, what you own, and where the responsibilities are divided.

TRANSPARENT SHARED RESPONSIBILITY
Look for a clear explanation of how security, compliance, and operations responsibilities are shared.

REPEATABLE ASSESSMENT PROCESS
Choose a provider with a proven, repeatable approach to assessments that reduces your burden.

CREDIBLE OPERATING SUPPORT
Ensure they offer long-term support after authorization, including monitoring, incident response, and ongoing compliance.

BETTER QUESTIONS, STRONGER OUTCOMES.

6

AVOID THE PENALTIES

COMMON MISTAKES COST TIME AND MONEY.

FedRAMP requires sustained planning and execution. Avoiding these common mistakes can help keep your program on schedule and positioned for long-term success.

1. **Underestimating the effort**
   FedRAMP requires sustained investment across people, process, and technology.
2. **Choosing the wrong partner**
   Not all providers offer the same flexibility, support, or transparency.
3. **Lack of internal alignment**
   Success requires buy-in across technical, legal, procurement, and leadership teams.
4. **Inadequate documentation**
   Incomplete or inconsistent evidence is one of the top causes of delays.
5. **Ignoring continuous monitoring**
   Authorization is just the beginning. Ongoing compliance is a long-term commitment.
6. **Not planning for what you'll own**
   Understand your exit options and what you will retain if you change providers.



7 BUILD YOUR ROSTER

– THE RIGHT TEAM WINS –

FedRAMP success takes a coordinated team with the right expertise, clear ownership, and a shared commitment to the mission. Here's a typical roster for a successful engagement.

YOUR TEAM

DRIVE THE MISSION

Executive Sponsor
Provides strategic direction, removes roadblocks, and ensures organizational alignment.

Project Manager
Coordinates activities, timelines, and internal stakeholders.

Product / Application SME
Brings deep knowledge of your application, requirements, and mission use case.

Infrastructure / Network SME
Supports cloud environment setup, connectivity, and integration.

Security / Compliance Lead
Owns internal security requirements, policy alignment, and risk decisions.

Engineering / Deployment Support
Implements changes, supports testing, and assists with remediation.

stackArmor TEAM

BRING THE EXPERIENCE

Engagement Manager
Serves as your primary point of contact and keeps the program on track.

Senior FedRAMP SME
Brings deep expertise in federal requirements, 3PAO coordination, and authorization strategy.

FedRAMP SME
Supports control implementation, evidence development, and ongoing compliance activities.

Senior Solutions Architect
Designs the secure, compliant architecture aligned to your requirements (AWS, Azure, or GCP).

DevSecOps Engineers
Help implement, harden, and validate your environment using proven security automation and tooling.

Compliance & Package Support
Assists with documentation, POA&M tracking, and prepares artifacts for assessment and authorization.

Battle-tested design. Our proprietary solutions operate on a proven foundation of security and compliance – refined across hundreds of federal engagements.



8 BUILD FOR TOMORROW
A PLATFORM FOR WHAT'S NEXT

Getting to authorization is a major milestone. Staying ahead is the real advantage. With the right foundation, you can scale, adapt, and expand—supporting today's mission and tomorrow's opportunities.

SCALE

Built to support your growth.

A secure, repeatable architecture that can scale across agencies, workloads, and mission areas—so you can pursue new opportunities without starting from scratch.

ADAPT

Flexible by design.

Supports cloud-native, virtual machine, and containerized application models across AWS, Azure, and GCP through stackArmor's managed in-boundary approach — without forcing a one-size-fits-all architecture

EXPAND

Ready for what's next.

Position your organization for broader federal requirements (FedRAMP, DOD, CMMC, FISMA), new mission use cases, and emerging technologies—supported by a platform designed for continuous compliance and long-term success.

- Automation at work -

99%+
reduction in analyst processing time

3 days to 10 minutes
stackArmor's RADAR security automation platform

85-90%
decrease in evidence retrieval effort

Fit the compliance model to the application — not the application to the compliance platform.

BUILT FOR YOUR ENVIRONMENT.

aws Azure

Hosted through The Armory on Google Cloud, or managed in-boundary across AWS, Azure, and GCP.

9 THE GAME PLAN

FROM STRATEGY TO SUCCESS.

Every journey is different, but a proven approach helps you move faster, reduce risk, and stay focused. Here's an illustrative implementation timeline for a typical FedRAMP engagement with stackArmor.

1 DISCOVERY & DESIGN

TYPICAL: 2–4 WEEKS

- Define goals and scope
- Review current environment
- Design security architecture and boundary approach
- Align on requirements, roles, and timeline

2 DEPLOYMENT

TYPICAL: 2–4 WEEKS

- Stand up cloud environment (AWS, Azure, or GCP)
- Implement security controls and tooling
- Configure access, logging, and monitoring
- Integrate with your application and infrastructure

3 MIGRATION & HARDENING

TYPICAL: 2–4 WEEKS

- Migrate or onboard workloads
- Apply hardening and configuration changes
- Conduct vulnerability scanning and remediation
- Prepare evidence and documentation

4 OPERATIONAL READINESS

TYPICAL: 90 DAYS

- Establish continuous monitoring processes and tooling
- Manage POA&Ms and ongoing vulnerabilities
- Establish reporting and analytics
- Validate processes and prepare for authorization

PROVEN TRACK RECORD

Actual timelines depend on application readiness, customer feedback, scope, and review availability. stackArmor works alongside your team to keep the program on track and remove roadblocks.

Successfully guided 60+ organizations through the most rigorous federal compliance frameworks over the past five years with a 100% Authorization success rate.

SAME MISSION. HIGHER GROUND.

Let's build what's next.

FedRAMP isn't the end zone — it's the starting point for greater impact. With the right strategy, partners, and execution, you can turn compliance into a competitive advantage and focus on what matters most: serving the mission.

PEOPLE
Experienced teams who've been in the game.

PROCESS
Proven methodologies that reduce risk and accelerate results.

ARCHITECTURE
Secure, scalable foundations built for government.

MISSION
A stronger, more secure tomorrow for those who serve.

SCHEDULE AN ATO ACCELERATION BRIEFING.

Let's discuss how stackArmor can help you achieve compliance faster, with less friction, and greater confidence.

VISIT US AT STACKARMOR.COM

PEOPLE
PROCESS
ARCHITECTURE
COMPLIANCE
MISSION

COMPLIANCE TODAY.
GREATER
OPPORTUNITIES
TOMORROW.

stackArmor
QUANTUM SKY