RegScale

E-BOOK

Automating FedRAMP 20x

The Insider Guide to Federal Compliance Efficiency

TABLE OF CONTENTS

Full FedRAMP 20x compliance workflow in

(Yep, ninety.)

FROM THE DESK OF OUR CO-FOUNDER

THE PATH TO 20X EFFICIENCY

Anyone who's gone through the Federal Risk and Authorization Management Program (FedRAMP) knows that the process is painfully slow and administratively heavy. Companies spend enormous amounts of time and money on document development and manual paperwork instead of driving cybersecurity excellence.

Enter FedRAMP 20x, an open collaboration between the FedRAMP PMO, industry stakeholders, and government agencies to fundamentally reimagine federal cloud security assessment. The five goals driving FedRAMP 20x are ambitious but achievable: automating security requirements, leveraging existing commercial security frameworks, implementing continuous monitoring, building trust through direct business relationships, and enabling rapid innovation without artificial checkpoints.

Having helped numerous companies navigate their FedRAMP journey — and having **achieved our own FedRAMP High authorization 3-4x faster than the industry average** — we've developed some strong opinions about where the biggest efficiency gains are. We believe the real transformation will come from technical innovation in three key areas: compliance as code, artificial intelligence, and common mapping frameworks.

This e-book will explore these technical innovations and offer a **roadmap for completing a full FedRAMP 20x compliance workflow in 90 minutes**. (Yep, ninety.) We envision a future FedRAMP driven by self-updating paperwork, automated risk assessments, and real-time and full-scope AI audits: a process that will cost less, cut down on cybersecurity risks, and be achievable in weeks. Instead of drowning in documentation, we'll be able to focus our engineering cycles on what really matters: building stronger, more secure cloud architectures.

This isn't just about making federal compliance easier and more accessible — it's about building the secure, efficient government infrastructure that America deserves.

Travis Howerton
Co-Founder and CEO, RegScale

OVERVIEW OF THE FEDRAMP 20X PROCESS CHANGES

FedRAMP 20x came out blazing in spring 2025 with some fast wins on the process front. The results should be less paperwork, more automation, and much more focus on operational excellence in security.

Goodbye controls, hello Key Security Indicators (KSIs). Starting with a pilot for FedRAMP Low, FedRAMP 20x is shifting away from prescriptive administrative controls and toward KSIs that drive real-world security outcomes.

Swapping the Significant Change Request (SCR) for the Significant Change Notice (SCN). This change allows Cloud Service Providers (CSPs) to innovate more quickly on their service offerings without having to wait for formal approvals.

Minimizing redundant approvals. The PMO has dramatically restructured its review process to place more accountability for authorization with the agencies, resulting in an approval process that shaves months off the authorization timeline.

Recommendations for Further Improvements

Now that FedRAMP 20x has locked in these initial wins, where do we go next?

1. **Kill the federal sponsor requirement.** First, we suggest moving to a more commercial fee-for-service model. This would eliminate the burden of finding a sponsor, reduce the need for federal funding, and offer a faster path to get started with predictable costs.

2. **Stop reinventing the wheel.** It just doesn't make sense to ATO common services like Office 365 hundreds of times across different government agencies. For common CSP services, we recommend government-wide risk envelopes approved by the CISO Council or another governance body. That would eliminate rework, cut out the needless custom government software when viable commercial alternatives exist, and reduce wasteful spending across the board.

Top Technical Innovations for FedRAMP 20x

FEDERAL COMPLIANCE LEADERSHIP AT REGSCALE

- ✓ Members of the CSA CAR Working Group and the ATARC Continuous ATO Working Group
- ✓ Founding members of the NIST OSCAL Foundation
- ✓ Active participants in FedRAMP 20x community working groups
- ✓ FedRAMP High authorized with sponsorship from the Department of Homeland Security and DOD IL5 authorized

#1

RegScale

Leverage Compliance as Code

The technological foundation for FedRAMP 20x automation is compliance as code: a scalable, standards-based way of conducting real-time, automated, full-lifecycle security assessments. Compliance as code can dramatically reduce manual labor requirements and expedite FedRAMP's authorization and continuous monitoring processes.

- ✓ **NIST OSCAL transforms controls into code.** No more wrestling with PDFs and websites. With the Open Security Control Assessment Language, controls become machine-readable (XML, JSON, YAML) so you can track changes in Git and feed them directly into your automation pipeline.

- ✓ **SBOM provides insights.** The Software Bill of Materials acts like an ingredient list on a grocery store item, helping you understand the composition of your software so you can avoid harmful supply chain vulnerabilities.

- ✓ **OCSF standardizes security data exchange.** Instead of custom integrations for every tool, the Open Cybersecurity Schema Framework (OCSF) creates a common language for assets, vulnerabilities, configurations, and tickets — simplifying integrations and data sharing in continuous monitoring.

- ✓ **OSCAL compiles your FedRAMP artifacts.** Your System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), and Plans of Action and Milestones (POA&Ms) become machine-readable, so you can compile them against risk tolerances and instantly spot compliance gaps — like a compiler catching code errors before deployment.

FedRAMP   OSCAL FOUNDATION   NIST OSCAL   OCSF

#2
Implement AI

The second promising technology solution for FedRAMP 20x is artificial intelligence (AI). From selecting your controls and performing your control attestations to identifying POA&Ms and conducting risk assessments, the FedRAMP process is currently powered by extensive manual work. AI is poised to be a game changer.

RegScale's agentic AI approach uses custom-trained models and agents to perform common tasks that were previously only possible with highly trained personnel. This includes:

- ✓ **AI Explainer** Offers context-based explanations of security controls in plain language.
- ✓ **AI Author** Generates full SSP packages based on existing policies, other certifications (e.g. SOC 2, CMMC), or high-level questionnaire responses.
- ✓ **AI Auditor** Reviews SSP packages to generate the SAP/SAR.

Easy wins with **RegScale AI**

- ✓ Slash months-long document development processes to < 1 hour.
- ✓ Reduce weeks-long audits to minutes.
- ✓ Democratize the FedRAMP authorization process for small companies that are eager to provide solutions to the federal market.

#3

Get a Common Mapping Framework

The third technological improvement for FedRAMP 20x involves making security tools more context-aware via a common mapping framework. **Multiple commercial solutions could serve this purpose:**

- ✓ CYBER RISK INSTITUTE **Cyber Risk Institute (CRI) Profile**
- ✓ CSA cloud security alliance® **Cloud Security Alliance Cloud Controls Matrix (CSA CCM)**
- ✓ SCF SECURE CONTROLS FRAMEWORK **Secure Controls Framework (SCF)**
- ✓ UCF **Unified Compliance Framework (UCF)**

These frameworks allow for mapping common regulations to a unified control framework, allowing companies to attest or assess once and then reuse across other regulations. However, in spite of these existing frameworks, there is a lack of precision from security tool attestations that poses major challenges to FedRAMP automation.

To solve this problem, we would advocate for a Universal Mapping Framework that maps controls across all the common frameworks so that security vendors can perform one attestation and then apply it to any global cyber framework. This mapping foundation would serve as a strong basis for continuous monitoring automation across the industry.

SPOTLIGHT

FEDRAMP 20X WORKFLOW IN 90 MINUTES

The FedRAMP 20x pilot program shifts away from administrative controls and replaces them with Key Security Indicators (KSIs). Using those KSIs, we delivered a proof of concept to fully implement the FedRAMP 20x KSIs in under 90 minutes. **Here's how we did it:**

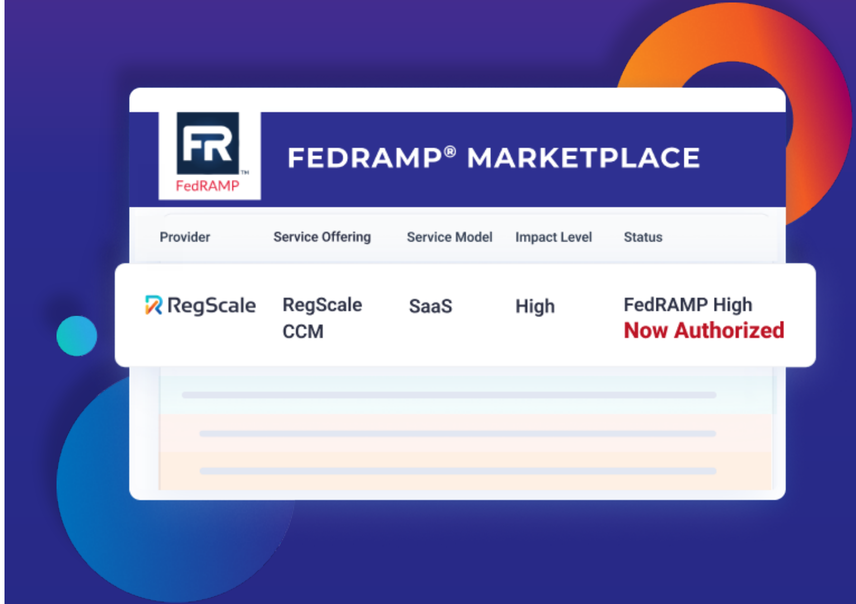
- ✓ Ingested the FedRAMP 20x Key Security Indicators (KSIs) as a new catalog in RegScale and converted it to NIST OSCAL in under 60 minutes.
- ✓ Developed a FedRAMP Low profile based on the KSI catalog in under 5 minutes.
- ✓ Leveraged RegScale AI agents to perform attestations against the KSIs in under 15 minutes.
- ✓ Generated a NIST OSCAL System Security Plan (SSP) with the click of a button.

Read the full details here

Forging FedRAMP Success with RegScale

RegScale's platform offers faster, more cost-effective federal compliance with:

- ✓ **50% cost reduction** from the typical **$2M investment**
- ✓ **3-4x faster timelines** for authorizations
- ✓ AI-powered control implementation statements completed in **2 weeks instead of 12-16**
- ✓ OSCAL-native documentation and one-click artifact export
- ✓ Continuous controls monitoring with real-time visibility
- ✓ Compliance as code to eliminate manual processes
- ✓ Full support for **FedRAMP 20x KSIs**



FEDRAMP® MARKETPLACE

Provider	Service Offering	Service Model	Impact Level	Status
RegScale	RegScale CCM	SaaS	High	FedRAMP High Now Authorized

How we got FedRAMP High at half the cost

Read the success story

RegScale

Ready for faster, easier **FedRAMP results?**

Let’s get started.

Visit RegScale.com to learn more.

✉ Sales@RegScale.com RegScale.com