E-book

# Rackspace Government Solutions

Delivering FedRAMP, StateRAMP and CMMC readiness solutions designed to meet new government cybersecurity compliance requirements

rackspace technology® GOVERNMENT SOLUTIONS

Rackspace Government Solutions offer public and private entities a full range of Federal Risk and Authorization Management Program (FedRAMP), State Risk and Authorization Management (StateRAMP) and Cybersecurity Maturity Model Certification (CMMC)-complaint services including:

- Security and compliance across the design, build, migrate, operate and optimize Lifecycle
- Multicloud solutions and managed services for AWS, Microsoft® Azure®, Google Cloud™ and VMware®
- Rackspace Government Cloud on AWS and VMware
- Authorization to Operate (ATO) on AWS and VMWare private cloud

# What is FedRAMP?

FedRAMP is a United States Federal Government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

- FedRAMP authorization accelerates risk-based digital transformation. As a government-wide program, FedRAMP promotes the adoption of cloud services in a secure way by providing a set of security and risk assessment standards that can be used by all government entities.
- FedRAMP authorization is required.
- FedRAMP authorization provides credibility.

## FedRAMP changes in 2022

- FedRAMP is now law.
- Language from the FedRAMP Authorization Act was included in the National Defense Authorization Act (NDAA) enacted in December 2022 after the FedRAMP bill was "hotlined" in the Senate in early 2022 as part of an effort led by Sen. Gary Peters, D-Mich.

## Impact to commercial enterprises, defense industrial base companies and those looking to enhance their government business presence

- FedRAMP has been around since 2012, when cloud technologies really began to replace outdated tethered software solutions. It was born from the U.S. Government's "Cloud First" strategy, which required agencies to look at cloud-based solutions as a first choice.
- Before FedRAMP, cloud service providers had to prepare an authorization package for each agency they wanted to work with. The requirements were not consistent, and there was a lot of duplicate effort for both providers and agencies.
- FedRAMP introduced consistency and streamlined the process.
- Now, evaluations and requirements are standardized. Multiple government agencies can reuse the provider's FedRAMP authorization security package.
- However, cloud service provider must be FedRAMP Low-, Moderate- or High-certified, depending on the project characteristics and data that will be handled.

Cloud solutions providers (CSPs) excel at building and delivering technologies that help solve their customers' biggest challenges. It's what they're best at. CSPs are not, however, typically well-versed in comprehensive federal security and compliance standards and the hundreds of requirements involved.

Yet, to sell their cloud-based solutions to the U.S. Federal Government, CSPs must first achieve a FedRAMP Authority to Operate (ATO), demonstrating they meet the FedRAMP standard.

**The FedRAMP ATO certification process can be daunting, expensive and time-consuming for CSPs. And to make matters worse, CSPs often approach the process with misconceptions that can lead to delays, cost overruns and fall short of the objective.**

Through our experience helping businesses achieve their FedRAMP ATO over the years, we've identified seven misconceptions that occur most frequently. By sharing these with you, we hope you can avoid making the same mistakes and have a more-successful journey toward your own FedRAMP ATO.

### Misconception #1: I do/don't need to be FedRAMP compliant.

Depending on which services you provide, you may be required to be FedRAMP compliant, even if you're not actively seeking a government contract. In other cases, you may be seeking compliance when it's not actually needed (e.g., you aren't a cloud service). Do you know your situation?

### Misconception #2: You can get FedRAMP-ready on your own.

Unfortunately, there's not an itemized list of best practices that you can check off as you move down the path to authorization. FedRAMP ATO is a formal government designation that must be implemented, assessed by a third-party and validated by the government.

There are timelines to meet, schedules to build and testing to coordinate. Some processes can track in parallel, while others must proceed in tandem. Documentation must be managed properly so that there are easy-to-follow paper trails. Any delay will cost you money.

And don't forget, you also have your own business to run at the same time, with finite IT resources that might be at risk of being stretched thin.

### Misconception #3: Once you become authorized, you are authorized forever.

While it would be nice if, after all your hard work to get authorized, you would just stay that way — but unfortunately this is not the case. You must get reauthorized every year, usually at a cost of around $1 million per provider, per year. You must also continuously monitor and document security and governance requirements to maintain your FedRAMP ATO.

### Misconception #4: JAB authorization is better than an agency authorization.

While a Joint Authorization Board (JAB) Provisional ATO (P-ATO) may streamline some things, an agency ATO is just as effective. In addition, an agency ATO is typically faster and cheaper to achieve, as you get to skip the FedRAMP Ready step. In addition, only a few JAB P-ATOs are considered per year, lowering the probability.

### Misconception #5: You must use a 3PAO for advisory services.

Many third-party assessment organizations (3PAOs) pitch costly (and often unnecessary) consulting services up front that can put you "behind the eight ball" financially. It's better if you can establish the requirements your system meets and plan which actions your team must take to address vulnerabilities before you engage a 3PAO.

### Misconception #6: Federal agencies are reluctant to sponsor a FedRAMP authorization.

With all of the regulation and rules around the FedRAMP ATO process, it's easy to think that federal agencies are reluctant to sponsor FedRAMP authorization. Thankfully this couldn't be further from the truth. The federal government realizes that the intrinsic benefits of the cloud (e.g., remote access, scalability, collaboration efficiency) help it achieve its mission to deliver services to the public. They are always looking to sponsor new CSPs.

### Misconception #7: Attaining a FedRAMP ATO is straightforward.

Attaining a FedRAMP ATO is an arduous process. You must meet more than 300 requirements, as outlined in 1,200+ documentation pages. With an average investment of $2.25M to get authorized, you'll want to make sure you're investing your time and money properly. Thankfully, there exists a shortcut of sorts via inheritable security controls, which can minimize the amount of controls your organization must complete in-house, saving you time and money.

# Streamline your journey to secure, compliant and fully managed PaaS

With Rackspace Technology, you can leverage the power of inheritable security controls and be FedRAMP ATO authorized in as little as four months. Rackspace Government Cloud became the first JAB-authorized platform-as-a-service, back in 2015. Since then, we've helped over a dozen CSPs obtain their FedRAMP ATO. And we can help you, too.

Ready to take a deeper dive? Register for a complimentary discovery session where you'll learn first-hand how to innovate on a Zero Trust, scalable, continuously compliant and fully managed PaaS. You'll also learn what it takes to manage security and governance requirements and get your government cloud solutions to market faster. Topics we'll cover include:

- Achieving FedRAMP ATO three times faster while saving 70% on monthly operational costs
- Reducing advisory, engineering and audit costs to free up time and resources for innovation
- Automating security governance and documentation to ace the assessment
- Attaining always-on, scalable and secure infrastructure and accessing managed capabilities and tools when you need them — whether your cloud is private, public or hybrid.

## How Can Rackspace Technology Government Solutions help your company accelerate FedRAMP compliance?

- From start to finish, it's estimated that a company will spend about $2 million dollars and 18 months navigating the FedRAMP process to achieve certification.
- There's also ongoing monitoring and audit processes that need to be submitted to the Federal government once FedRAMP Low, Moderate or High status has been achieved.

## Rackspace Technology Government Cloud is already FedRAMP compliant.

- Rackspace Technology has provided cloud security and compliance for government agencies and companies working with the government for over 20 years. Rackspace Technology has helped agencies and organizations meet the federal government's rigorous guidelines and solve real-world security challenges. Public companies can leverage our long-standing government-approved capabilities to develop their federally approved cybersecurity and compliance program — saving years of work and significantly lowering the cost.
- Currently, Rackspace Technology supports over 40 customers in the government supply chain, delivering high security and compliant environments.

The following are federally approved cloud security and compliance capabilities that Rackspace Government Solutions can provide private sector organizations to help them become federally compliant with EO 14028:

- Asses an organization's current state and develop a strategy and roadmap to meet the new directives
- Transition its own federally approved "inheritable controls" for cybersecurity compliance to the organization
- Supplement the organization's cybersecurity team with an elastic team of experts who can provide ongoing support
- Provide an ATO on AWS to further accelerate AWS application adoption.

# What is StateRAMP?

- StateRAMP is a 501(c)6 nonprofit, whose mission is to promote cybersecurity best practices through education and policy development to improve the cyber posture of public institutions and the citizens they serve.
- StateRAMP's **governance committees** adopt policies and procedures based on FedRAMP's cybersecurity framework that standardize security requirements for providers. StateRAMP's Program Management Office then verifies those cloud offerings utilized by government satisfy adopted security requirements through independent audits and continuous monitoring. Products that are working towards or have achieved StateRAMP Authorizations are included on an authorized product listing available to all state and local government entities.

## How does StateRAMP impact cloud service providers?

- State and local governments may require service providers to engage with StateRAMP and obtain a StateRAMP security status at any time. Service providers are encouraged to seek a StateRAMP Ready status independent of any RFP publication.

## How can Rackspace Technology help your company accelerate to StateRAMP compliance?

- As more states look to align with FedRAMP security standards as part of their StateRAMP initiatives, Rackspace Technology has extensive experience in working with providers and customers to bring FedRAMP authorized solutions to market and production. We apply this experience directly to helping state and local governments cost-effectively prepare for and accelerate their own security standardization and compliance initiatives.
- More and more states are applying FedRAMP initiatives by embracing StateRAMP security compliance standards in the protection of state information.
- TexRAMP: In the 87th Legislative Session, the Texas Legislature passed Senate Bill 475, requiring the Texas Department of Information Resources (DIR) to establish a state risk and authorization management program that provides "a standardized approach for security assessment, authorization and continuous monitoring of cloud computing services that process the data of a state agency."

# Cybersecurity Maturity Model Certification (CMMC)

## What is CMMC Compliance?

CMMC is a system of compliance levels that helps the government, specifically the Department of Defense (DoD), determine whether an organization has the security necessary to hold, process and handle controlled unclassified information (CUI). Companies that are interested in working with the DoD will need to be CMMC rated and follow specific CMMC regulations. Generally, this is done by building and meeting the CMMC framework.

## What is CMMC?

CMMC is a cybersecurity maturity assessment used to determine whether a company adequately safeguards CUI data. This can be an extensive process; many organizations need the help of an expert partner to identify gaps in their CMMC program and how to properly remediate them.

The cybersecurity maturity assessment considers the organization's capacity to not only maintain its security, but to also maintain data integrity and availability. It also includes how an organization proactively or reactively manages the program.

## What organizations need to be CMMC-certified?

CMMC certification is required by organizations operating with DoD controlled unclassified information. Most organizations will only need a Level 2 clearance or below. If the organization is operating with high-value information, it will likely need a clearance of Level 3. However, levels are set by the data security designation.

## What are the levels of CMMC Certification?

There are three total levels of CMMC certification, with Level 1 being the most basic and Level 3 being the most secure.

**Level 1: Foundational Cyber Hygiene Practice:** This level requires basic cybersecurity protocols deployed by most companies. To reach Level 1, firms need to implement 17 NIST SP 800-171 Rev2 controls.

**Level 2: Advanced Cyber Hygiene Practice:** This level requires all 110 NIST SP 800-171 Rev2 controls to achieve Level 2 certification.

**Level 3 Expert Practice:** This level includes advanced cybersecurity processes implemented, reviewed and updated across the enterprise. Companies need to implement all NIST 800-171 controls plus an additional subset of NIST 800-172 controls.

Levels under the CMMC build upon each other. So, Level 3 companies will fulfill Level 2 and Level 1 requirements.

Most organizations, whether they work with the government or not, should strive for at least Level 2 compliance. Level 3 compliance is reserved for the most sensitive of controlled unclassified information.

## How does an organization get CMMC certification?

Companies achieving level 1 compliance can self-attest their assessments; however Level 2 and 3 destined companies are not allowed to self-certify. Rather, government contractors and those who work with government entities will need to go through a third-party certification process. This third party will audit their current security measures and methods and attest to the company's degree of compliance for their respective CMMC level.

A managed services provider can help a company go through the CMMC framework, determine whether there are improvements that could realistically be made and organize the certification process itself. Once the certification process has been completed, a managed services provider can also create a game plan for improving the level of certification — if needed. Even Level 1 CMMC goals are easier to achieve with a partner well versed in CMMC.

CMMC compliance is poised to impact many companies operating in the Defense Industrial Base. Those companies evaluating their current state against CMMC will fare better than those that react too late. CMMC resources will be in greater demand, and federal compliance timeframes will be finite and compelling.

## Is it worth getting a CMMC Compliance Certification?

If a company holds, handles or processes CUI designated information the organization will need to be CMMC compliant. CMMC compliance requirements are going to vary depending on contract, with many contracts requiring only Level 1 or Level 2 compliance — but other contracts requiring up to Level 3. The contracts that require higher CMMC certification levels are also the contracts that are most likely to be very lucrative. Contract opportunities such as these may make CMMC certification worth the cost and process to obtain the highest level possible.

# CMMC -v- NIST 800-171

## What is NIST 800-171?

The NIST SP 800-171 lays out the requirements for any non-federal agency that handles CUI, or other sensitive federal information. It details how organizations should protect this information. First published in 2015, the goal is to strengthen the federal supply chain and ultimately protect national security.

## What are the differences between CMMC and NIST 800-171

- NIST 800-171 is a cybersecurity framework, a set of standards, while CMMC is an assessed cybersecurity model.
- CMMC Levels 2 and 3 require third-party audit and certifications while NIST 800-171 does not.

## How can Rackspace Technology help your organization prepare for the CMMC Certification?

- Our Rackspace Technology-Government Solutions Platform as a Service (PaaS) provides a head start towards achieving CMMC compliance with Low, Medium and High Tier project configurations.

rackspace technology. GOVERNMENT SOLUTIONS

# Learn More About Rackspace Government Solutions

## Take the Next Step

Let's talk about how Rackspace Technology expertise helps you achieve your goals.

russell.rodd@rackspace.com
813-733-1095
www.rackspace.com/industry/government

rackspace technology. GOVERNMENT SOLUTIONS

## About Rackspace Technology

Rackspace Technology is the multicloud solutions expert. We combine our expertise with the world's leading technologies — across applications, data and security — to deliver end-to-end solutions. We have a proven record of advising customers based on their business challenges, designing solutions that scale, building and managing those solutions, and optimizing returns into the future.

As a global, multicloud technology services pioneer, we deliver innovative capabilities of the cloud to help customers build new revenue streams, increase efficiency and create incredible experiences. Named a best place to work, year after year according to Fortune, Forbes, and Glassdoor, we attract and develop world-class talent to deliver the best expertise to our customers. Everything we do is wrapped in our obsession with our customers' success — our Fanatical Experience® — so they can work faster, smarter and stay ahead of what's next.

Learn more at www.rackspace.com or call 1-800-961-2888.



TSK-10080 CMMC eBook_v3 :: January 2, 2024