DATABANK
Data Center Evolved™

# FEDRAMP COMPLIANCE

## Working with the Right Compliant Cloud Service Provider

FedRAMP

In 2011, the government sought to reduce the risks of cloud services by implementing the Federal Risk and Authorization Management Program (FedRAMP), a program to empower government agencies to transform their infrastructure and encourage secure cloud adoption.

**How does a company work with a FedRAMP compliant cloud service provider? This eBook provides an overview of FedRAMP, including its history and requirements, and how to meet its rigorous standards.**

FedRAMP

# FedRAMP DEFINED

## FEDRAMP OVERVIEW

On December 11, 2011, Federal Chief Information Officer Steven VanRoekel issued a memorandum detailing the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is an innovative partnership between public and private organizations that bridges the gap between FISMA and cloud-enabled environments. It applies to all areas of the federal government and aims to standardize security assessments for the implementation of cloud services. By focusing on standardization processes and the alleviation of risk across all agencies, FedRAMP uniquely positions the federal government to reduce costs and resources employed in security measures.

The development of FedRAMP involved a close collaboration among various agencies, including the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) as well as private industry organizations.

## KEY PLAYERS OF FEDRAMP

Three key players drive FedRAMP initiatives: agencies, cloud service providers (CSPs) and third party assessment organizations (3PAOs). Initially, an agency selects a cloud service provider that has met all FedRAMP requirements and is in a "FedRAMP Ready" status. Following this, the 3PAO audits the CSP, compiling and providing evidence of compliance to ensure FedRAMP requirements continue to be followed.

The development of FedRAMP involved a close collaboration among various agencies, including the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) as well as commercial industry organizations.


## NON-COMPLIANCE RISK

Any agency found to be working with a non-compliant vendor may be subject to a review. If they are in violation of FedRAMP, the OMB determines a course of action that the non-compliant agency must complete to become FedRAMP compliant. The OMB may determine that the agency and CSP can remain partners while both parties achieve compliance; other situations may necessitate the selection of a new CSP.

Since cybersecurity is ever-changing, FedRAMP standards are periodically updated to reflect current vulnerabilities faced by government agencies. The current standards are based upon NIST SP800-53 revision 4 and Department of Homeland Security Binding Operational Directives (BOD's).

# WORKING WITH A FEDRAMP COMPLIANT CLOUD SERVICE PROVIDER

## CONSIDERATIONS FOR CHOOSING A CSP

The most important step an agency can take before beginning the CSP selection process is to create a comprehensive understanding of what their organization will gain from cloud technology.

Next, the agency should thoroughly investigate FedRAMP compliant CSPs and compare their strengths and weaknesses against their organization's goals. This can be done by reviewing the CSP package contained within the OMB MAX product (Max.gov). Lastly, the agency will assess the specific details of each CSP's proposed migration plan. This assessment ensures data security and helps the agency prepare for the technical realities of a live migration.

It is important to understand the CSP's role for security deliverables. CSPs may provide simple infrastructure/colocation, infrastructure plus tools (both IaaS), infrastructure plus the operating system (PaaS) or a complete turnkey solution with operations and support. Transparency of the lines of demarcation of responsibilities between vendors and customers are important in this relationship.

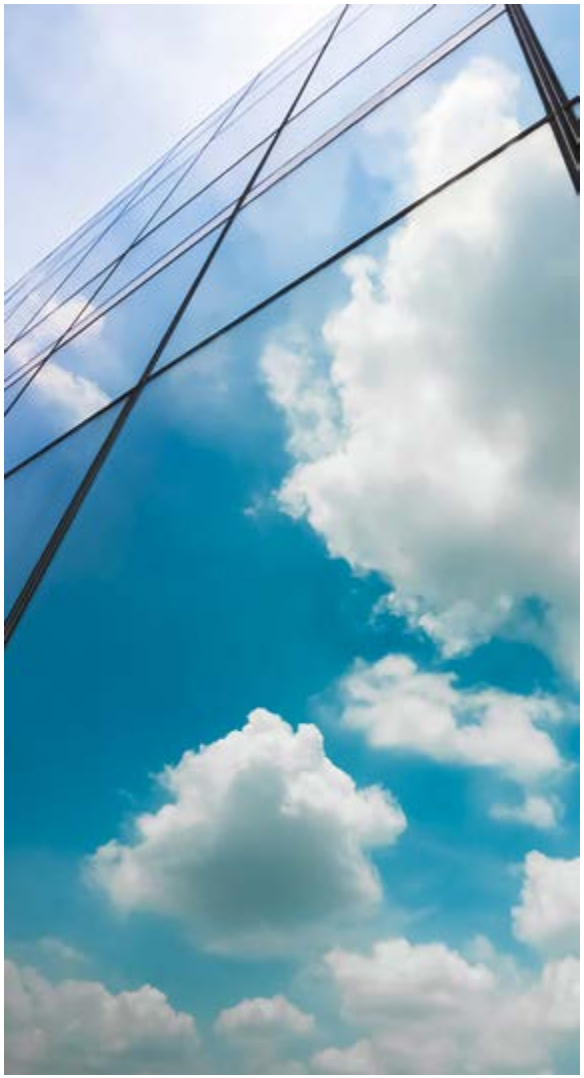
## OBTAINING AN ATO

FedRAMP requires that agencies apply for an Authority to Operate (ATO). Since FedRAMP is designed to be a rigorous process of security assessment, the government has created a detailed guide for agencies applying for an ATO, including the responsibilities of each party involved and the specifics of the application process itself.

To initiate the application process, the agency and CSP must draft a detailed System Security Plan (SSP) regarding how their CSP's protocols will be applied to their business needs and address any pending cybersecurity issues that they have yet to resolve. Open items are compiled into a Plan of Actions and Milestones (POA&M) and any open issues requiring immediate attention are resolved.

Additionally, the agency or CSP must hire a 3PAO certified assessor to complete the testing against their chosen CSP and create a Security Assessment Report (SAR). FedRAMP requires these assessors to be private organizations in order to maintain rigorous standards and avoid the use of additional government resources; they maintain a list of certified assessors on their website (https://goo.gl/idSbuL).

Once the SSP, all other documentation, and the SAR have been completed, the agency will submit both documents to the CIO for an ATO. The CIO retains the ability to revoke an ATO at any time. Alternatively, an agency CIO may leverage an existing ATO that a CSP has been awarded through another agency.



# DISCOVER THE DATABANK DIFFERENCE

## FOCUS ON COMPLIANCE

DataBank offers a unique opportunity for government agencies, System Integrators and SaaS providers looking to implement a versatile, affordable cloud solution that also meets the robust security requirements outlined by FedRAMP. The DataBank CloudPlus platform initially achieved FedRAMP certification as both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) in August 2014.

DataBank offers public and private FedRAMP compliant cloud environments quickly, enabling existing and new applications to function within FedRAMP's comprehensive security framework.

## A ROBUST SYSTEM SECURITY PLAN (SSP)

FedRAMP has played a key role in raising and codifying the minimum-security standards for agencies and CSPs that work with the Federal Government, but DataBank takes security even further by offering every partner a customized SSP.

DataBank's SSP explains every aspect of their system as it relates to NIST standards. The SSP may be customized to meet customer needs; DataBank experts can also assist in drafting the customer relationship on a contractual basis.

## PROVEN FEDRAMP TRACK RECORD

As detailed above, FedRAMP has designed the ATO process to be an arduous test that allows only the most secure platforms to emerge with an ATO. Beyond that, the ATO process typically costs hundreds of thousands of dollars. Leveraging the DataBank CloudPlus solution, with an existing approved ATO, saves considerable time, money and frustration and improves time to market for SaaS providers and integrators. DataBank also has the unique ability to create custom solutions for each of their customers. It is a significant achievement for any CSP to pass the FedRAMP certification process and emerge with a system that meets the exacting FedRAMP security requirements while also presenting a unique and actionable value proposition.

## COMMITMENT TO CLIENTS

One of the hallmarks of the DataBank strategy is a comprehensive, discovery-based approach to building cloud solutions for customers. This process is tied to the development of a customized SSP, wherein the platform is evaluated on a point-by-point basis. In fact, DataBank's solution architects strive to learn as much as possible about a customer's needs, strengths and areas of risk to design a solution that integrates seamlessly with their operations.

DataBank CloudPlus security is built directly into its framework, which allows customers to gain access to a complete suite of services designed to facilitate the cloud transition and increase cloud adoption. DataBank provides comprehensive monitoring, recovery, tech support, patching, backups, security, and operations.

Further, DataBank built a world-class infrastructure in geographically diverse locations. Their data centers are powered by the latest technology and incorporate multiple layers of security, including compliance with FedRAMP standards.

# LOOKING FORWARD

As cloud computing intertwines more with government processes, federal officials have sought to enhance the FedRAMP user experience for agencies. The cornerstone of this effort was the launch of a new FedRAMP. gov website in 2017, complete with numerous training modules and an impressive collection of manuals, application materials and more.

Additionally, officials are seeking new ways to make FedRAMP regulations more flexible while maintaining the robust security standards that are pivotal to the program. The realities and vulnerabilities of cloud technology are changing rapidly, and government agencies must have their security tools updated on a constant basis to maintain an optimal security environment.

In fact, the OMB has made it an official policy for all government agencies to investigate cloud solutions as their first option for new IT implementations. As CSPs and public and private organizations continue to work together to address evolving security risks, the possibilities offered by cloud computing will undoubtedly become more diversified as we move through the 21st century.

## SIMPLE, SECURE AND POWERFUL

Because of the complex nature of FedRAMP, DataBank's mission is to provide agencies with a simple, secure and powerful cloud solution that is designed with a customer's needs in mind. DataBank achieves this through their adaptable, consultative approach to design, wherein they work with partner agencies to leverage their unique attributes and protect against risk.

## 24/7/365 CUSTOMER SERVICE

DataBank includes 24/7/365 customer service and tech support for all customers because data security never runs on a set schedule. DataBank also includes data reporting services for customer convenience, and they offer each agency the opportunity to take advantage of their approved ATO, further simplifying the typically long and costly FedRAMP requirements.

## EXCEED CUSTOMER EXPECTATIONS

Above all, DataBank is constantly striving to build cloud solutions that exceed customer expectations in terms of security, features and customer service. If your agency is searching for a FedRAMP compliant cloud solution that can revolutionize day-to-day operations and offer unparalleled security protection, consult with an DataBank representative today at 800.840.7533 or reach out via link to sales@databank.com.

DATABANK
Data Center Evolved™

## About DataBank

DataBank is a supplier of secure FedRAMP IaaS and PaaS solutions, holding an authorization from multiple agencies and servicing seven other agencies. Navigating FedRAMP requirements, developing an SSP (System Security Plan) and altering operations to be compliant doesn't have to be complex and costly. DataBank's goal is to help Federal Agencies, Systems Integrators and SaaS providers simplify the process of transforming their infrastructure and applications into a FedRAMP Complaint Managed Cloud.

### CONTACT:

DataBank
120 E. Baltimore Street, Suite 1900
Baltimore, Maryland 21202
800.840.7533
www.databank.com