KYBERSTORM

FEDRAMP: MOST COMMON QUESTIONS ANSWERED

FedRAMP (Federal Risk and Authorization Management Program) is a risk management program designed by the government to take advantage of commercial Cloud Service Offerings (CSO). The program was introduced in response to the Cloud First Policy issued in 2011 and establishes an assessment and authorization process for CSOs. To receive a FedRAMP authorization to operate (ATO) Cloud Service Providers (CSPs) can either pursue an Agency path by getting one agency to sponsor them or go through a Joint Authorization Board (JAB) by applying through FedRAMP Connect. Even though FedRAMP has been around for over 10 years it can still be a daunting and challenging process. In this article we will try to answer some of the burning questions most CSPs have.

1.Does your organization need FedRAMP?

FedRAMP authorization is required for CSOs who are planning to process, transmit or store government data or data about government's data. So, let's break that down more. If your organization is looking to sell cloud services to the federal agencies, you will be required to implement security controls and assess them to meet FedRAMP requirements. Additionally, if you are selling services to another CSP who already has a FedRAMP authorization and is planning to use your services to complement their services, you will need a FedRAMP ATO. For example, if your solution is a ticketing system used by another CSP to store security incident data about their FedRAMP authorized CSO then FedRAMP ATO is required.

2.What are the benefits of FedRAMP ATO?

FedRAMP authorization opens new revenue streams and growth opportunities by allowing you to sell services to the federal government. Additionally, FedRAMP authorized CSOs can be used by other CSPs pursuing a FedRAMP authorization.
Lately, local governments have started to demand adequate cloud security controls that mirror FedRAMP controls. FedRAMP ATO can easily be translated into StateRAMP ATO, allowing CSPs to win additional work with the local and state governments. What we are witnessing now is that FedRAMP has become a gold standard amongst security and compliance frameworks which can give your organization a competitive advantage with enterprise clients or other verticals you wish to pursue.

3.How much will FedRAMP cost?

Overtime, there have been studies and statistics on the cost of FedRAMP showing numbers of $2 million to get authorized and up to $5 million for ongoing operational cost. From our experience these numbers can vary greatly based on the organizational security maturity. There are many variables that affect this number, these are some of the things we consider when calculating the cost:

People:

- Do you have enough supporting staff? At the minimum you will need: a dedicated ISSO, a senior engineer and/or architect, a DevOps engineer, a SIEM engineer, SOC analysts, a compliance subject matter expert.
- Can you train your current employees on new services, or do you need to hire industry experts?

Technology:

- Are you using the right technology that is FedRAMP approved/compliant?
- Is the system design and build process compliant with FedRAMP or is a redesign necessary?
- Does the redesign require migration to different infrastructure as a service (IaaS)? For example, if your commercial solution is built on AWS US East/West but you are seeking FedRAMP High authorization then you must migrate your CSO to the AWS GovCloud.

Processes:

- Have the organization processes been established?
- Do you have documentation to support your processes? This includes a system security plan, policies, procedures, and supporting plans.
- Do you have anyone in the house who can develop these?

4.How quickly can a CSO get FedRAMP ATO?

Depending on the CSPs readiness status it can take anywhere from 8 to 24 months to be listed as FedRAMP authorized CSO on the FedRAMP Market place. We have witnessed a perfect case scenarios in which a CSP can get ready within 60 days, then they go through a 3PAO assessment which typically takes 3 months, and then the package gets submitted to the FedRAMP PMO and agency for review, which takes another 3 months. But in most cases, it takes much longer for CSPs to get ready prolonging that time to a year plus.

5.Should you pursue an Agency or JAB authorization route?

The Agency path is the easier and quicker path to FedRAMP ATO due to agencies have varying degrees of risk acceptance. And they are typically highly motivated to get CSPs authorized so they can take advantage of those services.
JAB path on the other hand has its own benefits. If you have 6+ agencies that are waiting to use your services, then we suggest going JAB route. But keep in mind JAB has extremely low tolerance for risk so it won't be any room for alternate implementations.

6.How do you get an agency to sponsor you?

If you are currently not working with the federal government, the first step would be to hire an experienced federal sales resource to help you understand the federal market and obtain necessary vehicles in order to work with the government. Look for any Request for Information (RFI) or Request for Proposal (RFP) that are soliciting solutions like yours.
If you already have a federal customer establish a relationship with them and include FedRAMP PMO. The PMO office has an evangelist who works with agencies to educate them and guide the process, which can be much easier for agencies to accept the sponsorship. We suggest you reach out to the FedRAMP PMO to request their help. Also we are always here to help navigate that process and educate stakeholders.

How can KyberStorm help?

KyberStorm specializes in FedRAMP advisory services, our experts have working experience as assessors and advisors and have worked with various cloud platform.

What we offer:

- Workshops to prepare your teams for successful FedRAMP journey
- Gap analysis to evaluate your current security posture against FedRAMP requirements
- FedRAMP roadmap for meeting the requirements
- System design that is FedRAMP compliant
- Documentation development, including the system security plan and supporting documents
- Support during the assessment
- Support after the assessment

To learn how KyberStorm can help you prepare for and achieve FedRAMP authorization, contact **info@kyberstorm.com**.