PREPARING FOR FEDRAMP

WHAT YOU NEED TO KNOW

MARCELLE CONSULTANTS

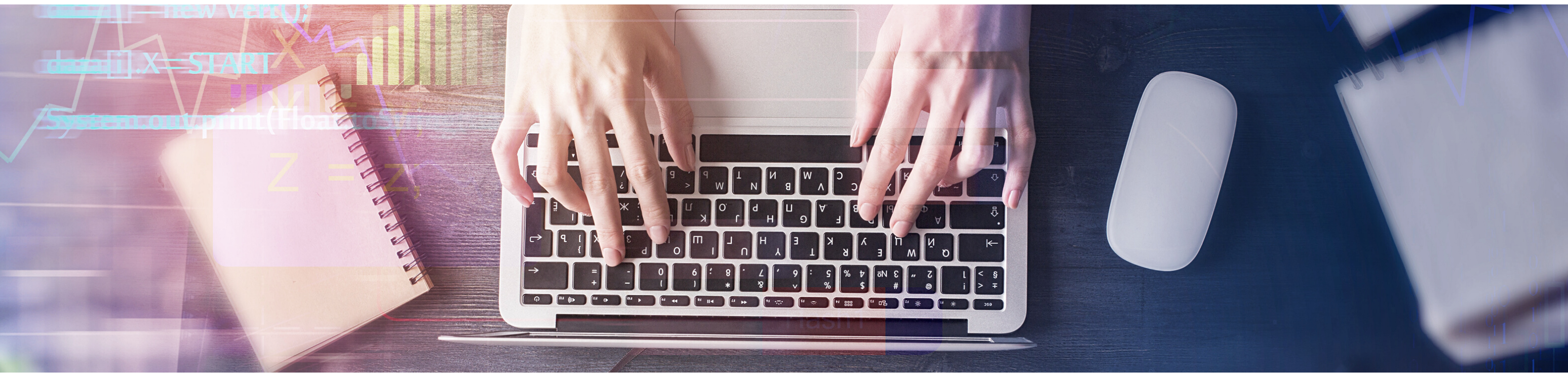
MARCELLECONSULTANTS.COM
CONTACT@ MARCELLECONSULTANTS. COM

WHAT IS FEDRAMP?

Compliance with FedRAMP is necessary for cloud service providers (CSP) to bag federal or other contracts with major clients. CSPs comply with the Federal Risk and Authorization Management Program (FedRAMP) if they adhere to the standardized requirements for information security assessment, monitoring, and authorization of Cloud Service Offering (CSO).

If CSPs store or process federal data, they are expected to receive an Authorization to Operate (ATO) from the agency CSP is serving, and there are mainly three types of FedRAMP ATOs:

- Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO)
- Agency Authority to Operate (ATO)



WHY DOES THIS MATTER TO YOU?

The US government's cloud-first initiative means a more significant number of agencies are moving to the cloud. Thus, FedRAMP-certified CSPs will be in great demand in the future. An enterprise that attains the FedRAMP certification is authorized to serve agencies processing data at their risk level.

For example, if a CSP is in the moderate category, it is eligible for contracts with agencies who want to deal with moderate-level data.

Compliance with FedRAMP is also beneficial for enterprises who do not want to pursue federal contracts. Implementing strict IT security controls ensures customers that the cloud offering is safe for business and that the CSP is serious about data security.

FedRAMP, on the other hand, ensures adequate, repeatable cloud security for the government departments and agencies.

HOW CAN CSP ORGANIZATIONS ACHIEVE FEDRAMP COMPLIANCE?

- **DOCUMENT**: The CSP categorizes the service or product for FedRAMP compliance according to NIST publication FIPS-199. The three categories for consideration are low, moderate, and high. Then, it documents the plan to implement the required controls.

- **ASSESS**: Next step is implementing a security assessment plan through a third-party assessment organization (3PAO) to test the controls. These tests are performed on the system planned for use and not a test system.

- **AUTHORIZE**: The federal agency will review the CSP's security assessment report, issue the ATO, or ask for additional tests.

- **CONTINUOUSLY MONITOR**: After getting the ATO, the CSP continuously monitors the cloud security controls to maintain compliance.