FedRAMP Risk Impact Levels

✓ LOW IMPACT RISK
Encompasses data intended for public use. Any loss of data wouldn’t compromise an agency’s mission, safety, finances, or reputation.

✓ MEDIUM IMPACT RISK
Includes data that’s not available to the public, such as personally identifiable information. A breach of this data can have a serious impact on an agency’s operations.

✓ HIGH IMPACT RISK
Includes sensitive federal information, such as law enforcement, emergency services, and healthcare data. Breaches to government systems containing this data would likely be catastrophic—potentially shutting down operations, resulting in financial ruin, posing a threat to intellectual property, or maybe even human life.

The Federal Risk and Authorization Management Program, or FedRAMP, applies to any cloud service or solution provider aiming to work with the U.S. federal government.

In 2011, the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), the Department of Homeland Security (DHS) and other government agencies collaborated to develop the framework. The resulting government-wide program establishes a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FedRAMP, like other federal frameworks such as FISMA, ties to the NIST 800-53 control library. However, FedRAMP includes additional controls regarding the unique aspects of cloud computing, enhancing the standard baseline controls.

Furthermore, FedRAMP is divided into 3 levels of risk impact. The levels are used to determine the set of controls an organization must adhere to, depending on their inherent risk. See left column for additional details.

Process for a FedRAMP certified Cloud Service Provider (CSP):

1) Pre-Authorization – Confirm an interest from a potential sponsor agency. Develop a relationship with a 3rd Party Authorizing Organization (3PAO).
3) Post-Authorization – CSP provides monthly continuous monitoring reports to prove compliance.
4) “Do Once, Use many Times” – Once authorized, CSP can be used by other agencies. Listing on FedRAMP Marketplace.

Ongoing compliance with FedRAMP requirements is a constant concern for all cloud service providers. As such, continuous monitoring deliverables must be presented to and reviewed by the Government Agency (or Agencies) that are using the service.

Further, agencies submit quarterly reports of all existing cloud services being used that do not meet FedRAMP requirements. And, if the agency and provider cannot provide sufficient rationale and a proposed resolution plan, the provider will be deemed non-compliant and their contract is jeopardized.

Confidentiality
Availability
Integrity
FedRAMP was designed to mitigate agencies’ risk, but also provide an easy way to acquire authorized cloud services. If a provider is FedRAMP approved, then issuing a new Authority to Operate (ATO) is the only step that must be taken. This prevents CSPs and Agencies from duplicating work that has already been done as part of the initial authorization. Additionally, once a service offering is authorized, it is listed in the FedRAMP Marketplace, a common source for government work. To say the least, this makes security professional’s lives easier, and saves everyone time and money.

Your FedRAMP Solution: Q-Compliance is purpose-built to help you streamline and automate complex cybersecurity auditing and compliance requirements like FedRAMP. As a native Splunk solution, Q-Compliance leverages continuous monitoring and reporting to ensure compliance against FedRAMP in real-time.

Qmulos makes ongoing FedRAMP compliance easy with automated alerting tied to passing and failing controls. If a control fails, a detailed report with actionable information to address the issue is generated. The solution gives the user the ability to upload policy, procedure and file evidence as well as automatically log human activity, and keeps evidence needed for future audits all in one place.

The FedRAMP dashboard helps you track how your organization and systems are scoring against each control category, and where you need to improve to pass an audit. The dashboard provides the ability to quickly drill into specific domains to view compliance against the capabilities, practices and processes set forth. Furthermore, you can drill into individual controls to see the specific systems, events, and assets that are non-compliant.

Q-Compliance makes keeping up with FedRAMP and maintaining compliance with other standards like NIST 800-53 simple. FedRAMP specific scorecards provide real time answers to your operational status to prepare for and pass audits. Contact sales@qmulos.com for more info or to see a free demo of our FedRAMP capabilities.