**Lack of understanding of FedRAMP packages**

The federal government has been under a “Cloud First” mandate since 2010. More than seven years later, there is only fitful progress among agencies in making the cloud their first priority for IT services and infrastructure.

One of the key initiatives intended to help speed this process was The Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment for cloud-based resources. Launched with the best of intentions, FedRAMP quickly presented a number of the same kinds of roadblocks to deployment that FISMA and other federal compliance standards have imposed. Instead of facilitating moving to the cloud, FedRAMP itself became something of a barrier to entry.

The FedRAMP program has recently been streamlined to address these concerns. Still, confusion remains about the specifics required of cloud service providers that want to make their offerings available to the federal market. In particular, many CSPs aren’t familiar with the complex package of documentation they must submit for FedRAMP compliance. The complete package can run from hundreds to well over a thousand pages of documents, including:

**System Security Plan (SSP):** The SSP is the multi-part documentation of a cloud offering’s security requirements, providing the framework to capture the system environment, system responsibilities, and the current status of the baseline controls required for the cloud offering.

**Controls Implementation Summary (CIS):** This outlines the FedRAMP security control responsibilities of CSPs and customer agencies. It provides a summary of all required controls and enhancements across the system as well as implementation responsibility and status of the controls.

**Security Assessment Plan (SAP):** The SAP is developed by a third-party assessment organization (3PAO) to document the methodology it will use to test the controls implementation of the cloud offering. It identifies the assets within the scope of the assessment and also provides a roadmap and methodology for execution of the tests.

**Security Assessment Report (SAR):** This is an assessment prepared by the 3PAO containing information about vulnerabilities, threats, and risks discovered during the testing process and guidance for CSPs in mitigating them.

**Plan of Action and Milestones (POA&M):** A document prepared by the CSP to identify, assess, prioritize, and monitor the progress of its efforts to correct and mitigate any security weaknesses in its cloud offering as revealed by the SAR.

Other elements of the package include the FIPS-199 categorization, a privacy impact assessment, incident response plan, penetration test report, and a host of supporting evidentiary artifacts.

CSPs also need to know that many of these are living documents that must be kept up-to-date as part of FedRAMP’s continuous monitoring requirements.