FedPlatform

FedRAMP Executive Overview 2012.06.01

The Mandate

On December 8, 2011, the Federal Chief Information Officer issued a memo addressing the importance of security for cloud computing within the federal space. The Federal Risk and Authorization Management Program (FedRAMP) was developed to provide a cost-effective, risk-based approach for the adoption and use of cloud services within the federal space. FedRAMP sets forth guidelines and requirements for agencies and vendors to adequately assess, authorize, and monitor cloud services and products throughout its lifecycle.

The General Services Administration unveiled a single authentication standard for government cloud-computing services.

Commonly referred to as FedRAMP, <Federal Risk and Authorization Management Program> this program will standardize the basic security requirements that cloud-computing providers, will have to meet before receiving government contracts.

The new guidelines will require contractors to hire third-party assessment organizations that will verify whether they meet the basic security requirements.

The program, developed by GSA, the Defense and Homeland Security departments and the Office of Management and Budget, will set one government-wide cloud security program, which means a vendor such as Microsoft would not have to repeat the security approval process every time it wants to bid on a cloud-computing contract.

FedRAMP's Web site lists nine accredited third-party assessment organizations that vendors can use to authenticate more than 160 basic security controls, including spam filter capabilities and encryption standards.

This is the latest development in the White Houses's cloud-first policy, to streamline many government computing functions. Cloud services are often more efficient and more secure than computing handled in house, said Steven Van Roekel, the U.S. chief information officer.

"The key to security is consistency," Van Roekel said in an interview. "When you're in these disparate federal systems you don't have as many consistent guidelines or controls as companies do on one system."

However, there are contradictory views as to if this initiative should also help smaller vendors compete for cloud-computing contracts. Recently Dan Cruz, GSA's deputy press secretary is quoted as stating:

"FedRAMP's model of 'do once, use many times' is helpful to smaller cloud service providers seeking to do business with the federal government by eliminating the need to expend resources for duplicative security authorizations with each federal agency"

Surely, there are as many opinions on these matters as there are pebbles in a pond, but non-the-less it is clear that FedRamp is here to stay and in its totality will benefit the public and the agencies who serve them.

FedRAMP was developed in collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), and the Department of Homeland Security (DHS). Many other government agencies and working groups participated in reviewing and standardizing the controls, policies and procedures.

FedRAMP sets a common standard for providing cloud services to the federal government. The General Services Administration announced the program last year as part of a broad initiative to simplify the IT services procurement process and ensure that those trusted with transmitting and storing government data meet key security standards.

The major participants in the FedRAMP process are:

- **Federal agency customer** – has a requirement for cloud technology that will be deployed into their security environment and is responsible for ensuring FISMA compliance

- **Cloud Service Provider (*CSP*)** – is willing and able to fulfill agency requirements and to meet security requirements

- **Joint Authorization Board (*JAB*)** – reviews the security package submitted by the CSP and grants a provisional Authority to Operate (ATO)

- **Third Party Assessor (*3PAO*)** – validates and attests to the quality and compliance of the CSP provided security package

- **FedRAMP Program Management Office (*PMO*)** – manages the process assessment, authorization, and continuous monitoring process

The FedRamp Process—Abbreviated

A CSP follows the process for a provisional authorization under FedRAMP and uses a 3PAO to assess and review their security control implementations. CSPs then provide documentation of the test results in a completed assessment package to the FedRAMP PMO. The security package is then reviewed by the JAB and if a CSP system presents an acceptable level of risk, a provisional Authorization is granted. Agencies can then leverage the Provisional ATO and grant their own ATO without conducting duplicative assessments.

Cloud Computing has been slowly but surely moving towards the federal government over the past few years. More and more agencies are starting to see the drastic cost and efficiency benefits of the cloud over On Premise or Co-location hosting. Among some of the factors that caused reluctant adoption, security seemed to be the most visible. The FedRAMP Program addresses the new risks and security concerns that are associated with this new technology.