Federal Risk and Authorization Management Program (FedRAMP)

The cloud computing market contributed about $77 billion in revenue in 2011 and is expected to represent $240 billion worth of revenue by 2016, according to Visiongain (http://www.tmcnet.com/topics/articles/246856-how-big-will-cloud-computing-revenues-be-2016.htm). The federal government is expected to purchase over $20 billion of cloud services in 2012 with the expectation that each agency will be migrating at least 3 applications to the cloud between 2012 and 2013.

Over the past decade, the federal government has spent enormous amounts of resources, time, and money on duplicate, inconsistent, and inefficient Information Technology (IT) security risk management approaches. These same ineffective approaches were applied to the emerging cloud systems and services. There was little to no incentive to use existing security assessments across agencies. Many preferred to perform their own assessments when other agencies and cloud service providers had undergone and obtained authorization and approval for the same cloud systems or services. Recognizing the growth and potential of cloud computing, the federal government sought to find a more targeted and efficient approach to IT security risk management in the cloud environment.

On December 8, 2011, the Federal Chief Information Officer (CIO) Council released a policy memo (http://www.cio.gov/fedrampmemo.pdf) establishing the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP was developed through collaboration with CyberSecurity and cloud experts from various federal agencies, working groups, and private industry to foster the adoption of cloud computing by the federal government. It is considered to be a government-wide initiative that will standardize the approach to security assessments, authorizations, and continuous monitoring for cloud products and services provided by the Cloud Service Provider (CSP). The approach will use a “do once, use many times” framework that will save the cost, time, and staff required to conduct redundant agency security assessments of the services provided by the CSPs.

FedRAMP program will authorize cloud systems in a four-step process: initiating, assessing, authorizing, and leveraging. The FedRAMP assessment process can either be *initiated* by agencies or CSPs. The process starts with a security *assessment* using the FedRAMP requirements, which are Federal Information Security Management Act (FISMA) compliant and based on the National Institute of Standards and Technology (NIST) 800-53 rev3 publication. CSPs must implement the FedRAMP security requirements on their environment and hire a FedRAMP-approved third party assessment organization (3PAO) to perform the independent audit of the cloud system and provide a security assessment package for review. The package, which includes the security assessment report, plan of actions and milestones, and other relevant documents, will be reviewed by the FedRAMP Joint Authorization Board (JAB) and the board may grant a provisional *authorization*. Upon further detailed review of the package, the JAB will approve and authorize the federal agencies to use the CSP system. The federal agencies can *leverage* CSP authorization packages and grant the Authority to Operate (ATO), saving time and money.

Some of the expected key benefits for FedRAMP are:

- Re-use of existing security assessments across agencies
- Substantial savings in overhead (cost, time, resources) – “do once, use many times”
- Risk-based security management and improved security visibility
- Transparency between CSPs and federal agencies
- Improvement of the trustworthiness, reliability, consistency, and quality of the federal security authorization process.

For more information on FedRAMP, visit www.fedramp.gov.