**Continuous Monitoring and Compliance**

Continuous monitoring is an important element in FedRAMP. Early efforts at enforcing agency compliance with security controls for on-premises systems overlooked the need for ongoing security assurance, resulting in a static point-in-time approach to security that left federal systems vulnerable over time.

FedRAMP includes an ongoing assessment and authorization program to account for intended and unintended changes to a system and its environment once it has received a FedRAMP authorization. This continuous monitoring element of FedRAMP helps to maintain the authorization of cloud offerings on a rolling basis.

However, effective continuous monitoring requires ongoing interaction among the cloud service provider, the agency, and the 3PAO. Supporting that work requires detailed updates to the documents within the security authorization package as well as supplemental reports that provide evidence of system changes and how those changes are being reconciled with the system’s security posture.

Xacta’s continuous monitoring capabilities are ideally suited to this requirement. They empower organizations to correlate scan results from multiple security products into a single view and map them to the relevant FedRAMP controls for security and risk management. Xacta’s integration with the cloud host’s APIs also supports scanning, testing, and monitoring to continuously validate the security compliance of cloud-based resources.

Xacta then produces updated documents for the FedRAMP security authorization package including updates to the plan of action and milestones (POA&M). These documents provide sound evidence that FedRAMP baseline security controls continue to safeguard the system as originally envisioned. With Xacta, the goal of a “continuous ATO” is within reach for agencies that use cloud-based resources.