**Overly Manual FISMA Accreditation Processes**

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to develop, document, and implement programs to provide security for the information and systems that support them.

FISMA directs these agencies to implement a large range of security controls, guidelines, and frameworks developed by the National Institute of Standards and Technology (NIST). Agencies must successfully apply these standards for each system in order to receive an authorization to operate (ATO) that allows the system to be put into operation.

FISMA’s original certification and accreditation (C&A) process was extremely report-heavy and labor-intensive, resulting in the production of expensive multi-part documents running to thousands of pages in scores of volumes. Systems only needed to be recertified every three years, so that even a minor change to a system early on would immediately render its ATO effectively meaningless, with no recertification on the horizon.

FISMA was amended by The Federal Information Security Modernization Act of 2014 in an effort to address these concerns. Its changes resulted in less overall reporting, greater focus on managing risk, and a greater emphasis on continuous monitoring to assure the ongoing authorization and accreditation (A&A) of a system.

Nevertheless, the current A&A process for achieving ATO is still daunting. Driven by the NIST Risk Management Framework (and by FedRAMP for cloud-based systems), it is a comprehensive evaluation of an information system’s security policies, technical and non-technical security components, controls documentation, and vulnerabilities. It details the extent to which a system complies with federal mandates for security as well as the agency’s own unique guidelines. Its continuous monitoring provision requires the agency to detect and document any change in the security posture of the system to enable decision-making based on current information.

Many agencies still labor with manual tools and processes to do this work, using documents, spreadsheets, and email to manage the compliance posture of every system. Relying on manual processes to achieve and maintain their systems’ ATOs is very time-consuming, error-prone, and paper-intensive. It can take months or even years to gain approval, delaying the standup of critical systems and jeopardizing an agency’s mission as a consequence.