The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

Status:
Laureate

Year:
2013

Organization Name:
Federal Risk and Authorization Management Program

Organization URL:
www.fedramp.gov

Project Name:
Federal Risk and Authorization Management Program

Please select the category in which you are submitting your entry:
Innovation

Please provide an overview of the nominated project. Describe the problem it was intended to solve, the technology or approach used, how it was innovative and any technical or other challenges that had to be overcome for successful implementation and adoption. (In 300 words or less.)

Currently each agency manages its own security risks and provides security assessments and authorizations for each information technology (IT) system it uses, even if other agencies have assessed, authorized, and deployed the same system. This is duplicative, inconsistent, costly, and inefficient. The Federal Risk and Authorization Management Program (FedRAMP) provides a unified and government-wide risk management framework that addresses these problems. FedRAMP increases agency confidence in the security of cloud systems by providing security assessments and authorizations based on a standardized baseline set of security controls aligned to NIST SP 800-53 controls; accrediting independent assessors' ability to consistently evaluate a Cloud Service Providers

(CSPs) implementation of security controls; and coordinating continuous monitoring services. The program facilitates faster adoption of cloud services and expedites implementation of next-generation technologies. The program is the result of close collaboration with cybersecurity and cloud experts from GSA, NIST, DHS, DOD, NSA, OMB, the Federal CIO Council and its working groups, as well as private industry. A key aspect of FedRAMP is its Joint Authorization Board that brings together the Chief Information Officers (CIOs) from DOD, DHS, and GSA to: Define FedRAMP security authorization requirements; Approve accreditation criteria for third party assessment organizations; Review FedRAMP authorization packages and grant joint provisional authorizations. In addition, a conformity assessment process qualifies independent assessors as Third Party Assessment Organizations according to the following requirements: Independence and quality management in accordance with ISO/IEC 17020 standards; Information assurance competence - experience with FISMA and testing security controls; Competence in the security assessment of cloud-based systems. A secure repository provides agencies the ability to review and leverage FedRAMP security packages to make their own risk-based decision to grant an authority to operate.

When was this project implemented or last updated? (Please specify month and year.) Has it incorporated new technologies and/or other innovations since its initial deployment? (In 300 words or less.)

The Federal Risk and Authorization Management Program (FedRAMP) achieved initial operational capability in June 2012. At this point, the program had accredited a number of third party assessment organizations (3PAOs); processes, procedures, and templates had been created to guide agencies, CSPs, and 3PAOs in meeting FedRAMP requirements; and cloud providers could apply for a FedRAMP provisional authorization. In December 2012, FedRAMP granted its first provisional authorization to Autonomic Resources, a certified 8a small business from North Carolina offering Infrastructure as a Service capabilities to federal agencies. A provisional authorization is an initial approval of the CSP authorization package by the Joint Authorization Board that an agency can leverage to grant a security authorization and an accompanying Authority to Operate (ATO) for the use of the cloud service within the agency.

Is implementation of the project complete? If no, please describe the project’s phases and which phase the project is now in. (In 300 words or less.)

The program is currently in the initial operational capability phase. During this phase the program is focusing on establishing the program’s processes and procedures; updating the concept of operations, continuous monitoring requirements, and CSP guidance; and establishing performance benchmarks. In

Spring 2013, the program will move into the full operational capability phase and this will be followed in 2014 by a move into sustaining operations. As the program progresses, it will scale operations to authorize more CSPs to meet demand.

Please provide at least one example of how the technology project has benefited a specific individual or organization. Feel free to include personal quotes from individuals who have directly benefited from the work. (In 300 words or less.)

While FedRAMP is not yet fully operational, the program benefits both government and the private sector by standardizing the processes and security controls agencies and companies must go through together in order to certify an IT system. Before FedRAMP, agencies conducted their own assessments in a vacuum - now, agencies can leverage another department's work. This greatly reduces time to market for IT systems, speeding capabilities to end users and supporting agency mission requirements. Recently, the FedRAMP PMO released the first Provisional Authorization certified by the Joint Authorization Board (an oversight group comprised of the Department of Defense, Department of Homeland Security, and the U.S. General Services Administration). Within the first day of the authorization being available for agencies to leverage, four agencies expressed interest in doing so and contacted the FedRAMP PMO to begin the process.

Would this project be considered an innovation, a best practice or other notable advancement that could be adopted by or tailored for other organizations and uses? If yes, please describe that here. (In 300 words or less.)

FedRAMP is an excellent example of a best practice and is a notable advancement in the fields of cybersecurity, innovation, and open government. The program leverages a first-of-its-kind approach that revolutionizes how federal agencies certify, accredit and continuously monitor their IT systems, reducing redundant effort across government, saving the federal enterprise money, and allowing redirection of critical resources towards mission needs. FedRAMP's central tenet is enabling reuse and reducing redundancy. The FedRAMP PMO modeled all processes and documentation used within the program itself with reuse in mind - this approach ensures that agencies see a clear business need to leverage FedRAMP as opposed to conducting their own security assessment and certification. The program is also beneficial to private sector cloud service providers (CSPs), as they no longer have to go through a different process for each agency - FedRAMP reduces level of effort, time to market, and overall expenditure for the private sector.

If there are any other details that the judges should know about this project, please note them here. (In 300 words or less.)

FedRAMP leverages independent assessors to ensure that documentation received from CSPs is complete and that these companies conform to the program’s processes. This allows agencies to consume FedRAMP certifications secure in the knowledge that the packages themselves are standardized and are held to a high quality standard. Additionally, FedRAMP continues to conduct agency and industry days, maintains a website that serves as the authoritative source for program templates, documentation, and information on processes, and hosts a regularly held webinar series on specific topics germane to FedRAMP. This constant outreach effort ensures that agencies and industry alike are well educated on critical aspects of the FedRAMP program, and have an avenue for feedback.