Introduction

As technological trends rapidly advance, federal agencies have been tasked with meeting the increasing needs of employees and citizens—whether they be greater access to information, flexible telework requirements, or innovative digital platforms. At the same time, government must contend with the looming threat of cyber attacks from a wide range of pernicious actors, including state-sponsored agents, identity thieves, and other cyber criminals.

Although these factors continue to challenge technology leaders, cloud computing has assisted agencies in mitigating risk, improving productivity, and leveraging new capabilities. Moreover, over the past few years the federal government’s foresight and relatively unified efforts in implementing the Federal Risk and Authorization Management Program (FedRAMP) has helped agencies safely access a wide range of cloud-based technologies. Still, many agencies have yet to leave the ground and realize the benefits of cloud computing. In an austere and uncertain budget environment, FedRAMP may assist agency leaders to optimize limited resources and enhance mission effectiveness through cloud adoption, while having the peace of mind that newly implemented technologies have met stringent standards for security.

Early Returns from “Cloud First”

The White House’s February 2011 “Cloud First” policy and Federal Cloud Computing Strategy (FCCS) outlined a bold new direction for the federal IT reform, and in the years since, agencies have rapidly warmed to the idea of cloud technologies.

For some agencies, cloud adoption has already provided clear cost saving benefits. Department of Treasury Chief Information Officer (CIO) Sonny Bhagowalia credits cloud data storage solutions for providing agencies greater flexibility and enhanced capabilities, at a fraction of the cost.1 Previous CIO David Bray attributes cloud for slashing IT maintenance budgets at the Federal Communications Commission in half, results that in part encouraged him to take on a lead role at the Federal Cloud Center of Excellence (CCOE), an inter-agency group recently established by the General Services Administration (GSA). Bray notes that “cloud services, done correctly, allow you to be more streamlined and nimble in your processes and provide better service for your public stakeholders.”2

Meanwhile, other early adopters have also reported how cloud-enabled data analytics, digital tools, and agile development can improve agency productivity better equip government employees to deliver services to the public.3 By moving its Total Ammunition Management Information System to the cloud, Department of the Army was able to shorten the timeframe for some work tasks from three weeks to as quick as three hours, allowing employees to spend more time on other mission objectives.4 In the Department of Transportation, technology leaders praise cloud for enabling the organization to take an enterprise approach to IT, especially when it comes to unifying disparate applications and data environments.5 And significantly, federal leaders are increasingly noting the importance of cloud-based cybersecurity to more effectively mitigate attacks and manage defenses; in May 2017, President Trump signed an Executive Order effectively establishing a single cloud-based structure to unify cybersecurity postures across agencies.6


To help agencies tap into these benefits of cloud computing and navigate the myriad security considerations prerequisite to its adoption, in 2011 the Obama Administration launched FedRAMP, the Federal Risk and Authorization Management Program. FedRAMP provides authorization and certification for commercial cloud providers serving federal agencies. Cloud companies must meet a list of requirements defined by the National Institute of Standards and Technology (NIST) before receiving approval to sell cloud services to government. These security controls span all aspects of technology service delivery and management, including:

- **Rules for Governance:** audit and accountability, contingency planning, program management, risk assessment, security assessment and authorization
The program has also overcome initial setup hurdles occurring in its first few years of operation. From the start, GSA officials have firmly asserted that the program’s rigorous certification is meant to establish trust, and designed to take approximately six months to clear. Even after ATOs are awarded, providers must follow ongoing security monitoring requirements to keep the certification.

Initial Returns from FedRAMP

Over the past five years, the FedRAMP approach to cloud computing has already benefited many agencies grappling with limited resources and shrinking budgets. The Federal CIO Council estimates that FedRAMP helps the federal government save 30-40% in total IT implementation costs, a figure totaling more than $40 million in just the first two years of operation. By 2017, many agency leaders have come to rely on FedRAMP when it comes to procuring secure technologies. John Hale, chief of enterprise applications at the Defense Information Systems Agency (DISA), notes that “from a Department of Defense perspective, when we look at computing and cloud computing going forward, we are 100 percent dependent on the FedRAMP process. So all of our commercial cloud providers who want to provide services to the DOD, the very first question we ask them is ‘What level of FedRAMP certification have you achieved?’”

The Future of FedRAMP and Federal Cloud Computing

Despite this significant process, FedRAMP’s management team and federal cloud advocates continue to look for ways in which they can improve the program and encourage greater cloud adoption. Although the Office of Management and Budget set a 2016 governmentwide target of 15 percent for cloud computing adoption, the Federal CIO Council reports that no agency has yet to reach that level. Significantly, even
with these limited efforts, the Government Accountability Office estimates that the “Cloud First” policy has already saved the federal government more than $3.6 billion in its first four years of action.\textsuperscript{18}

Additionally, use of FedRAMP has also been uneven across federal agencies. While larger agencies (led by Defense, Health and Human Services, Commerce, Energy, Interior, Homeland Security, and Energy) have leveraged multiple CSPs approved through FedRAMP,\textsuperscript{19} an estimated 60 percent of federal agencies have yet to participate in the program, most of them small and mid-sized agencies.\textsuperscript{20}

Fortunately, leaders in both the Federal Cloud Center of Excellence and FedRAMP have striven in recent months to address these deficits. In recent months, the CCOE has been working to provide educational outreach and guidance to agencies that have yet to adopt cloud services and assist them in overcoming contracting and change management difficulties.\textsuperscript{21} Concurrently, FedRAMP made several changes in 2016 that have already yielded positive results. These include a “FedRAMP Accelerated” initiative that would hasten the CSP approval process,\textsuperscript{22} as well as a “High Baseline Requirements” certification for highly sensitive applications and systems in hopes of wooing agencies with more stringent security requirements.\textsuperscript{23} FedRAMP Director Matt Goodrich has also articulated ambitious goals for 2017, including doubling both the number of cloud service offerings and ATOs by the end of the year, as well as completing all authorizations in under six months.\textsuperscript{24} FedRAMP is also making further changes to the continuous monitoring process by which providers maintain their authorization, and will be looking to increase collaboration with industry.\textsuperscript{25}

Cloud computing’s promise to provide agencies greater agility, operational resilience, and technological capabilities has already been realized in several federal organizations. By owning the wieldy security certification process, FedRAMP will continue to help agencies reduce costs, safely acquire new capabilities, and focus instead on key mission objectives, rather than the nitty-gritty of technology implementation. With further improvements on the way, FedRAMP can hopefully help even more agency leaders feel prepared to implement and realize the vast benefits of cloud computing.
Infor builds beautiful business applications with last mile functionality and scientific insights for select industries delivered as a cloud service, on premises, or both. With 15,000 employees and over 90,000 customers in more than 170 countries, Infor is a leading provider of software applications. Infor delivers a comprehensive suite of integrated, industry-specific solutions, including purpose-built for the public sector. Infor solutions increase operational efficiency, government accountability, process transparency, and are transforming how governments provide services to citizens.

infor.com/publicsector

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis. To learn more, visit Govexec.com/Insights


5. CIOs must herd cats before enjoying benefits of cloud. https://federalnewsradio.com/cloud-computing/2016/02/cios-must-herd-cats-enjoying-benefits-cloud/


7. NIST Special Publication 800-53 (Rev. 4) https://nvd.nist.gov/800-53


12. FedRAMP is proving to be a tough test for cloud providers. https://gcn.com/articles/2013/02/13/fedramp-tough-test-cloud-providers.aspx

13. Finally, a faster FedRAMP? https://fcw.com/articles/2016/05/03/faster-fedramp-revamp.aspx


