Moving beyond compliance to the business benefits of FedRAMP cloud migration

In 2012, the U.S. Government established the Federal Risk and Authorization Management Program (FedRAMP) to protect data collected by government agencies and stored in the cloud. Seven years later, legacy systems and patchwork digital networks still dominate the federal digital domain. In 2018, concerned about the "lack of agency buy-in" to FedRAMP, U.S. Representative Gerald Connolly presented **H.R. 6550**, a bill that sought to make FedRAMP the law.[1]

But is FedRAMP compliance just a question of ticking the mandated boxes? Or is there a mission-critical case for agencies to make the transition to cloud-based IT using the FedRAMP marketplace? This paper examines the business benefits to federal, state, and local agencies as well as businesses in other industries who are exploring a FedRAMP-guided cloud migration.

The issue: Low adoption of FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) has established itself as the common standard for cloud security assessment, authorization, and continuous monitoring across the United States Government, and increasingly for state and local agencies as well as businesses in other industries. It's a tough, rigorous process, and necessarily so, given the range and severity of cybersecurity threats confronting governments and industry every day.

Though FedRAMP has been policy since 2012, a recent survey conducted by the Government Business Council revealed that only 11% of agencies had migrated to the cloud using partners and products in the FedRAMP marketplace. Why aren't those numbers higher? Would the pace quicken if more agencies were aware of the business benefits FedRAMP provides to agencies, their customers, and constituents?

FedRAMP: Confidence through security

It's a basic truism of public service that customers' and citizens' confidence is difficult to earn and easily imperiled. Nowhere is that observation more pertinent than in online services and cybersecurity, where a single breach or loss of service could produce measurable costs in the billions of dollars, plus human and institutional costs that are incalculable.

But there would be an equal and opposite cost if security concerns led government agencies to forego the significant efficiency gains, cost reductions, productivity improvements, and other customer service benefits of an integrated, cloud-based software platform.[2]

The only solution for the 21st century public service was to come up with an overarching framework that could reconcile two absolute needs—for cloud-specific security, and cloud-enabled performance.

Given the clear benefits of operating in the cloud and the growing need for uniform security practices, why aren't more agencies migrating to the cloud with FedRAMP-authorized partners and products?

The cost of legacy systems

The General Services Administration and Office of Management and Budget **named** reliance on legacy systems and "patchwork network architectures" as one of the primary obstacles to a "more modern, secure, and resilient information technology" at the federal level.[3]

Preserving legacy systems accounts for close to **70.3%** of IT budgets government-wide.[4] And that figure doesn't take into account the millions lost to inefficiency, reduced productivity, and security mitigation.

But many agencies are heavily invested in legacy on-premises systems that are grandfathered—and industry analysts say those outdated systems are cash cows to the companies that provide them. Add to that the reality that some agencies are wary of perceived risks associated with new systems and processes, and the result is a mired modernization process.

Nevertheless, some industry watchers pointed to a **decided uptick** in the number of agencies transitioning to cloud-based IT over the last year, so the emerging question may no longer be "if" but "when" the outlying agencies make the move.[5]

Business benefits of FedRAMP cloud migration

Public sector migration to cloud-based IT serves a variety of government objectives, including:

- Improving public and executive confidence in IT system security management
- Providing a baseline standard for consistent security authorizations
- Ensuring rigorous application of IT security practices
- Providing continuous monitoring through increased automation and near real-time data
- Delivering on all the operational efficiencies and productivity improvements that make cloud computing a breakthrough opportunity for front-line program managers and staff

Complying with FedRAMP during a cloud transition offers clear business benefits to agencies of all sizes, no matter where in the migration process the agency is today. FedRAMP enables agencies to:

Accelerate their mission

Agencies like the National Aeronautics and Space Administration (NASA)—an agency the public expects to see at the forefront of technology evolution—have used FedRAMP and the cloud to push their missions into new directions and capabilities. **Steve Hunt**, IT Governance Lead of NASA's Enterprise Managed Cloud Computing Office and winner of FedRAMP's **2018 Large Agency Tech Lead Award**, explained how a custom cloud solution made it possible for NASA to livestream the Mars landing of the Curiosity rover back in 2012.[6 & 7]

"The ability to share that moment, across the entire planet, in real time via websites with live coverage and streaming video, was enabled by intelligent and creative people at NASA, passionate about working at the leading edge of cloud technology," he said. "Being involved with the cloud program at that moment in time was really something to behold, and foreshadowed a new era in information technology."

Other agencies like the Department of Health and Human Services and the Department of Energy are now leveraging machine learning, artificial intelligence (AI), and other mission-advancing technologies because they've invested time and resources developing **a digital strategy that's AI ready** and able to handle the security needs of the big data explosion.[8] Plus, security and contingency planning are also automatically scaling with new technology insertion. To realize the promise of AI and other data-dependent solutions, agencies of all sizes need to start building secure digital pathways now.

One of the **key performance indicators** set forth by the Office of Management and Budget and General Services Administration is providing people with a public sector customer service experience like they have come to expect from the private sector.[9]

Yet 80% of federal agencies scored in the lowest categories on **Forrester's 2018 U.S. Federal Customer Experience Index**.[10] One of the primary reasons for the negative ratings? Government processes are still seen as too difficult, and customers feel they can't get help quickly.

Moving business processes to the cloud enables agencies to deliver faster, smoother customer experiences. And using FedRAMP-authorized partners and products with continuously monitored security builds public trust in an environment that is increasingly concerned about the endangerment of personally identifiable information.

Speed up cloud migration

In 2017, responding to concerns about the complexity and cost of the authorization process, FedRAMP rolled out the **Tailored Program** to offer Cloud Service Providers (CSPs) and agencies an expedited path to authorization.[11] Industry leaders report that in the ensuing months, the time frame for authorization dropped from roughly 18 to four months.

The **FedRAMP marketplace** features trusted partners that can help guide an agency through the process of selecting authorized CSPs, platforms, and products, streamlining the transition even further.[12]

And the FedRAMP program management office trims the time frame by offering agencies its guidance and support during and after the transition. **Industry analysts** say collaborating with a FedRAMP liaison gives agencies access to a "wealth of knowledge."[13]

Keep costs in check

As has been much discussed among public sector IT professionals, the **Technology Modernization Fund** prioritizes cloud migration for agencies of all sizes, enabling many federal agencies to implement much-needed changes.[14]

FedRAMP offers an additional advantage: Once a platform, product, or partner has met authorization standards, it can be used again and again across numerous agencies, driving down costs. The **FedRAMP PMO** estimates this "do-once, use many times" capability saves an average of 30 to 40% of the cost of authorization.[15] FedRAMP Acting Director **Ashley Mahan** told *Washington Exec* that the approach is "hugely beneficial for both vendors and agencies in terms of saving time and resources."[16]

And when an agency uses a **FedRAMP-authorized platform**, it effectively **transfers much of the costs** of obtaining an Authority to Operate, along with the annual costs of maintaining compliance, to the third-party provider.[12 & 17] Also shifted: the cost of liability for security breaches. For small and medium-sized agencies, that cost savings could mean the difference between successful cloud migration and failure to modernize.

But perhaps the most important cost-saving step for agencies is to ensure they have categorized their system correctly up-front with the appropriate security controls. In the past, agencies have adopted a slew of cyber-defense tools in the hopes of covering all their bases. Allocating resources based on actual risk avoids overspending on security.

Operate in a continuously monitored and updated ecosystem

FedRAMP authorization requires CSPs to perform continuous vulnerability scanning, reporting, and remediating any potential security problems. And because authorized products and platforms operate in the cloud, they obviate the need for time-consuming patches and updates, continually tracking newly discovered vulnerabilities and detecting when deviations from the authorized baseline occur. It's also possible to dramatically reduce down time and allow agencies to focus on their mission and customers rather than on security.

The CSP's responsibilities under FedRAMP: Four rules of thumb

One of FedRAMP's strengths is the way it defines the key factors Cloud Service Providers (CSPs) must take into consideration in describing and depicting their authorization boundaries. The clarity and precision in those specifications are a boon to all parties, enabling vendors to align their SaaS architecture with authorization requirements, and giving both vendors and agencies a clear sense of the boundary definitions that will be required in security documentation.

Much of that work was guided by four rules of thumb for system components on both sides of the authorization boundary:

- For federal information that is processed, stored, or transmitted by or for the federal government, in any medium or form, CSPs must conduct their own due diligence to define their authorization boundary, with clear delineations among internal and external services and service providers. FedRAMP requirements for documentation, testing, and continuous monitoring apply to all system components within the boundary.
- All external services that affect the confidentiality, integrity, and availability (CIA) of federal information or metadata must be depicted within the authorization boundary and assigned the appropriate impact level. If interconnecting systems have the same authorizing official, organizations do not need to execute Interconnection Security Agreements.
- Corporate services in areas like customer relationship management (CRM), ticketing, and billing can operate outside the authorization boundary as long as they have no impact on data confidentiality, integrity, and availability.
- With some limitations, development environments may be able to function outside the authorization boundary.

Deep security, extensive reach

The extensive reach FedRAMP has accumulated in the short time it's been in operation points to its central importance as the go-to resource for cloud security.

It establishes a government-wide baseline for agencies and vendors alike, defining the minimum set of security requirements that should be considered.

It already covers more than **five million assets** held by the world's largest cloud providers, touching an astonishing one-third of the world's Internet traffic.[18]

Its four security baselines—high, moderate, low, and low-impact—bring together more than 900 individual controls that allow government agencies to align the security settings for any cloud-based function with its assessed risk level.

It's become the centering point for an extended public-private network that already includes more than 100 government agencies, more than 150 cloud service providers, and more than 40 auditors, with key executive branch entities working together to develop, manage, and operate the program.

And here's the statistic that gets at the return on investment FedRAMP is already delivering, and the powerful, continuing benefits the public treasury can expect to take away from the program: with agencies reusing their FedRAMP authorizations an average of six times, the platform had delivered more than $130 million in cost avoidance as of 2017.

Given the federal modernization mandate, the growing list of business benefits, and the customer service imperative from consumers, many industry experts believe the majority of federal agencies will migrate to the cloud in compliance with FedRAMP standards in the next three to five years.

Deputy federal CIO **Margie Graves** told a recent panel: "Every agency is going to have to march down this pathway in a prioritized manner."[19] At present, over 130 federal agencies are already working with 160+ industry partners in the FedRAMP program.

Looking ahead: From compliance to opportunity

At its most basic, FedRAMP is a government-wide initiative that establishes a core set of processes to ensure effective, repeatable cloud security across participating agencies and systems.

For public sector officials, it facilitates collaboration by providing a platform to share lessons learned, use cases, and practical, hands-on solutions. For vendors, it's the epicenter of a mature marketplace for secure, reliable cloud services.

FedRAMP is a standard security baseline for authorized cloud products in the marketplace, providing the most detailed requirements for design and operations. FedRAMP's rigor and consistency make it a key platform for establishing marketplace capabilities, building trust and reciprocity across stakeholders, driving much faster deployment, and supporting innovation and collaboration across departments and agencies.

By reaching into every participating agency and across all relevant supply chains, FedRAMP plays a mission-critical role, accelerating the public sector's shift from old, insecure, legacy systems to far more cost-effective, cloud-based IT.

1. **H.R. 6550**.
2. Arthur, Joe. Infor. Personal Interview. 2019.
3. **Performance.gov Cross-Agency Priority Goals Overview: Modernize IT to Increase Productivity and Security**. Accessed April 19, 2019.
4. **Office of Management and Budget. Budget, Fiscal Year 2018**. Accessed April 20, 2019.
5. **Bloomberg Government. "Getting Smart About Government Cloud**." February 28, 2019. Accessed April 17, 2019.
6. **FedRAMP Staff. "Congratulations to the 2018 FedRAMP Five Award Winners!"** June 12, 2018. Accessed April 19, 2019.
7. **Hunt, S.**, quoted in FedRAMP.gov Profiles in Cybersecurity. September 28, 2018.
8. **Schneider, T. "Your agency isn't ready for AI," Federal Computer Week**. April 19, 2019. Accessed April 20, 2019.
9. **Performance.gov Cross-Agency Priority Goals Overview: Improving Customer Experience with Federal Services**. Accessed April 19, 2019.
10. **Parrish, R. "The US Federal Government Still Ranks Near The Bottom Of Forrester's Customer Experience Index,"** Accessed April 20, 2109.
11. **"FedRAMP Tailored Lessons Learned,"** Accessed April 17, 2019.
12. **FedRAMP Marketplace**. Accessed April 19, 2019.
13. **El-Attrash, F. "Ready for Takeoff: The Role of FedRAMP in the Path to Digital Transformation," GovLoop**, June 20, 2018. Accessed April 17, 2019.
14. **GSA Technology Modernization Fund**. Accessed April 19, 2019.
15. **FedRAMP Federal Agencies**. Accessed April 19, 2019.
16. **Kirkland, R. "FedRAMP Evangelist Ashley Mahan Outlines Program Changes, Goals," Washington Exec**. April 4, 2019. Accessed April 20, 2019.
17. **Valdes, T. "The True Costs of Self Compliance for SLED Organizations,"** July 10, 2018. Accessed April 20, 2018.
18. **FedRAMP Program Overview.** Accessed April 19, 2019.
19. **"Margie Graves: Making Modernization Happen," Federal Computer Week**. March 28, 2019. Accessed April 20, 2019.

Learn more ›

INF-2243950-en-US-1119-2