

Simplifying FedRAMP Compliance

RESEARCH BRIEF

ANITIAN



Introduction

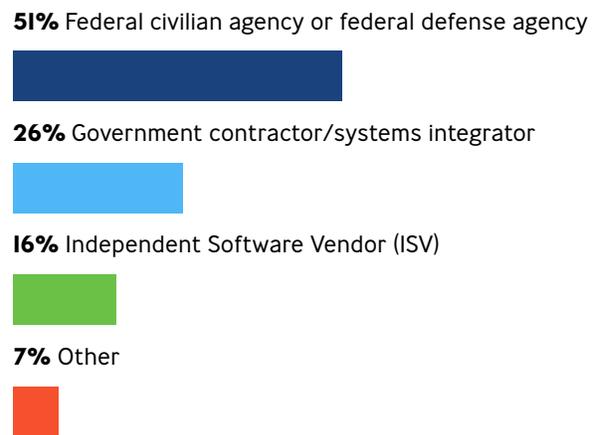
The federal government spends more than **\$80 billion** on IT each year, with a growing portion of that dedicated to cloud enablement and cloud-based applications. As a result, more agencies are looking for products certified by the Federal Risk and Authorization Management Program (FedRAMP).

Established in 2011, FedRAMP provides a standardized approach to cloud security. It has grown significantly, keeping pace with the rise of cloud throughout government. In September 2020, the Government Accountability Office **reported** that agencies can now take advantage of more than 200 FedRAMP-authorized cloud service offerings, and that number is destined to grow as agencies move forward with modernization initiatives that require cloud infrastructure and applications.

With more agencies than ever requiring or at least preferring FedRAMP-certified solutions, the vendors, systems integrators and government contractors that serve them are working hard to achieve that compliance. It's not easy; in fact, it's notoriously difficult to achieve. There are numerous hurdles to jump through, thousands of pages of documentation to contend with and hundreds of controls to comply with. By streamlining and automating as many of these steps as possible — including configuration, deployment and documentation — products and services get through the entire process much faster, while saving money, effort and time.

To learn more about how to accelerate and simplify FedRAMP compliance, GovLoop teamed with Anitian, a leading cloud security and compliance company, and Amazon Web Services (AWS) to survey federal agencies and their contractors to learn how they deal with the challenges of compliance. The results demonstrate how faster, more automated FedRAMP compliance methods can increase agency satisfaction, boost revenue and improve the DevOps pipeline. The survey also found that FedRAMP compliance was a pressing concern: Overall, 43% of respondents say they had to deal with FedRAMP in their day-to-day work or had to learn a lot about it.

Figure 1: I work for...



FedRAMP At-a-Glance

(as of November 22, 2020)

206 products authorized
54 products in process
33 products ready to begin the process

12,000: The estimated number of Software-as-a-Service solutions in the private sector

The players involved at least:
220 cloud service providers
150 agencies
35 auditors



FedRAMP

The Impact of Slow FedRAMP Approval

Federal agencies are under increasing pressure to modernize IT infrastructure and improve efficiencies across the board. To do that, they need to replace legacy infrastructure and applications with modern, secure cloud-based solutions. Software vendors, systems integrators and government contractors want to provide those solutions, but when the process requires FedRAMP compliance, it can be slow going.

Increasingly, applications intended for federal agencies need to achieve FedRAMP compliance. Many agencies strongly prefer FedRAMP-compliant solutions, and some won't even consider those that aren't compliant. Often, they have **no choice**; agencies looking for cloud deployments at the Low, Moderate or High Impact levels require FedRAMP authorization, and that authorization is more often mandatory for organizations that want to sell cloud solutions, including sought-after Software-as-a-Service (SaaS) solutions, to government agencies.

Despite the cost, difficulties and time required to achieve it, FedRAMP compliance is worth the effort for

cloud-based software vendors, especially in the area of security. Because it requires them to implement a set of standardized security controls, many agencies **report** that FedRAMP improves their overall security posture.

Yet despite federal agencies' desire and providers' willingness, the road to FedRAMP certification is often complicated, expensive and long. The preparation process can take 12 months or longer, followed by even more time to get through the third-party assessment process (3PAO) and Authority to Operate (ATO) reviews. The entire process can take 24 months or more.

This results in high opportunity costs on all sides. For federal agencies, it slows projects with ambitious timelines, resulting in missed deadlines. For software vendors, government contractors and systems integrators, it's about lost business opportunities and revenue, according to our survey (see Figure 2). The survey also found that these delays can put a squeeze on the market, leaving agencies concerned about having a limited choice of FedRAMP-certified products (see Figure 3).

Figure 2: What is your most pressing concern about applications that are not FedRAMP certified?

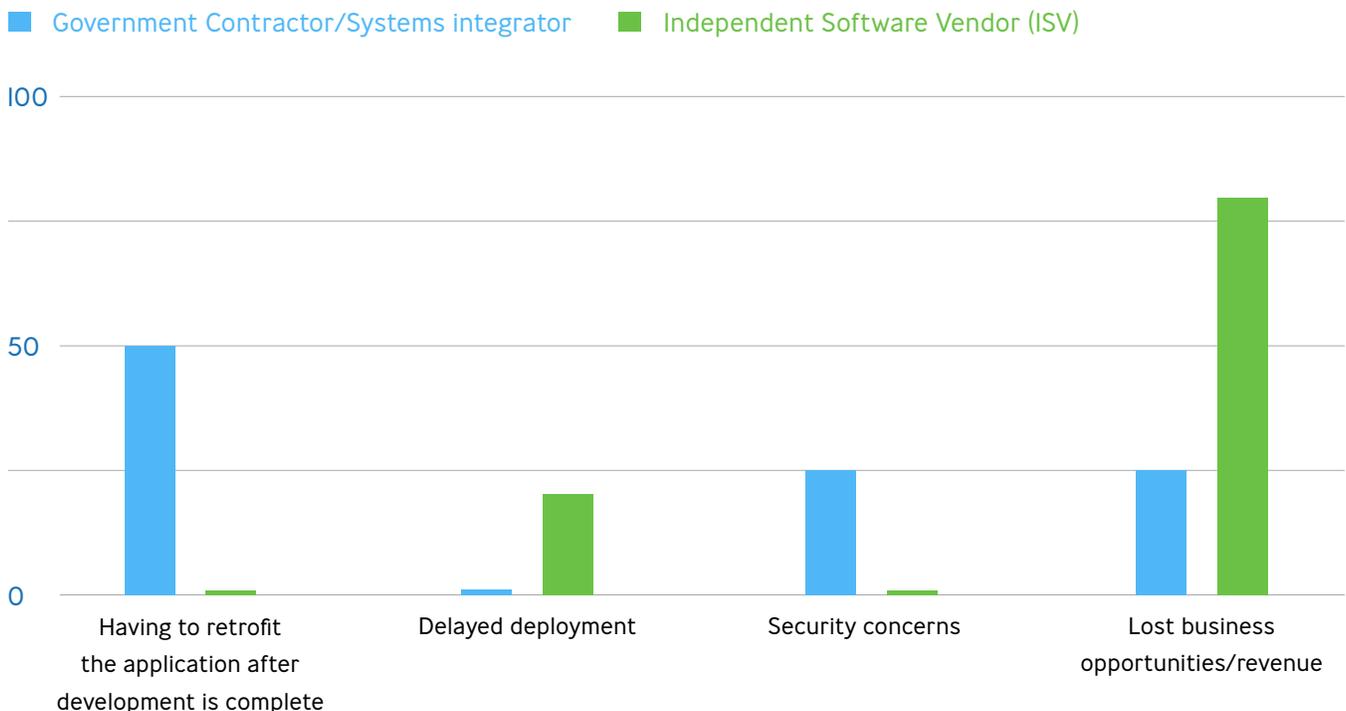
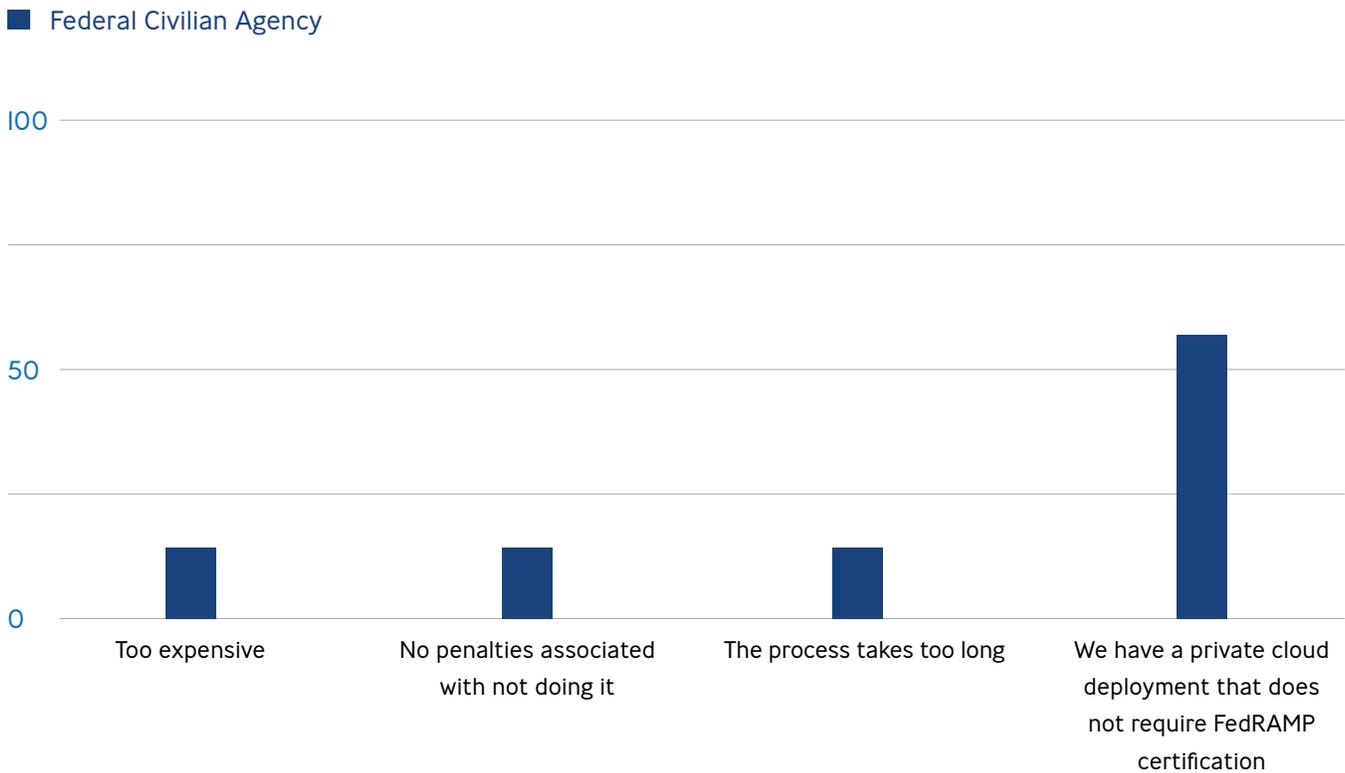


Figure 3: In cases where you are not requiring FedRAMP certification, why not?



Although some of the time-to-compliance issues can't be controlled, there are ways to significantly accelerate critical parts of the FedRAMP compliance process — including building a secure and compliant FedRAMP environment and getting audit-ready. For example, the typical non-automated process for making a cloud-based application secure and standards-compliant involves 12 to 18 months of information-gathering, evaluation, product integration, configuration, customization, testing and documentation.

“Often, a software development team will either go it alone or work in concert with a consulting services company to get things up and running” explained John Vecchi, Chief Marketing Officer at Anitian. “That can be a popular approach, but takes a lot of time and money, because vendors have to learn the FedRAMP process, assemble and configure the tools, satisfy hundreds of controls, complete thousands of pages documentation, and make sure they are complying with complex FedRAMP requirements at every stage. It’s all incredibly complicated and takes a lot of time, money and resources.”

Speeding up the process requires automating as much as possible. By relying on an automated, standardized, pre-built framework where resources are already integrated and controls are standardized and preconfigured, an organization can be ready for the 3PAO audit in as little as 60 days.

For one vendor looking to deliver a product to a federal customer, the automated approach worked well. The company, whose flagship product is a healthcare data sharing solution, needed to deploy a FedRAMP-compliant solution quickly on both AWS GovCloud and the agency's network, while ensuring a stable, secure and compliant environment for the long term. Using a standardized Compliance Automation Platform with pre-built technology, documentation, DevOps and 24x7 Security and Operations (SecOps) stacks, the team stood up an AWS FedRAMP environment with all controls, processes and documentation in 30 days and received a temporary ATO from the agency in just 60 days.

DevOps and FedRAMP: Better Together

Across the board, a growing number of organizations are adopting some form of DevOps. Also called Continuous Integration/Continuous Deployment (CI/CD), DevOps is a way of splitting application development into two parts, done simultaneously: development and operations. The result is much faster development and deployment, along with greater agility and lower costs.

In a world where faster is often better, it's not surprising that DevOps, which largely takes place on cloud-based platforms, is growing so quickly. According to the survey, a significant number of federal agencies, software vendors, systems integrators and government contractors are either actively developing cloud-native applications and services or aggressively moving in that direction.

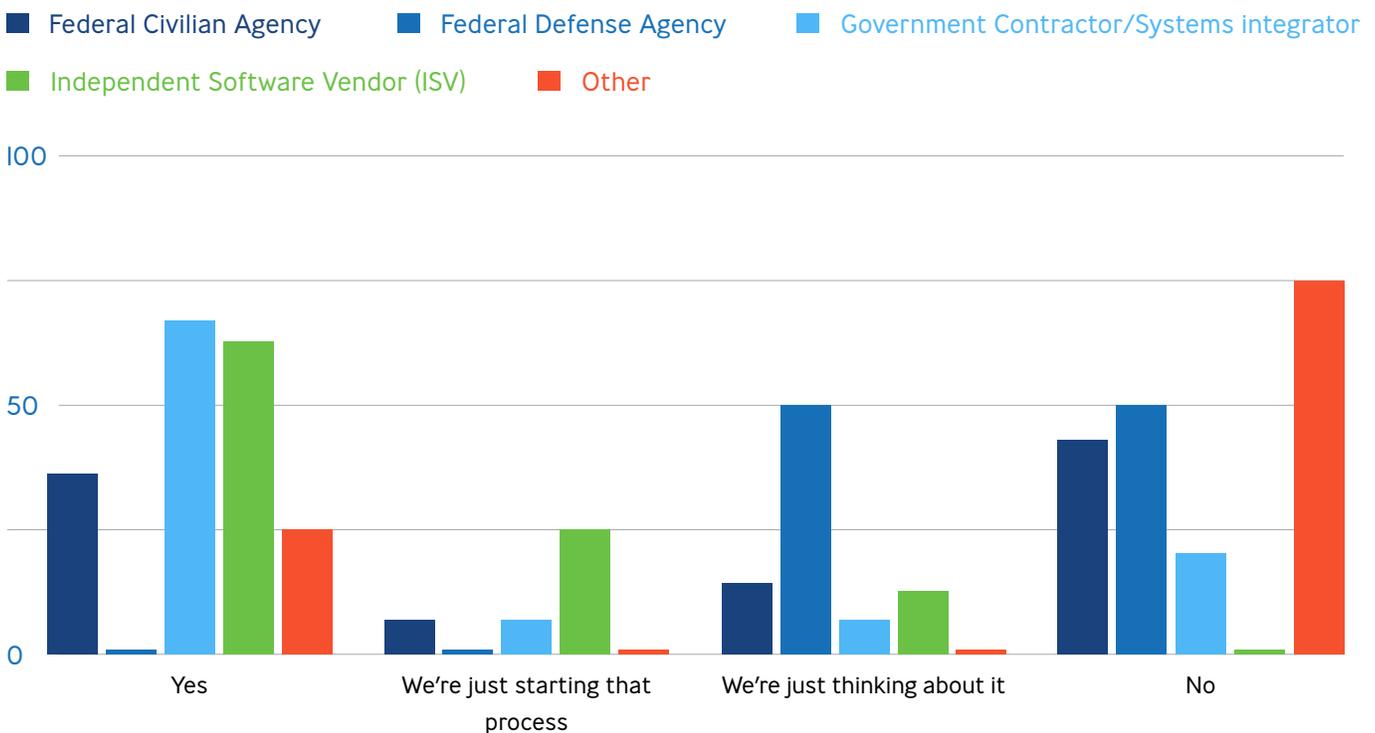
Yet the main benefit of the DevOps approach — fast application development and deployment — can slow to a crawl when FedRAMP is involved. Not only does

meeting FedRAMP compliance require additional steps in the DevOps process, but the completed application must undergo full vetting and testing before it can be deployed.

Integrating the FedRAMP process with DevOps is a more streamlined and effective approach to application development. The idea is to build FedRAMP security controls into the development and CI/CD process itself, instead of first developing an application and putting it through the FedRAMP approval process afterward. When organizations use this approach, they can help accelerate the FedRAMP process.

“For DevOps teams, the goal is fairly simple: get the code to production and delivery as fast as possible. When security is an inhibitor to that — which it is almost every time — it can significantly slow this process down,” Vecchi said. “Baking security into the DevOps process and automating as much as possible removes a real security impediment for DevOps teams.”

Figure 4: Are you actively developing cloud-native applications and services?



Compliance Automation with Anitian

That’s the goal of Anitian’s solution, which provides a standardized, preconfigured and pre-engineered security and compliance environment. This allows developers to deploy code faster, knowing that it will be secure and compliant by design and by default.

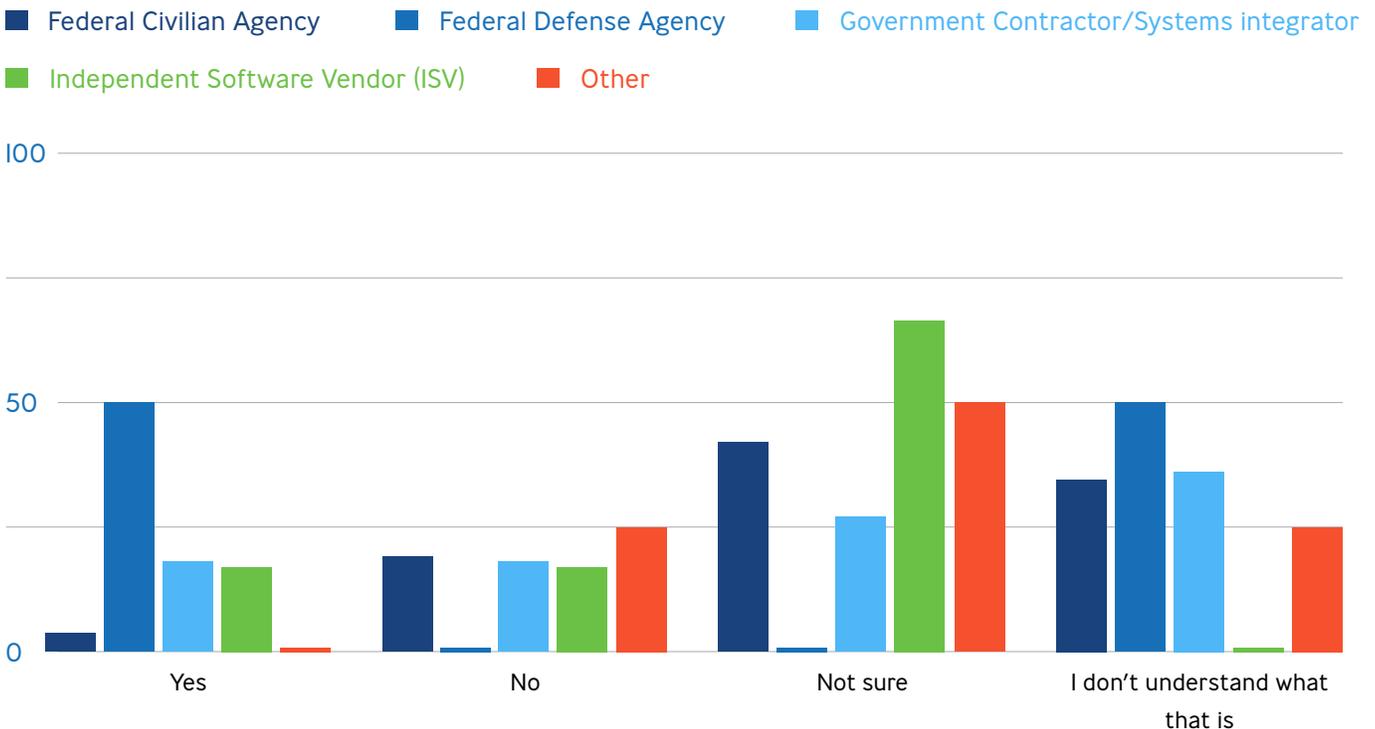
Anitian’s platform devotes an entire DevOps Stack to its FedRAMP compliance process. The stack includes all CI/CD integrations, pre-engineered scripts, reference architectures, code snippets and hardened images. The DevOps Stack builds on top of the Tech Stack and includes a set of more than a dozen preconfigured security controls. Together with the rest of the stack, which includes documentation automation, it enables cloud software providers to get to market 80% faster, and at 50% of the cost compared to do-it-yourself and consulting services approaches.

While baking FedRAMP security requirements into the DevOps process helps speed the compliance process significantly, integrating security deeply into the software delivery lifecycle is a good idea in all cases. Not only does it make teams more than twice as confident in their security posture, but it improves security policies and practices throughout the organization.

“FedRAMP aside, security integration into DevOps practices results is critical in today’s cloud-centric environment,” Vecchi said. “It helps DevOps and security teams work together on their shared goals — building agile, secure, compliant and capable applications for customers.”

It’s worth noting that a significant number of respondents were not certain whether their organizations were doing DevOps as part of their FedRAMP process — and some were not sure what DevOps was. In part, these results likely reflect that many people outside development shops are still learning about DevOps and its role in their organization (see Figure 5).

Figure 5: Are you using DevOps as part of your FedRAMP compliance process?



The Value of Automation

Achieving FedRAMP compliance is critical for any organization that wants to do business with the federal government, and for federal agencies themselves. By insisting on FedRAMP-compliant solutions, agencies can be sure they are getting fully secure products.

The road to FedRAMP compliance is notoriously long and complicated. In our survey, most vendors reported that the process took 13 to 24 months (see Figure 6).

That includes time spent developing processes, hiring staff, performing a gap analysis and other types of preparation, followed by tool implementation, deployment, assembly, integration, configuration and application development. Then there is the documentation phase, typically consisting of hundreds or even thousands of pages and hundreds of controls. All together, it takes a tremendous amount of effort, money and time.

Figure 6: If you have previously achieved FedRAMP compliance, how long did the process take?

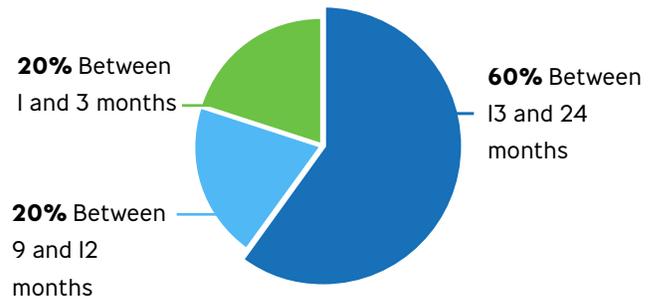
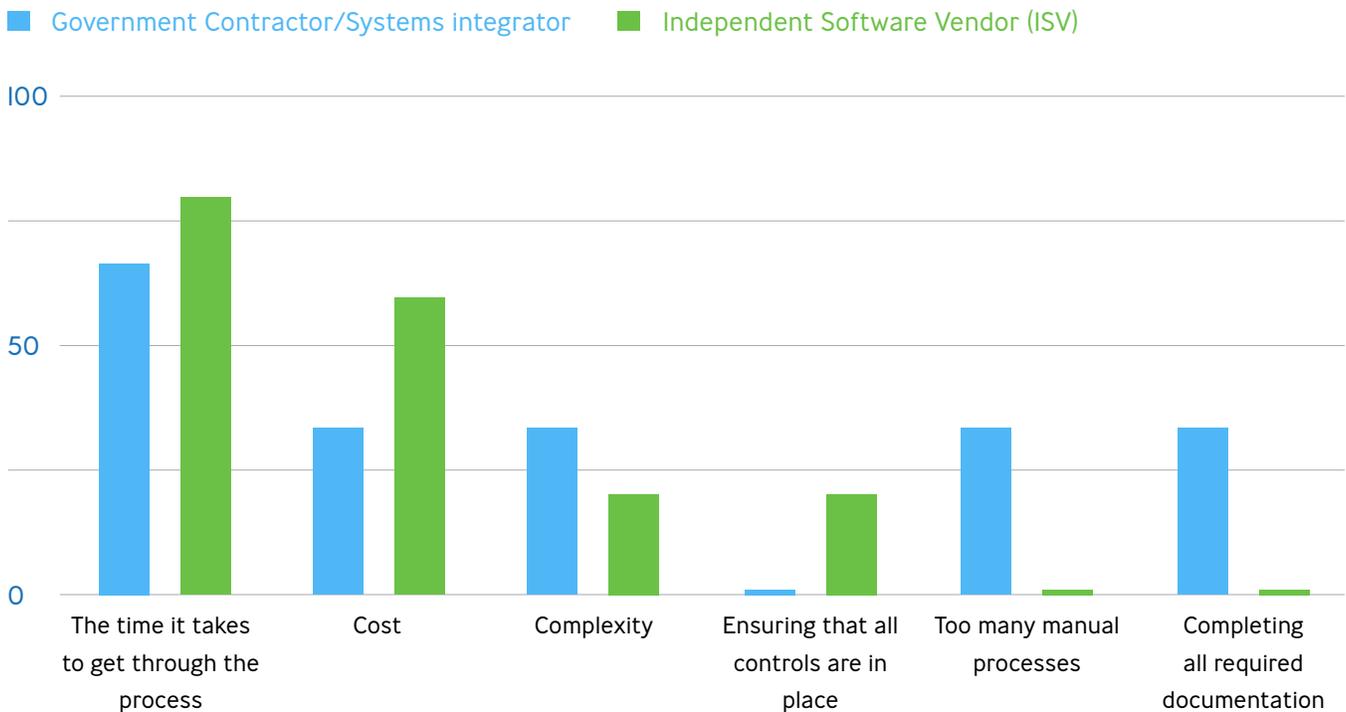


Figure 7: What have been your biggest challenges in getting applications FedRAMP certified? Choose up to three.



Often, the burden of money and effort results from the massive amount of manual labor and processes involved. Just one of those tasks — performing a gap analysis, or choosing and deploying tools, for example — can take months if done manually. That’s especially true in the documentation arena, where manually paging through documents is laborious and time-consuming.

Increasingly, organizations are looking to automate the FedRAMP preparation process as much as possible. By doing so, they can eliminate much of the manual work and human error that often accompanies FedRAMP preparation. According to the survey, the most important benefits of an automated solution are accelerating the compliance process, reducing costs and risks, and ensuring continuous monitoring (see Figure 8).

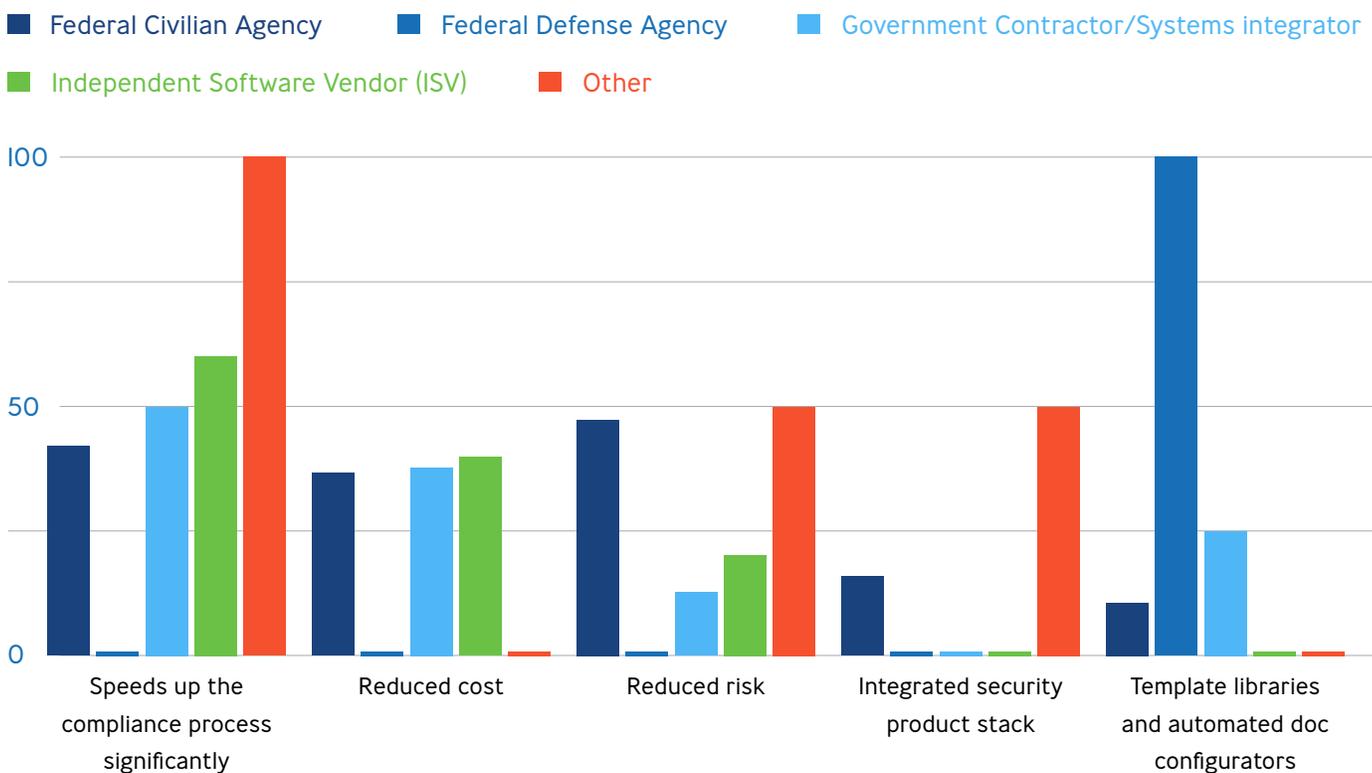
Automation can both ease and accelerate most of the pre-3PAO audit processes. That includes preconfiguration and standardization of all tools and

processes in compliance with FedRAMP standards, from endpoint security and vulnerability scanners to pushing security policies. It also means automating the coding process, configuring all controls to meet compliance requirements and automating as much of the documentation process as possible.

These improvements can make a big difference. Through automation, organizations can deploy a technology stack in as little as one day. As noted earlier, it can dramatically reduce both the time to compliance and the costs of the process.

One software vendor, whose SaaS collaboration and work management platform required satisfying 325 FedRAMP controls, used this automated process to deliver its solution to its customer faster. The result was having their cloud-based software fully ready for their FedRAMP 3PAO audit in 60 days — while achieving its Provisional ATO in less than four months.

Figure 8: If you were to consider an automated solution for FedRAMP compliance, what would be the most important features? Choose up to three.



After compliance

When a product is ready for submission for FedRAMP ATO certification, the 3PAO phase begins, with the formal preparation of the Security Assessment Plan and Security Assessment Report. These documents are then submitted to the agency or Joint Authorization Board (JAB), which reviews the report, creates a Plan of Action & Milestones (POA&M), documents vulnerabilities and eventually grants an ATO.

Once an organization achieves FedRAMP certification, there is still the matter of ongoing compliance checking, continuous monitoring, and monthly POA&M reporting. Automating processes such as ongoing threat hunting and actively testing for compliance validation and weaknesses can relieve agencies and vendors of these tasks. Automation also can ensure that processes can change over time to meet new threats and requirements, and help organizations better define continuous monitoring strategies and programs — two of the priorities that agencies, contractors and software vendors cited in the survey (see Figure 9).

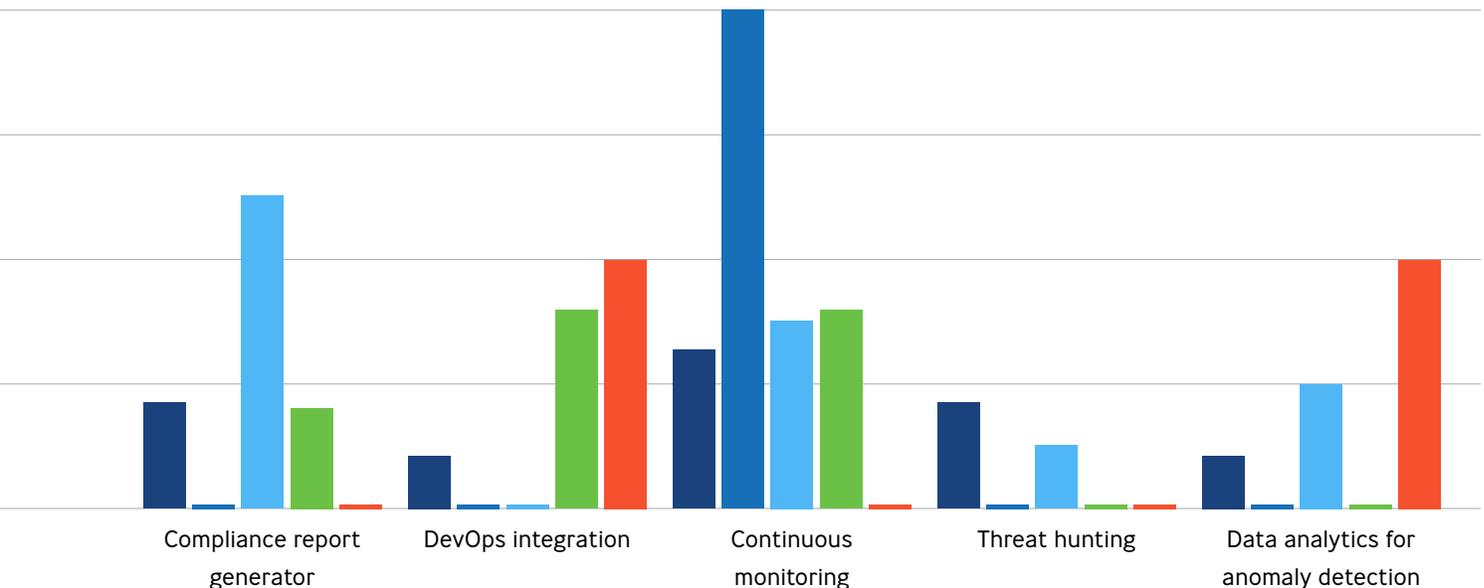
Most importantly, by automating these processes, organizations can be sure that their solutions will remain compliant, so as to confidently submit required reporting attesting to that compliance.

Some organizations choose to go one step further, using a service to ensure continued compliance and security. This method combines automated functions such as threat hunting and change management with 24x7 SecOps professionals dedicated to keeping the solution secure and compliant.

Figure 9: What would you like to improve about your continuous monitoring process? Choose up to three.



Figure 8 continued



Conclusion: How Anitian and AWS Help

The Anitian Compliance Automation Platform offers the fastest path to security and compliance for existing and new cloud applications, enabling high-growth SaaS enterprises to dramatically accelerate time-to-market and time-to-revenue. The Anitian pre-engineered platform wraps more than 15 critical security technologies around a cloud application in minutes, helping cloud-based applications become ready for FedRAMP audits in days instead of months. In addition, the Compliance Automation Platform uses numerous native AWS services. As an AWS Technology Partner, Anitian maintains multiple certifications, including Azure, Certified Cloud Security Professional, Kubernetes, Certified Information Systems Security Professional, Certified Information Security Manager, GPEN, GIAC

Exploit Researcher and Advanced Penetration Tester and Payment Card Industry (PCI). Cloud software vendors can be assured that the Anitian platform is seamlessly compatible with the AWS GovCloud to get cloud applications audit-ready fast.

The company's full-stack solution directly integrates with DevOps CI/CD pipelines and includes configurations, documents, licenses and onboarding to make existing or new cloud applications secure and compliant with FedRAMP, the PCI Data Security Standard, the International Organization for Standardization/General Data Protection Regulation, the Cybersecurity Maturity Model Certification (CMMC) and more – all in up to 80% less time and at 50% of the cost vs. the consulting services approach.

Unifying Security and DevOps with AWS and Anitian

 <h3>Tech Stack</h3> <p>All security controls licensed and pre-configured.</p>	 <h3>DevOps Stack</h3> <p>Rapid application onboarding.</p>	 <h3>Doc Stack</h3> <p>Documentation templates and automation.</p>	 <h3>SecOps Stack</h3> <p>24x7x365 continuous monitoring.</p>
 Trend Micro	 Code snippets	 Automated doc. generation	 24x7 USA SOC
 Red Hat	 DevOps support	 Audit-ready templates	 Threat hunting
 elastic	 CI/CD integration	 Compliance advisory	 Incident handling
 Qualys	 Pre-engineered scripts	 Central artifact repository	 Change management
 GitHub	 Reference architectures	 Audit support	 Penetration testing
 Splunk	 Hardened images	 Project management	 Weekly reports

To learn more, please visit www.anitian.com/aws-and-anitian.



About Anitian

Anitian delivers the fastest path to security and compliance in the cloud. Anitian's Compliance Automation Platform and SecureCloud service help high-growth SaaS companies get applications to market quickly, so they can unlock revenue in weeks, not months or years. Our automated cloud platform and service delivers a full-suite of security controls – pre-engineered and pre-configured to rigorous security standards such as FedRAMP, PCI, CMMC, GDPR, or ISO27001. Anitian's pre-engineered environment and platform use the full power and scale of the cloud to accelerate time-to-market and time-to-revenue so you can start secure, start compliant, and stay ahead.

Find out more at www.anitian.com.



About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop

About AWS

With over 2,000 government agencies using AWS, we understand the requirements US government agencies have to balance economy and agility with security, compliance and reliability. In every instance, we have been among the first to solve government compliance challenges facing cloud computing and have consistently helped our customers navigate procurement and policy issues related to adoption of cloud computing. Cloud computing offers a pay-as-you-go model, delivering access to up-to-date technology resources that are managed by experts. Simply access AWS services over the internet, with no upfront costs (no capital investment), and pay only for the computing resources that you use, as your needs scale.

To learn more about AWS, please visit www.aws.amazon.com



1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421 | F (202) 407-7501
www.govloop.com
[@GovLoop](https://twitter.com/GovLoop)

