COALFIRE

Securing Your Cloud Solutions

Research and Analysis on Meeting FedRAMP/Government Standards

securities

Introduction by: THE CHERTOFF GROUP

V.1.1

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Federal Risk and Authorization Management Program (FedRAMP) drives the convergence of cloud computing, cybersecurity, and government technology needs. The government's Cloud First policy requires federal agencies to use FedRAMP-authorized solutions whenever possible to reduce costs and streamline IT procurement.

FedRAMP establishes cybersecurity requirements for cloud service providers (CSPs) delivering to the federal market, and utilizes independent experts to advise organizations and assess their compliance. Coalfire is the largest provider of FedRAMP services to the CSP market, and our extensive history, deep industry relationships, and technical expertise all factored into this research.

CSP PARTICIPATION IS GROWING BUT FACES CHALLENGES

- Despite beliefs that FedRAMP is too expensive and only for large companies, more than 40% of authorized CSPs have less than $100 million in revenue.
- While a broad range of authorized solutions exists, competitive depth is shallow, providing entry opportunities.
- 51% of participating CSPs only serve one or two agencies.

GOING THROUGH FEDRAMP IS RIGOROUS BUT THE TIME REQUIRED IS DECREASING

- Many tech firms have focused on solutions at the expense of cybersecurity, and have been unprepared in areas like vulnerability scanning, where 70% of CSPs need to improve.
- Since 2014, the average time needed to obtain authorization has decreased 65% for CSPs working with the Joint Authorization Board (JAB) and 59% for those working directly with an agency.
- 65% of a CSP's resource allocation for FedRAMP comes from IT, but a broad cross-section of the organization is typically involved in the process.

CLOUD AND FEDRAMP ADOPTION HAS PROGRESSED WELL BUT MORE NEEDS TO BE DONE

- Twenty federal agencies have leveraged FedRAMP five or more times, and cabinet-level departments use an average of 16 solutions.
- Agencies do not regularly report their level of FedRAMP participation, making overall adoption analysis challenging.
- Our best estimate indicates that approximately 60% of federal agencies, primarily small and medium-sized, do not yet participate.
- Cybersecurity and cloud innovations have moved faster than the government's ability to keep pace, leading to shadow and/or outdated legacy infrastructure.

As the cloud services market continues to grow and government CIOs face shrinking budgets, tighter security requirements, and the need to modernize technology, FedRAMP will see increased participation. For CSPs interested in entering the market or expanding their presence, the information in this report provides guidance on common pitfalls, successful strategies, and typical resourcing and budgeting approaches.

INTRODUCTION FROM THE CHERTOFF GROUP

ADAM ISLES | PRINCIPAL

In an era where federal agency chief information officers are expected to do more with less, leveraging the economies of scale delivered by cloud computing services is imperative. Moreover, the federal government continues to struggle with managing cyber risk, due in part to the challenges of supporting legacy information technology (IT) infrastructure. Cloud migration offers an avenue to replace legacy IT and enables a key recommendation in the 2016 report from the Commission on Enhancing National Cybersecurity, where the "President and Congress should promote technology adoption and accelerate the pace at which technology is refreshed within the federal sector." The report continues:

> "General Services Administration (GSA) should expand the development and use of standard service platforms (e.g., endpoint devices, shared data clouds, software as a service) to provide agencies with high-performance infrastructure and tools for their mission, while minimizing direct agency responsibility for managing and operating the infrastructure. Greater sharing of services, such as web hosting, standard software, and common cloud services, would enable government to take advantage of its scale to negotiate and obtain higher-performance and lower-cost IT equipment and services. By sharing, agencies can focus on aspects of the IT infrastructure that most directly address their mission. They retain the authority and responsibility for optimizing IT services to meet their mission needs, and benefit from the embedded security features that are part of their network and shared procurement."[1]

Indeed, cloud adoption has been a federal priority for several years. In 2010, after a decade in which federal IT spend almost doubled, the U.S. Chief Information Officer launched a 25-point comprehensive effort to increase the operational efficiency of federal technology assets. One element of this plan was for agencies to follow the Office of Management and Budget's (OMB) Cloud First policy, which required federal agencies to implement cloud-based solutions whenever a secure, reliable, and cost-effective option exists; and reevaluate their existing IT budget strategies to include cloud computing.

Cloud migration has generated many success stories, including NASA's ability to reduce system development time from weeks to hours and NOAA's consolidation of email systems from 14 to 1.[2] In addition, GSA published high baseline requirements in June 2016 intended to increase cloud adoption for high-impact applications and systems.[3]

And yet, data on actual cloud uptake is mixed.[4] Why is there drag on cloud adoption? Many reasons have been cited, ranging from limited reciprocity (one agency's reliance on another's authorization to operate [ATO]) to a more basic challenge in doing effective tradeoff analyses on cost, efficiency, accessibility, agility, reliability, privacy, and – in particular – security.

A 2014 Government Accountability Office report identified that CSPs lack the understanding of security requirements unique to government agencies, such as continuous monitoring and maintaining an inventory of systems, as a key challenge for cloud adoption.[5] At the same time, private sector reports also indicate growth in unsanctioned cloud-related shadow enterprise IT utilized by federal agency employees.[6]

For its part, GSA is working to streamline FedRAMP certification, announcing the FedRAMP Accelerated process in March 2016.[7] The FedRAMP Accelerated process begins with a readiness assessment of a CSP's operational system before the bulk of the required documentation is submitted. CSPs assessed as ready are then prioritized for ATO.

This improved efficiency and understanding will be key preconditions to unleashing the benefits of cloud for the federal sector. In this spirit, the Coalfire findings described in this report are acutely important because they highlight how CSPs going through the FedRAMP process tend to trip up. These lessons learned will allow CSPs to plan smarter, leading to quicker certification and a lower burden on personnel. In turn, more FedRAMP-certified CSPs will offer greater diversity of cloud offerings to meet individual agency needs and reduce shadow enterprise IT.

---

[1] "Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, December 2016", available at https://www.nist.gov/cybercommission

[2] "GSA Cloud Computing Acquisition Vehicles and Services", available at https://www.gsa.gov/portal/mediaId/139610/fileName/2016_Cloud_Success_Brochure.action

[3] https://www.gsa.gov/portal/content/137586

[4] Contrast Federal News Radio, "Agencies on a roller coaster ride with cloud spending," Oct. 17, 2016, available at http://federalnewsradio.com/reporters-notebook-jason-miller/2016/10/agencies-roller-coaster-ride-cloud-spending/, with IDC Research, "Federal Government to Spend 8.5% of all IT Spending on Cloud in FY 2016, According to IDC Government Insights," Feb. 10, 2016, available at https://www.idc.com/getdoc.jsp?containerId=prUS41019516

[5] Government Accountability Office report, "Cloud Computing: Additional Opportunities and Savings Need to be Pursued," Sept. 2014, p.10, available at http://www.gao.gov/assets/670/666133.pdf

[6] Skyhigh Networks Blog Post, "New Data on Federal Cloud Usage in the Age of FedRAMP," available at https://www.skyhighnetworks.com/cloud-security-blog/new-data-on-federal-shadow-it-in-the-age-of-FedRAMP/

[7] https://www.FedRAMP.gov/participate/FedRAMP-accelerated-process/

RESEARCH BACKGROUND AND APPROACH

The cloud services market shows no sign of slowing. Gartner predicts end-user spending in public cloud services will reach $436.4 billion by 2021.[8] Companies and consumers increasingly rely on the convenience, speed, and availability of information that the cloud provides, while businesses continue to realize operational efficiencies and financial savings from migration.

The public sector is no exception. In the U.S., our federal government fully recognizes the benefits of scale, innovation, and cost reduction that cloud adoption delivers. Federal policy directs departments and agencies to utilize cloud-based computing solutions whenever possible. FedRAMP helps smooth these transitions by establishing cybersecurity requirements for CSPs serving the federal market.

FedRAMP, one of the only cloud-focused accreditations in existence, establishes a high bar for cybersecurity. Beyond the federal market, FedRAMP provides both service differentiation and a stronger security baseline for:

- CSPs not currently targeting government entities
- Organizations in other industries looking to improve their cloud security profile
- International firms operating without local regulatory guidance

Coalfire is the largest provider of advisory, assessment, and engineering services to the CSP market, as well as the leading FedRAMP 3PAO. Our extensive history, deep industry relationships, and technical expertise have all contributed to the insights outlined in this publication.

For our research, we reviewed more than 500 applicable FedRAMP advisory and assessment projects performed by Coalfire over the last five years – emphasizing 2016 results to identify common findings. Additionally, we surveyed information security executives with FedRAMP experience to better understand how firms prepare for – and progress through – the various FedRAMP phases.

This report provides information about why FedRAMP matters, adoption, common pitfalls, strategies that have worked for other organizations, and practices for resource and budget allocation. We encourage organizations that are maintaining, pursuing, or considering FedRAMP authorization to leverage the information in this report for their benefit.

[8] Gartner. "Forecast: Public Cloud Services, Worldwide, 2015-2021, 1Q17 Update" Published April 4, 2017 (Current U.S. Dollars)

Cloud opportunities

$436.4B
by 2021

The public cloud services market is estimated to grow to $436.4 billion by 2021.

15.9%
per year

Cloud usage is projected to exhibit a 15.9% compound annual growth rate to 2021.

FedRAMP PROGRAM OVERVIEW AND ADOPTION

WHAT FedRAMP DOES

The Cloud First policy requires federal agencies to use cloud-based solutions whenever a secure, reliable, and cost-effective option exists. Therefore, OMB originated FedRAMP to standardize the security requirements, assessment, and authorization approach, and establish the ongoing monitoring of cloud solutions serving departments and agencies. OMB monitors and enforces agency adoption of FedRAMP-authorized cloud solutions. Participating CSPs must obtain an independent security assessment conducted by an accredited 3PAO.

Depending on the categorization of a FedRAMP candidate environment, the 3PAO assessment utilizes one of three different sets of controls (low, moderate, and high-risk systems), with additional agency-specific requirements assessed as needed. These security controls are defined in revision 4 of the National Institute of Standards and Technology (NIST) Special Publication (SP) *Security and Privacy Controls for Federal Information Systems and Organizations* 800-53.

WHY FedRAMP MATTERS

Cloud computing has a substantial and growing impact on the federal government that we don't anticipate slowing down anytime soon. OMB's efforts to accelerate legacy infrastructure and application modernization should drive further increases in cloud usage, with Gartner projecting a 15.9% compound annual growth rate (CAGR) 2016 to 2021.[9]

The rapid growth of the Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) markets led by Amazon Web Services (AWS), Microsoft, IBM, Google, Salesforce, and others illustrates the ready availability of cloud development and deployment environments. These leaders have all actively participated in the FedRAMP process. Additionally, Software-as-a-Service (SaaS) solutions continue to gain traction in federal agencies by providing services supporting mission-critical areas, which has created a commensurate uptick in cybersecurity assessments.

As FedRAMP continues to mature, we foresee:

- Growth in authorized Cloud-as-a-Service offerings for the Department of Defense (DoD)
- Further migrations of agency applications and shared services to cloud solutions
- Convergence with federal Internet of Things (IoT) and mobility initiatives

FedRAMP has made cloud adoption more efficient, standardized security assessments, and eliminated redundant systems and assessments, saving the federal government time, staffing, and financial resources. 2016 saw more than 80% growth in the number of authorized cloud services,[10] the addition of new requirements for the high baseline, and a reduction in the overall time to obtain security authorizations. In 2017, the program will continue to evolve, incorporating updates for low-impact SaaS offerings, efficiencies in the continuous monitoring process, and ongoing expansion.

[9] Ibid.

[10] FedRAMP. "2016: A look back." FedRAMP.gov/2016-a-look-back

2016 saw more than 80% growth in the number of authorized cloud services.

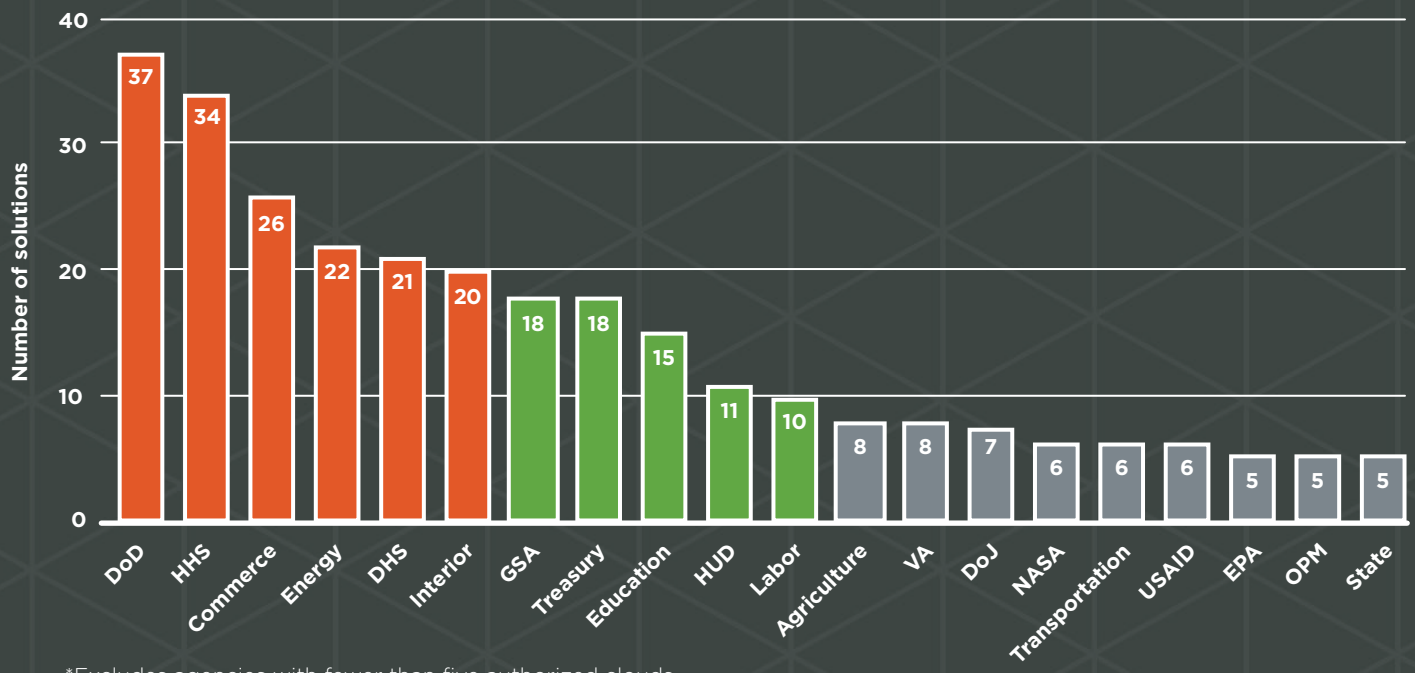
FedRAMP ADOPTION

One of FedRAMP's principles is "do once, use many," and the program allows government agencies to successfully leverage and reciprocate ATOs, eliminating duplicative efforts, inconsistencies, and cost inefficiencies in assessing and authorizing cloud solutions. Each of the 15 federal cabinet-level departments and many independent agencies and government-owned corporations use a wide array of cloud services for mission-critical functions.[11]

CSPs across the full spectrum of the technology stack (IaaS, PaaS, and SaaS) participate in FedRAMP. Infrastructure providers were early adopters in creating secure environments for value-added services. Several agencies deliver their own services, shared with other parts of the federal government. FedRAMP tracks products; some CSPs have obtained additional ATOs for services that are uniquely tailored to particular product environments, but those service ATOs are not included separately in these statistics.

In our review of CSP participation in FedRAMP, two factors stood out: number of authorized cloud products and number of agencies using those products. Most CSPs provide a single product and work with one or two agencies, but several have been able to grow their relationships with more agencies as they build depth in their government expertise. A small number of CSPs offer expanded portfolios of authorized products, delivering a wider variety of solutions throughout the federal government.[12]

FedRAMP authorized clouds in use by agency*



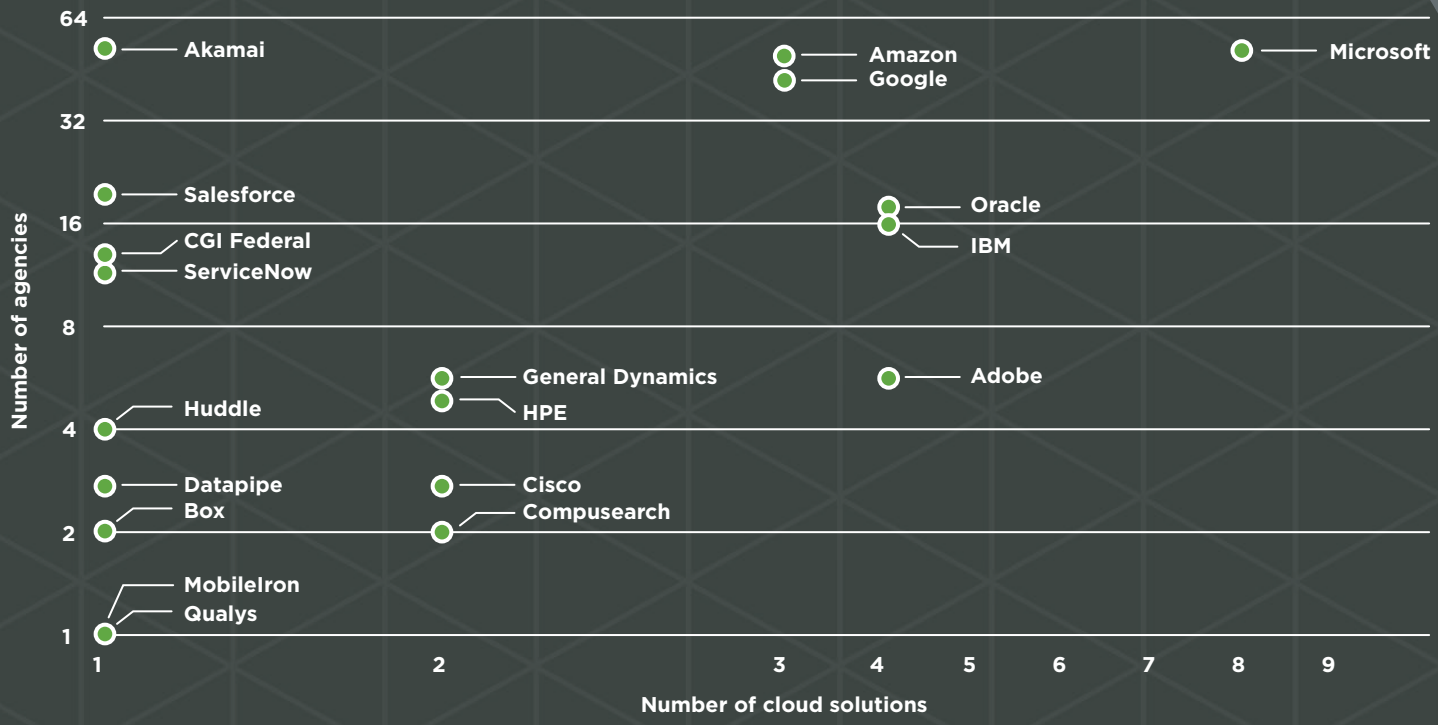
*Excludes agencies with fewer than five authorized clouds.

[11] https://marketplace.FedRAMP.gov, accessed April 2017

[12] Ibid.

The FedRAMP Program Management Office (PMO) is responsible for driving adoption for the cabinet-level departments and nine key independent agencies, including GSA and the Environmental Protection Agency. All organizations under the PMO's purview have issued ATOs, but adoption in small and medium-sized agencies has lagged. Since agencies do not regularly report their level of participation centrally, it is difficult to identify conclusive findings. Our best estimate indicates approximately 60% of federal agencies do not yet participate in FedRAMP.[13] This provides an opportunity for OMB to strengthen its oversight of FedRAMP requirements and for CSPs to continue to pursue new markets for their cloud solutions.

Authorized clouds and agency use*



*Due to space constraints, a sample of CSPs represent those with one solution and lower agency adoption.

[13] Estimated with agency listing data from catalog.data.gov/dataset/federal-agency-list, compared to authorizations from marketplace.FedRAMP.gov, data accessed April 2017

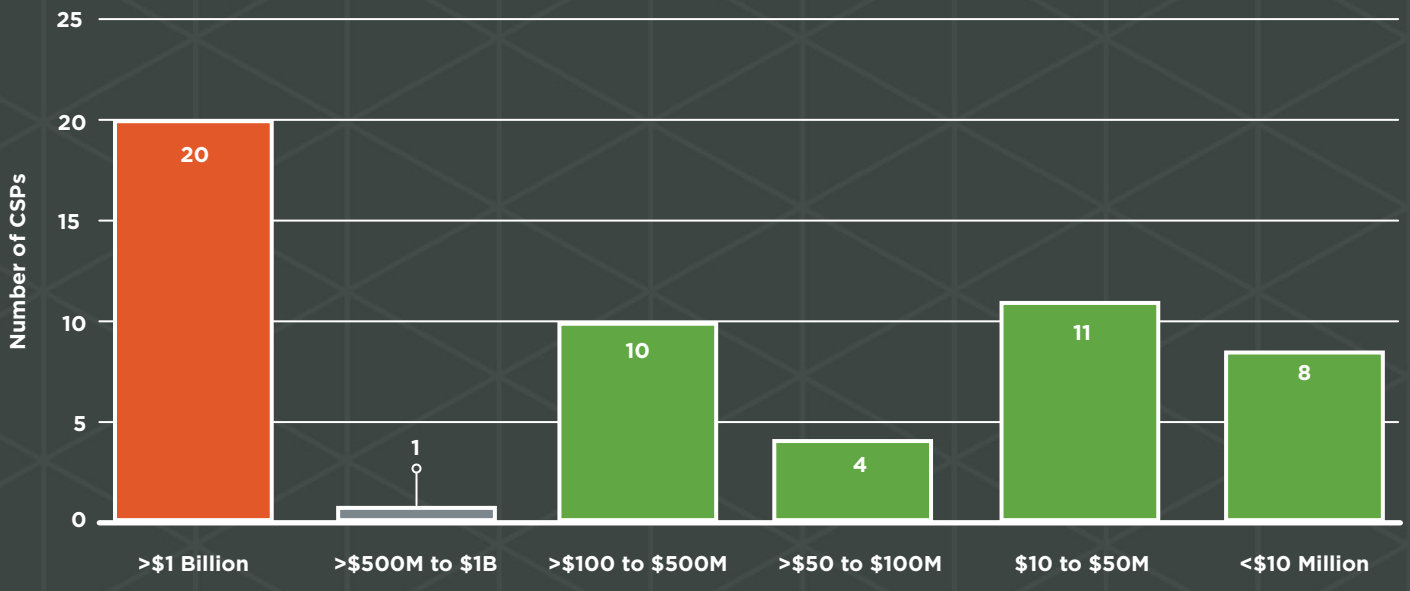
FedRAMP is fortunate to have a variety of participating CSPs, including the largest cloud companies and many smaller specialist firms. More than 40% had revenues less than $100 million in 2016, and 14% were less than $10 million. Regardless of size, if an organization delivers a valuable cloud technology solution, then FedRAMP authorization can be successfully achieved. The new FedRAMP Tailored security controls baseline is ideal for low-risk cloud offerings, enabling even greater CSP participation and greater adoption in smaller agencies.

COMMON PITFALLS AND HOW TO AVOID THEM

Moving through FedRAMP requires more than just a focus on technology. Many CSPs bringing commercial solutions to the FedRAMP process have needed to make modifications to meet the requirements. It's important to rigorously test your system ahead of a 3PAO engagement, but the overall assessment is more broadly based. The ideal FedRAMP preparation also addresses governance, allowing an organization to ensure areas, including risk management, reporting, testing, training, and accountability, receive proper attention.

The graphic on the following page highlights the NIST SP 800-53 controls we've found to cause the most difficulty, the percentage of CSPs that needed to make changes to be compliant, and common approaches to mitigate those issues.

Cloud service providers by 2016 revenue*



*Various public sources, accessed April 2017

Using FedRAMP to access the cloud services market?

Here are the most common pitfalls and ways to avoid them.[14]

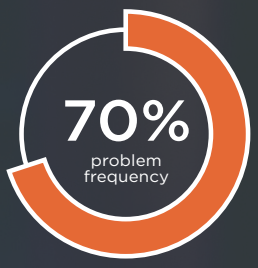
VULNERABILITY SCANNING (RA-5)

Common pitfalls

- Scans not always complete or frequent enough
- Findings not addressed within approved timeframes

How to avoid them

- Regular updates and patching of scanning tools
- Improved reporting and responsiveness



CONFIGURATION SETTINGS (CM-6); LEAST FUNCTIONALITY (CM-7)

Common pitfalls

- System hardening based on easily changed parameters
- Inconsistency in levels of access allowed

How to avoid them

- Standard baselines for configuration settings based on federal benchmarks
- Restrict access to essential capabilities only, and provide limited exceptions

CONTENT OF AUDIT RECORDS (AU-3)

Common pitfalls

- System transactions not tracked to allow auditable evidence
- Records not easily retrievable

How to avoid them

- Granularity including time stamps, addresses, identifiers captured for audit records
- Common storage with appropriate security

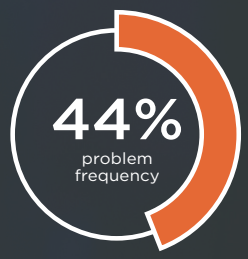
ACCOUNT MANAGEMENT (AC-2) AND LOGON ATTEMPTS (AC-7)

Common pitfalls

- Separation of duties not in place
- Inconsistent authentication protocols

How to avoid them

- Baseline of current access levels and controls
- Apply least privilege doctrine to better segregate access roles



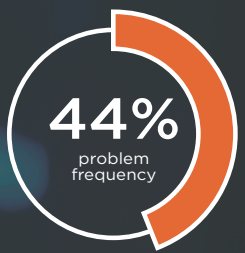
INFORMATION SYSTEM COMPONENT INVENTORY (CM-8)

Common pitfalls

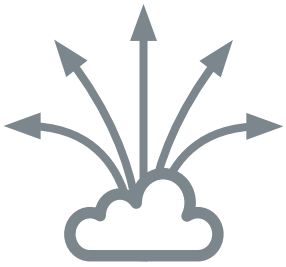
- Inaccurate, incomplete, or outdated system inventory

How to avoid them

- Automated detection of inventory and configuration changes



[14] Based on analysis of historical Coalfire FedRAMP projects



SUCCESSFUL COMPLIANCE STRATEGIES

Several FedRAMP requirements have proven to cover areas where CSPs regularly improve as their compliance programs grow in maturity. By successfully leveraging these strong practices, you can be confident that your processes align with expectations for the following NIST SP 800-53 controls.

(PL-2)

SYSTEM SECURITY PLAN (PL-2)

The assembly of a system security plan (SSP) is a core component of FedRAMP. A SSP provides an overview of the cloud solution's security requirements, and should describe its controls and the responsibilities of all individuals with access. As you develop and manage your SSP, consider the following:

- **Clearly define and document your system boundary.** It is safe to assume that all data used or created by your federal customers will always be in scope for FedRAMP, leading to stringent requirements on handling data. Make sure all third-party dependencies, data flows, and shared services that cross the boundary are understood and documented.
- **Your documentation efforts will be substantial.** Compliance experience is useful in understanding the level of precision required, but FedRAMP requires a more rigorous, granular approach than frameworks like PCI DSS or ISO 27001. Plan for a significant time commitment to thoroughly document how you meet security compliance requirements for your federal customers. The FedRAMP SSP template is more than 300 pages, and can exceed 800 pages once completed.
- **Incorporate federal customer requirements.** Federal organizations interpret FedRAMP requirements in various ways – some are strict, while others may accept additional risk by allowing CSPs to use mitigating controls. By conducting a proactive, thorough review of your customer's requirements, expectations, and requests, you can incorporate and address them early in the solution's design, planning, and documentation.

(CM-5)

ACCESS RESTRICTIONS FOR CHANGE (CM-5)

Physical and logical access restrictions must be defined, documented, and enforced for all changes made to the cloud solution. Typically, this is achieved through a combination of procedures and technology. Strong change management procedures provide protection to services in the live production environment and directly reduce the risk of unauthorized changes. There are a wide variety of robust change management technology tools available to CSPs, helping you provide further evidence of your process's maturity.

(SA-3)

SYSTEM DEVELOPMENT LIFE CYCLE (SA-3)

A strong development strategy incorporates information security at every step of a solution's lifecycle. Tools used for planning, creating, testing, and deploying an information system are mature and protect against unauthorized changes, including any development, programming, configuration, or operational changes and modifications. Lifecycle activities will need to be defined within a process, with documented evidence of implementation.

(SI-4)

INFORMATION SYSTEM MONITORING (SI-4)

Security information and event management (SIEM) software products and services provide real-time analysis of security alerts generated by network hardware and applications. Tools offering packet inspection, firewall, antivirus, integrity monitoring, and logging inspection greatly assist with system operations assurance.

(AT-2)

SECURITY AWARENESS (AT-2)

Basic security awareness training is required for all users. Content should include specific actions to maintain security and respond to suspected security incidents, while increasing awareness. Best practices provide role-based security training detailing which functions each type of user can perform. Individuals such as system administrators, engineers, and information systems security officers have greater security responsibilities than general employees.

(IR-6)

INCIDENT REPORTING (IR-6)

Organizations are required to have procedures and processes to identify, manage, and report information-security incidents. Using the NIST *Computer Security Incident Handling Guide* (SP 800-61) as the base policy for incident response helps you meet the criteria for reporting and acting on security incidents on an ongoing basis.

FedRAMP TIME, MONEY, AND PEOPLE

MOVING THROUGH FedRAMP

Over the last three years, the average time for a FedRAMP authorization has significantly improved. Several factors have contributed:

- Higher quality SSPs
- Increased agency support and commitment to cloud adoption
- Improved CSP preparation and internal processes
- Standardization of 3PAO reporting formats and interpretations
- FedRAMP Accelerated, which streamlined the JAB authorization path and introduced FedRAMP Ready

As indicated on the next page, the average number of months required to obtain an ATO has dropped for both paths each of the last three years.[15]

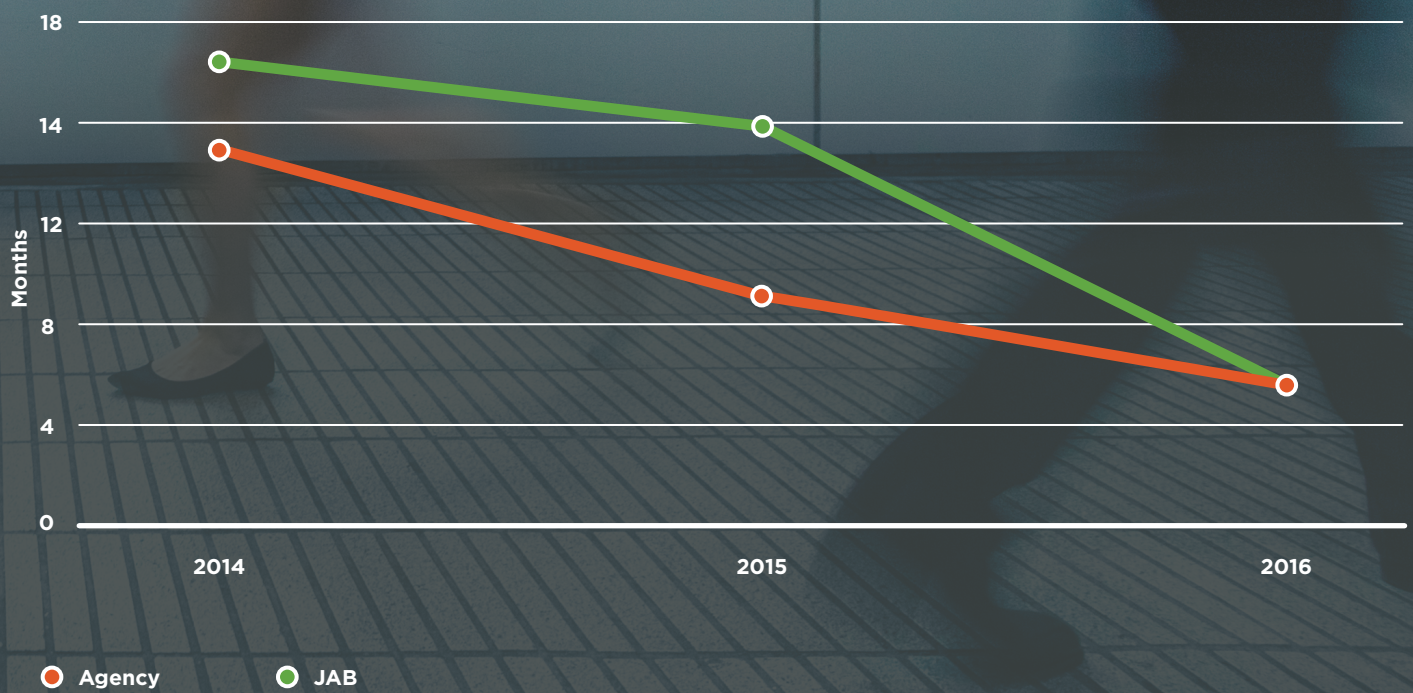
The two biggest factors in determining the time required for your organization to complete the FedRAMP process are advance preparation and your preferred authorization route.

The amount of preparation necessary is driven by your security maturity and experience with the federal government's security requirements. Typically, CSPs will engage external resources to conduct a gap analysis or technical review to identify areas that must be addressed prior to the formal assessment process. These projects serve as demonstrations to internal decision-makers as to the effort required to successfully complete the FedRAMP process.

Common activities arising from this advisory work include creating documentation that aligns with the cloud solution's security controls or defines the system boundary, and remediating non-compliant controls through engineering architecture, design, and implementation. We find the amount of time required to complete these activities will vary substantially based on the CSP's security maturity. The graphic on page 18 provides an indicative timeline for comprehensive FedRAMP projects.

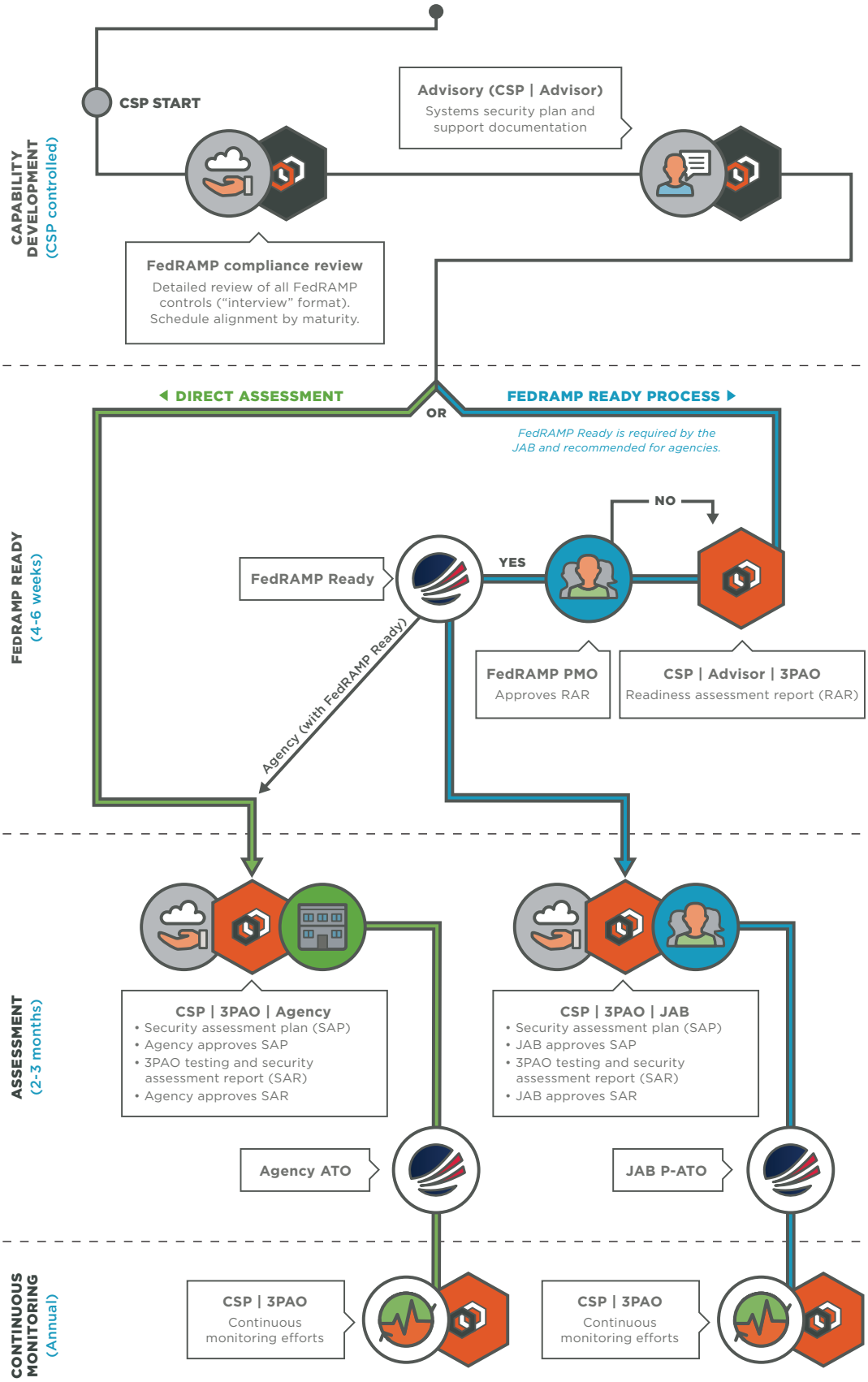
[15] https://marketplace.FedRAMP.gov, accessed April 2017

Average time to FedRAMP authorization*



*Time measured from in-process date to authorization following FedRAMP Accelerated process. Often months have been spent before the official start of authorization, and time required is typically significantly greater for hyperscale service providers.

Moving through FedRAMP



*Coalfire can act as an assessor or an advisor, but a 3PAO is not allowed to play both roles for a client.

ATO is granted by either the FedRAMP JAB or directly from a specific agency. JAB comprises the chief information officers of the Department of Homeland Security (DHS), DoD, and GSA, supported by technical security experts from within their departments. CSPs choose the JAB route to enable the solution's adoption across multiple federal agencies and for the prestige and differentiation associated with passing an increased level of scrutiny.

JAB reviews typically take longer than agency reviews due to the level of coordination required across DHS, DoD, and GSA, and the rigorous risk profiles and in-depth analysis utilized. JAB also requires a two-week readiness assessment prior to the formal FedRAMP assessment, as well as a business case from the CSP highlighting the service's demand and demonstrable ROI for the government.

Business factors including existing relationships and market strategy often drive the decision to pursue an agency authorization. If an organization is already working with a specific agency, is in a similar market, or has time pressures, the agency route offers an alternative. Although not required in this route, some agencies prefer CSPs go through a readiness assessment to illustrate security posture.

FINANCIAL INVESTMENT

Public information regarding the cost of FedRAMP completion is hit and miss due to wide variability in how spending is classified and the supporting investments required. In addition, there is a widespread lack of transparency in the reporting of these details.

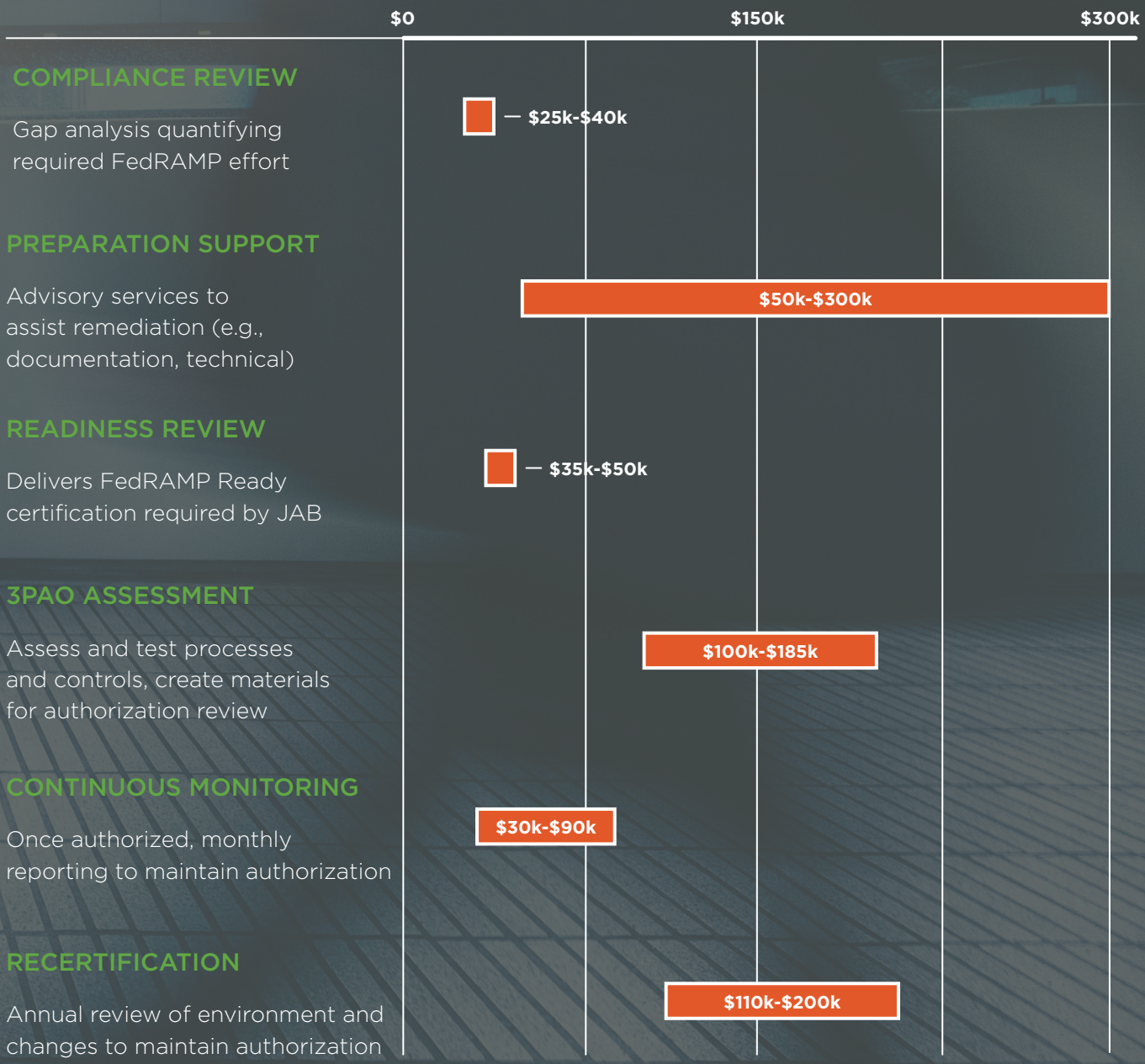
Our experience shows that FedRAMP spending is often focused on architecture, cyber defense, or security monitoring and analytics. Common drivers of cost in those areas include:

- **Application design** – When creating a new solution, you can incorporate security by design principles. Formalizing features including account design, automation of security controls, auditing, and encryption into the requirements can be less expensive and time consuming than retrofitting.
- **Infrastructure** – SaaS providers have several infrastructure options available. As they define their offerings, factors like inheritable services can affect decisions regarding development and investment in native controls.
- **Operational segregation** – Some solutions will require the implementation of a dedicated government cloud. If your organization already offers both federal and commercial services, many of the required policies and procedures will be in place. For those new to the federal market, governance to define, document, and develop this separation will be required.
- **Engineering** – Appropriate network architecture and deployment of cybersecurity solutions and sensors are critical to properly detecting and defending against compromise. CSPs need to engineer their networks and continuous monitoring activities and tools to isolate critical business functions. Compartmentalization should reduce the impact of a security event.

Professional services dedicated to helping CSPs become FedRAMP-authorized are also available. Some are optional, such as helping organizations determine the business case for pursuing FedRAMP. Others, like 3PAO assessments, are a requirement for all. The graphic on the next page provides examples of the services you may find valuable, along with potential costs.

Financial investment*

Your possible costs range from $350k to $865k for typical SaaS solutions, excluding engineering costs



*Based on Coalfire competitive research. Cost estimates do not apply to hyperscale solutions.

RESOURCE ALLOCATIONS

Most successful FedRAMP assessments employ a diverse and engaged support team leveraging many areas within the organization. The critical interaction among various organizational roles, more than the number of individuals dedicated to the preparation and assessment activities, drives effective development and maintenance of security objectives.

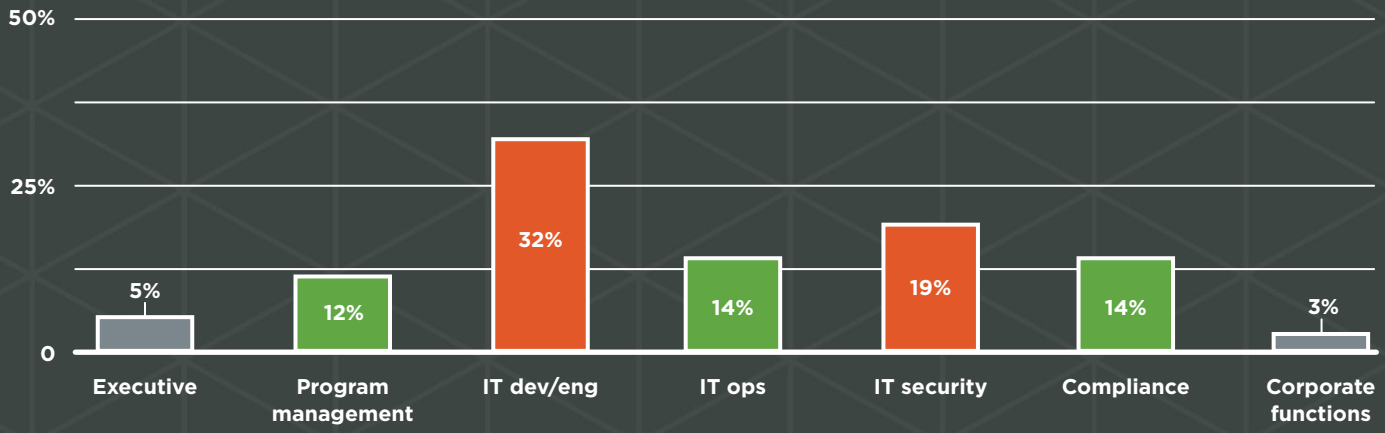
You'll find certain key positions like executive management, human resources, and legal will play important roles for short periods of time, while those responsible for IT security, compliance, and IT operations will be involved for extended durations.

Major roles, functions, and responsibilities beyond compliance include:

- **Executive management** – FedRAMP's scope requires management to allocate resources properly for both the project itself and ensuing remediation activity. Executive leadership keeps the organization balanced between meeting the FedRAMP requirements and delivering against corporate objectives.
- **IT engineering** – Controls to protect the confidentiality of information, integrity of data, and appropriate user access must be embedded in your cloud solution. These controls are best constructed when security requirements are incorporated in the solution's design, which is driven by the engineering team.
- **IT operations** – Depending on the size of your organization, responsibilities for system scanning may be allocated to separate security operations or compliance groups. Make sure to incorporate these teams in FedRAMP planning to ensure that deployment, verification, installation, instantiation, execution, continuous monitoring, and maintenance meet federal requirements.
- **Corporate functions** – FedRAMP includes input from parts of the organization usually uninvolved with compliance. Functions including training, personnel security, and procurement (both for suppliers and subcontractors) need to devote some time to FedRAMP.

Resource allocations*

A broad cross-section of the organization is typically involved.



*Source: 2017 survey of CSPs with FedRAMP experience

CONCLUSIONS

Secure cloud computing is essential for the federal government to move from its costly legacy infrastructure computing operations and applications. However, it presents an interesting challenge. For cloud computing to be widely accepted, it must be secured comprehensively and effectively – no small task in the ever-changing cyber threat ecosystem we live in today. At the same time, cloud security assessments must be done in a timely and cost-effective manner for the government to take full advantage of fast-moving technology cycles and innovative software advancements, especially in smaller agencies that can benefit greatly.

As our report illustrates, CSPs have challenges with FedRAMP compliance in both basic and complex requirements areas – such as proper baseline configuration settings and expected vulnerability scanning capabilities, to name a few. Concurrently, additional controls and requirements have been added to the FedRAMP baseline sets of controls over the last few years as the level of understanding around cloud computing vulnerabilities has evolved. These activities will task CSP compliance teams to regularly review their environment and support processes. For CSPs that are designing new systems, planning for security in the beginning will save time and effort down the road.

Still, as our research and market involvement demonstrate, CSP experience and maturity with cloud security continues to progress. New CSPs entering the federal market for the first time should note the lessons we've learned and presented here. Used wisely, they can be a conduit for quicker, more complete, and more successful security assessments.

THE AUTHORS

Tom Bolger
Director, Portfolio Management

Michael Carter
Vice President, FedRAMP and Assessment Services

Marshall England
Industry Marketing Director, Technology and Cloud

Tom McAndrew
Executive Vice President, Commercial Services

Dave McClure
Chief Strategist, Federal

Nick Son
Vice President, Cyber Risk Advisory

Abel Sussman
Director, Cyber Risk Advisory

Andrew Williams
Product Director, Public Sector

ABOUT COALFIRE

As cybersecurity risk management and compliance experts, Coalfire delivers cybersecurity advice, assessments, testing, and implementation support to IT and security departments, executives, and corporate directors of leading enterprises and public sector organizations. By addressing each organization's specific challenges, we're able to develop a long-term strategy that improves our clients' overall cyber risk profiles. Armed with our trusted insights, clients can get to market faster with the security to succeed. Coalfire has offices throughout the United States and Europe. Coalfire.com

RR_Q1_05242017

Reduce risk and simplify compliance with trusted insight from the cybersecurity experts.

877.224.8077 | **Coalfire.com**