SANS | Research Program

White Paper

Securely Moving to the (Government) Cloud

Written by **Matt Bromiley**

March 2024

cisco

Introduction

It's safe to say that the cloud has changed the infrastructure landscape for every organization. Federal agencies are no exception, with many addressing the transition to cloud and hybrid work models. However, moving infrastructure to the cloud is not a simple "flip of the switch." It requires careful planning, implementation, and navigating a complex regulatory environment.

Moving to the cloud does more than open operational benefits. The burden of maintaining hardware and software diverts resources from protecting networks and potentially exposes sensitive data and system vulnerabilities. In today's dynamic technology landscape, staying tethered to outdated infrastructure leaves agencies vulnerable, inflexible, and unable to serve the public effectively.

In this SANS white paper, we will examine the security requirements for cloud-based resources and how to best position your agency for that transition. It's no secret that FedRAMP compliance is the staple of government cloud operations. However, there are many regulatory requirements, executive orders, and advisories. Let's navigate through them at a high level, identifying some of the critical rules, regulations, and issues to be aware of.

Many of you are likely going through this "cloud transition" yourself. As you work your way through this paper, look for areas where we highlight difficulties or challenges you might be facing and some ways to approach them. If these changes are something you were planning, or even if you are in the process of implementing them, we highly recommend treating this white paper as a guide of best practices or recommendations.

Securely Moving to the (Government) Cloud

The federal government has made no secret about its prioritization of cloud-first technologies. The 2017 *Report to the President on Federal IT*[1] established a "Cloud Smart" strategy that "equips agencies with actionable information and recommendations" for cloud technology adoption. However, as federal agencies move their infrastructure to the cloud, they must adhere to a complex web of regulations and requirements.

Increased Cloud Pressure

Moving to the cloud should come as no surprise. However, many agencies still find themselves caught asking, "What do I do next?". This is in the face of increased pressure from a hybrid workforce and an administration that is pushing for cloud adoption. The longtail effects of the COVID-19 pandemic only accelerated the need for a cloud-first approach.

[1] "From Cloud First to Cloud Smart," https://cloud.cio.gov/strategy

When speaking about cloud migrations, some of the most notable regulations, requirements, and/or guidance to be aware of include:

- **Federal Risk and Authorization Management Program (FedRAMP)[2]—**This is the standardized approach for assessing and authorizing cloud service providers used by the government. FedRAMP offers three "levels" with increasing security controls and assists with pre-vetted solutions.
- **Cybersecurity Maturity Model Certification (CMMC)[3]—**CMMC is primarily aimed at contractors working with the DoD. However, it enforces stronger cybersecurity standards and reduced risk.
- **Cybersecurity and Infrastructure Agency (CISA) Cloud Security Guidance[4]—**CISA offers best practices and guidance for secure cloud adoptions, which are often utilized as supporting evidence in regulatory development.
- **Executive Order 14028[5]—**This policy amplifies the need for a "zero trust" approach to cybersecurity for federal agencies, emphasizing authentication and authorization controls for cloud resources.

Although the list above is not exhaustive, it does highlight the federal government's focus to move agencies toward the cloud. It also identifies the various complexities agencies must face when moving to the cloud. Common questions may include:

- Does one type of compliance supersede another?
- Is the responsibility on my vendors and contractors or on me?
- What happens if I am already in a transition and the rules/regulations change?

To help government agencies navigate these complex matters, our first recommendation is to use FedRAMP-certified vendors to help streamline the cloud-adoption process.

Why FedRAMP?

If there are so many different rules and regulations, why all the fuss about FedRAMP? For federal agencies navigating the dynamic and complex world of cloud computing, choosing the right solution(s) is key. FedRAMP-compliant vendors and solutions help you in more ways than one, including:

- FedRAMP is more than a label, it's a *rigorous vetting process*. Prerequisites include security assessments, ensuring controls, policies, and procedures meet government standards. This removes guesswork and provides agencies with the confidence necessary to focus on deployment.

[2] https://www.fedramp.gov

[3] https://dodcio.defense.gov/CMMC/about

[4] "CISA Releases Cloud Services Guidance and Resources," June 2023, www.cisa.gov/news-events/news/cisa-releases-cloud-services-guidance-and-resources

[5] "Executive Order on Improving the Nation's Cybersecurity," May 2021, www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

- FedRAMP provides *streamlined compliance*, as it already aligns with key government mandates and information security best practices, like FISMA[6] and HIPAA.[7] Another excellent resource, which we will examine in detail later in this paper, is NIST's 800-53 publication.[8]
- FedRAMP compliance *reduces risk* of data breaches and cyberattacks with a robust security framework that incorporates continuous monitoring requirements.

Luckily, compliance with FedRAMP creates a list of pre-vetted solutions agencies can use to bypass lengthy individual security assessments. Instead, they can *move quickly*, accelerating their adoption of the cloud.

Moving to the (Government) Cloud

As agencies plan to move to cloud services and infrastructure, it is essential to have a phased transition plan in place. We have outlined potential steps to ensure a secure, efficient, and user-centric migration from your current legacy tech stack to a cloud-first stance.

Lay the Foundation

1. **Define the necessary technologies or use case(s)—**Define your agency's cloud objectives. Is it improving collaboration, gaining a better security posture, or complying? Align the goals of the agency with specific cloud capabilities and leadership priorities.
2. **Take a current inventory—**Take stock of your security infrastructure, applications, and data. For many agencies, this may be a vast undertaking. However, it will streamline your cloud adoption. Evaluate their candidacy for cloud migration and potential roadblocks.
3. **Source a partner—**Develop a comprehensive strategy that maps out your cloud adoption. This or the previous step is also the best time to start sourcing cloud service providers (CSPs) or FedRAMP-compliant organizations to assist with adoption. This also may be an excellent time to discuss migration requirements with your current vendors and assess their FedRAMP status.

Pilot and Learn

1. **Start small—**As mentioned earlier, moving to the cloud is not a "one and done" or "flip of the switch" transition. Ensuring that agencies don't suffer downtime or impact critical services takes time. Consider migrating security capabilities in a stepped fashion, sorted by speed of deployment. For example, in order:

   a. DNS security or other rapid deployment protections

   b. Cloud-hosted web/application security, firewalls, etc.

   c. Security for hybrid/remote workers, such as zero trust implementation

   d. Security to remote sites, such as SD-WAN to secure access to cloud applications

[6] "Federal Information Security Modification Act (FISMA)," https://security.cms.gov/learn/federal-information-security-management-act-fisma

[7] "U.S. Department of Health and Human Services," www.hhs.gov/hipaa/index.html

[8] "Security and Privacy Controls for Information Systems and Organizations," December 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

2. **Identify what works—**Don't try to do everything at once. Learn from the first migrations to help make the latter more successful. Utilize an iterative approach, learning and incorporating feedback to optimize the cloud deployment.
3. **Empower the workforce—**Transitioning to the cloud is not just a technology movement; it's also an enormous undertaking for staff. Invest in training opportunities for cloud security, application deployment, and collaboration tools, empowering your workforce to use your modernized technology stack effectively.

Expand Your Tech Stack

1. **Keep moving in the right direction—**Leverage takeaways from initial deployments to adjust your cloud-adoption strategy as needed. Keep the priority on mission-critical functions and systems while exploring the best strategy for future adoption.
2. **Optimize hybrid cloud capabilities—**As you explore and uncover your needs, rely on the capabilities of a hybrid cloud environment. Leverage the flexibility of the cloud to meet users' needs while still maintaining on-premises infrastructure, if needed, for specific services.
3. **Continuously monitor and improve—**Implement robust monitoring tools to track security and compliance requirements. Keep an eye on your security posture, ensuring that your team gains the efficiencies and performance benefits expected from a cloud-first stance.

Remember, adopting cloud services is not just about technology. It's also a cultural shift. Focus on open communication and opportunities to involve users and employees, encouraging feedback and user engagement. Use compliance and regulatory guidelines, such as CISA's guidance, to help select and determine the next best steps.

Paving the Way with NIST's 800-53

One of the most critical roadmaps, with best practices and controls, is NIST's 800-53 publication, Security and Privacy Controls for Information Systems and Organizations. This publication provides a comprehensive framework of security controls applicable to various information systems, notably cloud environments. NIST's 800-53 offers a structured approach for identifying, selecting, implementing, and assessing security controls. Furthermore, one of its critical pillars is understanding that each agency must assess its specific needs and risk profiles. As such, government agencies can confidently navigate their cloud journey by aligning with NIST 800-53.

The core of NIST 800-53 lies in the security control catalog, which outlines a broad range of controls across various security domains. These include, but are not limited to, physical security, access control, network security, and incident response. Leveraging these controls can help organizations align with critical objectives:

- **Identify and address security risks** to identify potential vulnerabilities and threats associated with cloud adoption.
- **Select appropriate controls** to mitigate the assessed risks effectively.
- **Implement and assess controls** to achieve effectiveness and the desired security posture.
- **Demonstrate secure cloud practices** and achieve compliance as required for agencies handling sensitive data or subject to specific regulations (some of which we covered above).

NIST's 800-53 is not just a checklist—it's a strategic guide that can assist you in planning your cloud migration. Furthermore, it highlights building a secure and resilient cloud environment that easily aligns with vendors qualified within FedRAMP and StateRAMP requirements, which we'll cover next. By understanding core principles and aligning with your agency's needs and concerns, you can harness the power of the cloud while ensuring that security best practices and data protection are paramount.

It's Not Just Federal

Although much of this white paper focused on FedRAMP migration best practices, another area to highlight for government agencies and organizations is the State Risk and Authorization Management Program, or StateRAMP. The state-level equivalent of FedRAMP, StateRAMP develops standardized cloud security frameworks specifically tailored to the needs of individual states.

This further aims to streamline cloud adoption via:

- **Establishing consistent security requirements** via a standard set of security controls and assessment procedures (eliminating the need for multiple, state-specific certifications).
- **Simplifying compliance for cloud providers** with a single assessment and qualification.
- **Enhancing security for state agencies** with rigorous security practices that protect sensitive data and establish trust with citizens.

Like FedRAMP, StateRAMP reduces compliance complexity and makes it easier for state agencies to choose an approved, qualified vendor for their cloud transition. This is a win-win because a wider pool of qualified cloud providers and streamlined compliance allow faster cloud adoption.

Closing Thoughts

Moving to the cloud is not a dream or a "maybe one day." It's a legal requirement that federal agencies cannot afford to delay. Failing to move quickly can result in outdated infrastructure, missed opportunities to secure technology and user data, and overall inefficiencies in agency security. Furthermore, delaying can result in withholding funds or other punitive measures until the required minimums are met.

However, cloud migrations are complex. They require a mindful approach, prioritizing security and ensuring compliance at every step. In this white paper, we provided high-level guidance, pulling on the experience developed by vendors who have achieved FedRAMP status and are best to advise agencies on the next step(s).

Understanding your compliance and regulatory requirements and leaning on frameworks like FedRAMP or guidance from NIST's 800-53 publication can help streamline the migration process. Additionally, migrating in phases and fostering a culture where employees and users provide feedback helps minimize roadblocks. Cisco offers helpful information about the benefits of the FedRAMP framework.[9]

Sponsor

SANS would like to thank this paper's sponsor:

CISCO™

[6] "What is FedRAMP?," www.cisco.com/c/en/us/solutions/industries/government/federal-government-solutions/fedramp.html#~q-a