Mutual Monitoring in the Cloud

A.J. Stein
Georgia Institute of Technology
astein38@gatech.edu

Abstract. Cloud computing infrastructure is essentially ubiquitous, but adoption is not without challenges. Cloud service providers must cater to customers in regulated sectors. Their use of popular cybersecurity frameworks create high barriers to entry. One barrier, often resulting in centralized bureaucracies, is the periodic monitoring of the provider's cybersecurity posture. By analyzing one prominent example, FedRAMP's Continuous Monitoring Program, this paper considers if such bureaucracies are the only valid solution. To refute this hypothesis, the paper presents an alternative architecture for multi-party monitoring of cloud services' cybersecurity posture, mutual monitoring.

1 Introduction

Cloud computing infrastructure is essentially ubiquitous, but adoption is not without challenges. Cloud service providers must cater to customers in regulated sectors, complying with cybersecurity frameworks that create high barriers to entry. One barrier is ongoing monitoring of the provider's cybersecurity posture, often resulting in centralized bureaucracies. FedRAMP oversees and documents a prominent example of such a program, the Continuous Monitoring Program (2025, p. 14).

Are these bureaucracies an optimal solution, or a last resort that fails to keep pace with cloud technology as it proliferates and evolves? If they are a last resort, is there a better way? This paper presents an alternative, the mutual monitoring architecture, as a measurably more effective solution.

1.1 Why Does This Problem Matter?

The cybersecurity of cloud services poses many challenges, but the inefficiency of continuous monitoring has systemic impact on the economics and timely, accurate

risk modeling for heavily interconnected, interdependent systems built on cloud services. FedRAMP is a highly visible and representative example that other regulatory frameworks emulate, so any improvement or optimization will yield significant improvement to cloud service adoption across regulated industries.

1.2 Economic Impacts

Although FedRAMP is a highly visible cloud security program, there is limited public data with details about costs and economic impact for providers, auditors, and customer agencies. However, industry estimates significant costs for all these stakeholders, even when considering global expenditure on cloud services.

Gartner estimates that global spending on cloud infrastructure in 2024 was $595.7 billion dollars (2024). The think tank CSIS estimates that the United States government spent $17 billion of its total $130 billion dollar IT budget in 2024 on cloud services alone (2025, p. 1). Although federal agencies are not fully compliant with FedRAMP's requirements mandated in the FedRAMP Authorization Act, the long-term goal is maximal oversight over the cloud building blocks of this seventeen billion dollar investment. And continuous monitoring is a sizable component of this investment.

FedRAMP processes require specialized tools and staff for all stakeholders. Analysts at stackArmor estimate that a FedRAMP authorization costs a provider $250,000 to $750,000 dollars, and continuous monitoring support constitutes from $100,000 to $400,000 of that amount (2024). Given this conservative estimate, any improvement or optimization can benefit all stakeholders in reducing $42,600,000 spent, but potentially a much larger sum.

1.3 Cybersecurity Impacts

Even with all this investment, the staff from cloud service providers, auditors, and agency customers experience strategic and operational bottlenecks for heavily interconnected cloud services, increasing ambiguity in a holistic view of cybersecurity posture in real-world composite systems for all parties involved, not only auditors.

Firstly, a centralized review process finalized by a small number of FedRAMP staff constitutes a single point of failure. As FedRAMP documents, cloud providers, au-

ditors, and agency customers must use a single, centralized wiki site, USDA's connect.gov, [1] and coordinate out of band with FedRAMP staff for final review (2025, pp. 3,14). Paradoxically, providers and auditors get no guarantees for the cybersecurity posture of this system where they store data for FedRAMP's reviewers.[2] There is no mutual monitoring or assurance. Access to this data on connect.gov is manually coordinated on an ad hoc basis, hindering sharing between different agency staff who need FedRAMP data, and even those outside these agencies focused on other regulatory frameworks. They rely on reciprocity guarantees to justify the use of FedRAMP authorization and continuous monitoring, which is not particularly feasible in practical terms given restricted access to this data.

The impacts of manually curated data from FedRAMP's continuous monitoring extend beyond its stakeholders. Interrelated regulatory frameworks depend upon it. Given FedRAMP's rigorous review process, especially continuous monitoring, many providers and their auditors use artifacts from FedRAMP for equivalency, or reciprocity, as evidence for controls in other regulatory frameworks preferred by the defense (Department of Defense, 2023), commercial (ORock, 2021), and finance sectors of the United States. Therefore, any optimization in FedRAMP's processes has second order effects on the quality, quantity, and speed of cloud security review methodologies across industry.

The impacts of manually curated data from FedRAMP's continuous monitoring extend beyond its stakeholders. Interrelated regulatory frameworks depend upon it. Given FedRAMP's rigorous review process, especially continuous monitoring, many providers and their auditors use artifacts from FedRAMP for equivalency, or reciprocity,as evidence for controls in other regulatory frameworks preferred by the defense, commercial, and finance sectors of the United States. Therefore, any optimization in FedRAMP's processes has second order effects on the quality, quantity, and speed of cloud security review methodologies across industry.

[1] This system is essentially the same as max.gov, which the Office of Management and Budget (OMB) handed off to the Department of Agriculture subsequently, which FedRAMP had used in the years prior. USDA rebranded the system in 2023 during the transition.

[2] FedRAMP's official package access request form indicates only employees with email addresses for a government or military domain may request access. Providers or auditors that are not government or military contractors may not request a FedRAMP package.

1.4 Solution

The focus of this paper is an alternative solution to centralized continuous monitoring as exemplified by FedRAMP, mutual monitoring. Mutual monitoring facilitates federated data services with ledgers[3] of digitally signed data using an architecture popular for other security use cases, transparency services. The positives and negatives of FedRAMP's continuous monitoring model will inform its design. Operating such services can change the incentives, behavior, and thereby economics, of cloud service providers, auditors, and customers for true "shared responsibility" for cloud security monitoring.[4] A new architecture should incentivize auditors to sell value-add analytics via these federated data services, obsoleting centralized authorities for continuous monitoring, like FedRAMP, and a market of inconsistent third-party auditors required to support them. To valid this hypothesis, I present a viable alternative in the form of my architecture for mutual monitoring.

To best explain the merits (and challenges) of mutual monitoring, the paper will provide an overview of past, present, and ongoing modernization of FedRAMP's continuous monitoring and how it relates to the "whole" of "getting FedRAMP authorized." This context will inform the following section, that outlines the key elements of the proposed mutual monitoring architecture. And finally, the paper will conclude with a qualitative and quantitative evaluation of the solution, highlight key limitations, and identity future work to advance this solution.

[3] Many associate the term "ledger" primarily with cryptocurrency and their popular underlying blockchain implementations, such as Bitcoin and Ethereum. In computing, a ledger is "tamper-resistant shared distributed ledger composed of temporally ordered and publicly verifiable transactions" (Bashir, 2022). Transparency service implementers and standards authors employ the same fundamental concept, but use the interchangeable term Append-only Log, which they define as "a Statement Sequence comprising the entire registration history of the Transparency Service. To make the Append-only property verifiable and transparent" (Birkholz, Delignat-Lavaud, Fournet, Deshpande, & Lasker, 2025). All are examples of distributed ledger technology.

[4] FedRAMP, like many cloud security programs, asserts that "[t]here is a shared security responsibility model when using cloud products. Cloud service providers (CSPs) and customers (agencies or leveraging CSPs) both assume important security roles and responsibilities to ensure data is protected within cloud environments" (2025). As practical as it sounds, there are many concerns and criticisms on how to meaningfully realize the shared responsibility model, which has direct implications on the current continuous monitoring process and the mutual monitoring model proposed in this paper.

2 Background

2.1 Overview of Cloud Service Security Monitoring

Despite the prominence of FedRAMP in cloud security inside and outside of government,[5] there is a body of work from different academic and industry experts with a variety of approaches to cloud security monitoring. As FedRAMP evolved, these different approaches evolved alongside of it. The following section discuss relevant highlights to current challenges to FedRAMP's continuous monitoring approach and the proposed mutual monitoring solution.

2.1.1 Academic Research in Cloud Security Monitoring

Over the last decade, academic researchers have affirmed the fundamentals of cloud deployment and security properties. Much literature uses the same taxonomy as Majumdar and his co-authors for cloud security auditing as reactive, intercept-and-check, or proactive (2019, pp. 9-13). Nonetheless, this research does not focus on transparency services or similar solutions to audit or monitor security information with the express goal of externally communicating this information from the cloud service providers' operators to external customers.[6]

In their survey, Ramachandra and his colleagues identify a key property to security and risk exposure of cloud infrastructures past and present: the two most important aspects in determining impact and exposure to vulnerabilities is the choice of deployment (e.g. public or private) and delivery model (e.g. Infrastructure-as-a-Service (IaaS); Platform-as-a-Service (PaaS); Software-as-a-Service (Saas)) (2017, p. 468). This research focuses primarily on public deployment for the various delivery models. According to this research, this subset experiences heightened security challenges due to a large customer footprint, management of publicly available resources, and a multitude of external factors outside of their immediate control, including legislation and data protection laws (Ramachandra et al., 2017, p.468). The matrix of cloud deployment models and security responsibility still holds true today, in that

[5] As ORock analysts note, FedRAMP is not required for customers outside of the federal government, but still popular as an important signal for acceptable cloud servces in regulated use cases nonetheless (2021).

[6] Both academia and industry, based on my literature survey, often conflate auditing and monitoring to have the same meaning in the cloud security domain.

customers bare more responsibility with IaaS to shape their own infrastructure accordingly. Conversely, PaaS to a great extent, and SaaS to the greatest extent, burden the cloud providers with securing the system, not the customer. (Ramachandra et al., 2017, p. 469). Interestingly, in this 2017 survey there is no mention of monitoring, coordination, or transparency about security posture with well-informed customers as an impact or challenge in current literature and practice. The paper does not list them as defensible controls or counter-measures either.

Similarly, older surveys of cloud monitoring (not just specifically to security), such as Aceto and his colleagues, do not identify these themes or trends relevant to security monitoring for multi-tenant cloud customers (2013).

Hakani and Mann have a more current survey for cloud security mechanisms, confirming deployment types and models have not much changed, but expounding more on updated detailed security threats and techniques for cloud data security, cloud firewalling, and cryptographic key management (2022). Although there is hardly any discussion of research of monitoring or coordination between cloud provider, auditor, or customer, this survey does allude to their absence as a significant challenge stating that "both customers and providers face several security concerns and issues. Such issues may make it harder for customers as well as suppliers to believe one another" (2022, p. 475).

Although general surveys do not focus on the challenges of transparently communicating cloud security information external to service operators, or solutions similar to transparency services, there is a wide variety of proposed strategies and techniques for cloud service operators to internally monitor and remediate cloud security weaknesses. Majumdar and his colleagues advocate for proactive auditing with a system supported by formal methods to detect security violations from events and recycling verification results to restore policies (2022, p. 2518). The design of Aldribi and his team employs underlying hardware isolation to empower customers to independently configure and monitor their own systems accordingly in complex multi-tenant environments (2015). Carvallo and other researchers present a design for a comprehensive security assurance platform with network, system, and application monitoring sensors for internal reporting (2017). Torkura and his colleagues have their own novel solution for monitoring misconfigurations with their CSBAuditor, using transition analysis and the reconciler pattern, (2021), but all these solutions

predominantly focus on internal communication, coordination, and mitigation.

As promising as all of these solutions are, whether proactive, intercept-and-check, or reactive, no solution takes a similar multi-party approach to mutual monitoring.

2.2 Cybersecurity Frameworks and Cloud Security Monitoring

The previous section identifies a wide variety of research into cloud security monitoring, but without explaining why there is practical industry interest in monitoring. A primary reason is that common cybersecurity frameworks, used by both cloud service providers and their customers, recommend or require periodic monitoring of their infrastructure. This section will identify those requirements in the most common cybersecurity frameworks.

2.2.1 CIS Critical Security Control

The Center for Internet Security maintains a popular cybersecurity framework for industry best practices applicable to wide spectrum of companies and with a focus on simplicity and ease of implementation. One control in their Critical Security Controls framework is CSC-7, which requires continuous vulnerability management (2024).

2.2.2 Cloud Security Alliance Cloud Controls Matrix

The Cloud Security Alliance (CSA) is a reputable organization that promulgates security guidance for cloud service providers, including their own cybersecurity framework, the Cloud Control Matrix (CCM). The CSA maintains a registry, STAR, for certified providers that meet different maturity levels for their implementation of the CCM controls. In 2024, CSA published STAR Level 3, which requires continuous monitoring for their new highest maturity level (2021).

2.2.3 ISO/IEC 27001:2022

The International Organization for Standardization (ISO) is a voluntary standards body that promulgates standards for many nations, unlike the previous examples that are predominantly focused on the United States. ISO 27001:2022, their framework for building information security management systems, has control Appendix A 8.16,

which recommends continuous monitoring (2022).

2.2.4 NIST Risk Management Framework

As detailed in Section 2.3.1, the NIST Risk Management Framework is the foundation of FedRAMP program's design. FedRAMP's staff have tailored the RMF's lifecycle and process framework (defined in NIST Special Publication 800-37) with its catalog of controls (defined in NIST Special Publication 800-53) specifically for cloud services. Nonetheless, most government agencies require RMF for many other systems, not just those deployed with cloud services. Most tailored uses of RMF, whether FedRAMP's particular use or that of a federal agency security program, mandate implementation of control CA-7, requiring an organization to establish an continuous monitoring program (2020, pp. 90-91).

2.3 FedRAMP History and Continuous Monitoring

Per its official website, the Federal Risk Authorization and Risk Management Program, more popularly known as just FedRAMP, is "a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services" (2025). Given the spending and impact of cloud services for the government's digital services as described in Section 1.2, it is not surprising that the whole program has evolved many times over fourteen years, not just for the continuous monitoring portion.

Therefore, it is important to highlight relevant history and the current state of FedRAMP continuous monitoring processes as it pertains to continuous monitoring.

2.3.1 History

Although the Federal Chief Information Officer formally established FedRAMP in 2011, it originated in 2009 with an interagency working group, the Cloud Computing Security Working Group, and its Federal Cloud Computing Initiative. The initiative sought to determine how to best perform security authorizations and, the central topic of this paper, continuous monitoring for multi-agency systems outsource to cloud service providers (Metheny & Krush, 2017, p. 239). These problems

were hardly new to government technologists or early cloud service providers, but what was novel with FedRAMP was the idea for a unified risk management and continuous monitoring program.

To unify the varying information security and privacy management programs across the federal government, the original design focused on three areas: authorization, continuous monitoring, and federal security requirements (Metheny & Krush, 2017, p. 240). This design based the single assessment by consistent application of the NIST RMF. As described in Section 2.2.4, the continuous monitoring approach embraced by FedRAMP, and later other cybersecurity frameworks, stems from its basis in the RMF. The fledging FedRAMP Program Management Office (PMO) announced this design publicly after eighteen months of stakeholder collaboration for public feedback in November 2010 (Metheny & Krush, 2017, p. 240).

After more collaboration, the Federal Chief Information Officer published the *Security Authorization of Information Systems in Cloud Computing Environments*, formally establishing the initial organizational structure of FedRAMP and its methodology (Metheny & Krush, 2017, p. 241). Not only did define the initial organizational structure, the memo instructed the PMO to create "[i]n coordination with DHS, a framework for continuous monitoring, incident response and remediation, and FISMA reporting" (2011, p. 3).

There were many changes from 2011 to 2021, by FedRAMP's own admission, that "focused on continued evolution — from redesigning processes to increasing transparency, or re-focusing on security while streamlining documentation," (2021), but the general organizational structure and overall process remained the same.

Significant organizational and process changes occurred in two phases for FedRAMP, the "FedRAMP Act" Phase and the "20x Phase," respectively.

From 2021 to 2022, Congress proposed legislation to fully codify FedRAMP into law and not only depend on the memoranda and direction from OMB's executive direction. By December 2022, the FedRAMP Act was integrated with the National Defense Authorization Act for Fiscal Year 2023 (117th Congress, 2022). In FedRAMP's blog post, they hinted at "additional information on how the Act may impact our stakeholders in the near future, including more information on the new Federal Secure Cloud Advisory Committee" (2023). Soon after, FedRAMP and OMB refined and published their plan for a new organization, approach, and resulting processes.

The final OMB memo, M-24-15, complemented the FedRAMP Act at the strategic level with tactics at the operational level.

2.3.2 Continuous Monitoring

2.4 Transparency Services for Other Use Cases

3 Solution

3.1 Mutual Monitoring Transparency Service

3.2 Quantitative Framework

4 Evaluation

4.1 Method and Results

4.2 Limitations and Future Work

4.3 Conclusion

5 Appendix

References

117th Congress. (2022). *H.r.7776 - james m. inhofe national defense authorization act for fiscal year 2023.* Retrieved 2025-07-22, from https://web.archive.org/web/20250415062420/https://www.congress.gov/117/bills/hr7776/BILLS-117hr7776enr.pdf#page=1055

Aceto, G., Botta, A., de Donato, W., & Pescapè, A. (2013, June). Cloud monitoring: A survey. *Computer Networks*, *57*(9), 2093-2115. Retrieved from http://dx.doi.org/10.1016/j.comnet.2013.04.001 doi: 10.1016/j.comnet.2013.04.001

Aldribi, A., Traore, I., & Letourneau, G. (2015, August). Cloud slicing a new architecture for cloud security monitoring. In *2015 ieee pacific rim conference on communications, computers and signal processing (pacrim)* (p. 18-22). IEEE. Retrieved 2025-05-24, from http://dx.doi.org/10.1109/PACRIM.2015.7334802 doi: 10.1109/pacrim.2015.7334802

Bashir, I. (2022). *Blockchain consensus: An introduction to classical, blockchain, and quantum consensus protocols* (1st edition ed.). Apress L.P. Retrieved 2025-07-

20, from https://learning.oreilly.com/library/view/blockchain-consensus/9781484281796/

Birkholz, H., Delignat-Lavaud, A., Fournet, C., Deshpande, Y., & Lasker, S. (2025). *An architecture for trustworthy and transparent digital supply chains* (Internet-Draft). Retrieved 2025-06-02, from https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/12/

Carvallo, P., Cavalli, A. R., Mallouli, W., & Rios, E. (2017). Multi-cloud applications security monitoring. In *Green, pervasive, and cloud computing* (p. 748-758). Springer International Publishing. Retrieved from http://dx.doi.org/10.1007/978-3-319-57186-7_54 doi: 10.1007/978-3-319-57186-7_54

Center for Internet Security. (2024). *Cis critical security control 7: Continuous vulnerability management* (v8.1 ed.). Retrieved 2025-07-20, from https://web.archive.org/web/20250523105159/https://www.cisecurity.org/controls/continuous-vulnerability-management

Cloud Security Alliance. (2021). *The evolution of star: Introducing continuous auditing.* Retrieved 2025-07-20, from https://cloudsecurityalliance.org/download/artifacts/evolution-of-star-introducing-continuous-auditing

Department of Defense. (2023). *Federal risk and authorization management program moderate equivalency for cloud service provider's cloud service offerings.* Department of Defense. Retrieved 2025-07-19, from https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf

Federal Chief Information Officer. (2011). *Security authorization of information systems in cloud computing environments.* Retrieved 2025-07-20, from https://web.archive.org/web/20250401120534/https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf

FedRAMP. (2021). *Fedramp turns 10!* Retrieved 2025-07-22, from https://web.archive.org/web/20250413100853/https://www.fedramp.gov/blog/2021-12-08/FedRAMP-Turns-10/

FedRAMP. (2023). *Fedramp announces the passing of the fedramp authorization act!* Retrieved 2025-07-22, from https://web.archive.org/web/20250708095421/https://www.fedramp.gov/blog/2023-01-11

-announces-passing-fedramp-auth-act/

FedRAMP. (2025). *Fedramp csp authorization playbook.* Retrieved 2025-05-18, from https://web.archive.org/web/20250413105351/https://www.fedramp.gov/assets/resources/documents/CSP_Authorization_Playbook.pdf

FedRAMP. (2025). *What is fedramp?* Retrieved 2025-07-20, from https://web.archive.org/web/20250623215527/https://help.fedramp.gov/hc/en-us/articles/27700231586459-What-is-FedRAMP

FedRAMP. (2025). *Who is responsible for the cloud security controls?* Retrieved 2025-07-20, from https://web.archive.org/web/20250324200835/https://help.fedramp.gov/hc/en-us/articles/27700955089563-Who-is-responsible-for-the-cloud-security-controls

Gartner. (2024). *Gartner forecasts worldwide public cloud end-user spending to total $723 billion in 2025.* Retrieved 2025-05-18, from https://web.archive.org/web/20250415023404/https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025

Hakani, D., & Mann, P. S. (2022, December). A comprehensive survey on cloud security mechanisms. In *2022 international conference on automation, computing and renewable systems (icacrs)* (p. 471-475). IEEE. Retrieved from http://dx.doi.org/10.1109/ICACRS55517.2022.10028990 doi: 10.1109/icacrs55517.2022.10028990

Information security, cybersecurity and privacy protection — Information security management systems — Requirements (Vol. 2022; Standard). (2022). Geneva, CH: International Organization for Standardization.

Lewis Commission. (2025). *Faster into the cloud: Accelerating federal use of cloud services for security and efficiency.* Center for Strategic and International Studies. Retrieved 2025-05-18, from https://web.archive.org/web/20250116234900/https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-01/250115_Lewis_Cloud_Commission.pdf

Majumdar, S., Chawla, G. S., Alimohammadifar, A., Madi, T., Jarraya, Y., Pourzandi, M., … Debbabi, M. (2022, July). Prosas: Proactive security auditing system for clouds. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2517-2534.

Retrieved from http://dx.doi.org/10.1109/TDSC.2021.3062204 doi: 10.1109/tdsc.2021.3062204

Majumdar, S., Madi, T., Wang, Y., Tabiban, A., Oqaily, M., Alimohammadifar, A., … Debbabi, M. (2019). *Cloud security auditing*. Cham, Switzerland: Springer Nature. Retrieved 2025-05-23, from https://link.springer.com/book/10.1007/978-3-030-23128-6

Metheny, M., & Krush, W. (2017). *Federal cloud computing: The definitive guide for cloud service providers* (Second Edition ed.). Elsevier Science and Technology Books, Inc.

NIST. (2020). *Security and privacy controls for information systems and organizations* (Tech. Rep. Nos. NIST Special Publication (SP) 800-53, Rev. 5). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved 2025-06-04, from http://dx.doi.org/10.6028/NIST.SP.800-53r5 doi: 10.6028/nist.sp.800-53r5

ORock. (2021). *Why fedramp matters to the private sector.* Retrieved 2025-07-19, from https://orocktech.com/blog/why-fedramp-matters-to-the-private-sector/

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. *Procedia Computer Science, 110*, 465-472. Retrieved from http://dx.doi.org/10.1016/j.procs.2017.06.124 doi: 10.1016/j.procs.2017.06.124

stackArmor. (2024). *How much does fedramp compliance cost?* Retrieved 2025-05-18, from https://web.archive.org/web/20240808151743/https://stackarmor.com/how-much-does-fedramp-compliance-cost/

Torkura, K., Sukmana, M. I., Cheng, F., & Meinel, C. (2021, March). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security, 102*, 102124. Retrieved from http://dx.doi.org/10.1016/j.cose.2020.102124 doi: 10.1016/j.cose.2020.102124