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 (2025a, 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 (2025a, 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. 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 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.

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[2] 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"[3] for cloud security monitoring. A new architecture should incentivize auditors to sell value-add analytics via these federated data services, potentially obsoleting centralized authorities for continuous monitoring like FedRAMP. To validate this hypothesis, I propose the list of deliverables below, in addition to the final report summarizing their outcome.

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 overall processes. 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.

[2] Many associate the term "ledger" primarily with cryptocurrency and popular blockchain solutions, 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.

[3] FedRAMP, like many cloud security programs, assert 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."(2025b) 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 or mutual monitoring.

2 Background

2.1 Overview of Cloud Service Security Monitoring

2.2 FedRAMP Continuous Monitoring

2.3 Transparency Services for Other Use Cases

2.4 Solution

2.5 Mutual Monitoring Transparency Service

2.6 Quantitative Framework

3 Evaluation

3.1 Method and Results

3.2 Limitations and Future Work

3.3 Conclusion

4 Appendix

References

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/

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

FedRAMP. (2025a). *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. (2025b). *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

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

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/

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/