

Practicum Proposal: Mutual Monitoring in the Cloud

Alexander Stein
astein38@gatech.edu

1 Problem Statement

Cloud computing infrastructure is nearly ubiquitous across all industries, but its use is not without challenges. Cloud service providers must cater to customers in regulated sectors with high barriers to entry. One barrier is evaluation of the provider's cybersecurity posture, mostly with centralized bureaucracies. Although preemptively limiting cybersecurity risk, such mandatory evaluation often means significant delay and investment before regulated customers can use new or changing building blocks they urgently need for their digital services. Are these bureaucracies an optimal solution or a last resort that failed to keep pace with cloud technology? If the latter, is there a better way?

Many regulatory frameworks require frequent, periodic reviews of provider's security posture. Such reviews have significant compounding costs for the cloud service providers, contracted independent auditors, and customers who leverage these cloud services in their products and services to account for centralized assessment methodology. The resulting processes involve frequent manual data exchange and coordination between staff of these different parties, despite the proliferation of automation platforms and security analysis tools. These manual processes form bureaucracies. And those bureaucracies prefer qualitative security analysis over quantitative means, which scales poorly. I will confirm this claim with a critical analysis of FedRAMP's Continuous Monitoring Program (2025, p. 14) as an example. I will then use this analysis to identify requirements and test the feasibility of an alternative to the FedRAMP model of continuous monitoring: mutual continuous monitoring without a centralized regulatory body.

2 Choice of Problem

The cybersecurity of cloud services poses many challenges, but the inefficiency of continuous monitoring has systemic impact on the macroeconomics and risk modeling for heavily interconnected 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.

2.1 Economic Impacts

Although FedRAMP is a highly visible cloud security authorization program, there is limited precise data on the costs and economic impact for providers, auditors, and customer agencies. However, industry estimates significant costs for all these stakeholders.

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 seventeen of its total \$130 billion dollar IT budget in 2024 on cloud services alone (2025, p. 1). Although there is not complete compliance with FedRAMP requirements in government agencies, the goal of the FedRAMP Authorization Act that mandates FedRAMP's program, especially the continuous monitoring program, is ongoing oversight over the cloud building blocks of this seventeen billion dollar investment. And even without precise public data, all stakeholders admit to significant, onerous investment in the continuous monitoring process alone.

FedRAMP processes required specialized tools operated by dedicated staff, from the cloud service provider and often the customer agencies. Analysts at stackArmor estimate that an initial authorization costs a provider \$250,000 to \$750,000 dollars, of which \$100,000 to \$400,000 alone is for continuous monitoring activities (2024). Given a conservative estimate, any improvement or optimization can benefit all stakeholders in reducing \$42,600,000 in spend by 426 services currently authorized, but potentially a much larger sum.

2.2 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.

Firstly, a centralized review process finalized by a small number of FedRAMP staff

constitutes a single point of failure. As FedRAMP documents, cloud providers, auditors, and agency customers must use a centralized wiki site, USDA's connect.gov, and coordinate out of band with FedRAMP staff for final review (2025, pp. 3,14). Paradoxically, providers and auditors paradoxically get no guarantees for its cyber-security posture of the system they use to document their own posture. Additionally, the system and underlying processes limit sharing with auditors and customers focused on other regulatory frameworks that rely on reciprocity guarantees to justify the use of FedRAMP authorizations.

The impacts of manually curated data from FedRAMP's continuous monitoring extend beyond its stakeholders. Interrelated regulatory frameworks that depend upon it. Given FedRAMP's rigorous review process, especially continuous monitoring, many providers and their auditors use artifacts from FedRAMP authorization for equivalency, or reciprocity, for deliverables as evidence for other regulatory frameworks, especially in the defense, commercial, and finance sectors in 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.

3 Expected Deliverables

To best research alternatives to popular centralized models for continuous modeling, I propose the list of deliverables below, in addition to the final report summarizing their outcome.

1. a critical of the centralized FedRAMP model for continuous monitoring
2. an architecture specification for mutual continuous monitoring
3. prototype code for transparency services for mutual continuous monitoring
4. a quantitative measurement framework for cloud service security to use in this architecture

References

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

- 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
- 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/>