

Practicum Proposal: Mutual Monitoring in the Cloud

Alexander Stein
astein38@gatech.edu

1 Problem Statement

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 evaluation 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?

2 Choice of Problem

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.

2.1 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 operated by dedicated staff, from providers, auditors, 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 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, auditors, and agency customers must use a single, 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 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, 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.

3 Expected Deliverables

I will use this research to design and evaluate an alternative to centralized continuous monitoring, mutual monitoring. The foundation of mutual monitoring will be federated data services, known in other security use cases as transparency services. The services will necessarily change cloud service provider and customer behavior, while also incentivizing auditors to sell value-add analytics services in these data services, and possibly obsolete centralized authorities like FedRAMP. To do so, I propose the list of deliverables below, in addition to the final report summarizing their outcome.

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

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/>