Practicum Proposal

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 services they urgently need. 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. 18) 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. 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 $679 billion dollars. The think tank CSIS estimates that the United States government spent seventeen of its total $130 billion dollar IT budget on cloud services alone. Although there is not complete compliance with FedRAMP requirements in government agencies as the law requires, the goal of the FedRAMP Authorization Act that mandates FedRAMP's authorization and continuous monitoring program is essentially oversight over this seventeen billion dollars. And even without precise public data, all stakeholders invest significantly in the continuous monitoring process.

FedRAMP processes required specialized tools operated by dedicated staff, from the cloud service provider and often the customer agencies. Analysts at stackArmor report 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. 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 quite likely more.

2.2 Cybersecurity Impacts

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