Mutual Monitoring in the Cloud

Problem Statement

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?

Appendix

Research

Continuous cloud monitoring

FedRAMP

- (Lewis Commission, 2025)
  - "Fully automate FedRAMP processes. Eliminate written, qualitative assessments and document review in favor of automated security controls that can be verified through the continual assessment of network security telemetry. Rather than requiring cloud service providers (CSPs) to provide proof that they have met control requirements that cannot be automated and have those artifacts reviewed, CSPs should be allowed to 'attest' that they have met requirements for areas such as personnel training and documentation." (p. 2)
  - "The slow pace of government cloud adoption increases both costs and risks for federal operations and hinders the provision of better services to citizens. Cloud technologies offer advantages in modernization, efficiency, cybersecurity, and resilience. An agency can access and use cloud computing resources without having to buy, maintain, or modernize hardware—actions that are problematic given cumbersome federal budgeting and certification processes." (p. 3)
  - "Despite the potential gains, law, regulation, policy, and agency culture all remain obstacles to reaping the benefits of federal cloud adoption." (p. 3)
  - "To place FedRAMP on more solid legal footing, in 2022 Congress passed the FedRAMP Authorization Act. The act strongly encouraged automation and continuous monitoring to speed up the accreditation process." (p. 5)
- (FedRAMP, 2025)
- (Gartner, 2024)
- (stackArmor, 2024)

FedRAMP. (2025). *FedRAMP CSP authorization playbook*. Retrieved 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 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; International Studies. Retrieved 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 from https://web.archive.org/web/20240808151743/https://stackarmor.com/how-much-does-fedramp-compliance-cost/