

- I. Introduction
 - A. Problem Statement
 - B. Solution Statement
 - 1. Methodology
 - a. Architecture specification
 - b. Qualitative analysis of gaps in current FedRAMP monitoring processes
 - c. Quantitative analysis
 - i. Duration and cost for continuous monitoring operations
 - ii. Duration and cost for transparency service architecture for mutual monitoring
 - Estimates for development from parallel use cases
 - certificate transparency
 - binary transparency
 - supply chain transparency services
 - Estimates for operation from parallel use cases
 - certificate transparency
 - binary transparency
 - supply chain transparency services
 - 2. Key components and deliverables
- II. Continuous Monitoring for Cloud Services
 - A. NIST Risk Management Framework (SP 800-37; SP 800-53)
 - B. Cloud Security Alliance CAIQ/STAR
 - C. CIS Controls Assessment Specification
 - D. ISO 27001:2022
 - E. SOC 2
- III. FedRAMP Continuous Monitoring
 - A. Background
 - B. History
 - C. 20x Working Programs and Modernization
 - D. Critical Requirements, Challenges, and Criticism from FedRAMP Modernization
 - 1. Infrastructure CSPs support dependent CSPs and agency customer application reporting
 - 2. Accurately deriving summarized statistics verifiably from raw data
 - 3. Challenges and limitations of OSCAL and other existing data standards
 - 4. Effective use of signatures, verifications, and trust indicators
 - 5. Timely report submission and repeatable report verification
 - 6. Challenges to current scanning techniques for compliance and vulnerability scanning
 - 7. Inventory approaches and challenges
 - 8. Challenges to the current Significant Change Request process and future modernization
 - 9. Privacy-enhancing and least privilege access to cloud security data
 - 10. Challenges due to current third-party auditors' staff knowledge and skills
 - 11. Centralization versus decentralization
 - 12. Economics and incentives
- IV. Transparency Services for Adjacent Security Domains
- V. Mutual Monitoring Service
 - A. Use Cases
 - B. Personas
 - C. Components
 - 1. Core Transparency Service
 - 2. Adjacent Services
 - D. Processes

1. Statement Registration
 2. Transparent Statement Publication
 3. Registering Statements of Quantitative Inventory and Configuration Measurements
- E. Mapping to Use Cases
- VI. Quantitative Framework
- VII. Evaluation
 - A. Scope and gaps
 - B. Quantitative methods
 - C. Qualitative methods
- VIII. Limitations and future work for mutual monitoring
 - A. Incomplete MVP implementation of transparency service, client, and adjacent services
 - B. Extending the quantitative framework outside inventory and configuration management
 - C. Complete architecture for multi-party network of transparency services with quantitative measurement across heterogeneous services
 - D. Encrypted data stores for high-risk and high-sensitivity cloud service data
 - E. Custom attribute or role-based access control for high-risk and high-sensitivity cloud service data
 - F. Concrete privacy-enhancing techniques for mandatory transparency service operations
 1. Signed statement registration
 2. Accessing Adjacent Service for Storage
 3. Accessing Adjacent Service for Queries
- IX. Conclusions