

# Mutual Monitoring in the Cloud

Final Presentation

A.J. Stein

OMS Cybersecurity Masters Practicum

Georgia Institute of Technology

PUBP-6727 OCY

# The Problem

- Cloud computing infrastructure is essentially ubiquitous.
- Cloud service providers must cater to customers, especially regulated ones.
- A major barrier is ongoing evaluation of the provider's cybersecurity posture.
- The results are often centralized bureaucracies.

## The Problem

- Are cloud security bureaucracies the right way?
- Are they the only way?
- Who watches the watchers?



## The Problem

"I think the cloud is so freaking complex. No one knows what is happening and how it works. I think we passed this point several years ago. We've lost our means to even evaluate our risk with the complexity of the cloud."

Participant 8, experienced FedRAMP assessor

# The Solution

- Analyze FedRAMP ConMon's strengths and weaknesses.
- Design an alternative model, for FedRAMP *and* similar programs.
  - Stakeholders mutually monitor each other with transparency services.
  - Forgo control-driven assessment, focus measurable security properties.
  - Use a simple quantitative framework for measuring properties.
- Do not certify, do not authorize, but **measure** *each other*.

## The Solution

"I feel like the optimal end state of this would be there is ingestion of logs and they [the stakeholders] know what's happening. Why not do it [and decentralize continuous monitoring data]? We are throwing all these man hours into it and we could have better data."

Participant 8, experienced FedRAMP assessor

## How Did You Design This Solution?

- Previous engagement in standards bodies (NIST; FedRAMP; IETF)
- Analyzing industry trends and academic research
- Coding public feedback in FedRAMP's 20x forums

# Background

- What is FedRAMP?
- What is FedRAMP ConMon?
- What works?
- What doesn't?



## What is FedRAMP?

In mid-2009, an interagency effort, created under the Federal Cloud Computing Initiative, was established to focus on solving a single problem statement—How do we best perform security authorization and *continuous monitoring for out-sourced and multiagency systems*?

Metheny, M. (2017). Introduction to the federal cloud computing strategy. In Federal Cloud Computing (pp. 239). Elsevier. <https://doi.org/10.1016/b978-0-12-809710-6.00001-9>

## How Did FedRAMP Evolve?

2011 December: FedRAMP policy signed

2012 May: Announcement of third party auditors

2012 June: FedRAMP officially launches

2012 December: First provisional FedRAMP authorization

2013 May: First full authorization of AWS with HHS

<https://www.nextgov.com/modernization/2016/05/a-brief-history-of-fedramp/218162/>

## How Did FedRAMP Evolve?

2022 December: FedRAMP Act codified into law

2023 October: Draft modernization memo published

2024 March: Centralized platform announced

2024 July: M-24-15 disbands JAB; establishes new FedRAMP board

2024 July: M-24-15 requires agency uploads to platform by July 2025

<https://www.fedramp.gov/updates/changelog/>

## How Did FedRAMP Evolve?

2025 March: Centralized platform contract halted

2025 April: FedRAMP downsizes most contractor staff

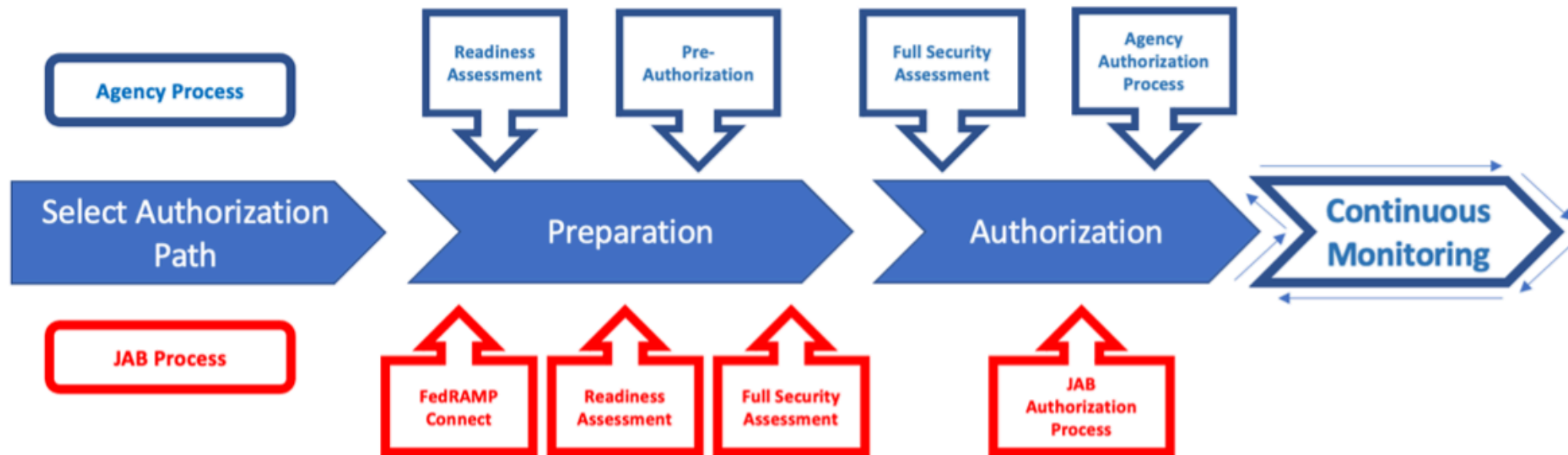
2025 March: 20x Modernization Pilots and KSIs announced

2025 May: Announcement of secure storage standard

<https://www.fedramp.gov/updates/changelog/>

# What Were the FedRAMP Processes? (+ JAB)

## FedRAMP Authorization Process



**Note:** Readiness Assessment is required for the JAB Process and is optional but highly recommended for the Agency Process

# What Are the FedRAMP Processes? (— JAB)

## 01 Preparation

### Readiness Assessment

(Optional, but highly recommended)

- RAR Development
  - FedRAMP PMO Review of RAR
  - Remediation (if needed)
- FedRAMP Marketplace Designation – Ready



### Pre-Authorization

- Partnership Establishment
- Authorization Planning
- Kickoff Meeting
- FedRAMP Marketplace Designation – In Process

## 02 Authorization

### Full Security Assessment

- Security Authorization Package (SSP, SAP, SAR, POA&M)\*



### Agency Authorization Process

- Agency Review of Security Authorization Package
- SAR Debrief
- Remediation
- Agency Final Review
- Agency Issues ATO
- FedRAMP PMO Review
- Remediation (if needed)
- FedRAMP Marketplace Designation - Authorized

## 03 Continuous Monitoring

### Post Authorization

- Ongoing Continuous Monitoring Deliverables
- Annual Assessment

\* The full security assessment may be prepared in advance of the authorization phase, or completed during the authorization phase. This is dependent on the agency's review approach.

## What is FedRAMP ConMon?

- Monthly assessments
  - Updated inventory; vulnerability scans; remediation plan
- Significant change requests
- Annual assessments
  - Updated inventory; vulnerability scans; remediation plan
  - Subset of full initial assessment

## What is FedRAMP ConMon?

- Out-of-band coordination between provider and agency customers
- Manual upload of all data to max.gov or high repository
- Review by agency and FedRAMP PMO staff (sometimes separately)
- Synchronous meetings to review and adjust POA&Ms



## What works?

- Consistent process (when followed)
- Rigor in third-party analysis and checking
- Standardized reporting
  - Detecting gaps in coverage at points in time
  - Analyzing trends in cloud security posture

## What doesn't?

- Manual review and analysis mechanisms
- Too many different processes based on provider details
- No automation to retrieve continuous monitoring data
- No automation to combine data with "CSPs of the CSP"
- Centralized reviews and approvals slow change

## What doesn't?

- No means to continuously check auditor, agency, or FedRAMP repository
- Lack of verifiable trust mechanisms for alternatives
  - Decentralized systems
  - Federated systems

# Solution

- Prototyping software
- Architecture specification

## Prototyping

- Started Transparency Service API after first rough draft of spec
  - Python 3 and Flask REST API framework
  - Open-source [cryptograph](#), [cwt](#) and [requests](#) libraries
- Finished initial shared utils works
- Encountered trouble interpreting multiple IETF specs with more time allotted













## Architecture Specification

- Use Cases
- Architecture
- Components
- Flows

# Evaluation

	Yes	No
Did you request access to max.gov FedRAMP package?	2	6
Did you receive max.gov's FedRAMP package?	3	5

# Evaluation

	-2	-1	0	1	2	
MAX.gov effective?	2	1	2	3	-	
Leveraged system data effective today?	1	1	5	-	1	
<b>Leveraged system data important in future?</b>	-	-	-	1	7	  
Submitting raw data effective today?	-	4	2	2	-	
Submitting raw data important in future?	-	-	1	3	4	 
Summarizing and linking to it important?	-	-	-	3	5	  

 key:  negative  neutral  positive













# Evaluation

	-2	-1	0	1	2	
OSCAL important today?	1	2	2	-	4	 
<b>OSCAL important in future?</b>	1	-	1	2	4	 
Digital signatures effective today?	3	2	3	-	-	 
Use digital signatures often today?	4	1	1	-	2	 
<b>Digital signatures important in future?</b>	-	-	1	2	5	  












 key:  negative  neutral  positive

# Evaluation

	-2	-1	0	1	2	
Common scanning support effective today?	1	2	-	3	2	
<b>Common scanning support important in future?</b>	1	-	-	1	6	  
Significant change tracking effective today?	3	2	2	1	-	 
<b>Significant change tracking important in future?</b>	-	1	-	1	6	  















 key:  negative  neutral  positive

# Evaluation

	-2	-1	0	1	2	
Vulnerability management effective today?	1	2	2	1	2	
<b>Vulnerability management important in future?</b>	-	-	1	-	7	  
Securing confidential data effective today?	1	-	1	4	2	  
<b>Securing confidential data important in future?</b>	-	-	1	-	7	  

 key:  negative  neutral  positive

# Evaluation

	-2	-1	0	1	2	
3PAO measurement effective today?	2	3	2	1	-	 
<b>3PAO measurement important in future?</b>	-	-	2	3	3	  
Economic incentives effective today?	3	3	-	2	-	 
<b>Economic incentives important in future?</b>	-	1	-	-	7	  
Centralization effective today?	-	2	3	2	1	
<b>Decentralization important in future?</b>	3	-	2	1	3	 

 key:  negative  neutral  positive

## Solution Limitations

- Incomplete transparency service implementation
- Additional use cases for quantitative measurement framework
- Interaction patterns for ecosystem of different transparency services

## Solution Limitations

- Encrypted data storage for adjacent service confidentiality
- Custom role-based access control for adjacent service confidentiality
- Concrete privacy-enhancing techniques for transparency service confidentiality

## Next Steps and Future Work

- Complete a prototype implementation 🙌
- Vet new use cases for economic incentives of mutual monitoring
- Design applications of quantitative framework for new use cases
- Design privacy-enhancing techniques for transparency service confidentiality

# Feedback

- You can provide feedback in multiple ways.
- Post in the class discussion board in Canvas.
- Open issues in my GitHub repo at [github.com/aj-stein/practicum/issues](https://github.com/aj-stein/practicum/issues).





# Conclusion

Et fin.

(Find me on the Internet if you want to learn more.)