Mutual Monitoring in the Cloud

A.J. Stein
Georgia Institute of Technology
astein38@gatech.edu

Abstract. Cloud computing infrastructure is essentially ubiquitous, but adoption is not without challenges. Cloud service providers must cater to customers in regulated sectors. Their use of popular cybersecurity frameworks create high barriers to entry. One barrier, often resulting in centralized bureaucracies, is the periodic monitoring of the provider's cybersecurity posture by way of scanning for inventory, configuration, and vulnerability management gaps. By analyzing one prominent example, FedRAMP's Continuous Monitoring Program, this paper considers if such bureaucracies are the only valid solution. To refute this hypothesis, the paper presents an alternative architecture for multi-party monitoring of cloud services' cybersecurity posture, mutual monitoring.

1 Introduction

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 monitoring 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? This paper presents an alternative, the mutual monitoring architecture, as a measurably more effective solution.

1.1 Why Does This Problem Matter?

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, or sometimes indirectly depend upon, so any improvement or optimization will yield significant improvement to cloud service adoption across regulated industries.

1.2 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 and staff for all stakeholders, adding cost and friction. Analysts at stackArmor estimate that a FedRAMP authorization costs a provider $250,000 to $750,000 dollars, and continuous monitoring support constitutes from $100,000 to $400,000 of that amount (2024). Given this conservative estimate, any improvement or optimization can benefit all stakeholders in reducing $42,600,000 spent, but potentially a much larger sum.

1.3 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, [1] 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.[2] 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. Those outside these agencies focused on other regulatory frameworks who want it cannot access it. They rely on reciprocity guarantees to justify the use of FedRAMP authorization and continuous monitoring, which is practically infeasible without this prerequisite 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 assurance (or less formal "reciprocity") with other regulatory frameworks preferred by the defense (Department of Defense, 2023), commercial (ORock, 2021), and finance sectors of the United States. Therefore, any optimization in FedRAMP's processes has second order benefits for cloud security across industry.

1.4 Solution

The focus of this paper is an alternative solution to centralized continuous monitoring as exemplified by FedRAMP, mutual monitoring. Mutual monitoring facilitates federated data services with ledgers[3] of digitally signed data using an archi-

[1] This system is essentially the same system as max.gov. The Office of Management and Budget (OMB) handed off its management to the Department of Agriculture (USDA) in 2023. The USDA subsequently rebranded the system during the transition, but FedRAMP has continuously used it.

[2] FedRAMP's official package access request form indicates only employees with email addresses for a government or military domain may request access. Staff from cloud providers or auditors not actively assigned to government or military contracts cannot even initiate these requests for a package.

[3] Many associate the term "ledger" primarily with cryptocurrency and their popular underlying blockchain implementations, such as Bitcoin and Ethereum. In computing, a ledger is "tamper-resistant shared distributed ledger composed of temporally ordered and publicly verifiable transactions" (Bashir, 2022). Transparency service implementers and standards authors employ the same fundamental concept, but use the interchangeable term Append-only Log, which they define as "a

tecture popular for other security use cases, transparency services. The positives and negatives of FedRAMP's continuous monitoring model will inform its design. Transforming to a mutual monitoring model can change the incentives, behavior, and thereby economics, of cloud service providers, auditors, and customers for true "shared responsibility" for the security of cloud services.[4] This new architecture can incentivize auditors to sell value-add analytics via these federated data services, obsoleting centralized authorities for continuous monitoring, like FedRAMP, and a market of inconsistent third-party auditors required to support them. To validate this hypothesis, I present a viable alternative in the form of my architecture for mutual monitoring.

To best explain the merits (and challenges) of mutual monitoring, the paper will provide an overview of past, present, and ongoing modernization of FedRAMP's continuous monitoring and how it relates to the "whole" of "getting FedRAMP authorized." This context will inform the following section, that outlines the key elements of the proposed mutual monitoring architecture. And finally, the paper will conclude with a qualitative and quantitative evaluation of the solution, highlight key limitations, and identity future work to advance this solution.

2 Background

2.1 Overview of Cloud Service Security Monitoring

Despite the prominence of FedRAMP in cloud security inside and outside of government,[5] there is a body of work from different academic and industry experts with a variety of approaches to cloud security monitoring. As FedRAMP evolved, these dif-

Statement Sequence comprising the entire registration history of the Transparency Service. To make the Append-only property verifiable and transparent" (Birkholz, Delignat-Lavaud, Fournet, Deshpande, & Lasker, 2025). All are examples of distributed ledger technology.

[4] FedRAMP, like many cloud security programs, asserts that "[t]here is a shared security responsibility model when using cloud products. Cloud service providers (CSPs) and customers (agencies or leveraging CSPs) both assume important security roles and responsibilities to ensure data is protected within cloud environments" (2025). As practical as it sounds, there are many concerns and criticisms on how to meaningfully realize the shared responsibility model, which has direct implications on the current continuous monitoring process and the mutual monitoring model proposed in this paper.

[5] As ORock analysts note, FedRAMP is not required for customers outside of the federal government, but is still popular as an important signal for vetting cloud services in other regulated environments nonetheless (2021).

ferent approaches evolved alongside of it. The following section discusses relevant highlights to current challenges to FedRAMP's continuous monitoring approach and the proposed mutual monitoring solution.

2.1.1 Academic Research in Cloud Security Monitoring

Over the last decade, academic researchers have affirmed the fundamentals of cloud deployment and security properties. Much literature uses the same taxonomy as Majumdar and his co-authors for cloud security auditing as reactive, intercept-and-check, or proactive (2019, pp. 9-13). Nonetheless, this research does not focus on transparency services or similar solutions to audit or monitor security information with the express goal of externally communicating this information from the cloud service providers' operators to external customers.[6]

In their survey, Ramachandra and his colleagues identify a key property to security and risk exposure of cloud infrastructures past and present: the two most important aspects in determining impact and exposure to vulnerabilities is the choice of deployment (e.g. public or private) and delivery model (e.g. Infrastructure-as-a-Service (IaaS); Platform-as-a-Service (PaaS); Software-as-a-Service (Saas)) (2017, p. 468). This research focuses primarily on public deployment for the various delivery models. According to this research, this subset experiences heightened security challenges due to a large customer footprint, management of publicly available resources, and a multitude of external factors outside of their immediate control, including legislation and data protection laws (Ramachandra et al., 2017, p.468). The matrix of cloud deployment models and security responsibility still holds true today, in that customers bare more responsibility with IaaS to shape their own infrastructure accordingly. Conversely, PaaS to a great extent, and SaaS to the greatest extent, burden the cloud providers with securing the system, not the customer. (Ramachandra et al., 2017, p. 469). Interestingly, in this 2017 survey there is no mention of monitoring, coordination, or transparency about security posture with well-informed customers as an impact or challenge in current literature and practice. The paper does not list them as defensible controls or counter-measures either.

Similarly, older surveys of cloud monitoring (not just specifically to security), such

[6] Both academia and industry, based on my literature survey, often conflate auditing and monitoring to have the same meaning in the cloud security domain.

as one from Aceto and his colleagues, do not identify these themes or trends relevant to security monitoring for multi-tenant cloud customers (2013).

Hakani and Mann have a more current survey for cloud security mechanisms, confirming deployment types and models have not much changed, but expounding more on updated detailed security threats and techniques for cloud data security, cloud firewalling, and cryptographic key management (2022). Although there is hardly any discussion of research of monitoring or coordination between cloud provider, auditor, or customer, this survey does allude to their absence as a significant challenge stating that "both customers and providers face several security concerns and issues. Such issues may make it harder for customers as well as suppliers to believe one another" (2022, p. 475).

Although general surveys do not focus on the challenges of transparently communicating cloud security information external to service operators, or solutions similar to transparency services, there is a wide variety of proposed strategies and techniques for cloud service operators to internally monitor and remediate cloud security weaknesses. Majumdar and his colleagues advocate for proactive auditing with a system supported by formal methods to detect security violations from events and recycling verification results to restore policies (2022, p. 2518). The design of Aldribi and his team employs underlying hardware isolation to empower customers to independently configure and monitor their own systems accordingly in complex multi-tenant environments (2015). Carvallo and other researchers present a design for a comprehensive security assurance platform with network, system, and application monitoring sensors for internal reporting (2017). Torkura and his colleagues have their own novel solution for monitoring misconfigurations with their CSBAuditor, using transition analysis and the reconciler pattern, (2021). Nonetheless, all these solutions predominantly focus on a cloud provider's internal coordination and mitigation.

As promising as all of these solutions are, whether proactive, intercept-and-check, or reactive, no solution takes a similar multi-party approach to mutual monitoring.

2.1.2 Cybersecurity Frameworks and Cloud Security Monitoring

The previous section identifies a wide variety of research into cloud security monitoring, but without explaining why there is practical industry interest in monitoring.

A primary reason is that common cybersecurity frameworks, used by cloud service providers, their auditors, and their customers alike, recommend or require periodic monitoring of their infrastructure. This section will identify those requirements in the most common cybersecurity frameworks.

2.1.3 CIS Critical Security Control

The Center for Internet Security maintains a popular cybersecurity framework for industry best practices applicable to wide spectrum of companies, with a focus on simplicity and ease of implementation. One of their only eighteen Critical Security Controls is CSC-7, which requires continuous vulnerability management (2024).

2.1.4 Cloud Security Alliance Cloud Controls Matrix

The Cloud Security Alliance (CSA) is a reputable organization that promulgates security guidance for cloud service providers, including their own cybersecurity framework, the Cloud Control Matrix (CCM). The CSA maintains a registry, STAR, for certified providers that meet different maturity levels for their implementation of the CCM controls. In 2024, CSA published STAR Level 3, which requires continuous monitoring for their new highest maturity level (2021).

2.1.5 ISO/IEC 27001:2022

The International Organization for Standardization (ISO) is a voluntary standards body that promulgates standards for many nations, unlike the previous examples that are predominantly focused on the United States. ISO 27001:2022, their framework for building information security management systems, has control Appendix A 8.16, which recommends continuous monitoring (2022).

2.1.6 NIST Risk Management Framework

As detailed in Section 2.2.1, the NIST Risk Management Framework is the foundation of FedRAMP program's design. FedRAMP's staff have tailored the RMF's lifecycle and process framework (defined in NIST Special Publication 800-37) with its catalog of controls (defined in NIST Special Publication 800-53) specifically for cloud services. Additionally, most government agencies require RMF for many other

systems, not just those deployed with cloud services.[7] Most tailored uses of RMF, whether FedRAMP's particular use or that of a federal agency security program, mandate implementation of control CA-7, requiring an organization to establish an continuous monitoring program (2020, pp. 90-91). Moreover, the NIST RMF controls refer to the agency's companion standard for design and implementation of continuous monitoring of federal systems, Special Publication 800-137 (2011). Similarly to SP 800-53, statute requires most federal agencies to follow this guidance. Unsurprisingly, FedRAMP used it as a blueprint for the Continuous Monitoring Program, which will be described further in Section 2.2.2.

2.2 FedRAMP History and Continuous Monitoring

Per its official website, the Federal Risk Authorization and Risk Management Program, more popularly known as just FedRAMP, is "a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services" (2025b). Given the spending and impact of cloud services for the government's digital services as described in Section 1.2, it is not surprising that the whole program has evolved many times over fourteen years, not just for the continuous monitoring portion.

Therefore, it is important to highlight relevant history and the current state of FedRAMP continuous monitoring processes as it pertains to continuous monitoring.

2.2.1 History

Although the Federal Chief Information Officer formally established FedRAMP in 2011, it originated in 2009 with an interagency working group, the Cloud Computing Security Working Group, and its Federal Cloud Computing Initiative. The initiative sought to determine how to best perform security authorizations and, the central topic of this paper, continuous monitoring for multi-agency systems outsourced to cloud service providers (Metheny & Krush, 2017, p. 239). These problems were hardly new to government technologists or early cloud service providers, but

[7] As NIST explains in Special Publication 800-53, the use of these controls is mandatory for government information systems due to OMB's Circular A-130 and the Federal Information Security Modernization Act (2020, p. 2).

what was novel with FedRAMP was the idea for a centralized risk management and continuous monitoring program.

To unify the varying information security and privacy management programs across the federal government, the original design focused on three areas: authorization, continuous monitoring, and federal security requirements (Metheny & Krush, 2017, p. 240). This design based the "assess once, reuse anywhere in government" model by adapting the NIST RMF. As described in Section 2.1.6, the continuous monitoring approach embraced by FedRAMP, and later other cybersecurity frameworks, stems from its basis in the RMF. The fledging FedRAMP Program Management Office (PMO) announced this design publicly after eighteen months of stakeholder collaboration for public feedback in November 2010 (Metheny & Krush, 2017, p. 240).

After more collaboration, the Federal Chief Information Officer published the *Security Authorization of Information Systems in Cloud Computing Environments*, formally establishing the initial organizational structure of FedRAMP and its methodology (Metheny & Krush, 2017, p. 241). Not only did define the initial organizational structure, the memo instructed the PMO to create "[i]n coordination with DHS, a framework for continuous monitoring, incident response and remediation, and FISMA reporting" (2011, p. 3).

There were many changes from 2011 to 2021, by FedRAMP's own admission, that "focused on continued evolution — from redesigning processes to increasing transparency, or re-focusing on security while streamlining documentation," (2021), but the general organizational structure and overall process remained the same.

Significant organizational and process changes occurred in two phases for FedRAMP, the "FedRAMP Act Phase" (from December 2022 to March 2025) and the "20x Phase" from March 2025 to present.

From 2021 to 2022, Congress proposed legislation to fully codify FedRAMP into law, not only depend on the OMB's executive direction.[8] By December 2022, the FedRAMP Act was integrated with the National Defense Authorization Act for Fiscal Year 2023 (117th Congress, 2022). In FedRAMP's blog post, they hinted at "additional information on how the Act may impact our stakeholders in the near future, including more information on the new Federal Secure Cloud Advisory Com-

[8] If not fully codified into law, the the permanence of FedRAMP's authority and funding could be curtailed or removed by successive executive action.

mittee" (2023). Soon after, FedRAMP and OMB refined and published their plan for a new organization, approach, and resulting processes. The final OMB memo, M-24-15, complemented the revolutionized strategy of FedRAMP Act with revolutionary tactics at the operational level to match. As Section 2.2.2 will explain, the Joint Authorization Board was the multi-agency board that shepherded heavily leveraged cloud providers (or put differently, the "cloud providers of the cloud providers") and those providers used for the high risk use cases (those with the coveted FedRAMP High Impact Level designation). As this memo was published, the FedRAMP PMO announced the rollout of new authorization paths and "details about how these changes will impact [cloud service providers] with provisional authorizations issued by the *former JAB* [emphasis added]" (2024b). The PMO piggybacked on the memo to mandate the use of NIST's Open Security Control and Assessment Language for completely digital authorization packages[9] and long-awaited automation for the authorization and continuous monitoring of cloud services (2024b). Not soon after, the PMO announced they would host an automation platform for cloud service providers and auditors to integrate directly with FedRAMP's program (2024a). These announcements were a significant step in actionable progress to automating FedRAMP processes and reducing a growing backlog of cloud services awaiting authorization or reauthorization.

Despite the focused vision and speed in the PMO during the "FedRAMP Act Phase," the PMO soon pivoted strategy in the "20x Phase." In March 2025, FedRAMP announced this surprise rapid change in direction with a new modernization program called 20x (2025a). Instead of the new alternatives proposed to high impact and high risk JAB authorizations in the "FedRAMP Act Phase," only legacy agency authorizations would remain (2025a). Talk of the automation platform disappeared, alongside many other initiatives of the last year. Instead, the PMO announced that "FedRAMP will not build on the old ways to consolidate resources and services that turn FedRAMP into a slow bureaucratic behemoth operating on behalf of the entire government. Instead, FedRAMP will clear the way for the development of new paths that focus on true security and eliminate the inefficiencies, making central ser-

[9] In the parlance of FedRAMP stakeholders, digital authorization packages were to be machine-readable collections of data for automated processing and dynamic presentation to stakeholders with different personas. This artifact contrasted the contemporary state of affairs, where FedRAMP packages were static documents almost exclusively edited and viewed with the Microsoft Office and PDF readers, using the templates the PMO provided.

vices unnecessary" (2025a). This announcement was a stark change, and later the FedRAMP Director and other staff would reveal more details. The director admitted that "[his staff] canceled [the FedRAMP Platform project contract] in February as the new administration directed reductions in unnecessary spending because the overall project would've cost more than FedRAMP's *entire current budget*" (2025). With this rapid shift to industry-led approach and rejection of previous strategies, Curran reported that the PMO let its contractor for eighty contractors lapse, and only eighteen government employees remained (2025). The remaining staff were to support the existing program, including continuous monitoring, and this modernization effort. As the title's article implied, FedRAMP officials detailed the planned unwinding of continuous monitoring, and most of FedRAMP's extant processes as well.

2.2.2 Continuous Monitoring

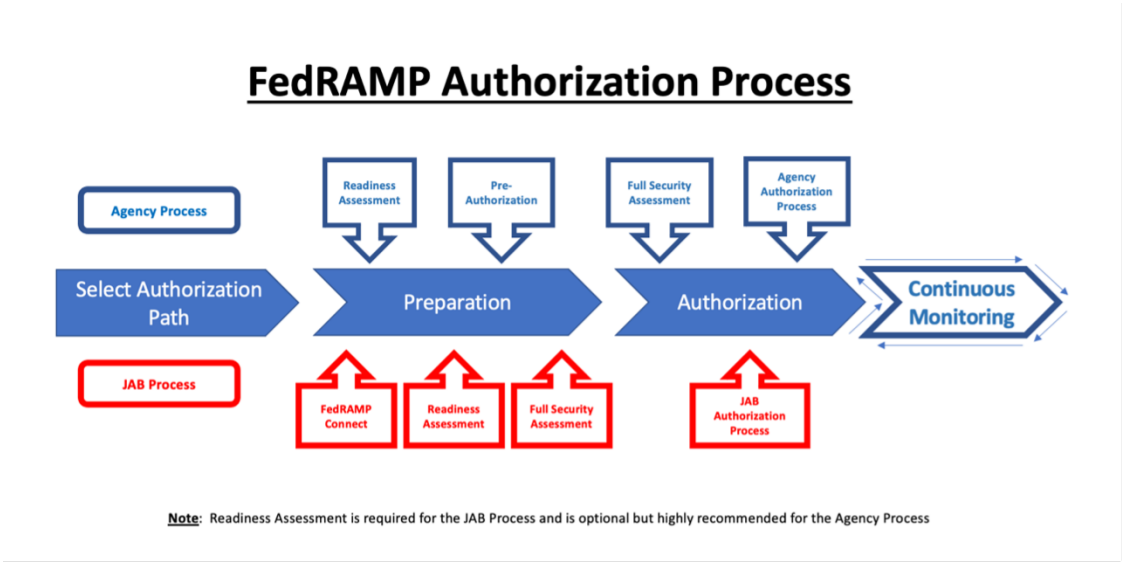

Figure 1: FedRAMP processes before 20x

2.2.3 20x, Looking Backwards and Forwards

3 Solution

Given the history and context of FedRAMP's Continuous Monitoring Program, themes from 20x criticism strongly suggest a winning architecture requires stakeholders

easily collaborate in a technology that underpins a robust process. People, process, and tools must be combined; the latter two cannot be tacked on later. This section describes the recent history of transparency services and how the mutual monitoring architecture is a foundation to this balance of people, process, and tools.

3.1 Transparency Services for Other Use Cases

The first and most notable use case for transparency services is Certificate Transparency. By 2011, Google had decided, in the wake of the DigiNotar certificate authority breach, that there were no acceptable existing solutions to detect misuse of web server certificates. So Laurie and a team of engineers decided the best solution was to"[create] a log of all certificates issued that does not need to be trusted because it is cryptographically verifiable ... [and] allows clients to check that certificates are in the log, and servers can monitor the log for misissued certificates" (2014, p. 4). There were a variety of alternatives, to be tried in isolation or combination, such as certificate pinning, centralized certificate notaries, DNSSEC, and even solutions implemented with Bitcoin, but all presented different downsides and tradeoffs that did not meet the mark.[10] The world's web browsers could not abide any latency, and decision-making could not be made with these end users' browsers. Browsers still had to check the logs however, and most importantly, interested intermediary parties (e.g. other certificate authorities, site operators, researchers) need to check the log. All the same, any one party from either category should know they have all seen the same log (Laurie, 2014, p. 7). Even in this early stage, Laurie and his colleagues deployed several log instances to achieve this goal, with other organizations pledging to deploy their own experimental instances, as he imagined other novel use cases early on (2014, pp. 809). By 2025, there are two major versions of the architecture (IETF RFC 6962 and RFC 9162), six organizations with public logs used by major browsers (Chrome, Firefox, and Safari) to verify website certificates before a browser effectively communicates with a valid, but not yet sufficiently trusted, web server encryption certificate.

[10] Despite the similarity to general-purpose blockchains such as Bitcoin, Laurie was explicit in using a purpose-built alternative for Google's security use case, after much research and experimentation. In his own words, "[a]part from being an extremely costly solution (in terms of wasted energy, in perpetuity), it also introduces new trusted third parties (those who establish the "consensus" in the block chain) and has no mechanism for verification" (2014, p. 4).

After certificate transparency proved successful, implementers applied it to other security use cases, like improved digital signature publication for software supply chain monitoring. The Sigstore project, and its publicly available, Internet-scale Rekor log instance, allows developers to use "a transparency log-backed signing repository with minimal friction for integration, while maintaining reasonable security guarantees" (Newman, Meyers, & Torres-Arias, 2022, p. 2365). At the time of this writing, the registries of open-source libraries for NodeJS and Python, among the largest programming language ecosystems in the world, integrate Sigstore in their package signature verification. Another major programming language ecosystem, Go, built a similar, but different, implementation of a transparency log for their open-source registry of software libraries (Hockman, 2019).

3.2 Mutual Monitoring Transparency Service

To transform FedRAMP's continuous monitoring to mutual monitoring, cloud service providers, auditors, and agency customers must coalesce around tools that consistently orchestrate processes. The foundational building block for this consistency is the architecture specification. Although the specification is highly applicable to FedRAMP use cases, the specification is generic and not particular to FedRAMP. The sections below will highlight key elements of the full specification, included in Section 6.1, and relate it to FedRAMP's specific needs.

3.2.1 Document Format, Conventions, and Terminology

The mutual monitoring specification intentionally approximates, but does not explicitly use, the format that the Internet Engineering Task Force (IETF) prefers for its consensus and standardization process (2023). Given this stage in the research, it is premature to formally publish a draft as part of the Request for Comment process, and becomes the intellectual property of the IETF once submitted. Nonetheless, this specification is customizing a generic architecture from another IETF specification, so it is prudent to approximate this format for possible publication as an IETF Internet Draft at a later date.

This document extends and customizes the IETF Supply Chain Integrity, Transparency, and Trust (SCITT) Working Group's SCITT Architecture specification (2025). The SCITT architecture is distinct, but has significant overlap from the latest and

original Certificate Transparency specifications, which are also established IETF standards (RFC 9162 and IETF RFC 6962, respectively). Moreover, approximating the IETF format with a tentative plan for possible IETF publication makes it approachable to implementers of related standards and the underlying normative references for transparency service building blocks, this approach is the most convenient.

As it is approximating IETF style, it is important to call out the conventions and terminology. For an effective specification, not just for transparency services, this specification uses RFC 2119 keywords, which many standards authors outside of IETF have adopted as well. The specification also makes heavy use of capitalized terminology itemized in the terminology section, like other IETF documents, and refers the reader to the normative definitions elsewhere if possible. As is good practice, this specification references upstream normative documents, and does not repeat or reframe those sources. This specification only adds information to extend those upstream references.

3.2.2 Use Cases

Like other IETF drafts, crisp, relevant use cases are integral to an effective specification. Although seemingly generic, these two use cases in this section of the document are specifically chosen for their relevance to FedRAMP and an improved alternative to the current continuous monitoring process.

As explained in more detail in Section 2.2.2, capable, successful cloud service providers who perform continuous monitoring well require a solid foundation in inventory management. Incomplete coverage, inconsistency, and poor labelling are not uncommon for cloud service providers of all sizes and maturiy in the current FedRAMP process. Having auditable, digitally signed records from a provider of its inventory sent for each creation, modification, and deletion event will mitigate all three of these challenges in inventory management. Additionally, current third-party auditors for FedRAMP are very familiar with the necessity and scanning techniques to detect publicly available infrastructure, potentially the creation, modification, or deletion of inventory items that cloud service provider did not report. This possible delta, or potential lack thereof, is an easily understandable for measuring inventory coverage as part of the quantitative framework.

Similarly, the configuration management use case is foundational to capable, suc-

cessful cloud service providers who perform well in the current continuous monitoring process. In the case of FedRAMP, this use case builds upon the previous inventory management use case. During annual assessments, and particularly for significant change requests, providers and auditors must work with FedRAMP PMO staff and the customer agency to articulate what changes happen to the system for new or updated components of a cloud service. This approach allows automated monitoring and the use of tags to map inventory to configuration changes and vice versa.

These use cases start simple, but the reader can consider advanced scenarios that realize the mutual monitoring flow. The primary scenario is for a cloud service provider to contract with one or more third-party auditors to monitor their infrastructure. For a more advanced scenario with mature adoption that reflects "fuller" mutual monitoring, the cloud provider can play the role of the auditor in later interactions: they may condition permission for access to more detailed security information for a new auditors or potential customer agency based upon their scored performance of that infrastructure that wishes to receive the provider's more detailed security data. A "leveraged" cloud service provider (i.e. a the cloud provider that is vendor to a downstream cloud provider) can condition access to their security data upon the performance of this new cloud provider with their new infrastructure, rather than a centralized government review scoped to only federal and military staff.

3.2.3 Architecture Components

For the transparency service to be robust, it is important that it has a modular architecture to account for different performance tradeoffs and flexibility to only deploy the right components for a given use case. This section of the specification describes the components accordingly, inspired by the SCITT Architecture: the core transparency service and optional adjacency services.

The core transparency service contains sub-components to implement the minimally viable capabilities of an Append-Only Log. The first necessary sub-component is the Registration Policy API, which defines the list of allowed identities (in the form of X.509 digital certificates) permissible for signing Statements. If the Issuer's signing certificate, whether for a cloud provider or auditor, is not allowed in the Registration Policy, Registration fails. In this way, Issuer authentication and authorization originates from the Statement, not bespoke API mechanisms.

When Issuers use another sub-component, the Submission API, any other form of authentication or authorization is not mandatory, simplifying integration. This API does not have to immediately return a receipt (i.e. a Statement countersigned by the Transparency Service itself). To support high throughput, the service will return a task ID and status for the client software, the Relying Party, to poll for. The Relying Party can then use the Entry API to look up tasks or existing Statements after Registration.

The final sub-component of the core is the Entry API. This final sub-component is to look up registered records. The Append-Only Log allows for bulk lookups to "replay the log" for consistency proofs (no tampering has occurred on the sequence of statements about inventory or configuration items). More commonly, Relying Parties will perform inclusion proofs (lookups for individual records is in the log to confirm they exist at a particular order in the sequence). As mentioned above, the Entry API also implements a task lookup functionality for Relying Parties to poll for the status of Registration for a given Statement. By combining all three sub-components, cloud service providers or auditors can check submission requirements, submit, and look up existing records for proof of existence.

One important consideration for scaling this architecture to efficiently process millions of Statements is Adjacent Services to store and query the full payload of the data independently from the core Transparency Service. In a simpler version of the architecture, the whole inventory or configuration record is signed and submitted. With this more modular architecture, the Relying Party opts to submit the payload itself to an Adjacent Storage Service. The service will store the raw data of payload, and return a hash formed from key record elements (the inventory identifier or configuration identifier). The Adjacent Search Service will be deployed with the Storage Service to perform reverse lookups for query matches and returning the hash that positively matches the arguments for queries. This keeps the size of the signed payload of the Statement lean and custom or advanced query features out of the high-bandwidth core system for submitting Statements as well as only performing consistency and inclusion proofs.

3.2.4 Flows, Example Statements, and the Quantitative Framework

The flow section and example statements secton of the appendix bring the architecture's building blocks together to demonstrate how multiple parties produce and consume measurements using a simple quantitative framework. In the data flows of the specification, a reader can understand how a cloud service provider integrates an existing inventory management system. As an Issuer, the cloud provider uses its Relying Party software to submit the original Statement (an inventory or configuration management event in the Open Cybersecurity Schema Format) to the cloud provider's own Adjacent Storage Service, which then pushes indexed fields to cloud provider's Adjacent Search Service, and returns the hash of the key fields. The Relying Party then uses its Certificate and Signing Key to digitally sign the hash and submit it to the cloud service provider's Transparency Service and the auditor's Transparency Service. The cloud service provider's Relying Party waits briefly for the Receipt of Registration from the auditor's transparency service. Once it receives that, it adds a new Transparent Statement, embedding the Receipt into the unprotected header of the original Signed Statement (with a hash as payload, not including the Receipt that did not yet exist). This approach allows the cloud provider to verifiably prove it detected the inventory event and had an auditor countersign it.

At this stage, the auditor's infrastructure will look for any inventory or configuration event that is anomalous and not initially reported by the cloud provider by checking provider's Adjacent Search Service and any hashes returned to confirm a finding that is not a false positive. If it detects changes the cloud provider made without notice, it appends Relying Party software uses its own key to make a record of this anomaly. Periodically, the auditor service will Register measurement events with quantitative measurements with the number of valid cloud provider records divided by the sum of cloud provider records and auditor findings from the epoch (i.e. when the provider registered its first inventory or configuration event) by sorting records based on the Issuers' signing keys.[11]

[11] At this time, the quantitative framework only measures from the epoch, or the first successful Registration of a Statement by a cloud provider in the auditor's Transparency Service, until present. In future designs, for a more complex and adaptive quantitative framework, the auditor's Relying Party can introspect its own Registration Policy to determine ad hoc requirements for the measurement payload, such a custom time range, freshness, or filtering requirements.

For a customer agency building dashboards or analytics software, their Relying Party software can read the whole history of the auditor's Append-only Log or filter only on measurement records, allowing it to have a verifiable source of metrics for a cloud provider. As the ecosystem stabilizes, a customer agency can aggregate different measurements from multiple third-party auditor services, with each with different specialties or niches, for a more robust assessment. All parties can change roles conditionally from their vantage point as well, such they can use this framework to mutually monitor each other.

4 Evaluation

4.1 Method and Results

4.2 Limitations and Future Work

4.3 Conclusion

5 References

117th Congress. (2022). *H.r.7776 - james m. inhofe national defense authorization act for fiscal year 2023.* Retrieved 2025-07-22, from https://web.archive.org/web/20250415062420/https://www.congress.gov/117/bills/hr7776/BILLS-117hr7776enr.pdf#page=1055

Aceto, G., Botta, A., de Donato, W., & Pescapè, A. (2013, June). Cloud monitoring: A survey. *Computer Networks*, *57*(9), 2093-2115. Retrieved from http://dx.doi.org/10.1016/j.comnet.2013.04.001 doi: 10.1016/j.comnet.2013.04.001

Aldribi, A., Traore, I., & Letourneau, G. (2015, August). Cloud slicing a new architecture for cloud security monitoring. In *2015 ieee pacific rim conference on communications, computers and signal processing (pacrim)* (p. 18-22). IEEE. Retrieved 2025-05-24, from http://dx.doi.org/10.1109/PACRIM.2015.7334802 doi: 10.1109/pacrim.2015.7334802

Bashir, I. (2022). *Blockchain consensus: An introduction to classical, blockchain, and quantum consensus protocols* (1st edition ed.). Apress L.P. Retrieved 2025-07-20, from https://learning.oreilly.com/library/view/blockchain-consensus/9781484281796/

Birkholz, H., Delignat-Lavaud, A., Fournet, C., Deshpande, Y., & Lasker, S. (2025). *An architecture for trustworthy and transparent digital supply chains* (Internet-Draft). Retrieved 2025-06-02, from https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/12/

Carvallo, P., Cavalli, A. R., Mallouli, W., & Rios, E. (2017). Multi-cloud applications security monitoring. In *Green, pervasive, and cloud computing* (p. 748-758). Springer International Publishing. Retrieved from http://dx.doi.org/10.1007/978-3-319-57186-7_54 doi: 10.1007/978-3-319-57186-7_54

Center for Internet Security. (2024). *Cis critical security control 7: Continuous vulnerability management* (v8.1 ed.). Retrieved 2025-07-20, from https://web.archive.org/web/20250523105159/https://www.cisecurity.org/controls/continuous-vulnerability-management

Cloud Security Alliance. (2021). *The evolution of star: Introducing continuous auditing.* Retrieved 2025-07-20, from https://cloudsecurityalliance.org/download/artifacts/evolution-of-star-introducing-continuous-auditing

Curran, J. (2025). *Fedramp officials detail planned unwinding of continuous monitoring.* Retrieved 2025-07-23, from https://web.archive.org/web/20250420040518/https://www.meritalk.com/articles/fedramp-officials-detail-planned-unwinding-of-continuous-monitoring/

Dempsey, K. L., Chawla, N. S., Johnson, L. A., Johnston, R., Jones, A. C., Orebaugh, A. D., … Stine, K. M. (2011). *Information security continuous monitoring (iscm) for federal information systems and organizations*. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-137 doi: 10.6028/nist.sp.800-137

Department of Defense. (2023). *Federal risk and authorization management program moderate equivalency for cloud service provider's cloud service offerings.* Department of Defense. Retrieved 2025-07-19, from https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf

Federal Chief Information Officer. (2011). *Security authorization of information systems in cloud computing environments.* Retrieved 2025-07-20,

from https://web.archive.org/web/20250401120534/https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf

FedRAMP. (2021). *Fedramp turns 10!* Retrieved 2025-07-22, from https://web.archive.org/web/20250413100853/https://www.fedramp.gov/blog/2021-12-08/FedRAMP-Turns-10/

FedRAMP. (2023). *Fedramp announces the passing of the fedramp authorization act!* Retrieved 2025-07-22, from https://web.archive.org/web/20250708095421/https://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/

FedRAMP. (2024a). *The missing piece of our modernization puzzle: The fedramp platform.* Retrieved 2025-07-22, from https://web.archive.org/web/20250523044856/https://www.fedramp.gov/2024-09-03-the-missing-piece-of-our-modernization-puzzle-the-fedramp-platform/

FedRAMP. (2024b). *The next phase of fedramp.* Retrieved 2025-07-22, from https://web.archive.org/web/20250624195908/https://www.fedramp.gov/2024-07-26-the-next-phase-of-fedramp/

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

FedRAMP. (2025a). *Fedramp in 2025.* Retrieved 2025-07-22, from https://web.archive.org/web/20250522223739/https://www.fedramp.gov/2025-03-24-FedRAMP-in-2025/

FedRAMP. (2025b). *What is fedramp?* Retrieved 2025-07-20, from https://web.archive.org/web/20250623215527/https://help.fedramp.gov/hc/en-us/articles/27700231586459-What-is-FedRAMP

FedRAMP. (2025). *Who is responsible for the cloud security controls?* Retrieved 2025-07-20, from https://web.archive.org/web/20250324200835/https://help.fedramp.gov/hc/en-us/articles/27700955089563-Who-is-responsible-for-the-cloud-security-controls

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

Hakani, D., & Mann, P. S. (2022, December). A comprehensive survey on cloud security mechanisms. In *2022 international conference on automation, computing and renewable systems (icacrs)* (p. 471-475). IEEE. Retrieved from http://dx.doi.org/10.1109/ICACRS55517.2022.10028990 doi: 10.1109/icacrs55517.2022.10028990

Hockman, K. (2019). *Module mirror and checksum database launched.* Retrieved 2025-07-23, from https://web.archive.org/web/20250430145617/https://go.dev/blog/module-mirror-launch

IETF. (2023). *Choosing a format and tools.* Retrieved 2025-07-23, from https://web.archive.org/web/20241014141737/https://authors.ietf.org/choosing-a-format-and-tools

Information security, cybersecurity and privacy protection — Information security management systems — Requirements (Vol. 2022; Standard). (2022). Geneva, CH: International Organization for Standardization.

Laurie, B. (2014, August). Certificate transparency: Public, verifiable, append-only logs. *Queue*, *12*(8), 10-19. Retrieved 2025-05-24, from https://dl.acm.org/doi/pdf/10.1145/2668152.2668154 doi: 10.1145/2668152.2668154

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

Majumdar, S., Chawla, G. S., Alimohammadifar, A., Madi, T., Jarraya, Y., Pourzandi, M., … Debbabi, M. (2022, July). Prosas: Proactive security auditing system for clouds. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2517-2534.

Retrieved from http://dx.doi.org/10.1109/TDSC.2021.3062204 doi: 10.1109/tdsc.2021.3062204

Majumdar, S., Madi, T., Wang, Y., Tabiban, A., Oqaily, M., Alimohammadifar, A., … Debbabi, M. (2019). *Cloud security auditing*. Cham, Switzerland: Springer Nature. Retrieved 2025-05-23, from https://link.springer.com/book/10.1007/978-3-030-23128-6

Metheny, M., & Krush, W. (2017). *Federal cloud computing: The definitive guide for cloud service providers* (Second Edition ed.). Elsevier Science and Technology Books, Inc.

Newman, Z., Meyers, J. S., & Torres-Arias, S. (2022, November). Sigstore: Software signing for everybody. In *Proceedings of the 2022 acm sigsac conference on computer and communications security* (p. 2353-2367). ACM. Retrieved from http://dx.doi.org/10.1145/3548606.3560596 doi: 10.1145/3548606.3560596

NIST. (2020). *Security and privacy controls for information systems and organizations* (Tech. Rep. Nos. NIST Special Publication (SP) 800-53, Rev. 5). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved 2025-06-04, from http://dx.doi.org/10.6028/NIST.SP.800-53r5 doi: 10.6028/nist.sp.800-53r5

ORock. (2021). *Why fedramp matters to the private sector.* Retrieved 2025-07-19, from https://orocktech.com/blog/why-fedramp-matters-to-the-private-sector/

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. *Procedia Computer Science, 110*, 465-472. Retrieved from http://dx.doi.org/10.1016/j.procs.2017.06.124 doi: 10.1016/j.procs.2017.06.124

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/

Torkura, K., Sukmana, M. I., Cheng, F., & Meinel, C. (2021, March). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security, 102*,

102124. Retrieved from http://dx.doi.org/10.1016/j.cose.2020.102124 doi: 10.1016/j.cose.2020.102124

Waterman, P. (2025). *Ongoing q&a for 20xp1 formal release standards.* Retrieved 2025-07-22, from https://web.archive.org/web/20250724033347/https://github.com/FedRAMP/community/discussions/28#discussioncomment-13537935

6 Appendix

6.1 Mutual Monitoring Architecture

The complete architecture specification is accessible at aj-stein.github.io/conmotion. Additionally, readers can download a copy of the specification in PDF format for offline reading.

6.2 20x Forum Archive

In June 2025, PMO staff archived posts and subsequently disabled public access to 20x forums created before consolidating the original four discussion boards into one, the FedRAMP/community discussion board.

To facilitate research for this project, I wrote a Python script to export all this public domain content from the four pre-existing discussion boards into a complete archive in Markdown format. This archive in a subdirectory of the github.com/aj-stein/practicum_conmon_analysis repository.

6.3 Coded 20x Forum Posts

As part of this research, I reviewed all archived posts from the 20x forum, as described in Section 6.2 and coded each one to confirm if there was relevant criticism for pre-20x FedRAMP processes, specifically continuous monitoring. If so, I organized each one into one or more thematic buckets to inform the design of the mutual monitoring service.

The coded posts labelled by theme can be found in this GitHub Gist.