PriMera Scientific Engineering
Volume 7 Issue 3 September 2025
DOI: 10.56831/PSEN-07-218
ISSN: 2834-2550

PriMera Scientific Publications

Governing Cloud and AI: Integrating Major Platforms with U.S. Federal Compliance Frameworks and Regulatory Instruments

Type: Research Article
Received: July 27, 2025
Published: August 22, 2025

Citation:
Jada-Ann Riggins. "Governing Cloud and AI: Integrating Major Platforms with U.S. Federal Compliance Frameworks and Regulatory Instruments". PriMera Scientific Engineering 7.3 (2025): 02-12.

Jada-Ann Riggins*

Cybersecurity Leadership, Capitol Technology University, USA

***Corresponding Author:** Jada-Ann Riggins, Capitol Technology University, 11301 Springfield Rd, Laurel, MD, USA.

Abstract

The growing adoption of cloud platforms, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), has introduced new complexities in aligning enterprise workloads with federal compliance frameworks. This paper presents a comparative analysis and practical alignment model that integrates these major cloud service providers with the Federal Risk and Authorization Management Program (FedRAMP), Federal Information Processing Standards (FIPS) 199/200, the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), and the directives established by Executive Order 14110 on the safe, secure, and trustworthy use of Artificial Intelligence. The study develops a multi-dimensional control mapping methodology tailored to ensure technical interoperability, compliance readiness, and risk transparency. Through structured evaluation of service categories, native controls, and governance mechanisms, the paper delivers a unified compliance architecture designed to support secure and auditable cloud deployments in federally regulated environments. Findings contribute actionable insights for IT leaders, cloud architects, and policymakers by offering a scalable and standards-based roadmap for AI-driven cloud governance.

Keywords: cloud compliance; fedramp; fips 199; fips 200; nist ai rmf; executive order 14110; aws; azure; gcp; artificial intelligence governance; cloud security; risk management

Abbreviations

AI RMF - Artificial Intelligence Risk Management Framework.
FIPS - Federal Information Processing Standards.
FedRAMP - Federal Risk and Authorization Management Program.
GCP - Google Cloud Platform.
AWS - Amazon Web Services.
RMF - Risk Management Framework.

Introduction

Rapid expansion of cloud and artificial intelligence (AI) technologies spanning across sectors has produced enhanced agility while simultaneously introducing new layers of risk and regulatory complexity. Organizations are facing increased pressure to implement standardized security controls and governance practices across their heterogeneous cloud environments. Ethical, secure, and compliant use of AI has also become a growing area of concern. These demands are codified in several key regulatory instruments:

- ***Federal Risk and Authorization Management Program (FedRAMP):*** Standardizes cloud security assessments for federal systems (FedRAMP, 2023).
- ***Federal Information Processing Standards (FIPS) 199/ 200:*** Define system categorization and baseline security controls (NIST, 2022).
- ***The NIST AI Risk Management Framework (AI RMF):*** Guidance for development of trustworthy AI systems (NIST, 2023).
- ***Executive Order 14110 (EO 14110):*** Underscores federal priorities for ensuring the safe, secure, and responsible development and use of AI technologies in critical infrastructure (White House, 2023).

Together, these instruments define the emerging standards for security, compliance, and operational trust in cloud and AI-powered environments. This paper proposes a structured methodology for mapping and aligning core services from leading cloud providers (AWS, Azure, and GCP) to highly utilized regulatory instruments. Furthermore, this paper responds to these regulatory instruments by providing a direct pathway for secure, compliant, and AI-ready cloud deployments.

Problem Statement

Significant technological advancements have been made over the last two decades, enabling the U.S. to leap ahead to the forefront of technological innovation in cloud computing and AI. Despite rapid adoption of these technologies, misconfigurations are the most prevalent factor contributing to numerous cybersecurity incidents. These vulnerabilities have resulted in substantial regulatory penalties and fines for multiple organizations.

Misconfigurations have been cited on countless occasions as the significant source of incidents that have led to security breaches. The prevalence of these vulnerabilities underscores the urgent need for comprehensive and robust governance frameworks to mitigate risks and protect sensitive information.

A 2025 study analyzing the Cloud Security Alliance (CSA) Top Threats Dataset and the Verizon Data Breach Investigations Report (DBIR) identified identity and access management (IAM) errors (183 instances) and exposed APIs (156 cases) as the most frequent misconfigurations, resulting in average financial losses of $7.6 million and regulatory fines of $2.5 million per breach (Metibemu et al., 2025). These findings underscore a persistent challenge: digital transformation is outpacing the modernization of compliance architectures.

The general problem is that many organizations have not developed integrated strategies to align multicloud deployments with the requirements of federal frameworks such as FedRAMP, FIPS 199/200, Executive Order 14110, and the NIST AI Risk Management Framework. The specific problem is consistent misalignment of cloud-native services across AWS, Azure, and GCP with these regulatory instruments, which have resulted in fragmented compliance approaches and increased governance complexity.

A gap exists in the literature regarding the practical, comparative mapping of cloud-native services to these regulatory instruments, particularly in light of the layered, service-specific architectures of major cloud platforms. While previous studies have addressed individual risks or compliance frameworks in isolation, this study proposes a cross-platform, unified control mapping matrix focused specifically on U.S. federal compliance mandates to address real-world alignment challenges in AI and cloud infrastructure governance.

Significance of the Paper

A 2024 compliance study examining organizations revealed that over 60% of organizations deploying AI in cloud environments simultaneously cited regulatory compliance as a primary operational challenge in their deployments (Molnar & Sabodashko, 2024). Respectively, the literature has revealed that inconsistencies in native cloud controls and shared responsibility models have proven challenging when applying regulatory frameworks across cloud providers uniformly (Alkhatib et al., 2025).

This paper addresses those challenges by introducing a comparative control alignment methodology that enables technical, governance, and leadership teams to proactively design AI-capable, compliance-ready architectures aligned with federal risk management standards.

This research holds practical value for cybersecurity leaders, practitioners, students, policy makers, and academics alike. The Riggins Cloud Governance Control Integration Matrix (Riggins-CGCIM), introduced in this study, is a novel and practical tool for assessing how cloud services align with the control families outlined in regulatory frameworks. It supports precise alignment, promotes transparent accountability, and improves the reliability of system design under regulatory scrutiny. The Riggins-CGCIM has the potential to significantly impact the field of cloud compliance and AI governance by providing a standardized and replicable model for assessing and ensuring compliance in cloud deployments.

The contribution of a scalable and standards-based framework, as presented in this paper, is timely and relevant. Furthermore, adding to the growing body of applied research in cloud compliance and AI governance, serving both academic inquiry and real-world implementation.

Materials and Methods

This study employed a qualitative comparative architecture analysis to examine how native services from leading cloud providers (Amazon Web Services (AWS), Microsoft Azure (AZ), and Google Cloud Platform (GCP)) align with U.S. federal regulatory instruments namely, FedRAMP, FIPS 199/200, Executive Order 14110, and the NIST Artificial Intelligence Risk Management Framework (AI RMF). This approach is well-suited for complex, policy-driven technical environments where structured comparisons of system architectures are necessary to evaluate regulatory alignment across platforms (Yin, 2018).

Literature Review Strategy

In the present study, a structured literature review was implemented to ground the analysis in current research, challenges, and best practices in cloud compliance and AI governance. Academic databases including IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink were searched using Boolean queries with combinations of terms such as:

("cloud compliance" AND "FedRAMP"), ("FIPS 199" OR "FIPS 200" AND "cloud security"), ("NIST AI RMF" AND "AI governance"), ("Executive Order 14110" AND "artificial intelligence"), and ("AWS" OR "Azure" OR "GCP" AND "compliance framework")

Inclusion criteria focused on peer-reviewed articles, government whitepapers, and technical reports published between 2018 and 2025. Seminal sources were utilized to enhance understanding and provide historical context regarding the present subject matter. A total of sixty-three sources were identified, of which 42 met the criteria for relevance, credibility, and direct applicability to the mapping objectives of this research.

Theoretical Framework

Systems Theory and Dynamic Capabilities Theory informed the analytical framework of this study.

Systems Theory (Bertalanffy, 1968) conceptualizes technological ecosystems as interconnected, interdependent components. This perspective supports the present study's focus on integrating compliance and governance interdependent structures holistically

across interconnected services, controls, and regulatory expectations. Key concepts such as system interoperability and feedback loops guide the architectural evaluation of how cloud-native controls support continuous compliance across platforms.

Dynamic Capabilities Theory (Teece et al., 1998) frames organizational capacity to integrate, reconfigure, and align IT systems in response to regulatory shifts. This theory supports the rationale for a flexible, cross-provider control mapping matrix that can adapt to evolving mandates, such as Executive Order 14110, and AI-specific governance functions in the NIST AI RMF. Core concepts applied include *sensing* (identifying compliance gaps), *seizing* (architecting responsive controls), and *transforming* (embedding compliant workflows).

Theory selection was based on the theoretical ability to guide strategic integration across diverse socio-technical systems. These theories emphasize responsive architecture and governance agility, aligning directly with the research objective of the present study.

Data Sources

Primary data sources included:

- ***Cloud Service Provider (CSP) Documentation:*** security and compliance whitepapers, shared responsibility models, and control implementation guides for AWS, Azure, and GCP.
- ***Regulatory Instruments:***
  - FedRAMP security controls (Rev. 5)
  - FIPS 199/200 publications (NIST SP 800-60 and SP 800-53),
  - Provisions from Executive Order 14110.
- ***NIST AI RMF:*** Trustworthiness functions including Map, Measure, Manage, and Govern (NIST, 2023).

These documents were systematically reviewed to extract control categories, service alignment requirements, and implications for AI governance.

Mapping Methodology

The ***Riggins Cloud Governance Control Integration Matrix (Riggins-CGCIM)*** was developed as a central tool for mapping CSP-native services across Azure, AWS, and GCP to federal regulatory instruments. The study methodology involved four steps:

1. ***Service Identification:*** Core services across compute, storage, networking, AI/ML, and security domains were selected across Azure, AWS, and GCP.
2. ***Control Extraction:*** Baseline controls and trustworthiness functions were extracted from FedRAMP, FIPS 199/200, EO 14110, and NIST AI RMF.
3. ***Mapping and Alignment:*** Each service was evaluated against applicable controls and governance requirements using a comparative scoring and classification model.
4. ***Gap Analysis:*** The framework highlighted:
   a. Control overlaps.
   b. Deficiencies.
   c. Strengths across platforms.
   d. Actionable insights for architecture alignment.

This methodological approach provides a replicable model for compliance validation. This approach thus provides a practical blueprint for practitioners navigating the regulatory complexities of AI-enabled cloud infrastructures.

Literature Review

The rapid adoption of cloud technologies and artificial intelligence has prompted increased attention to regulatory compliance and governance as a core challenge for secure digital transformation. Recent studies have consistently revealed organizations face substantial hardships with aligning cloud-native services with federal compliance mandates, especially when managing complex, multi-cloud environments (Zhou et al., 2020; Alkhatib et al., 2023).

This is compounded by variability in platform-specific control implementations and the absence of standardized cross-platform compliance models. These findings underscore the applicability of this study, which aims to develop a unified framework for aligning cloud providers with federal standards, including FedRAMP, FIPS 199/200, Executive Order 14110, and the NIST AI Risk Management Framework (AI RMF).

Several seminal works have examined the limitations of cloud compliance and governance strategies in isolation. For example, in Marinos and Briscoe's (2009) study, they examined the lack of transparency in shared responsibility models. The study concluded that the ambiguity in interpreted controls poses significant barriers to effective risk management across cloud providers.

Similarly, Agarwal et al. (2022) explored compliance-as-code across hybrid and public cloud environments. This study highlights that verification and management of cybersecurity controls remain fragmented. This is a result of the heterogeneity of standards and environments. The findings presented in this study underscore the importance of standardized, interoperable compliance mechanisms across cloud providers.

These insights directly inform the design of the Riggins Cloud Governance Control Integration Matrix proposed in this research (Agarwal et al., 2022). Research on the application of FedRAMP and FIPS in cloud ecosystems has focused primarily on certification processes and predefined baselines. For example, NIST Special Publication 800-53 Rev. 5 and FedRAMP's Moderate Baseline have been evaluated for their effectiveness in high-assurance environments (Ross et al., 2020).

However, much of the literature stops short of providing practical, cross-cloud mappings of native services to these controls, leaving a gap in actionable guidance for implementation teams. The present study aims to address this gap by developing a relative control alignment model that bridges technical configurations with policy expectations.

In the context of Executive Order 14110 and the NIST AI Risk Management Framework (AI RMF), AI governance has emerged as a critical area of inquiry. Literature by Li et al. (2021) and Herrera-Poyatos et al. (2025) explores the challenge of operationalizing trustworthiness in AI. These works highlight persistent issues such as aligning accountability, mitigating bias, wokeness, and ensuring explainability, particularly within cloud-based deployments.

The present study builds upon these foundations by integrating the NIST AI RMF's core functions (Map, Measure, Manage, Govern) into the practical compliance model presented in subsequent sections that supports secure, AI-ready cloud infrastructure.

Despite a growing body of work addressing individual components of the compliance landscape, few studies have attempted to synthesize a unified, cross-framework methodology that considers the full spectrum of controls relevant to U.S. regulatory instruments.

The lack of comparative architectures that align cloud provider services with evolving regulatory frameworks represents a critical literature gap. By addressing this intersection through structured control mapping, this research contributes a new layer of operational clarity to the practice of cloud and AI governance.

Results and Discussion

This section presents the comparative results of aligning AWS, Azure, and GCP native services with FedRAMP, FIPS 199/200, Executive Order 14110, and the NIST AI Risk Management Framework (AI RMF). Findings were organized through the Riggins Cloud

Governance Control Integration Matrix (Riggins-CGCIM), which serves as the central analytical tool for mapping provider-specific implementations to federal regulatory instruments.

FedRAMP Alignment

Each cloud platform demonstrates substantial support for baseline FedRAMP controls; however, depth and native tooling vary. AWS and Azure offer broad automation of audit and compliance reporting through tools such as AWS Audit Manager and Azure Compliance Manager, respectively.

GCP provides a similar function through Assured Workloads but lacks the out-of-the-box granularity found in its competitors. Discrepancies were also noted in how security assessments (CA-2) and continuous monitoring (CA-7) are operationalized, with Azure offering more integrated templates for structured assessments.

FIPS Categorization

FIPS 199/200 categorizes systems based on the principles of confidentiality, integrity, and availability (CIA). All three providers support encryption services and role-based access controls (RBAC/IAM), satisfying key confidentiality and integrity requirements. Azure's native tools (e.g., Key Vault, Policy, Sentinel) provide tight coupling between availability protection and policy enforcement.

AWS sustains key sovereignty for its users through CloudHSM, while GCP provides encryption maturity often through premium-tier services or third-party integrations. These notable yet comparable variations among each provider underscore the need for customized FIPS-based control configurations when designing multi-cloud architectures.

EO 14110 Alignment

Executive Order 14110 emphasizes the security, privacy, and public trust in high-risk infrastructure related to AI. In interpreting this directive, all providers offer foundational services (e.g., AI/ML platforms, data labeling, model deployment) but differ in how these services integrate with governance controls.

Azure leads with built-in Responsible AI dashboards and explainability tooling, while AWS and GCP depend more heavily on customizable models and third-party toolchains. This fragmented landscape presents challenges for the consistent application of policy and the automated documentation of AI governance practices.

NIST AI RMF Trustworthiness Functions

Each cloud provider demonstrates varying support across the NIST AI RMF's core functions:

- ***Map:*** All platforms support data lineage and model discovery, but only Azure currently offers end-to-end AI usage mapping.
- ***Measure:*** AWS SageMaker Clarify and Azure Responsible AI tools provide model bias and performance metrics. GCP's Explainable AI requires additional configuration.
- ***Manage:*** All providers support incident handling and model rollback, though Azure automates playbook generation more effectively.
- ***Govern:*** Only Azure embeds responsible AI guidance into the platform by default, whereas AWS and GCP require manual governance design and integration.

Observations and Platform Variations
The comparative analysis revealed key gaps, overlaps, and structural divergences

- ***Gaps:*** GCP lacks mature privileged identity management and integrated malware protection, often necessitating the use of third-party solutions.

- ***Overlaps:*** All platforms support core access control, encryption, and logging mechanisms, albeit with distinct implementation patterns.
- ***Variations:*** Azure demonstrated more integrated compliance tooling, while AWS emphasizes modular customization and GCP maintains strong interoperability through open APIs.

Implications and Governance Maturity

These findings suggest that achieving compliance maturity in AI-enabled cloud environments requires coordinated design decisions, control inheritance strategies, and platform-specific tuning. Control gaps and architectural fragmentation across providers complicate the standardization process. Organizations must adopt provider-agnostic mapping models that reflect both regulatory controls and trustworthiness objectives.

The Riggins Governance Model

The Riggins Cloud Governance Control Integration Matrix (Riggins-CGCIM) provides a structured, multidimensional approach for aligning cloud-native services with U.S. federal compliance frameworks, including FedRAMP, FIPS 199/200, Executive Order 14110, and the NIST AI Risk Management Framework (AI RMF). Unlike generalized reference architectures, the Riggins-CGCIM provides a provider-specific mapping that spans AWS, Azure, and GCP service offerings, aligning with key security and governance requirements.

Framework	*Control Category*	*AWS Services*	*Azure Services*	*GCP Services*	*Coverage Notes / Gaps*
FedRAMP	Access Control (AC)	IAM, Cognito, Control Tower	Azure AD, RBAC, Privileged Identity Mgmt	Cloud IAM, Identity-Aware Proxy	GCP lacks integrated privileged identity management; all enforce least privilege
FedRAMP	Audit and Accountability (AU)	CloudTrail, Config, Audit Manager	Monitor, Log Analytics, Purview	Cloud Audit Logs, SCC	Audit granularity varies; Azure offers richer native correlation
FedRAMP	System & Communications Protection (SC)	VPC, KMS, Shield	Virtual Network, Key Vault	VPC, Cloud Armor, KMS	All offer network encryption; Azure and AWS offer stronger DDoS bundling
FIPS 199/200	Confidentiality	Macie, S3 Encryption	Azure Information Protection Defender	Confidential VMs, CMEK	Encryption similar, but key control models differ; CMEK maturity varies
FIPS 199/200	Integrity	CloudHSM, CodeCommit	Azure DevOps, Purview	Cloud DLP, Artifact Registry	GCP lacks parity in code integrity tools; AWS strong with CodeCommit
FIPS 199/200	Availability	Route 53, CloudFront	Traffic Manager, Load Balancer	Cloud CDN, Global Load Balancing	GCP requires premium tier; AWS Inspector region-dependent
EO 14110	Secure AI Development	SageMaker Clarify, Model Monitor	Azure Machine Learning Responsible AI dashboard	Vertex AI Explainable AI	Azure and AWS offer richer monitoring; GCP maturing via Explainable AI

EO 14110	AI Risk Mitigation	CloudTrail, GuardDuty	Sentinel, Defender for Cloud	Security Command Center	Azure has mature threat visibility; GCP requires deeper tuning
EO 14110	Transparency & Documentation	SageMaker Model Registry, IAM	ML Ops, Data Catalog	AI Notebook Pipelines, IAM Roles	Azure provides stronger documentation pipelines; GCP less integrated
NIST AI RMF	Map	SageMaker Ground Truth	Data Labeling, ML Dataset registration	Vertex AI Data Labeling	All support training labeling; AWS has integrated human review tools
NIST AI RMF	Measure	CloudWatch Metrics, Model Monitor	Metrics Advisor, Monitor	Monitoring, AI Platform Pipelines	Metric fidelity varies; Azure excels in advisory tooling
NIST AI RMF	Manage	EventBridge, Step Functions	Logic Apps, Automation	Workflows, Cloud Scheduler	GCP orchestration weaker; Azure excels in automation integration
NIST AI RMF	Govern	Control Tower, Organizations	Blueprints, Policy	Resource Manager, Policy Intelligence	Azure strongest in native governance templates; GCP least mature

Table 1: Riggins Cloud Governance Control Integration Matrix (Riggins-CGICM).

Table 1 presents the Riggins Cloud Governance Control Integration Matrix (Riggins-CGCIM), which maps AWS, Azure, and GCP services against control categories drawn from four federal frameworks: FedRAMP, FIPS 199/200, Executive Order 14110, and the NIST AI RMF. The matrix adds a 'Coverage Notes / Gaps' column to highlight control maturity, integration limitations, and architectural strengths across providers. These insights guide enterprise teams in understanding cross-platform disparities and optimizing their compliance strategies.

This comparative model enables leaders, practitioners, policy makers and academics alike to identify where services meet or fall short of regulatory expectations and to design remediation pathways accordingly. The Riggins-CGCIM therefore serves as both a decision-support tool and a basis for institutionalizing control inheritance strategies, advancing cloud governance maturity, and ensuring AI-readiness in federally regulated cloud environments.

Conclusion

This study reinforces the need for standardized and interoperable governance frameworks to support AI-enabled workloads in multicloud environments. Through a structured comparative analysis, the Riggins Cloud Governance Control Integration Matrix (Riggins-CGCIM) was developed to align cloud-native services across AWS, Azure, and GCP with the control objectives of FedRAMP, FIPS 199/200, Executive Order 14110, and the NIST AI Risk Management Framework (AI RMF). While core FedRAMP and FIPS control mappings are well-supported across providers, significant disparities were found in AI-specific governance, auditability, and platform-native tooling.

The Riggins-CGCIM revealed that although foundational security mechanisms such as access control, encryption, and logging are universally present, their implementation differs in depth, automation, and maturity. The analysis in this study revealed Azure displayed the most remarkable native support for AI governance features (e.g., Responsible AI dashboards, policy blueprints). Simultaneously, AWS offered broader modular customization, and GCP trailed in privileged identity management and automation without third-party

integration.

Key Takeaways for Organizations and Cloud Leaders:

A. ***FedRAMP Alignment:*** All three platforms support baseline controls, but Azure and AWS deliver more integrated compliance tooling.
B. ***FIPS 199/200 Categorization:*** CIA triad support is foundational, though key management and availability protections vary in maturity.
C. ***EO 14110 Interpretation:*** Secure AI governance capabilities differ widely, Azure is strongest in native explainability and monitoring features.
D. ***NIST AI RMF Integration:*** Only Azure aligns natively with all four trustworthiness functions (Map, Measure, Manage, Govern).
E. ***Control Gaps:*** GCP lags in built-in privileged identity management, incident response playbooks, and SIEM integrations.
F. ***Governance Maturity:*** Organizations must consider architectural divergence when designing standardized, compliant infrastructures.
G. ***Control Inheritance:*** The Riggins-CGCIM aids in tracing how SaaS, PaaS, and IaaS components distribute governance responsibilities.
H. ***Decision-Support:*** The model helps practitioners anticipate regulatory mismatches and remediate design misalignments.
I. ***Scalability:*** The matrix allows for repeatable, enterprise-wide alignment across evolving workloads and mandates.
J. ***Policy Implications:*** The framework supports agencies in harmonizing compliance requirements and benchmarking CSP capabilities.

Discussion

These findings align with and extend previous works by Alkhatib et al. (2025) and Agarwal et al. (2022), who identified gaps in cloud-native compliance enforcement efforts. By integrating AI governance directly into control mapping exercises, this study moves beyond prior isolated evaluations and toward a unified, operationalized compliance framework as a direct response to fragmented compliance approaches and governance complexity. The structured comparison applied in this context, across cloud platforms, further advances the work of Li et al. (2023) and Herrera-Poyatos et al. (2025), who emphasized the challenge of embedding trustworthiness and explainability into cloud-based AI.

From a policy perspective, this research reinforces the need for centralized benchmarks and shared assessment tools. Without a unified framework like the Riggins-CGCIM, compliance teams must manually assess each platform's capabilities, introducing new risks such as delays, inconsistencies, and risk blind spots. For organizations, the Riggins-CGCIM provides an actionable roadmap to navigate evolving governance expectations, implement federal AI use cases, or manage supply chain risks in regulated environments.

Strengths and Limitations

A key strength of this study is the multidimensional alignment of CSP services with traditional security frameworks (FedRAMP, FIPS) and AI-specific governance regulatory instruments (EO 14110, AI RMF). However, limitations include the dynamic nature of cloud service offerings and regulatory interpretations, which may evolve after this analysis. Furthermore, the framework assumes a baseline of CSP documentation accuracy and availability, which may vary across implementations and regions.

Recommendations for Future Research

To build upon the Riggins-CGCIM and ensure its continued relevance, future research should pursue the following directions:

1. ***Operational Validation:*** Apply the matrix within live enterprise or government environments to assess its practical effectiveness and gaps in real-time compliance monitoring.
2. ***Tooling Integration:*** Develop API-driven software or dashboards to automate dynamic control mapping and compliance status

reporting.

3. ***Longitudinal Analysis:*** Track how changes in CSP service offerings and regulatory updates impact framework alignment over time.
4. ***Sector-Specific Extensions:*** Adapt the matrix for domain-specific regulations like HIPAA (healthcare), CJIS (law enforcement), or CMMC (defense).
5. ***Hybrid & Edge Scenarios:*** Extend the framework to include edge computing nodes, hybrid architectures, and non-traditional cloud topologies.
6. ***Cross-Border Compliance:*** Explore alignment with global governance models (e.g., GDPR, ISO/IEC 27001) in multi-jurisdictional deployments.
7. ***Governance Automation:*** Investigate how AI/ML can proactively identify misconfigurations or policy violations using the matrix as a control baseline.
8. ***Governance Culture Research:*** Study how organizational culture, leadership structure, and policy adoption impact control inheritance and compliance maturity.

By providing a repeatable and extensible framework, this study introduces new avenues for academic inquiry and practical implementation. It offers organizations a tangible method to align compliance priorities with technological realities and to build secure, trustworthy, and regulation-ready cloud architectures proactively.

Conflict of Interest

The author declares no conflict of interest.

Acknowledgements

This research received no specific funding and was conducted independently.

References

1. Agarwal V., et al. "Compliance-as-Code for Cybersecurity Automation in Hybrid Cloud". 2022 IEEE 15th International Conference on Cloud Computing (CLOUD) (2022): 427-437.
2. Alkhatib A, Shaheen A and Albustanji RN. "A comparative analysis of cloud computing services: AWS, Azure, and GCP". International Journal of Computing and Digital Systems 18.1 (2025): 1-15.
3. Evans DJ, Bond PJ and Bement AL. "Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)". Federal Information Processing Standards (2004).
4. Federal Risk and Authorization Management Program (FedRAMP). Rev 5 Baselines. Understanding Baselines and Impact Levels for FedRAMP® Authorizations (2023).
5. Gutierrez CM and Jeffrey W. "Minimum Security Requirements for Federal Information and Information Systems". Federal Information Processing Standards Publication (2006).
6. Herrera-Poyatos A., et al. "Responsible Artificial Intelligence Systems: A Roadmap to Society's Trust through Trustworthy AI, Auditability, Accountability, and Governance". Computers and Society (Cs.CY); Artificial Intelligence (Cs.AI); Machine Learning (Cs.LG) (2025).
7. Li B., et al. "Trustworthy AI: From Principles to Practices". ACM Computing Surveys 55.9 (2023): 1-46.
8. Marinos A and Briscoe G. "Community Cloud Computing". Proceedings of the 1st International Conference on Cloud Computin (2009): 472-484.
9. Metibemu OC., et al. "Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications". Journal of Engineering Research and Reports 27.3 (2025): 393-413.
10. Molnar V and Sabodashko D. "Comparative analysis of cybersecurity in leading cloud platforms based on the NIST framework". Journal of Scientific Papers "Social Development and Security 14.6 (2024): 68-80.

11. Ross WL and Copan W. "Security and Privacy Controls for Information Systems and organizations". NIST Special Publication 800-53 Revision 5, (2020) 800(53).
12. Tabassi E. "Artificial Intelligence Risk Management Framework (AI RMF 1.0)". National Institute of Standards and Technology 1 (2023).
13. Teece DJ, Pisano G and Shuen A. "Capabilities Building Through Dynamic Capabilities Approach". Management System for Strategic Innovation (1998): 13-44.
14. Von Bertalanffy L. "General System Theory: Foundations, Development, Applications". Leonardo 10.3 (1968): 248.
15. Yin RK. "Case Study Research and Applications: Design and Methods (6th ed.)". Sage Publication, Inc (2018).