International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cloud Governance Frameworks - An Empirical Analysis of AWS, Azure and Google Cloud Models

[1]Venkata Subramanya, [2]Sai Kiran Vedagiri

Submitted:01/06/2023 **Revised:**12/07/2023 **Accepted:**20/07/2023

Abstract: This paper has compared and contrasted the cloud governance systems of Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) through the mixed-method empirical viewpoint. The study compared maturity in governance, compliance system, security measures, automation, and policy enforcement frameworks on the three platforms. Structured surveys and interviews were used to gather primary data on cloud governance specialists, which was complemented by secondary analysis of published documentation and reports on the industry. The findings showed that AWS had the best governance maturity due to its automation of compliance, good security governance and well-defined policy management tools. Azure was next in line and it showed its capabilities of integrating with the enterprise and exercising centralized governance controls and especially so to organizations in the Microsoft ecosystem. Google Cloud demonstrated creativity in automation in security and intelligent threat detection, whereas it demonstrated relatively lower maturity in enterprise control and established compliance frameworks. The paper has highlighted the necessity to match the capabilities of platform governance with the organizational requirements and regulatory demands and especially in multi-cloud environments where platform governance architectures should be harmonized to achieve efficiency, security, and compliance.

Keywords: *Cloud Governance; AWS; Azure; Google Cloud; Compliance; Security Governance; Policy Enforcement; Multi-Cloud Strategy; Cloud Maturity Models.*

1. INTRODUCTION

The fast nature of cloud computing has transformed the current IT infrastructure where organizations have an increased ability to attain higher levels of scalability, operational agility and cost effectiveness. But with the growth of cloud environments, the necessity to have organized governance models emerged as urgent to provide security, regulatory adherence, cost management, and governance of uniformity in operation. Cloud governance is described as the strategic policies, processes, and controls used in regulating how cloud resources are managed, secured and optimized in an enterprise ecosystem. As Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) have become the major cloud service providers, the governance models of these tools have become a critical area of concern to any enterprise working through multi-cloud and hybrid architecture environments.

Each cloud platform proposes different governance tools, policy controls and automation frameworks, which have a bearing on the organizational cloud adoption and management strategies. The capabilities of AWS are broadly known to be mature in terms of governance and enforcement of policies and Azure is

[1]*Sr Software Developer & Architect*

(Independent Researcher)

[2]*Rackspace Cloud Services ,*

San Antonio, Texas, USA.

vvsskiran@gmail.com

orcid - 0009-0002-6760-8099

characterized by strong enterprise integration and centralized identity governance whereas GCP focuses on automated policy execution and AI-based security controls. Technology leaders have strategic considerations in spite of shared goals, governance maturity, ecosystems of tools, and compliance support.

This empirical paper sought to compare and contrast the cloud governance framework of AWS, Azure, and GCP based on the understanding of governance maturity, compliance models, security measures, and operational policies. This study aimed to determine the best practices, outline the platform-specific benefits, and reveal the problems of governance among enterprises through a mixed-method design based on the survey, interviews with experts, and the analysis of the documentation. The results can be used by the organizations that want to design the effective governance models according to their cloud adoption strategy and security demands in the fast-changing digital space.

2. LITERATURE REVIEW

Sharma (2020) studied the performance of Cloud Security Posture Management (CSPM) in a multi-cloud environment. The research found out that the enterprises, which implemented AWS, Azure, and Google Clouds at the same time, had to encounter the major problems regarding interoperability, centralized monitoring, and consistent implementation of a security policy. Sharma determined that CSPM tools enhanced security visibility and mitigation of risk greatly but needed strong integration strategies to surmount provider-specific security models diversity. The piece highlighted the necessity of smart, automated governance tools that would be able to handle heterogeneous cloud systems.

Singh and Sharma (2021) explored the topic of cloud governance using shared responsibility models. They claimed that good governance models should use shared responsibility concept to demystify the separation of responsibilities between cloud companies and consumers. Their study proved that security mispositions and compliance failures were largely due to lack of knowledge about the roles of governance among cloud stakeholders. The authors also pointed out that the governance models should keep up with multi-tier cloud systems in order to assist the scalable secure operations.

Goel (2021) made a comparative analysis of AWS, Azure and Google Cloud and paid attention to the governance scalability. The research results were the AWS provided the most mature governance services based on the comparison with the Azure, whereas GCP demonstrated the perspectives of automation and policy creation but needed additional maturity to be implemented on an enterprise level. The results of Goel revealed that the strength of platform-based governance played an important role in the enterprise cloud adoption strategy, especially in the hybrid and multi-cloud setting.

Zbořil and Svatá (2022) examined cloud adoption frameworks and emphasized the importance of governance as one of the fundamental aspects of effective cloud migration. They found that the structures of governance facilitated systematic implementation of the clouds through the creation of identity management policies, compliance policies, cost management and monitoring performances. Their study also established that companies that adopted formal governance frameworks were more productive and not as vulnerable to security threats as compared to other companies that adopted ad-hoc governance frameworks.

Galiveeti et al. (2021) covered the topics of cybersecurity and governance within the framework of AWS and Azure. They found that these two platforms were well-developed in security tools and automation of governance functionality but this could only be implemented successfully according to organizational maturity and experience. The article has highlighted the value of governance in data integrity and privacy particularly in areas where a sensitive data is concerned.

3. RESEARCH METHODOLOGY

The study was done to provide an empirical study of cloud governance models of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform

(GCP). As the multi-cloud and hybrid architecture became increasingly used by the organizations, the appropriate cloud governance was now a key towards achieving compliance, security, cost-efficiency, and operational control. The paper therefore aimed at discussing how the governance mechanisms of the three leading cloud platforms enabled the adoption of the cloud by enterprises, minimized risks, and put policies in place. In addition, the objective of the study was to test the best practices, maturity of governance, and potential gaps and strengths of cloud governance models.

3.1. Research Design

A mixed-method research was used in the study. This design was a qualitative evaluation of the documentation of cloud governance and expert interviews and a quantitative analysis, based on the survey. This enabled a critical evaluation of the governance structures, tools, and maturity mechanisms in the AWS, Azure and GCP in one serve. The cross platform benchmarking was accomplished in the form of the comparative nature of the design, and it helped in making actionable insights regarding the effectiveness of the governance implementations.

3.2. Study Objectives

The study was influenced by a number of research objectives of the research. First of all, it was to explore the governance processes, the control systems, and in-house cloud solutions offered by AWS, Azure, and GCP. Second, it was intended to compare governance maturity models across the three platforms. Third, the research was focused on defining significant challenges of governance and best practice activities that should be followed by enterprises when implementing cloud adoption. Lastly, according to the empirical results, the analysis also sought to come up with a conceptual governance reference model to inform enterprise cloud governance initiatives.

3.3. Population and Sampling

IT governance specialists, cloud security architects, DevOps engineers, and cloud administrators, with practical experience in an AWS, Azure, or GCP environment, were the target population. The purposive sampling was chosen to ensure the sampled respondents have relevant cloud governance expertise. The total number of respondents was 60 people who took part in the study, and there were 20 participants who represented each of the cloud platforms. This sampling methodology made sure that only informed professionals were used in the findings.

3.4. Data Collection Methods

Structured online questionnaires were the primary data sources which were administered to cloud professionals of various industry fields. Besides the surveys, semi-structured interviews were carried out with some of the cloud governance professionals to get more qualitative information. The sources of secondary data were official cloud governance documentation by AWS, Azure, and GCP, peer-reviewed journal articles and industry white papers and analyst reports published by Gartner and Forrester. Such sources of secondary data served to confirm the primary results and carry out a stronger comparative governance analysis.

3.5. Data Collection Instruments

Questions in the survey tools were formulated on the Likert-scale to determine the perception of the respondents on the maturity of governance, policy implementation, automatization, security measures, adherence to compliance. A set of open-ended interview questions was used as an interview guide to examine the issues of governance and strategic considerations in detail. Also, a document review checklist was used to uniformly review the governance aspects of the three cloud platforms.

3.6. Variables Studied

The research aimed at a number of variables. Governance aspects comprised identity and access administration strategies, audit documentation, surveillance equipment, and compliance controls. Some of the operational variables were automation support, DevOps integration, cost governance capabilities and scaling. The security-oriented variables comprised security governance policies,

datasets protection attributes, and certification of compliance. The indicators of governance maturity were the effectiveness of policy implementation, audit preparedness, integration of governance tools, and compliance to the industry best practices.

3.7. Data Analysis Techniques

The analysis of the quantitative data obtained via surveys was done with the help of the descriptive statistics (frequency distribution, mean value, and percentage score). Thematic content analysis was used to analyse qualitative interview responses to determine themes and problems of governance that recur. A cross-platform maturity matrix of governance was created in order to compare the capabilities of AWS, Azure, and GCP. This analysis method aided in outlining the comparative advantages and weaknesses of the governance model of each cloud provider to improve the model.

3.8. **Ethical Considerations**

The study involved ethical research principles. Those who participated did so voluntarily and the reason behind the research was explained to them. The confidentiality of the response was also taken care of and there was no personally identifiable information that was divulged in relation to the enterprise. All the sources used in the research were credited to give an acknowledgment to maintain academic integrity.

4. RESULTS AND DISCUSSION

This part was the presentation of the findings of the empirical study conducted to compare cloud governance of AWS, Azure, and Google Cloud Platform (GCP). The results were founded on the survey questions and the interviews with the specialists, and they were added with the analysis of the document of the governance models per platform. Findings identified governance maturity, abilities of automation, enforcement of security, and compliance posture in the three largest cloud providers. The findings were explained and conclusion on the need to adopt cloud and governance design proposals to enterprises discussed.

4.1. Governance Maturity Assessment

The researchers found out that AWS had the best governance maturity compared to the other two, Azure and GCP. The respondents have pointed out that AWS provided strong governance controls, a fully formed IAM solution, and a well-developed audit frameworks. The governance capability of Azure was explained by the alignment with the enterprise, integration with Microsoft ecosystem, and control by means of policies. GCP had a superior automation level and innovative security governance functions but a lesser enterprise governance maturity than AWS and Azure.

Table 1: Perceived Governance Maturity by Cloud Platform

Governance Maturity Level	AWS	Azure	GCP
High Maturity	15	12	9
Moderate Maturity	5	7	9
Low Maturity	0	1	2

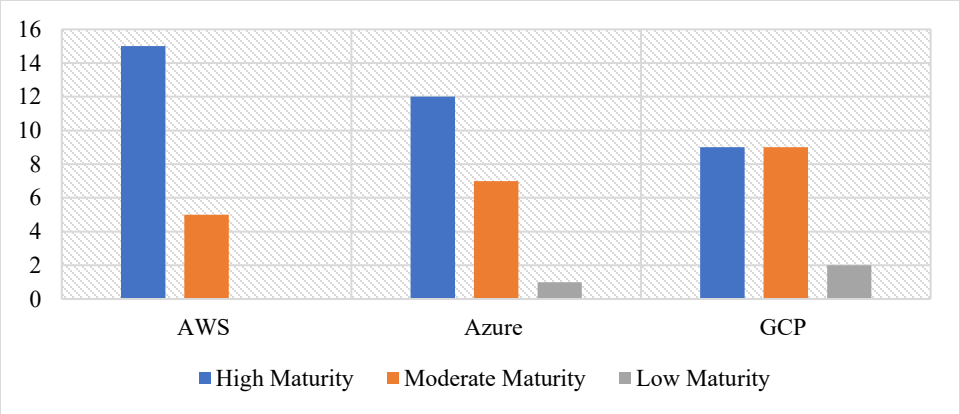

Figure 1: Perceived Governance Maturity by Cloud Platform

The information supported the idea that AWS had the highest maturity rate (75%), whereas GCP had a comparatively lower maturity rating, even though almost a half of the participants indicated GCP to be moderately mature. This corroborated the fact that AWS was the most developed cloud platform when it comes to governance mechanisms.

4.2. Policy Enforcement and Compliance

It was found that AWS and Azure offered great policy enforcement feature based on the survey responses, but GCP was seen as new, but expanding at a very high rate. The Azure Policy and AWS Config rules were also mentioned among the major sources of compliance automation. The Config Controller and organization policies of GCP were identified, with the respondents registering a smaller number of ready-made governance templates than those available to AWS and Azure.

Table 2: Policy Enforcement & Compliance Effectiveness

Rating Category	AWS	Azure	GCP
Highly Effective	14	13	8
Moderately Effective	6	7	10
Less Effective	0	0	2

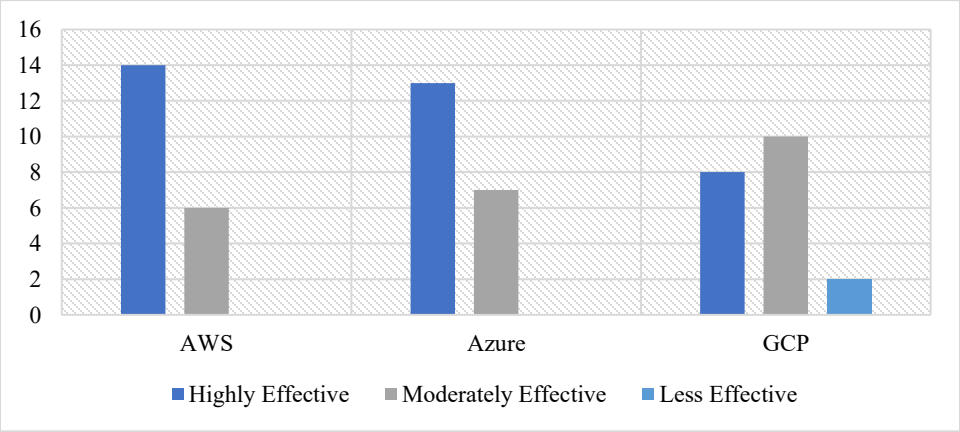

Figure 2: Policy Enforcement & Compliance Effectiveness

These results indicated that AWS and Azure governance services had higher levels of maturity in terms of compliance enforcement even at the same time GCP was still developing its compliance automation landscape.

4.3. Security Governance and Monitoring

Based on the insights of the interviews, it became clear that the three platforms had excellent security governance characteristics, although AWS and Azure had the best enterprise security policy orchestration. The fact that the Azure was compatible with the Active Directory and the Microsoft security suite provided it with a competitive advantage. GCP was acclaimed with advanced threat intelligence and AI-based security but was perceived to be less advanced in the thoroughness of policy guidelines.

4.4. Cost Governance and Resource Control

The participants reported that the AWS cost governance tools, such as Cost Explorer and Budgets had a better visibility and automation in comparison to other cost management tools (Azure Cost Management and GCP Billing). Azure was characterized as competitively performant but, most of the times, complexities that were involved in Microsoft enterprise licensing agreements were considered as heavyweight. GCP was recognized to be simple yet had few automated cost governance.

4.5. Discussion

The findings showed that AWS was still the best platform with respect to governance maturity, automation of compliance and control of costs. Azure proved to be very consistent with the enterprises governance requirements, which favor organizations that already have operating systems in the Microsoft ecosystems. GCP had current automation-based administration and inventive security features but had to be more mature in policy frameworks and enterprise controls.

The findings in general highlighted the fact that the choice of cloud governance required to meet the needs of the enterprise, current technology stacks, and regulations. The situations with hybrid environments and multi-cloud settings required structured governance frameworks to align the policies on the platforms. GCP adoption may be especially advantageous to enterprises adding third-party governance solutions to the native ones until it became mature in governance like AWS and Azure.

5. CONCLUSION

The comparative analysis has concluded that all three major cloud platforms, i.e., AWS, Azure, and Google Cloud, provide good governance capabilities, but AWS demonstrated higher governance maturity as a result of its well-developed policy implementation tools, sophisticated security measures and automation of compliance. Azure trailed behind with an advantage of deep integration in enterprises and robust policy-based governance aligned with a Microsoft environment. Google Cloud presented potentially advantageous automation-based governance and novel security functionality, but it continued to lose out on enterprise governance maturity and ready-to-deploy compliance packages. In general, the results indicated that efficient cloud governance plan was reliant on the matching of platform capabilities with organizational requirements, maturity, and regulatory concerns, and multi-cloud set-ups demand unified governance controls in order to perform optimally and comply.

REFERENCES

[1] Laxminarayana Korada, V. K. S., & Somepalli, S. (2022). Importance Of Cloud Governance Framework For Robust Digital Transformation And It Management At Scale. *Journal of Scientific and Engineering Research*, *9*(8), 151-159.

[2] Sharma, H. (2020). Effectiveness of CSPM in Multi-Cloud Environments: A study on the challenges and strategies for implementing CSPM across multiple cloud service providers (AWS, Azure, Google Cloud), focusing on interoperability and comprehensive visibility. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, *10*(1), 1-18.

[3] Singh, U. K., & Sharma, A. (2021). Cloud Computing Security Framework Based on Shared Responsibility Models: Cloud Computing. In *Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0* (pp. 39-55). CRC Press.

[4] GOEL, E. (2021). Evaluating Scalable Solutions: A Comparative Study of AWS, Azure, and GCP.

[5] Zbořil, M., & Svatá, V. (2022). Cloud adoption framework. *Procedia Computer Science*, *207*, 483-493.

[6] Galiveeti, S., Tawalbeh, L. A., Tawalbeh, M., & El-Latif, A. A. A. (2021). Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms. In *Artificial intelligence and blockchain for future cybersecurity applications* (pp. 329-360). Cham: Springer International Publishing.

[7] Badri, P., Goli, A. K. R., & Goli, S. R. (2022). Strengthening Data Governance and Privacy: Utilizing Amazon AWS Cloud Solutions for Optimal Results. *EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ)*, *11*(2).

[8] Quadri, S. (2017). *Cloud computing: migrating to the cloud, Amazon Web Services and Google Cloud Platform* (Master's thesis, S. Quadri).

[9] Shahane, R., & America, P. D. A. T. M. (2022). Enhancing Data Governance in Multi-Cloud Environments: A Focused Evaluation of Microsoft Azure's Capabilities and Integration Strategies. *Journal of Computational Analysis and Applications*, *30*(2).

[10] Goli, S. R., & Goli, A. K. R. (2022). Strengthening Data Governance and Privacy: Utilizing Amazon AWS Cloud Solutions for Optimal Results. *Available at SSRN 5317148*.

[11] Sivakumar, K., Kalaivani, S., Venkatesan, D., & Vetrivel, V. (2022). An empirical analysis data mining frameworks—an overview. *Ambient Communications and Computer Systems: Proceedings of RACCCS 2021*, 243-254.

[12] Mazzoni, L., & Costa, G. (2022). Value creation mechanisms of cloud computing: a conceptual framework.

[13] Ogeawuchi, J. C., Akpe, O. E., Abayomi, A. A., Agboola, O. A., Ogbuefi, E. J. I. E. L. O., & Owoade, S. A. M. U. E. L. (2022). Systematic review of advanced data governance strategies for securing cloud-based data warehouses and pipelines. *Iconic Research and Engineering Journals*, *6*(1), 784-794.

[14] Azevedo, L. (2021). The impact of cloud management platforms on nonprofit business models. *Journal of Technology in Human Services*, *39*(4), 405-425.

[15] Malawski, M., Gajek, A., Zima, A., Balis, B., & Figiela, K. (2020). Serverless execution of scientific workflows: Experiments with hyperflow, aws lambda and google cloud functions. *Future Generation Computer Systems*, *110*, 502-514.