Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2022, 9(8):151-159**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Importance of Cloud Governance Framework for Robust Digital Transformation and IT Management at Scale

Laxminarayana Korada[1], Vijay Kartik Sikha[2], Satyaveda Somepalli[3]

[1]ORCID: 0009-0001-6518-0060; laxminarayana.k@gmail.com
[2]ORCID: 0009-0002-2261-5551; vksikha@gmail.com
[3]ORCID: 0009-0003-1608-0527; satyaveda.somepalli@gmail.com

Abstract: In the rapidly evolving digital transformation landscape, robust cloud governance frameworks are essential for managing and optimizing cloud assets, ensuring security, and maintaining compliance. This study discusses the importance of cloud governance for large-scale IT operations by comparing traditional IT governance models with modern practices suitable for multi-cloud and hybrid-cloud environments. It highlights the challenges and advantages faced by different types of organizations, including digital natives and those transitioning from legacy systems. It also covers the critical components of a comprehensive cloud governance framework, such as security, cost management, and automation tools, and emphasizes the roles of standardization and business alignment. Real-world examples from leading tech organizations demonstrate the successful implementation of cloud governance strategies. The conclusion underscores the need for scalable and adaptable governance models to achieve seamless technological transition and sustain IT efficiency.

Keywords: Cloud Governance, Digital Transformation, IT Management, Multi-Cloud, Hybrid-Cloud, Public Cloud, Private Cloud, Security, Compliance, Automation Tools, Digital Natives, Standardization, Business Alignment, IT Governance Models, Cloud Adoption Framework

Introduction

Cloud governance refers to the establishment of proper policies, practices, and measures to enhance the optimum use, monitoring, and protection of cloud assets (Woldu, 2013). Today, the topic of digital transformation is rather popular, and the rate of technological advancement is continually accelerating. Organizations are offered a vast range of cloud-based offerings to develop and manage their software applications based on technologies like big data, artificial intelligence, and the Internet of Things (IoT). However, these offerings possess inherent risks, which include security, governance, and compliance across the diverse options available.

This paper discusses the significance of cloud governance as a critical element for digital transformation and IT operations on a large scale. It also describes the governance models before the emergence of public cloud offerings for both large enterprises and small businesses. It also explains the ease of implementing modern governance practices for digital native organizations.

The paper delves into the challenges in multi-cloud and hybrid-cloud environments and explains the need for a scalable and comprehensive model. This model must include crucial domains, such as security, compliance, networking, and data management, to enable a seamless technological transition.

The paper describes how automation tools aided the evolution of governance for efficient processing of activities and generated useful information. Through key examples from leading tech firms, it explains how good cloud governance ensures success for an organization.

Figure 1: Components of a Cloud Governance Framework

Evolution of Technologies Supporting Digital Transformation

Technological advances have opened a plethora of solutions to enable the much-needed digital transformation. However, that can introduce new security, governance, and/or compliance challenges. The following sections discuss some of these complexities:

Security Challenges

Organizations these days are using diverse technology stacks, and the vulnerability of the systems increases as they become more complex. These risks could be unique to each platform which if not addressed could potentially lead to a breach (Al-Ruithe et al., 2019). Moreover, the lack of consistent and secure policies and procedures across organizations exacerbates the problem. Therefore, it is essential to establish and implement uniform security measures that are rigorous and comprehensive.

Governance Complexity

Majority of customary IT governance models fail to adequately address the volatility that is prevalent in contemporary cloud environments (Woldu, 2013). These models, primarily designed for on-premise infrastructure, do not account for the level of flexibility expected in remote and dynamic environments. Moreover, governance approaches differ significantly according to the size and scope of the organization. Large organizations require strict control and maintenance owing to their complex processes and evolving standards, while small organizations benefit from fast and innovative processes with minimal formal regulations. Reconciling conflicting objectives and stakeholders is a significant challenge in digital transformation, complicated by changing business priorities and the need to balance flexibility with control.

Compliance Considerations

Legal and compliance requirements present another factor that complicates the problem. There are specific and different regulations depending on industry and location. To stay compliant, organizations are required to understand and follow the rules and regulations governing their operations (Al-Ruithe et al., 2019). Failing to abide by it will lead to penalties, fines, reputational losses, or possible legal prosecution of the people involved. Therefore, developing effective strategies that can navigate through the labyrinth of legal requirements is an essential aspect of any successful cloud governance strategy.

Digital Native Advantage

Digital organizations native to the digital era possess intrinsic advantages as they transition to cloud-native approaches. These entities, born during the dawn of the cloud era, typically embrace agile methods, automated processes, and collaborative organizational culture, such as DevOps (Al-Ruithe et al., 2019). These characteristics facilitate the seamless integration of new technologies into existing networks. They are not hindered by the barriers that traditional organizations face due to their reliance on outdated technologies, lengthy decision-making processes, and a reluctance to innovate.

Multi-Cloud and Hybrid Challenges

Achieving uniformity across various cloud providers poses a significant challenge in multi-cloud or hybrid-cloud environments. Each vendor offers distinct characteristics, such as landing zones, unique features, cost structures, APIs, and levels of customer service, which exacerbates the difficulties of integrating all activities across an enterprise (Al-Ruithe et al., 2019). Developing coordinated plans that address interoperability, standardization, and portability is critical. These plans enable organizations to navigate the intricate challenges of compatibility and guarantee seamless integration across different systems.

The need for well-defined governance frameworks is highlighted by the complexities identified. Such frameworks would provide clear guidelines for managing each of the dimensions discussed. For instance, implementing zero trust practices, continuous monitoring, and risk monitoring enhances overall cybersecurity posture. Additionally, adopting industry-standard reference architectures, templates, blueprints, and automation tools boosts productivity and reduces common human errors associated with manual processes. Lastly, fostering interdisciplinary collaboration among internal division representatives is crucial for securing the necessary commitment and support to achieve long-term successful outcomes in digital transformation initiatives.

Traditional IT Governance Models

Before the advent of public cloud computing, traditional IT governance frameworks were commonly used in organizations. These frameworks depended on physical infrastructure that was managed and maintained by in-house IT staff (Woldu, 2013). In this regard, large enterprises and small to medium-sized businesses (SMBs) approached IT governance differently due to their varying scales, resources, and priorities.

In substantial corporations, conventional IT governance frameworks have typically featured rigid frameworks, procedures, and controls (Balshakova, 2016). Centralized IT departments managed application installations, infrastructure maintenance, and technology acquisitions. The decision-making process often involved multi-tiered approval hierarchies, to ensure comprehensive review and authorization. Nevertheless, these highly structured and formalized governance frameworks have frequently resulted in bureaucratic obstacles, which in turn impeded innovation and flexibility.

Small-medium enterprises are often faced with resource constraints that impact their IT governance strategies. These constraints, including limited budgets and insufficient human resources, can make it difficult for these entities to focus on long-term aspirations. Due to their smaller size, these organizations often adopt more flexible approaches to governance, characterized by decentralized decision-making and less stringent control mechanisms. However, this flexibility can come at the expense of security and stability, as it may lead to issues that could jeopardize business operations (Balshakova, 2016).

Digital native organizations that emerged after the onset of cloud computing typically exhibit a higher familiarity with cloud-based IT governance models. By operating solely in the cloud, they eliminate the need for significant investments in physical infrastructure, freeing up resources for strategic initiatives. Digital natives often prefer flat organizational structures, fluid team compositions, and iterative development cycles, creating an environment that promotes innovation and experimentation (Balshakova, 2016). However, even digital natives face challenges transitioning from single-cloud to multi-cloud or hybrid-cloud configurations.

Multi-cloud and hybrid-cloud environments introduce additional layers of complexity due to the following factors:

Diverse Technology Stacks

As organizations increasingly adopt diverse technology stacks comprising various architectural patterns, programming languages, frameworks, and containerization techniques, the challenge of addressing these heterogeneous environments grows more complex. For instance, a three-tier Java-based web application, microservices powered by Node.js, or Docker and Kubernetes containers running .NET Core APIs (Truong et al., 2018) represent examples of such complex arrangements. Navigating these diverse systems requires significant expertise and a thorough understanding of interoperability issues. To bridge gaps between disparate components, custom development efforts, sophisticated middleware selection, and careful configuration tuning may be necessary. However, integrating these different systems can be a daunting task, necessitating deep technical knowledge and skillful project execution (Balshakova, 2016).

Non-uniform Security Protocols

Adopting multiple cloud platforms adds an additional layer of complexity due to the inconsistencies in security protocols among different cloud providers. Specifically, each cloud vendor implements unique authentication mechanisms, encryption techniques, and authorization policies, making comprehensive management challenging (Carvallo et al., 2017). Aligning these idiosyncrasies involves reconciling differences in identity and access management, policy enforcement, and auditing procedures. For instance, variations in password policies, single sign-on configurations, and logging and monitoring practices (Carvallo et al., 2017) illustrate this issue.

Overall, achieving uniform security postures and fulfilling legal and contractual obligations requires careful assessment of prevailing security paradigms and diligent harmonization efforts (Becker & Bailey, 2014).

Inconsistent Cost Structures

The diverse assortment of billing models, usage fees, and discount structures employed by various cloud providers presents a challenging landscape for cost estimation, tracking, and optimization endeavors. In the absence of effective governance mechanisms, organizations may encounter unanticipated expenses or fail to capitalize on cost-saving opportunities.

Variegated Performance Metrics

Different cloud service providers exhibit varying performance baselines, which are influenced by factors like network latency, load balancing, and resource allocation policies. To measure and compare performance across multiple platforms, it is necessary to have detailed insights and sophisticated analytics tools (Becker & Bailey, 2014).

To effectively handle the complexities of multi-cloud and hybrid-cloud environments, advanced governance models are needed. By establishing clear policies, guidelines, and automation frameworks, organizations can achieve a balance between flexibility and control, thereby maximizing the potential of digital transformation.

Role of Governance Model and Scalable Framework

A robust cloud governance framework is essential for successful digital transformation (Peiris et al., 2014). The following are some of the ways in which it contributes to the process:

Business Alignment

Implementing cloud governance is often aimed at ensuring that cloud adoption initiatives align with larger business goals. This approach differs from randomly selecting and adapting technology within an organization, as it ensures that all selected technologies contribute positively to the strategic direction of the organization and align with the intended business strategy (Peiris et al., 2014). IT benchmarking helps organizations align their investments with their corporate goals and objectives, create harmony between departments, enhance accountability, and minimize unnecessary costs on unproductive projects.

Deloitte's 2022 Global Tech Leadership Survey revealed that organizations with high levels of IT-business unit integration recorded a higher revenue growth rate of +14% compared to non-integrated organizations, which experienced a negative growth rate of -4% (Plyhm, 2022).

Therefore, it is essential for today's organizations to establish a clear and robust connection between cloud governance and their strategic direction to fully realize the value of digitalization initiatives.

Standardization

One of the key elements of effective cloud governance is the standardization of technology across the various layers of the technology stack found in cloud computing environments. By standardizing technology, the redundancy associated with adding, modifying, or updating new systems is reduced, and the transfer of knowledge among staff members becomes easier. This approach also leads to lower levels of technology debt, increased productivity, and higher-quality user interfaces (Peiris et al., 2014). Furthermore, standardization promotes modularity and interchangeability, which can be more effectively responded to and adapted to changes in the market. McKinsey's research shows that organizations with higher levels of modularity were able to respond to emergencies approximately three months faster than less flexible organizations. Therefore, incorporating standardization of IT infrastructures into the cloud governance framework prepares businesses to better handle contingencies and instability.

Crucial Areas

Effective cloud governance encompasses several essential areas, which are critical for safeguarding operations and maximizing return on investment:

1. **Security**

A strong cloud security strategy is essential for organizations that utilize cloud platforms to handle their critical workloads. A key element of this strategy is the shared responsibility model, which leading cloud service providers such as AWS, Azure, and Google Cloud adhere to. Under this model, providers are responsible for certain security aspects, while customers are responsible for securing their data, applications, and access configurations (Hendre & Joshi, 2015). In the case of Infrastructure as a Service (IaaS) deployments,

organizations must perform tasks such as applying OS patches, configuring firewalls, and implementing antivirus measures.

Identity and access management (IAM) tools are crucial for controlling user access, employing role-based access controls (RBAC) to align permissions with job roles. Encryption is also a vital component of cloud security, as it helps to safeguard data integrity. By employing protocols like Transport Layer Security (TLS) for secure communication and carefully managing encryption keys, organizations can further enhance their security posture (Hendre & Joshi, 2015).

Continuous monitoring and incident response frameworks are essential for detecting and mitigating security breaches promptly. Regular audits and vulnerability assessments are necessary to maintain compliance with industry regulations and internal policies. Implementing a zero-trust approach also reinforces security by verifying all access requests, regardless of network location or user identity.

Securing containers through best practices such as image scanning and runtime protection can enhance overall cloud security posture, while consolidating cybersecurity solutions streamline management and enhances threat visibility. Leveraging cloud detection and response tools further fortifies defenses, allowing organizations to effectively detect and respond to emerging threats in their cloud environments (Peiris et al., 2014).

2. Cost Management

Monitoring and controlling costs are a crucial aspect of any cloud governance program. Employing reserved capacity, right-sizing instances, and detecting idle resources can lead to substantial savings. In fact, as per Flexera's data, the typical organization that utilizes public cloud services often squanders around thirty percent of its annual budget on these services. Implementing effective tagging strategies and usage metering can help managers identify areas that require adjustments, ultimately resulting in more streamlined and cost-efficient operations.

3. Change Management

Utilizing formalized channels to expedite modification requests is essential in preventing unauthorized alterations, ultimately averting system downtime, corruption, and the potential loss of crucial data. Implementing change advisory boards (CABs), ticketing systems, and version controls facilitate prompt communication, assessment, and endorsement of proposed enhancements, leading to predictable and stable system behavior (Saidah & Abdelbaki, 2015).

4. Risk Management

Recognizing potential threats and weaknesses is an integral component of effective cloud governance. While closely associated with security, risk management encompasses broader operational risks, extending beyond security measures. Periodic evaluations and ongoing monitoring enable the identification of unusual patterns indicative of potential attacks, facilitating prompt actions to address them. Mitigation strategies include the implementation of firewall configurations, intrusion detection systems, log analysis tools, and routine penetration testing (Saidah & Abdelbaki, 2015). Adopting a comprehensive approach ensures protection against both security breaches and other operational risks, thereby preserving business continuity and enhancing overall resilience.

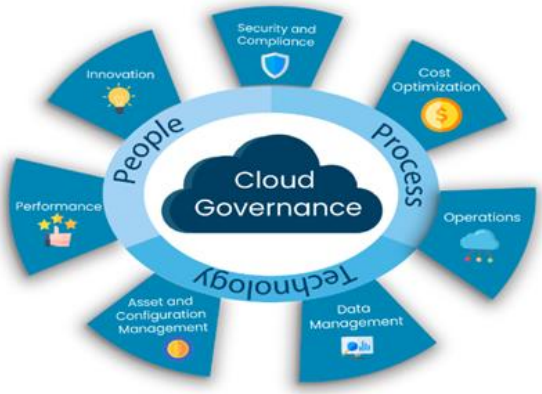

Figure 2: Risk Management Considerations for Cloud Governance

Automation Tools

Automation tools have a crucial function in streamlining cloud governance activities, facilitating precise policy enforcement and scaling efficiently with expanding cloud estates. Key automation tools that are essential to cloud governance frameworks comprise AWS Control Tower, Azure Blueprints, and Google Cloud Anthos Config Management. These tools concentrate on automating resource provisioning, conducting continuous compliance evaluations, and assigning routine tasks, leading to optimal resource utilization and increased agility.

1. **AWS Control Tower**

Amazon Web Services presents AWS Control Tower, a service designed to construct and manage secure, scalable, and compliant multi-account AWS environments. AWS Control Tower employs predefined guardrails to establish baseline security measures and best practice policies, thereby assisting organizations in navigating their cloud journeys. These guardrails encompass account structure design, network segmentation, and least privilege principles, which can be enforced automatically or manually activated. Moreover, ongoing tracking and visual summaries aid administrators in detecting risks and rectifying misconfigured resources (Chapel, 2020).

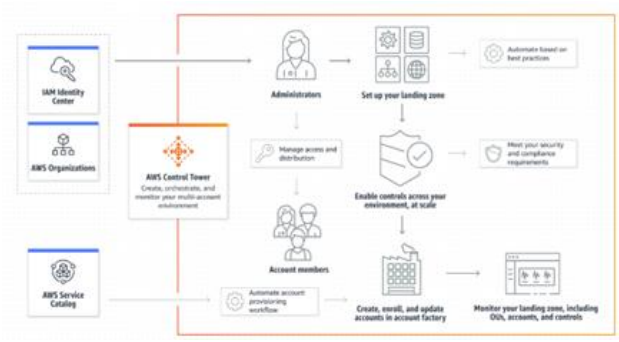

Figure 3: AWS Control Tower Console

2. **Azure Blueprints**

Microsoft Azure offers Azure Blueprints, a feature designed to streamline large-scale cloud deployments that adhere to corporate standards. This feature includes built-in artifact templates that incorporate ARM (Azure Resource Manager) templates, policies, roles, and resource groups, enabling rapid distribution and updates of blueprints (Ross, 2018). Additionally, customizable definitions provide extensive control over resource consistency, access permissions, and region availability (Ross, 2018). Once applied, blueprints propagate across subscriptions, establishing foundational constructs and immutable properties.

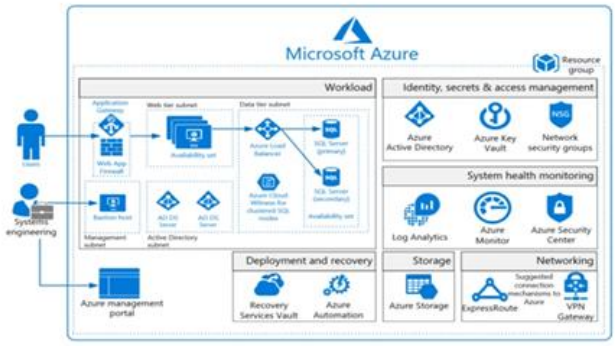

Figure 4: Sample Azure Blueprint Includes Role Assignments, ARM Template, and Artifacts

3. **Google Cloud Anthos Config Management**

Lastly, Google Cloud offers Google Cloud Anthos Config Management, a unified platform for configuring and managing clusters and workloads across multiple clouds. Anthos Config Management consists of Config Connector, Config Synchronizer, and Validation Tool, which promote GitOps workflows, declarative

configuration management, and drift prevention. With consistent baselines and continuous syncing, organizations can ensure policy compliance and prevent errors and misconfigurations in large-scale environments (Ananthampalayam, 2021).

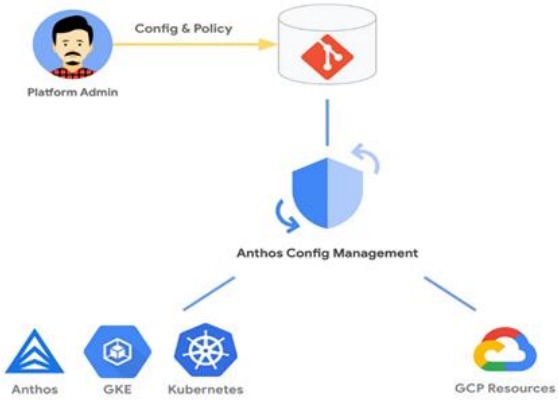

Figure 5: Anthos Config Management Architecture Overview

The utilization of automation tools has demonstrated significant benefits in streamlining administrative tasks, reducing the need for human intervention and minimizing errors, and enhancing cloud governance capabilities. It is recommended that users consult the respective documentation pages for comprehensive instructions, tutorials, and reference materials.

Successful Executions

1. **Netflix**

Netflix is an outstanding case study of the successful implementation of cloud governance and digital transformation in the realm of entertainment. By collaborating with Amazon Web Services (AWS), Netflix embarked on an extensive cloud migration process that revolutionized its business model. Instead of merely transferring existing systems, Netflix opted for a comprehensive rewrite of its applications, adopting a cloud-native approach. This tactical move empowered Netflix to unlock the full potential of AWS, allowing the company to deploy thousands of servers and petabytes of storage in a matter of minutes. Consequently, Netflix now offers a seamless global streaming service that is accessible to users worldwide.

2. **Asos**

ASOS, a prominent online fashion retailer with a global presence, implemented Microsoft Azure as an integral component of its digital transformation plan. By utilizing Azure's native services, such as Azure Kubernetes Service (AKS), and incorporating DevOps practices, ASOS successfully developed a resilient infrastructure capable of swiftly scaling during peak shopping periods without compromising performance or availability. In addition, the company adopted Azure Policy to establish consistent tagging, resource management, and regulatory compliance across all stages of development and production. These cloud governance measures enabled ASOS to expedite time-to-market and guarantee the secure, compliant, and efficient delivery of its digital services, particularly during high-traffic seasonal sales events.

3. **Spotify**

Spotify, the prominent music streaming service, epitomizes the implementation of a cloud governance framework on Google Cloud Platform (GCP). As the company expanded its operations globally, it recognized the need for a robust cloud strategy and governance model to manage its burgeoning GCP footprint.

Spotify adopted a federated model of cloud governance, which empowered individual engineering teams to make decisions while maintaining overall control and consistency. They implemented GCP resource hierarchy, utilizing folders and labels to organize and tag resources based on business units, environments, and cost centers. In addition, Spotify leveraged GCP IAM (Identity and Access Management) to define and enforce granular access controls, ensuring that teams had the necessary permissions to manage their resources while adhering to security best practices.

Conclusion

Cloud governance plays a critical role in contemporary IT strategies, as it is essential for coordinating digital transformation and strengthening IT operations. It serves as the foundation for a structured approach to managing cloud assets, monitoring, and security. Cloud governance is a key factor in addressing the challenges presented by advanced technologies, such as cloud solutions, big data, AI, and the Internet of Things. While these technologies offer significant opportunities for growth and efficiency, they also bring about substantial challenges related to security, oversight, and compliance in a varied cloud environment.

The significant challenges posed by cross-stack security vulnerabilities, the supervision complexities in fluid cloud environments, and stringent regulatory requirements underscore the importance of implementing reliable governance frameworks. Large corporations and smaller medium-sized businesses (SMBs) face distinct governance challenges due to their varying scales and resource capacities, while digitally advanced firms benefit from inherent adaptability and cloud-centric practices.

Considering the growing trend towards multi-cloud and hybrid-cloud environments, the necessity for comprehensive frameworks that encompass all aspects of security, compliance, networking, and data management become increasingly apparent. The implementation of strategies such as zero trust security, continuous monitoring, and automation tools like AWS Control Tower, Azure Blueprints, and Google Cloud Anthos Config Management serve to enhance governance capabilities and promote adherence to established guidelines.

The integration of artificial intelligence with cloud governance is expected to yield remarkable capabilities in forecasting, anomaly detection, and automated response techniques. Utilizing these advancements, entities can effectively mitigate risks, optimize resource allocation, and enhance operational efficiency. Consequently, it is imperative for organizations to remain informed bout these developments, in order to navigate the dynamic landscape of cloud technologies and maintain competitive advantages.

In conclusion, as organizations continue to refine their cloud strategies, the ongoing development of cloud governance remains crucial. By embracing best practices, leveraging automation tools, and closely monitoring emerging trends, such as the integration of AI, organizations can unlock the full potential of cloud technologies while bolstering defenses against emerging threats and complex situations. Therefore, adopting this tactical approach ensures that cloud governance not only supports but drives digital transformation efforts, ultimately paving the way for sustainable growth and innovation in the digital age.

References

[1]. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. Personal and Ubiquitous Computing, 23, 839-859.

[2]. Ananthampalayam. A. (2021, October 30). Introduction to Anthos Config Management - Arun Ananthampalayam - Medium. Medium; Medium. https://medium.com/@kasiarun/introduction-to-anthos-config-management-1a43917c26ae

[3]. Balshakova, T. (2016). Lean vs. Traditional IT Governance. Projectmanagement.com. https://www.projectmanagement.com/blog-post/61873/lean-vs--traditional-it-governance#_=_

[4]. Becker, J. D., & Bailey, E. (2014). IT controls and governance in cloud computing. In 20th Americas Conference on Information systems (AMCIS), Savanah.

[5]. Bradley, T. (2017, February 24). ASOS Streamlines Fashion With Microsoft Azure. Forbes. https://www.forbes.com/sites/tonybradley/2017/02/24/asos-streamlines-fashion-with-microsoft-azure/

[6]. Building Cloud Governance From the Basics. (2019). ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-3/building-cloud-governance-from-the-basics

[7]. Carvallo, P., Cavalli, A. R., Mallouli, W., & Rios, E. (2017). Multi-cloud applications security monitoring. In Green, Pervasive, and Cloud Computing: 12th International Conference, GPC 2017, Cetara, Italy, May 11-14, 2017, Proceedings 12 (pp. 748-758). Springer International Publishing.

[8]. Chapel, J. (2020, September 3). AWS vs. Azure vs. Google Cloud Governance Models - Jay Chapel - Medium. Medium; Medium. https://jaychapel.medium.com/aws-vs-azure-vs-google-cloud-governance-models-c664a97e2489

[9]. Hendre, A., & Joshi, K. P. (2015, June). A semantic approach to cloud security and compliance. In 2015 IEEE 8th International Conference on Cloud Computing (pp. 1081-1084). IEEE.
[10]. Management and Governance Customer Case Studies - Amazon Web Services. (2018). Amazon Web Services, Inc. https://aws.amazon.com/products/management-and-governance/case-studies/
[11]. Peiris, C., Balachandran, B., & Sharma, D. (2014). Governance framework for cloud computing. GSTF Journal on Computing (JoC), 1(1).
[12]. Plyhm, M. (2022, June). Max Plyhm on LinkedIn: #leadershipdevelopment #leadershipresearch #cio #cto #ceo #coo #cfo #chro…. Linkedin.com. https://www.linkedin.com/posts/max-plyhm-525062118_deloittes-global-technology-leadership-survey-activity-6937663718109401088-Luqa
[13]. Practical Guide to Cloud Governance. (2019). https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-governance.pdf
[14]. Ross, A. (2018, August 21). Expanded Azure Blueprint for FFIEC compliant workloads | Microsoft Azure Blog. Microsoft Azure Blog.
[15]. Saidah, A. S., & Abdelbaki, N. (2015). New Governance Framework to Secure Cloud Computing. In Cloud Computing and Services Sciences: International Conference in Cloud Computing and Services Sciences, CLOSER 2014 Barcelona Spain, April 3–5, 2014 Revised Selected Papers 4 (pp. 187-199). Springer International Publishing.
[16]. Spotify Case Study | Google Cloud. (2020). Google Cloud. https://cloud.google.com/customers/spotify
[17]. Sailakshmi, V. (2021). Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud.
[18]. Truong, H. L., Gao, L., & Hammerer, M. (2018, September). Service architectures and dynamic solutions for interoperability of iot, network functions and cloud resources. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings (pp. 1-4).
[19]. Woldu, L. (2013). Cloud Governance Model and Security for Cloud Service Providers.