The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 186-194
DOI 10.37547/tajet/Volume07Issue09-13

Check for updates

Comparative Analysis of Cloud Audit Programs: AWS, Azure, GCP, and COBIT 2019 Integration

Yogesh S. Thanvi CISA, CDPSE
Senior Software Development Engineer in Test II, MA, USA

OPEN ACCESS

SUBMITTED 05 January 2025
ACCEPTED 12 April 2025
PUBLISHED 25 September 2025
VOLUME Vol.07 Issue 09 2025

CITATION
Yogesh S. Thanvi. (2025). Comparative Analysis of Cloud Audit Programs: AWS, Azure, GCP, and COBIT 2019 Integration. The American Journal of Engineering and Technology, 7(09), 186–194. https://doi.org/10.37547/tajet/Volume07Issue09-13

Abstract: Cloud computing has rapidly established itself as the prevailing model for enterprise IT, with major providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) leading global adoption. The cloud promises scalability, flexibility, and cost efficiency, but it also creates complex governance, risk, and compliance challenges due to shared infrastructure, multi-tenancy, and interdependent service layers. To guide assurance efforts, ISACA has issued dedicated audit frameworks: the AWS Audit Program (2019), the Azure Audit Program (2020), the GCP Audit Program (2023), and a broader Cloud Computing Audit Program (2016). These programs structure risk assessment and testing across domains such as governance, identity and access management, incident response, configuration management, logging, and business continuity.

To integrate these audit practices with enterprise-level governance, the study employs the COBIT 2019 framework, ISACA's globally recognized model for governing and managing information and technology. COBIT 2019 provides structured objectives and processes across governance, planning, implementation, service delivery, and monitoring that link IT controls directly to business goals, risk optimization, and value delivery.

This study undertakes a comparative review of the cloud audit programs, aligning their focus areas with COBIT 2019's governance and management objectives. The findings highlight distinct emphases: AWS concentrates on configuration and misconfiguration risks, Azure underscores continuity, shared responsibility, and service reliability, GCP emphasizes hierarchical

structure, identity, and permission inheritance, and the general cloud computing program provides a broad governance foundation applicable across providers. Comparative analysis shows Azure exhibits the closest alignment with COBIT 2019, while AWS and GCP reveal gaps in governance integration. To address these gaps, the study proposes harmonization strategies involving cyber-risk quantification, structured risk registers, and continuous auditing. By linking technical audit domains to COBIT 2019's governance objectives, the study reframes cloud audits from static, checklist-based exercises into dynamic governance mechanisms that foster compliance, risk optimization, and digital trust.

Keywords: Cloud audit, AWS audit program, Azure audit program, GCP audit program, COBIT 2019, cloud compliance management, governance frameworks, IT risk management, audit integration, enterprise cloud security.

1. Introduction

Cloud computing has emerged as the prevailing model in enterprise information technology service provision, allowing organizations to scale infrastructure, applications, and services as needed. Gartner (2021) predicts that over 60% of enterprise information technology expenditures will transition to cloud services by 2025, highlighting its pivotal role in digital transformation. Hyperscale providers, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), dominate the market by providing comprehensive services in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The cloud provides agility and cost efficiency but presents new challenges in governance, risk, and compliance. Multi-tenancy, virtualized infrastructure, and intricate service chains broaden the attack surface, heightening apprehensions regarding misconfiguration, identity and access management (IAM), data protection, and regulatory compliance (Alhassan et al., 2018). For organizations governed by regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI-DSS), demonstrating the efficacy of controls in cloud environments is crucial for compliance and the maintenance of digital trust.

Audit and assurance functions connect business objectives with technical cloud risks. Conventional information technology audits are inadequate for the distinctive attributes of cloud environments, which necessitate consideration of elasticity, shared responsibility, and virtualized service layers (Fernandez et al., 2016). ISACA has created specific audit programs for Amazon Web Services (2019), Microsoft Azure (2020), and Google Cloud Platform (2023), in addition to a general Cloud Computing Audit Program (2016). These offer specialized coverage in governance, identity and access management, incident response, and business continuity.

Notwithstanding the existence of provider-specific audit programs, comparative analyses are still scarce. Current studies predominantly concentrate on either technical cloud security challenges (Hashizume et al., 2013) or governance frameworks in isolation (De Haes et al., 2020). Minimal research exists connecting hyperscaler audit programs with enterprise governance frameworks, such as the Control Objectives for Information and Related Technologies (COBIT) 2019 framework. The proliferation of multi-cloud strategies necessitates integration. Organizations utilizing Amazon Web Services, Microsoft Azure, and Google Cloud Platforms encounter fragmented assurance, redundant efforts, and possible compliance deficiencies. Integrating provider-specific audits with COBIT 2019 enables organizations to synchronize assurance, consolidate risk management, and enhance digital trust.

The objective of this study is fourfold. It aims to compare and synthesize ISACA's audit programs for Amazon Web Services, Microsoft Azure, Google Cloud Platform, and cloud computing. It aligns audit domains and risks with COBIT 2019 governance objectives. It delineates strengths, weaknesses, and deficiencies within hyperscaler audit programs. Ultimately, it suggests integration strategies that employ risk registers, cyber-risk quantification, and ongoing auditing. This study's contribution is to present the inaugural structured comparative analysis that connects hyperscaler audit programs with COBIT 2019, delivering practical recommendations for auditors and organizations implementing multi-cloud governance strategies

2. Literature Review

ISACA established the Amazon Web Services (AWS) Audit Program to assist IT auditors in assessing the

security, compliance, and governance of AWS environments. Given that AWS is a premier cloud platform extensively utilized for enterprise workload hosting, the program highlights the distinct dangers associated with its configuration and service design. The audit program encompasses AWS apps, functions, and containers, focusing on the configuration, access, and management of services. Essential audit domains encompass governance, network configuration and administration, asset configuration, logical access control, data encryption, incident response, logging and monitoring, and disaster recovery. The training mostly emphasizes configuration risk. The studies cited in the program indicate that default AWS configurations frequently create vulnerabilities, including administrative SSH access exposed to the internet, inadequate authentication methods restricted to single-factor passwords, and mismanaged identity and access management (IAM) roles. Such misconfigurations can result in significant repercussions, including denial-of-service attacks, unauthorized access, and excessive power assignment. The initiative recognizes AWS's contribution to facilitating agility and swift transformation for organizations. Nonetheless, in the absence of adequate internal expertise or robust governance frameworks, firms jeopardize their ability to link AWS adoption with strategic goals. The program delineates minimal audit competencies in accordance with ISACA's IT Audit Framework (ITAF) to assist auditors. Auditors must demonstrate professional skepticism, due investigation, and technological proficiency, especially in domains such as Identity and Access Management (IAM), encryption, and cloud-specific risk management. The AWS Audit Program offers a systematic framework of objectives, risk assessments, and testing procedures to guarantee that AWS deployments are secure, compliant, and in accordance with organizational objectives. It emphasizes that the primary assurance difficulty resides not in AWS's capabilities but in how organizations design and manage their utilization of the platform.

The Microsoft Azure Audit Program, released by ISACA in 2020, pertains to the increasing utilization of Azure as a prominent hyperscale cloud provider. The objective is to assist auditors in assessing whether Azure services are deployed in a manner that securely facilitates operational and compliance goals. The program encompasses governance, network configuration and management, identity and access management (IAM), resource security, logging and monitoring, incident response, and data encryption. These domains are intended to represent both Azure's service provisions and the distinct risks that organizations encounter while utilizing them. A fundamental concept in the Azure program is the shared responsibility paradigm. Although

Azure supplies the infrastructure and platform, organizations are accountable for maintaining data integrity, securing endpoints, and adhering to relevant requirements. Misunderstandings of these shared roles may lead to operational problems or noncompliance. The approach emphasizes company continuity and reliability as primary audit considerations. Previous Azure service disruptions, such as those involving Active Directory or multi-factor authentication, exemplify the necessity of proactive maintenance initiatives and continuity planning. In the absence of such planning, firms jeopardize not just financial and reputational integrity but also compliance with regulatory mandates. Auditors implementing this program must adhere to ISACA's ITAF criteria, demonstrating due professional diligence and exhibiting technical expertise in cloud auditing. The Azure Audit Program prioritizes the alignment of technical assurance with overall business resilience, distinguishing continuity as a key focus relative to other cloud audit frameworks.

The Google Cloud Platform (GCP) Audit Program, launched by ISACA in 2023, signifies the platform's emergence as the third-largest cloud provider and examines its unique operational and governance framework. This tool assists auditors in evaluating the configuration and management of GCP environments to ensure they safely align with company business, compliance, and risk objectives. The program encompasses governance, network and resource configuration, identity and access management (IAM), data security and integrity, security logging and monitoring, incident response, and business continuity. The GCP framework, in contrast to previous programs, includes auditing guidance for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Identity-as-a-Service (IDaaS), acknowledging the extensive range of GCP's service offerings. The GCP program prominently features a hierarchical resource model. GCP employs

organizations, folders, and projects that utilize inherited permissions and rules. Misinterpreting this structure—and the propagation of IAM roles or logging configurations—can result in unrecognized dangers or undue rights. The program identifies misconfigurations and ambiguous shared responsibilities as the primary causes of risk in GCP environments. The audit approach emphasizes the dynamic characteristics of GCP services, wherein new features, service discontinuations, and vulnerabilities develop swiftly. Auditors are encouraged to uphold professional skepticism and technical proficiency in evaluating both present configurations and the effects of continuing changes on security and compliance status. The GCP Audit Program emphasizes hierarchy, IAM, and adaptability, enabling auditors to pinpoint risks specific to Google's ecosystem while adhering to ISACA's ITAF criteria of professional diligence and expertise.

The COBIT 2019 framework, created by ISACA, is an internationally acknowledged model for the governance and management of organizational information and technology. It offers organizations organized objectives, methods, and practices intended to guarantee that technology not only aligns with business goals but also yields quantifiable value while effectively controlling risks. COBIT 2019 adopts a comprehensive perspective on governance, integrating strategy alignment, value delivery, performance assessment, and risk optimization within a

unified framework, in contrast to solely technical requirements. COBIT 2019 fundamentally comprises governance and management objectives that convert overarching governance requirements into implementable practices. The objectives are categorized into five principal domains: Evaluate, Direct, and Monitor (EDM) for governance; Align, Plan, and Organize (APO), Build, Acquire, and Implement (BAI), Deliver, Service, and Support (DSS), and Monitor, Evaluate, and Assess (MEA) for management. Every objective has specified procedures, control actions, and measurements that can be customized according to an enterprise's size, industry, and regulatory context. A notable characteristic of COBIT 2019 is its focus on adaptability. It enables firms to build governance frameworks aligned with enterprise objectives, risk tolerance, regulatory obligations, and stakeholder interests. The framework emphasizes integration with many standards and laws, including ISO/IEC 27001, NIST, and GDPR, thereby serving as a unifying tool across industries. COBIT 2019 functions as a reference model for auditors, connecting particular technical assurance activities—such as cloud configuration and identity management—to enterprise governance results, so ensuring that IT audits directly enhance business value, resilience, and digital trust.

3. Methodology

The principal materials for this study consisted of ISACA's officially published audit and assurance programs for the three leading hyperscale providers, like Amazon Web Services (AWS, 2019), Microsoft Azure (2020), and Google Cloud Platform (GCP, 2023), as well as the generalized *IS Audit/Assurance Program for Cloud Computing* (2016). Each of these programs provides detailed narratives of audit domains, specifies potential risks, and outlines step-by-step testing procedures for both hyperscaler-specific environments and generalized multi-cloud contexts. In addition to these programmatic sources, the *COBIT 2019 Framework: Governance and Management Objectives* served as the unifying reference point. This framework was essential for aligning the discrete domains identified in the audit programs with broader enterprise governance principles, enabling the study to move beyond isolated control testing toward an integrated governance perspective.

The research employed a qualitative, document-centric comparative review methodology, which is particularly well-suited for analyzing structured frameworks such as audit and assurance programs (Bowen, 2009). This methodological choice allowed for in-depth exploration of textual content and systematic extraction of audit-relevant concepts. The study unfolded across three principal phases. The first phase involved an exploratory familiarization process, during which each ISACA audit program was examined in detail to gain a comprehensive understanding of its stated objectives, coverage scope, explicit risk considerations, and prescribed control testing steps. This stage provided the necessary foundation for subsequent structured analysis.

The second phase was systematic extraction. Here, audit domains common across programs, such as governance, configuration management, identity and access management (IAM),

incident response, security logging and monitoring, and business continuity, were carefully delineated and documented. These extracted domains, along with their associated risk considerations, were then organized into structured tables to enable clear comparison.

The third phase comprised comparative synthesis, which entailed categorizing the domains, identifying both overlaps and divergences in emphasis among the hyperscalers, and mapping these findings to COBIT 2019's governance objectives. This phase highlighted, for instance, AWS's focus on configuration-related vulnerabilities, Azure's orientation toward continuity and resilience, and GCP's hierarchical approach to identity management and access control.

The programming of the review incorporated both deductive and inductive methodological elements. Deductive coding was guided by the governance structure of COBIT 2019, which organizes enterprise governance into five overarching domains: Evaluate, Direct, and Monitor (EDM); Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA). These COBIT domains provided the framework within which extracted audit elements could be evaluated. Inductive coding, by contrast, allowed for emergent themes unique to each hyperscaler to surface. For example, AWS audit materials highlighted recurring misconfiguration risks, Azure underscored continuity and shared responsibility, and GCP emphasized hierarchical identity constructs and logging practices.

The assessment was conducted through three interlinked analytical perspectives. First, the construction of a risk register enabled evaluation of each domain based on its potential contribution to organizational risk monitoring, focusing on probability of occurrence, potential business impact, and the effectiveness of existing control measures. Second, the study applied concepts of cyber-risk quantification, which translate risk exposures into financial metrics, thus equipping organizational leadership with a clearer basis for defining and adjusting risk appetite (Fairfield, 2020). Third, the analysis considered opportunities for continuous auditing, particularly the feasibility of embedding audit testing steps directly into continuous integration and continuous deployment (CI/CD) pipelines. This approach reinforces the principle of *security as code*, wherein assurance processes become integrated into the same automated workflows that govern software development and deployment (Alles et al., 2006).

The procedure adhered to a circular and iterative workflow as shown in Figure 1 that cycled through extraction, categorization, mapping, and evaluation. Each cycle incorporated feedback loops that allowed for refinement and ensured that findings were both comprehensive and consistent with the underlying governance framework. The reliance on ISACA's officially published audit programs provided reliability and authority to the extracted content, while triangulation with COBIT 2019 supplied a governance-level validation of the comparative results.

Nevertheless, the methodology is not without limitations. As a qualitative and document-based study, its findings are interpretive and dependent upon the published audit program content rather than empirical case data. Consequently, while the results provide theoretical alignment and structured comparative insight, empirical validation through field studies in enterprise multi-cloud environments remains an important avenue for future research.

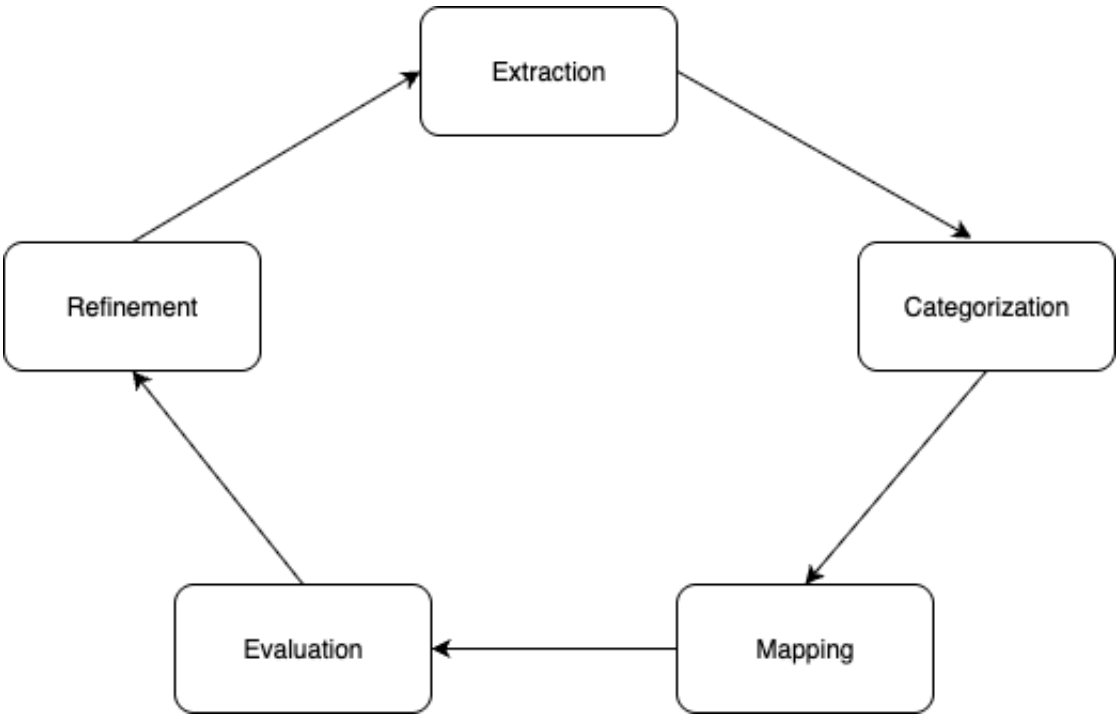

Figure 1: Continuous comparative review of the Audit program

4. Results and Discussion

The comparative analysis revealed that each hyperscaler's audit program embodies its operational philosophy and focuses on different risk priorities. The Amazon Web Services Audit Program is predominantly focused on configuration, emphasizing risks like default insecure settings, inadequate identity controls, and excessively permissive access rights. This emphasis illustrates the extensive flexibility of AWS's service catalog, wherein customization options heighten the probability of misconfiguration. The Microsoft Azure Audit Program is focused on continuity, emphasizing shared responsibility and resilience. It emphasizes the necessity for enterprises to establish business continuity plans and strategies for outages, mirroring Azure's predominantly enterprise clientele. The Google Cloud Platform Audit Program is structured around a hierarchy, emphasizing its Organization/Folder/Project framework and the consequential impact of identity and access management inheritance. The Cloud Computing Audit Program of 2016 establishes a governance framework, emphasizing vendor management, cross-border compliance, and reliance on third parties.

Mapping the audit domains to COBIT 2019 governance objectives revealed that Azure exhibits the strongest alignment with COBIT principles, especially in governance and continuity. AWS exhibited robust configuration management capabilities but showed deficiencies in aligning with governance objectives, whereas GCP excelled in the intricacies of identity and access management yet necessitated enhanced integration with governance oversight.

Table 1 (the alignment table) demonstrated disparities across governance, identity, incident response, continuity, monitoring, and configuration management domains, with Azure achieving the highest overall score.

Integration strategies are essential for aligning these programs. Risk quantification enables the financial expression of misconfiguration, outage, or inheritance risks, rendering them actionable for executives. Continuous auditing integrates assurance within DevOps pipelines, converting audit programs from static checklists into dynamic controls. COBIT 2019 establishes the governance connection, ensuring that technical insights from audits of AWS, Azure, and GCP are preseted at the board-level governance discussions.

The synthesis of insights indicates that no singular hyperscaler program is adequate for enterprises functioning in multi-cloud environments. AWS excels in configuration rigor, Azure provides resilience and governance alignment, and GCP enhances identity and access management. Integrated within COBIT 2019, these synergistic focuses offer a more comprehensive assurance framework.

A comparative case study exemplifies these findings. In instances of AWS misconfiguration, such as the public exposure of a storage bucket, the AWS Audit Program categorizes this as a configuration risk, whereas COBIT associates it with the governance objectives of BAI09 and DSS01. Cyber-risk quantification converts this into prospective financial loss. An Azure outage impacting Active Directory authentication emphasizes continuity and resilience as per the Azure Audit Program, while COBIT associates the incident with DSS04 and APO12, connecting it to enterprise risk appetite and continuity planning. A misconfiguration of GCP inheritance is characterized by the GCP Audit Program as an identity and access management risk, whereas COBIT associates it with DSS05 and APO13, thereby amplifying the risk from a governance and security services standpoint. Collectively, these cases demonstrate that although the hyperscaler audit programs focus on various aspects, COBIT integrates them within the framework of enterprise governance and digital trust objectives.

Table 1. Comparative Audit Domains and Unique Risk Emphases Across ISACA Cloud Audit Program

Audit Program	**Primary Focus**	**Key Audit Scope Areas**	**Major Risk Emphasis**	**COBIT2019 Governance Objectives Alignment**
Amazon Web Services Audit Program (2019)	Configuration-centric	Governance, network configuration, asset configuration, logical access control, data encryption, incident response, logging & monitoring, disaster recovery	Misconfiguration (e.g., open SSH ports, single-factor authentication, excessive IAM rights)	BAI09 (Manage Assets), DSS01 (Manage Operations), DSS05 (Manage Security Services)
Microsoft Azure Audit Program (2020)	Continuity-cen tric	Governance, network configuration, IAM, resource security, logging, monitoring, incident response, data encryption	Continuity and resilience, shared responsibility for data integrity, outage risks in Active Directory and MFA	DSS04 (Manage Continuity), APO12 (Manage Risk), DSS05 (Manage Security Services)

Cloud Computing Audit Program (2016)	Governance-centric	Cloud governance, vendor management, contractual compliance	Third-party dependency, transborder PII risks, immaturity of providers, compliance complexity	EDM01 (Governance Framework), APO01 (Manage the IT Management Framework), APO10 (Manage Suppliers)
Google Cloud Platform Audit Program (2023)	Hierarchy- & IAM-centric	Governance, network configuration, resource management, IAM, data security, incident response, continuity, logging & monitoring	IAM inheritance and role propagation risks, misconfigurations, rapid service evolution	DSS05 (Manage Security Services), APO13 (Manage Security), MEA02 (Monitor, Evaluate and Assess the System of Internal Control)

Table 1 compares ISACA's audit programs for AWS (2019), Azure (2020), GCP (2023), and the general Cloud Computing Audit Program (2016). While common domains such as governance, IAM, monitoring, and incident response appear across all programs, each emphasizes unique risks: AWS highlights misconfiguration, Azure stresses shared responsibility and continuity, GCP focuses on adaptability and IAM hierarchy, and the general program provides foundational multi-cloud and vendor risk guidance.

5. Conclusion

This study presented the first structured comparative analysis of ISACA's hyperscaler audit programs for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), alongside the generalized Cloud Computing Audit Program (CCAP), mapped to the governance objectives of COBIT 2019. The analysis highlighted distinct orientations across the programs: AWS is configuration-centric, emphasizing the remediation of misconfigurations and insecure defaults; Azure is continuity-centric, stressing shared responsibility, resilience, and recovery; GCP is hierarchy-centric, reflecting its focus on identity inheritance, organizational structures, and logging practices, while the CCAP is governance-centric, offering broad principles for vendor management and compliance. When aligned with COBIT 2019, Azure demonstrated the strongest integration with governance objectives, particularly in continuity and operational assurance, whereas AWS and GCP revealed weaker governance linkages. This mapping exposed strengths, limitations, and opportunities for improving alignment through COBIT's framework.

The findings suggest that auditors should move beyond checklist-based assurance models and instead embed audit procedures within governance reviews that are explicitly structured around COBIT. This integration ensures that audit outcomes not only test technical controls but also contribute to enterprise objectives of value delivery, risk optimization, and accountability. For organizations operating in multi-cloud environments, this requires synchronization of hyperscaler-specific

audits through unified risk registers, centralized compliance dashboards, and consistent governance reporting mechanisms.

Future directions emphasize the role of automation and intelligent audit tooling in maintaining audit relevance within rapidly evolving cloud ecosystems. Automated control testing, AI-assisted log analysis, and COBIT-aligned audit orchestration platforms can transform periodic audits into continuous assurance practices. Research and practice should focus on developing COBIT-aligned automation frameworks and validation models that allow enterprises to achieve scalable, repeatable, and governance-driven audit outcomes in multi-cloud contexts.

References

1. Alhassan, I., Sammon, D., & Daly, M. (2018). Data governance activities: An analysis of the literature. *Journal of Decision Systems, 27*(sup1), 64–81.
2. Alles, M., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous auditing: A new view. *Audit Research Monographs, 1*(1), 1–14.
3. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40.
4. Bowers, J., & Davis, K. (2019). Trust, risk, and governance in cloud outsourcing. *Computer Law & Security Review, 35*(3), 1–10.
5. De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2020). COBIT as a framework for enterprise governance of IT. *Journal of Information Systems, 34*(2), 67–75.
6. Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107–115.
7. Fairfield, J. (2020). Quantifying cyber risk: The role of cyber risk quantification in enterprise governance. *Journal of Cybersecurity, 6*(1), 1–12.
8. Faniyi, F., & Bahsoon, R. (2016). A systematic review of service level management in the cloud. *ACM Computing Surveys, 48*(3), 1–27.
9. Fernandez, E. B., Hashizume, K., & Washizaki, H. (2016). Cloud computing security patterns: A survey. *International Journal of Cloud Computing, 5*(1/2), 3–16.
10. Gartner. (2021). *Forecast: Public Cloud Services, Worldwide, 2021–2027*. Gartner Research.
11. Gunasekera, D., Nguyen, H., & Colman, A. (2020). Security misconfigurations in cloud computing: Risks and countermeasures. *Future Generation Computer Systems, 111*, 327–340.
12. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 1–13.
13. ISACA. (2016). *IS Audit/Assurance Program: Cloud Computing*. ISACA.
14. ISACA. (2019). *Amazon Web Services (AWS) Audit Program*. ISACA.
15. ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. ISACA.
16. ISACA. (2020). *Microsoft Azure Audit Program*. ISACA.
17. ISACA. (2023). *Google Cloud Platform (GCP) Audit Program*. ISACA.
18. Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems, 24*(1), 91–112.
19. Wang, Y., Chen, X., & Liu, Y. (2019). Security misconfiguration in cloud computing: An empirical study. *Computers & Security, 87*, 101602.