© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719815

Multi-Cloud Governance Framework for Secure and Scalable Enterprise Cloud Adoption in Saudi Arabia

MOHSIN TAHIR
ORCID: 0009-0007-2937-2587

Abstract- ***Multi-cloud adoption is shifting from an optional sourcing tactic to a strategic operating model for Saudi enterprises that need to scale digital services, protect regulated data and sustain business continuity across complex provider ecosystems. This paper proposes a governance framework for secure and scalable enterprise cloud adoption in Saudi Arabia, with a focus on critical workloads in government services, banking, energy, healthcare, logistics, retail, and industrial operations. The paper adopts a structured narrative review approach influenced by recent systematic review practice in cloud computing, social mobile analytics and cloud-based service environments. Literature and standards published between 2020 and 2025 were synthesised to identify domains of governance, barriers to adoption, security controls, mechanisms of resilience and enablers of implementation. The review argues that delivering multi-cloud value is more than just spreading workloads across multiple providers. Value is delivered when executive accountability, data classification, identity governance, policy-as-code, observability, financial control, incident response, sovereignty requirements and vendor exit planning are managed by a single control plane. Governance should also be aligned with the Saudi context in terms of national cybersecurity controls, cloud service provisioning rules, data localisation expectations, and Vision 2030 digital transformation priorities. Our proposed framework has six dimensions: Strategic alignment, regulatory compliance, secure architecture, operational resilience, FinOps enabled scalability and continuous assurance. The review is translated into an adoption roadmap with two graphical models and two synthesis tables. The study concludes that Saudi enterprises can reduce vendor dependency and accelerate innovation via multi-cloud but only if governance is continuous, evidence-based and embedded into engineering workflows.***

Keywords: Multi-Cloud Governance, Enterprise Cloud Adoption, Saudi Arabia, Cybersecurity, Cloud Compliance, Scalable Cloud Architecture, Cloud Resilience, Finops, Cloud Security, Digital Transformation.

I. INTRODUCTION

Cloud computing has become the basis for enterprise digital transformation, powering elastic infrastructure, platform services, data analytics, artificial intelligence, collaboration, and rapid software delivery. The adoption of cloud in Saudi Arabia is closely aligned with national modernisation objectives, digital government, smart cities, financial technology, digitisation of healthcare, industrial automation and data-driven public services. Meanwhile, enterprises are increasingly using public cloud platforms, local cloud regions, private infrastructure and software-as-a-service apps. This hybrid reality has created the need for multi-cloud governance — the coordinated management of policies, risks, costs, security controls, data flows and operational responsibilities across more than one cloud environment. Multi-cloud without governance can increase agility, but also complexity, shadow IT, redundant tools, unmonitored identities, inconsistent logging, fragmented compliance evidence, and surprise cost overruns. Recent cloud literature has noted that cloud computing, analytics, social platforms and mobile technologies generate substantial organisational benefits but also create challenges such as access control, privacy, interoperability, data processing, platform dependence and energy consumption [1,2]. In the multi-cloud, these problems are exacerbated by the heterogeneity of identity systems, policy models, networking patterns, monitoring formats, security services, and contractual terms among providers.

This topic is very relevant for Saudi companies because digital infrastructure is now a part of national competitiveness. Critical digital infrastructure includes the platforms underpinning government services, banking payments, oil and gas operations, smart grids, airport systems, telecom operations, healthcare records, logistics corridors, e-commerce,

education and citizen-facing applications. A lot of these services have to scale fast, while meeting expectations on cybersecurity, business continuity and data protection. In Saudi Arabia, regulatory bodies have reinforced cloud and cybersecurity requirements and international standards such as NIST CSF 2.0, NIST zero trust guidance, ISO/IEC 27001:2022 and the Cloud Security Alliance Cloud Controls Matrix provide structured control references [3–7]. However, it is not easy to adopt these references in a multi-cloud architecture. Enterprises need to translate high level controls into daily engineering practices, procurement rules, review of access, backup design, workload placement criteria, automated guardrails and recovery testing. So the question of governance is not if the cloud is useful but how to govern adoption in the cloud across providers without stifling innovation.

Multi-cloud governance is not old school IT governance. Traditional governance has often assumed stable infrastructure, a central network perimeter and a small number of technology suppliers. Multi-cloud environments are distributed, programmable and ever changing. Developers can provision resources fast, containers and serverless functions can come and go in minutes, data can be moved between analytics services, and managed services can hide infrastructure details from the enterprise. This dynamism requires controls that are also dynamic. Policy-as-code, identity federation, automated compliance scanning, centralised logging, configuration drift detection, cloud security posture management, workload tagging and FinOps practices are not anymore optional technical tools but governance instruments [8-10]. Simultaneously, senior leadership must determine which workloads can leverage global cloud regions, which must be hosted locally, how to assess provider concentration risk, and how to retain exit options when business-critical systems depend on proprietary services.

The problem addressed in this review is the lack of a Saudi-aligned framework integrating secure architecture, scalability and governance across enterprise multi-cloud adoption. Many organisations treat cloud migration as a series of isolated projects: a customer platform moves to one provider, analytics to another, collaboration services are licensed separately, and legacy systems stay on-premises. The result is an estate where business units accelerate but central governance struggles to keep visibility. Security teams might not see all workloads, finance teams might not know about consumption trends, compliance teams might be manually gathering evidence, and operations teams might not have standard recovery playbooks. Such a governance framework should bring these functions together to ensure adoption is secure, scalable, auditable and economically controlled. This review, therefore, develops a practical model that can guide Saudi enterprises, cloud architects, cybersecurity leaders, regulators, auditors and digital transformation teams.

II. AIM, OBJECTIVES AND CONTRIBUTION

This review aims to develop a multi-cloud governance framework for secure and scalable enterprise cloud adoption in Saudi Arabia. The first goal is to find governance problems caused by enterprises adopting multiple cloud providers These problems include fragmentation of identities, inconsistent security baselines, uncertainties over data residency, dependency on services, gaps in observability, opacity of costs and burden of proving regulatory compliance. The second aim is to synthesise security and compliance controls that can support Saudi cloud adoption, including zero trust access, data classification, encryption, continuous monitoring, incident response, third-party risk management and cloud resilience testing. Thirdly, we want to connect governance with scalability. Enterprises need to secure cloud platforms, and scale their services to meet increasing demand, volume of data and digital operations. The fourth goal is to create an adoption roadmap suitable for Saudi organisations operating in the context of the national digital transformation initiatives and regional regulatory expectations. The fifth objective is to discuss future research opportunities to validate empirically the use of Saudi organisational case studies, maturity assessment and cloud performance data.

We make three contributions in this paper. First, it consolidates recent literature on cloud adoption, multi-cloud security, zero trust, FinOps and cloud governance into a single enterprise framework. Second, it situates these concepts within the Saudi Arabian context, emphasising local compliance,

critical digital infrastructure, sovereignty concerns, and Vision 2030 digital growth. Third, it offers translation of the review into actionable guidance in the way of two conceptual figures and two tables. The framework is neither a vendor product nor does it favour one hyperscaler over another. Rather it describes governance capabilities that should be in place regardless of the provider selected. This is an important distinction because a lot of enterprise cloud failures aren't caused by a weak provider; they are caused by weak ownership, unclear policies, missing telemetry or unmanaged organisational change.

III. REVIEW METHODOLOGY

In this paper, we adopt a structured narrative review methodology, applying principles from systematic literature reviews. The attached Springer style reference paper followed a transparent process, starting with research area selection, research question formulation, search strategy, article retrieval, quality assessment and results reporting. A similar logic was used here but the scope was adapted to multi-cloud governance and Saudi enterprise adoption. The review was not designed as a meta-analysis as the evidence base encompasses academic articles, international standards, national regulatory documents, practitioner frameworks and technology governance guidance. Such diversity is appropriate for cloud governance, since the topic lies at the intersection of information systems research, cybersecurity regulation, enterprise architecture, procurement, service management and software engineering.

The review was in five stages. The first phase explained the research scope based on the secure and scalable multi-cloud adoption in Saudi Arabia. In the second stage, the sources published from 2020 to 2025 were identified by terms such as multi-cloud governance, cloud security, cloud adoption, zero trust architecture, cloud controls, cloud compliance, FinOps, cloud cost governance, Saudi cloud computing, data residency, cloud resilience and critical digital infrastructure. The third step was to filter sources by relevance to enterprise adoption, security governance, operational scalability, compliance or cloud resilience. The fourth step was to code the literature into governance themes including strategy and operating model, data and sovereignty, identity and access, secure architecture, compliance evidence, FinOps, monitoring and reliability, vendor and third-party risk, workforce capability. In the fifth stage, themes were synthesised into a framework and a roadmap. Sources were prioritised if they contained existing controls, clear governance mechanisms or cloud adoption challenges that were pertinent to regulated organisations.

There are limitations to this methodology. Instead of confidential cloud architecture documents from Saudi enterprises, it is based on publicly available literature and standards. It also does not quantify cloud cost savings, service level improvements or cybersecurity incident reduction using primary operational data. But the review is useful because many enterprises are still developing their governance maturity and need a conceptual framework before they can do benchmarking or field measurement. Future research needs to empirically validate the proposed framework by interviewing Saudi cloud architects, maturity scoring of regulated organisations and comparative case studies of public sector, banking, telecom and energy enterprises.

IV. SAUDI CLOUD ADOPTION CONTEXTS

Several forces shape the environment for cloud adoption in Saudi Arabia. Vision 2030 promotes a digital government, data-driven services, growth of the private sector, smart cities and localisation of advanced technology capabilities. Businesses need platforms that can scale to deliver customer-facing services, analytics, automation and artificial intelligence. At the same time, national regulations on cybersecurity and the cloud require better governance of information assets. Saudi cloud policy is not only a technology policy, it is an economic and sovereignty policy too because cloud platforms increasingly host data, processes and decision intelligence that impact citizens, businesses and critical sectors. So cloud adoption decisions must include not just speed and cost, but also control, accountability, recoverability and local regulatory alignment.

Adopting multi-cloud can support Saudi enterprises in many ways. It can reduce dependency on a single provider, allow workload placement based on

regulatory or latency needs, improve negotiation flexibility, facilitate disaster recovery across independent environments and empower teams to leverage specialised services from different providers . For example, an enterprise might have one provider for analytics, another for collaboration, a local cloud region for regulated workloads, and private infrastructure for latency-sensitive operational technology. But each new platform added increases the governance burden. Data classifications must be mapped to allowed locations, identity roles standardised, network connectivity segmented, logs normalised and incident response must work across provider boundaries. Therefore, cloud governance in Saudi Arabia requires the best global practices and local interpretation [3,5,6].

The meaning of scalability is also altered by the regulatory context. The scalability is often described as the ability to add compute or storage capacity on demand. Scalability adoption means scalability controls with usage for a regulated Saudi enterprise. When a dev team spins up a new cloud account, that account should automatically inherit baseline logging, encryption, tagging, budget alerts, vulnerability scanning and identity controls. If a workload is promoted from test to production, its risk classification should trigger additional approval, backup and monitoring requirements. If data is sensitive or there are local residency expectations, placement rules should ensure that they are not accidentally deployed to the wrong region. Therefore, scalable governance is a matter of automation, not manual review.

V. LITERATURE SYNTHESIS

The literature identifies several recurrent themes of governance. The first theme is security with a focus on identity. Zero trust guidance states that access decisions should be based on identity, device posture, context, resource sensitivity, and continuous verification, not implicit trust of a network perimeter [4,11]. In a multi-cloud environment, identity becomes the control anchor as users, service accounts, machines and applications operate across multiple environments. “Federated identity, privileged access management, just-in-time access, multi-factor authentication and service account lifecycle governance are essential. Another theme is consistency around configuration and policy. Multi-cloud environments often break down because of differences in security baselines between providers. Enterprises require baseline controls for encryption, key management, network segmentation, logging, vulnerability management, backup, and incident response that can be implemented consistently even when provider services differ [7,12].

Data governance is the third theme. Cloud adoption often leads to data sprawl without central classification, as teams create data lakes, analytics workspaces, backups, and replicated datasets. Saudi businesses need to define data ownership, data classification, data residency requirements, data retention rules, data encryption standards and cross border data transfer controls. Governance should link data policy with technical guardrails: storage buckets shouldn’t be publicly exposed, sensitive datasets should be tokenized or encrypted, and access should be logged and reviewed. The fourth theme is about observability and resilience. Enterprises cannot manage what they cannot see. Centralised logging, metrics, traces, asset inventories and security telemetry can be leveraged by operations and security teams to detect failures, misconfigurations and abnormal behaviour. Cloud resilience requires proven backup, recovery, failover, incident response and crisis communication processes. Multi-cloud risk research highlights that provider diversity does not necessarily imply resilience [13]. Systemic fragility can result from unmanaged dependencies.

Fifth theme is financial governance. Over-provisioning, duplicating environments, leaving idle assets on and choosing expensive managed services without business review can cause cloud scalability to spiral out of control and costs to balloon. FinOps is an operating model that creates financial accountability by aligning engineering, finance and business teams [8]. FinOps also helps with governance in a multi-cloud environment by providing visibility into consumption via tags, budgets, unit economics and chargeback models. The sixth theme is vendor and third-party risk. Multi-Clouds increase the number of contractual relationships, shared responsibility boundaries, audit requirements and service dependencies. Enterprises need to understand what controls are managed by cloud providers, what are

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719815

tenant controls, and what evidence is joint. This is especially true for Saudi critical digital infrastructure, where service interruption or data exposure could lead to national, economic or social consequences.

VI. PROPOSED MULTI-CLOUD GOVERNANCE FRAMEWORKS

The proposed framework consists of six dimensions. The first dimension is strategy fit. Executive leadership should determine the reasons for multi-cloud adoption: resilience, regulatory placement, access to innovation, cost optimisation, avoiding lock-in or all of these. The strategy must define critical workloads, targeted business outcomes, risk appetite, provider selection criteria and success measures. Without this alignment, multi-cloud becomes accidental architecture driven by project preference versus enterprise design. The second is compliance with regulations. Saudi enterprises should map local cybersecurity and cloud obligations to control requirements, evidence artefacts and owners responsible. Compliance should be operationalized using automated checks, where possible. A policy can for example prevent unencrypted storage, require approved regions, enforce key rotation and generate evidence for audit dashboards.

A third dimension is secure architecture. A multi-cloud architecture should enforce zero trust principles, segmentation, secure connectivity, baseline encryption, centralised identity, secret management, image governance, vulnerability management, and continuous posture monitoring. The secure architecture must also consider cloud-native services such as containers, serverless functions, managed databases, and data pipelines. The fourth dimension is operational resilience. Enterprises should design recovery tiers based on workload criticality, test backup restoration, create cross-provider incident playbooks and monitor service level objectives. Resilience isn't just about provider redundancy, it needs architecture reviews, dependency mapping, disaster recovery drills and post-incident learning. The fifth dimension is scalable governance of operations. Standard landing zones, reusable infrastructure templates, tagging standards, workload onboarding, guardrails and automated compliance pipelines should support cloud adoption. 6. The sixth dimension is the ongoing assurance. Governance should be measured by metrics such as policy violations, open vulnerabilities, privileged access exceptions, backup success rate, cost variance, service availability, audit readiness and incident response time.

This framework is shown as a unified governance control plane in Figure 1. The real workhorse is the control plane, which manages policies across public clouds, on-prem clouds, enterprise core systems, compliance layers and FinOps platforms. It requires one tool. It requires a common operating model. The control plane should have cloud asset inventories, identity providers, security posture tools, logging platforms, ticketing systems, configuration repositories and executive dashboards. This integration helps governance shift from periodic reporting to near real-time assurance. For example, if an untagged production database appeared in a cloud account the system could alert the owner, block public exposure, enforce encryption and record evidence of remediation. FinOps can tell engineering if a workload is over budget before cost becomes a board-level concern. If a privileged account is created, access governance can demand approval and expiration.

VII. IMPLEMENTATION ROADMAP

A Saudi business shouldn't try to manage all cloud risks at once. Maturity stages should be followed for implementation. The first phase is discovery and classification. Enterprises need to develop a cloud inventory, identify business owners, categorise data and workloads, document regulatory requirements and map existing provider usage. The second stage is the design of the foundation. "This includes standard landing zones, identity federation, logging baselines, network segmentation, encryption defaults, approved regions and tagging." Stage three is automatic barriers. Infrastructure-as-code, policy-as-code, and continuous compliance scanning should stop avoidable breaches. Stage four is resilience and FinOps integration Workload recovery tiers, backup tests, cost dashboards, optimisation reviews, and service level reporting should be routine. The fifth stage is ongoing assurance. It includes executive reporting, third-party risk reviews, red team exercises,

cyber drills, audit evidence generation and periodic provider exit planning.

A number of barriers could hinder implementation. Legacy systems may not get along with cloud identity and logging. If business units fear that centralised policies will slow down delivery, they may resist. Skills shortages may hinder advanced automation. Procurement may be optimised for individual project delivery rather than enterprise-wide cloud operating models. Native tools from the provider can produce inconsistent terminology and reporting. Interpretation of data residency may need legal and compliance review. Where platforms are shared by more than one department, cost ownership can be ambiguous. Those barriers are as much organisational as they are technical. Key enablers include executive sponsorship, cloud centres of excellence, cybersecurity leadership, architecture review boards, FinOps teams, standardised procurement, local cloud regions, managed service partners, and ongoing training. Cloud teams treat policies as product features. Security teams provide reusable patterns, not just approval gates. This improves governance maturity.

VIII. DISCUSSION

Think of multi-cloud governance as a dynamic capability. The enterprise exists in an environment of constantly changing technology, threats, regulations and business requirements. A static cloud policy document can't keep up with this reality." Instead governance must be built into the cloud lifecycle from planning to deployment, operation, optimisation and retirement. So, the proposed framework emphasises guardrails, observability and continuous assurance. The best governance models are not those that prevent change but those that make safe change repeatable. Such approach is in line with the need for accelerated digital transformation and high trust in critical services in Saudi Arabia. Those companies that can demonstrate where their cloud workloads live, how they're protected and recovered and what they cost are in a better place to scale responsibly.

Multi-cloud also creates a strategic tension between portability and specialisation. Portability mitigates vendor lock-in because workloads can be more easily moved between providers, but could inhibit the enterprise from taking full advantage of advanced managed services. Specialisation allows teams to access powerful analytics, artificial intelligence and platform services, but can also foster dependence. Governance should not force every workload into the lowest common denominator architecture. Instead, every workload should have a rationale for placement, an exit strategy and a record of risk acceptance. High-risk regulated systems may need more portability and local control. Low data sensitivity and resilience requirements may warrant provider specialisation for innovation workloads. This pragmatic approach is more realistic than treating all cloud services as equals. It also highlights the role of culture in the framework. Multi-cloud governance breaks down when security, finance, legal, procurement and engineering work in silos. Engineering teams need the freedom to build, but they need to understand cost and risk. Security teams need control, and they need to turn controls into reusable automation. Finance teams want visibility but need to know that cloud cost is a function of architecture and demand. "Compliance teams want evidence but they should not be dependent on manual spreadsheets." A mature operating model creates shared accountability. This is a reflection of the cloud shared responsibility model at the organisational level. Providers secure some parts of the platform, tenants secure their configurations and leadership secures the governance system that connects decisions to accountability.

IX. MANAGERIAL IMPLICATIONS AND FUTURE RESEARCH

The framework has implications for executives, cloud architects, cybersecurity teams, finance units and regulators. The key takeaway for executives: Multi-cloud adoption calls for clarity at the board level on who's in charge. Decisions about workload placement, provider concentration, data residency and acceptable downtime should not be left entirely up to project teams. A cloud steering committee or a cloud centre of excellence can translate strategy into standards, but executive sponsorship is required to resolve conflicts between the speed of innovation, regulatory caution and cost discipline. For cloud architects, this means that governance requirements need to be baked into reference architectures from the very start. Architectural foundations, not an afterthought.

Landing zones, identity federation, centralised logging, key management, backup design and network segmentation. The framework advocates for cybersecurity teams to move from manual approval to automated guardrails. Security scales better when safe patterns are delivered as reusable modules and violations are detected early in the delivery pipeline.

The framework shows that for finance and procurement teams; multi-cloud governance must include commercial resilience. Cloud contracts must define service responsibilities, audit rights, support models, data return procedures, termination assistance, region commitments and incident notification requirements. Procurement should take into account more than the unit prices to evaluate control transparency, portability, dependency on managed service and quality of evidence. FinOps teams should be speaking the language of business. They should be able to translate consumption into cost per transaction, cost per user, cost per workload, and cost per service outcome. This allows leaders to differentiate between waste and healthy scaling. The framework offers evidence-based confidence to regulators and auditors. Assurance can increasingly depend on automated evidence rather than static screenshots, such as reports of policy compliance, access review logs, encryption status, backup test results, vulnerability trends, and incident metrics. This type of evidence increases the timeliness of the audits and the burden on operational teams.

Also take into account the adoption by sector. Government platforms may focus on data sovereignty, trust of the citizen, interoperability and continuity of service. Banks and payment providers could show the strength of transactions, fraud monitoring, identity assurance and regulatory evidence. Both cloud systems and operational technology interfaces need to be secured by energy and industrial firms. Healthcare organisations should focus on patient data confidentiality, availability of clinical platforms and continuity of diagnostic services. Retail and logistics companies could focus on elastic customer demand, supply-chain visibility, and mobile application integration. These sector differences do not require different governance models but different workload classifications, control depths and recovery tiers within an enterprise framework. Thus, a mature governance model combines common policy with sector-sensitive implementation.

Future research should shift from conceptual governance to empirical validation. A potential research avenue might be interviews with Saudi cloud leaders to identify barriers to adoption and maturity patterns. Another stream could examine the reliability, cost and compliance results of single-cloud, hybrid-cloud and multi-cloud strategies across Saudi sectors. A third stream could develop maturity indices for automated cloud governance, with metrics for policy coverage, remediation speed, identity hygiene, audit readiness, cost predictability and recovery testing. A fourth stream could be on the relationship between localisation, sovereign cloud services and enterprise innovation. Finally, research should investigate how artificial intelligence can improve cloud governance through identifying misconfigurations, suggesting cost optimisation, summarising audit evidence and predicting resilience risks. The studies would provide the proposed framework with an empirical foundation for Saudi digital transformation.

X. CONCLUSION

Adopting multi-cloud can help Saudi enterprises to build scalable, resilient and innovative digital services, but it also introduces complexity that needs to be deliberately governed. Based on strategic alignment, regulatory compliance, secure architecture, operational resilience, scalable operating governance, and continuous assurance, this review developed a Saudi-aligned governance framework. The key conclusion is that multi-cloud should be viewed as an enterprise operating model not a collection of provider accounts. Identity governance, data classification, automated guardrails, centralised observability, FinOps practices, cloud resilience testing, and vendor risk management are all important for secure and scalable adoption. These capabilities are vital for trust, continuity and compliance for critical digital infrastructure.

Practical adoption is also supported by clear data stewardship, proven recovery evidence, shared dashboards, automated exception handling, local engineering capability, transparent risk acceptance, and routine post-implementation learning across

business, security, finance, legal, procurement and operations teams. Cloud teams that capture architectural decisions, identify key dependencies, audit privileged identities, validate backup restore, and connect service reliability metrics to customer, regulator, and executive expectations seem to derive more value. They should also define exception life cycles to ensure that temporary deviations from baseline controls do not become permanent hidden risks. Each exception should have: named owner, expiry date, compensating control, business justification and evidence of review. Likewise, a cloud architecture review should not be limited to when a production launch occurs; it should be recurring as data categories change, services are re-architected, providers introduce new managed capabilities, or threat intelligence signals new exposures. Governance leaders should measure adoption with pragmatic metrics such as the percentage of workloads onboarded with standard landing zones, the percentage of storage services encrypted with approved keys, the number of unmanaged identities, the mean time to remediate critical misconfigurations, the backup restoration success rate, the budget variance, and the percentage of cloud assets with full business tags. These indicators enable senior management to determine whether multi-cloud complexity is being converted into resilience or simply accumulating as invisible operational debt. Also, local capacity development is important. Saudi enterprises need to invest in cloud architecture training, secure DevOps skills, Arabic and English policy documentation, local managed-service ecosystems, and partnerships with universities and professional bodies. This kind of capacity building reduces reliance on external consultants and helps support the broader national goal of developing advanced digital talent. Governance is a development practice that improves enterprise trust, cyber readiness, financial discipline and long-term cloud innovation capability. Regular tabletop exercises, architecture retrospectives, supplier reviews and control-owner workshops further ensure lessons from incidents, audits, migrations and cost anomalies are translated into improved standards for future deployments and increasingly complex regulated digital ecosystems, securely, measurably, sustainably. Our proposed roadmap suggests starting with discovery and classification, and moving towards landing zones, automated guardrails, resilience testing, FinOps integration and continuous assurance. The Saudi enterprises need to focus on the workloads supporting the citizen services, payment systems, energy operations, healthcare, telecom, logistics and strategic industrial sectors. Future research should validate the framework through Saudi case studies, cloud maturity assessments, interviews with cloud security leaders, and quantitative analysis of cost, reliability, and compliance outcomes before and after governance automation. The broader point is clear: multi-cloud doesn’t automatically reduce risk. Governance as an intelligent system that produces evidence and improves continuously reduces risk.

Figures

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719815

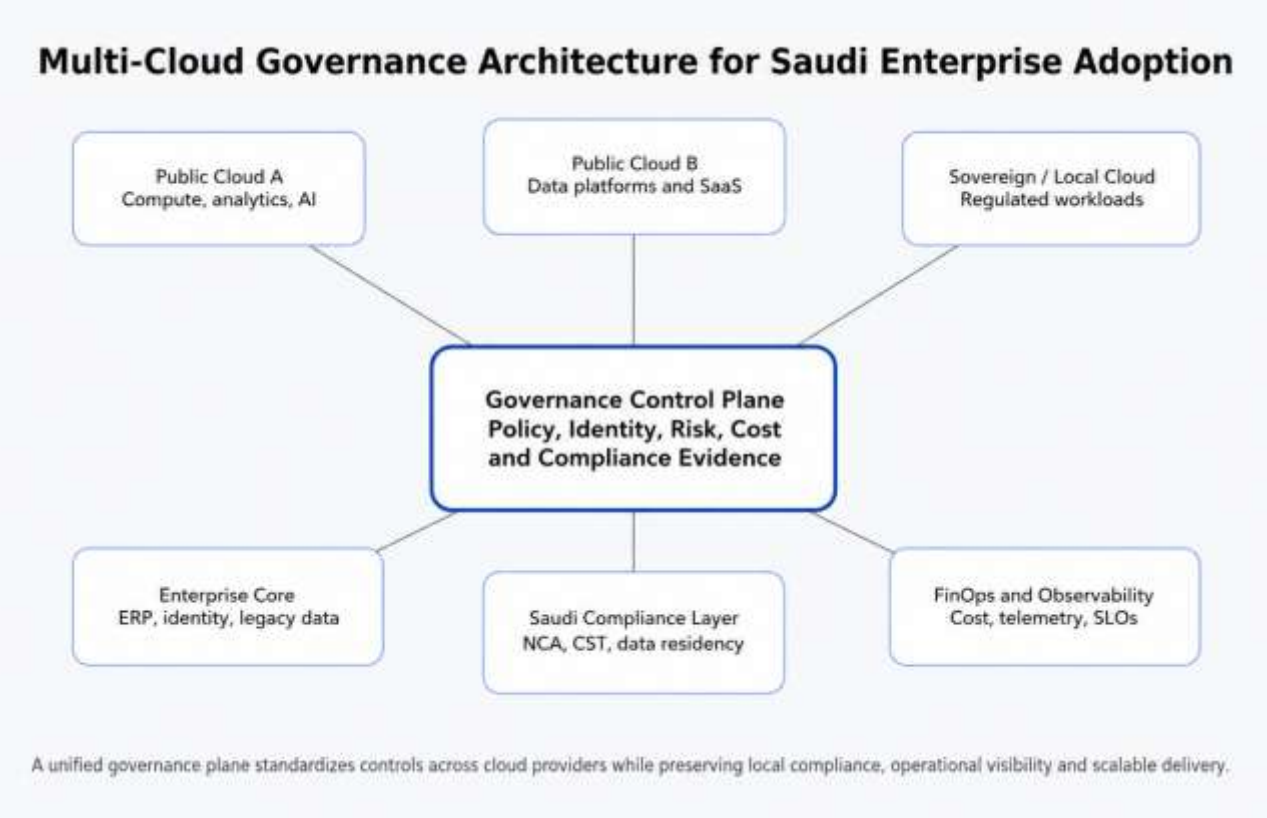

Figure 1. Multi-cloud governance architecture for secure and scalable enterprise cloud adoption in Saudi Arabia.

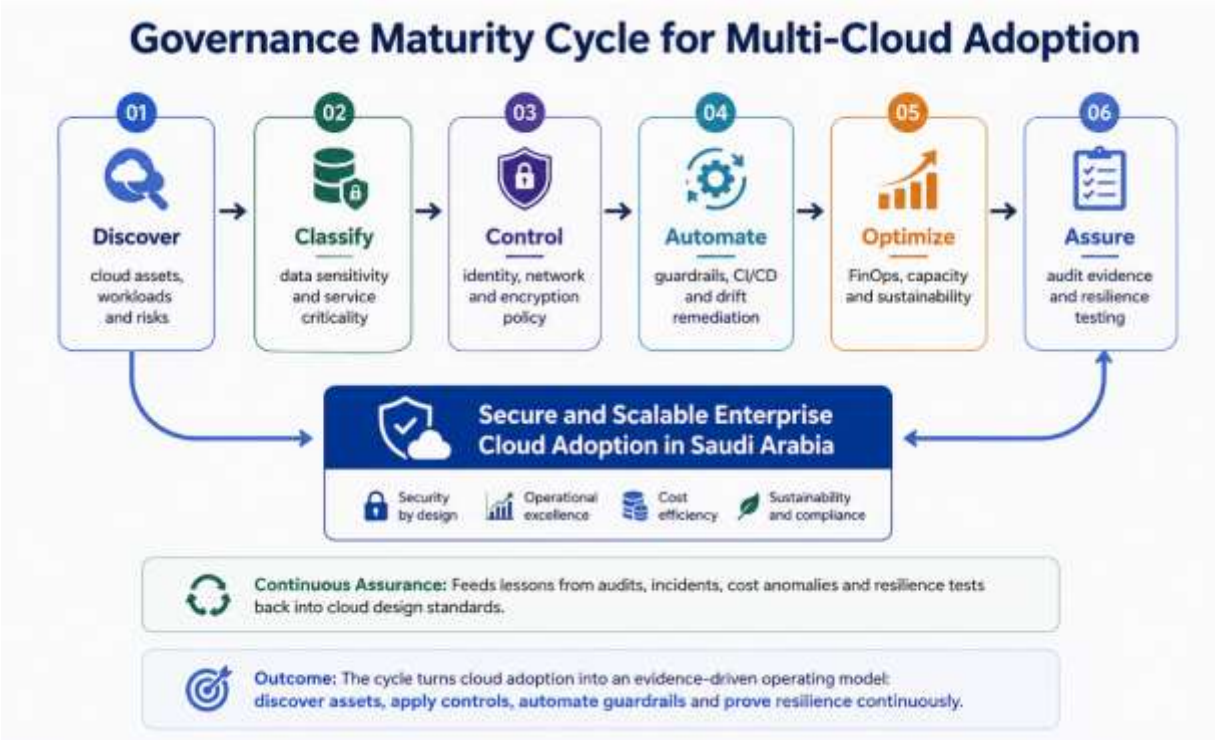

Figure 2. Governance maturity cycle linking discovery, classification, controls, automation, optimization and assurance.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719815

Tables

Table 1. Review synthesis of multi-cloud governance domains and enterprise value.

Governance domain	Enterprise cloud application	Security and scalability value	Saudi adoption consideration
Strategic alignment	Define cloud principles, provider criteria, workload tiers and risk appetite	Prevents accidental multi-cloud sprawl and aligns investment with business outcomes	Link cloud decisions to Vision 2030, critical services and sector priorities
Data and sovereignty	Classify data, set approved regions, govern keys and retention	Reduces exposure of sensitive information while enabling analytics at scale	Reflect NCA controls, CST rules and local data expectations
Identity governance	Federated identity, MFA, privileged access and service account lifecycle	Controls access consistently across providers and workloads	Integrate enterprise IAM with cloud tenants and Saudi workforce accountability
Secure architecture	Landing zones, encryption, network segmentation and posture management	Makes security repeatable without slowing project delivery	Apply standardized guardrails before production onboarding
FinOps and scaling	Tagging, budgets, unit economics, rightsizing and demand forecasting	Keeps elastic consumption economically sustainable	Create shared ownership between finance, engineering and business units
Resilience assurance	Backup tests, failover playbooks, logging and incident simulation	Improves continuity for critical digital infrastructure	Prioritize payments, energy, telecom, healthcare and government workloads

Table 2. Implementation roadmap for Saudi multi-cloud governance maturity.

Phase	Governance focus	Priority actions	Expected output
1. Discover	Inventory and risk baseline	Map cloud accounts, providers, SaaS, data owners, identities and critical workloads	Single cloud asset register and workload classification baseline
2. Standardize	Landing zones and common controls	Deploy baseline IAM, logging, tagging, encryption, network segmentation and approved regions	Controlled onboarding pattern for new cloud workloads
3. Automate	Policy-as-code and guardrails	Integrate CI/CD checks, compliance scanning, budget alerts and remediation workflows	Fewer misconfigurations and faster audit evidence collection
4. Assure	Resilience and incident readiness	Test recovery tiers, run cyber drills, review third-party risk and validate backup restoration	Measurable continuity confidence for critical digital services
5. Optimize	FinOps, skills and continuous improvement	Use cost analytics, rightsizing, workforce training, maturity scoring and executive dashboards	Sustainable cloud scaling with local capability development

REFERENCES

[1] Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., et al. (2020). Transformative effects of IoT, blockchain and artificial intelligence on cloud computing. Internet of Things, 12, 100250.

[2] Saxena, D., Gupta, R., & Singh, A. K. (2021). A survey and comparative study on multi-cloud architectures: Emerging issues and challenges for cloud federation. Journal of Cloud Computing Research.

[3] Saudi Communications, Space and Technology Commission. (2024). Cloud Computing Services Provisioning Regulations. Riyadh: CST.

[4] National Cybersecurity Authority. (2024). Essential Cybersecurity Controls ECC-2:2024. Riyadh: NCA.

[5] National Cybersecurity Authority. (2024). Cloud Cybersecurity Controls CCC-2:2024. Riyadh: NCA.

[6] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. NIST Cybersecurity White Paper 29.

[7] Cloud Security Alliance. (2021). Cloud Controls Matrix Version 4.0. Seattle: CSA.

[8] FinOps Foundation. (2024). FinOps Framework: Operating model for cloud financial management. Linux Foundation.

[9] International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Geneva: ISO.

[10] International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security controls. Geneva: ISO.

[11] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207.

[12] Rodigari, S., O'Shea, D., McCarthy, P., McCarry, M., & McSweeney, S. (2021). Performance analysis of zero-trust multi-cloud. IEEE Cloud Computing Workshops.

[13] Reece, M., Lander, T. E., Stoffolano, M., Sampson, A., Dykstra, J., Mittal, S., & Rastogi, N. (2023). Systemic risk and vulnerability analysis of multi-cloud environments. arXiv preprint.

[14] Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero trust: Applications, challenges, and opportunities. ACM Computing Surveys preprint.

[15] Khan, A., & Gupta, S. (2021). Cloud governance challenges and opportunities in enterprise digital transformation. Information Systems Frontiers, 23, 1-18.

[16] Kumar, R., & Goyal, R. (2022). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 43, 100434.

[17] Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of SMEs in Saudi Arabia. Sustainability, 16, 1880.

[18] Almulhem, A. (2020). Cloud computing adoption in Saudi Arabia: Security, compliance and organizational readiness. Journal of Information Security and Applications, 52, 102492.

[19] Alotaibi, M., & Almagwashi, H. (2021). Cybersecurity governance in Saudi organizations: Challenges and policy directions. International Journal of Advanced Computer Science and Applications, 12(9), 251-260.

[20] Alahmadi, B., & Duncan, B. (2021). Cybersecurity risk management in cloud computing for critical organizations. Computers & Security, 108, 102347.

[21] Dillon, T., & Vossen, G. (2020). Cloud computing and enterprise architecture: Review of integration and governance issues. Enterprise Information Systems, 14(8), 1083-1105.

[22] Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., & Gadekallu, T. R. (2022). Security and privacy issues in cloud computing: Survey and open challenges. Journal of Cloud Computing, 11, 1-31.

[23] Mohammed, F., Ibrahim, O., & Nilashi, M. (2020). Cloud computing adoption model for government organizations. Telematics and Informatics, 54, 101453.

[24] Alharbi, F., Atkins, A., & Stanier, C. (2020). Strategic value of cloud computing in healthcare and digital government. Health Informatics Journal, 26(4), 2813-2830.

[25] Carvalho, A., & Sousa, P. (2021). Cloud service provider selection and multi-cloud risk management. Journal of Systems and Software, 176, 110948.

[26] Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in cloud computing: A review. Journal of Network and Computer Applications, 184, 103058.

[27] Moura, J., Hutchison, D., & Gomes, D. (2022). Cloud resilience engineering: Concepts, patterns and evaluation metrics. Future Generation Computer Systems, 128, 1-15.

[28] Singh, A., Chatterjee, K., & Buyya, R. (2022). Cloud computing for digital transformation: Governance and sustainability perspectives. Sustainable Computing: Informatics and Systems, 35, 100748.

[29] Rashid, A., & Chaturvedi, A. (2023). Cloud governance and compliance automation for regulated enterprise systems. IEEE Access, 11, 57621-57639.

[30] McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., & Nowrozy, R. (2024). Evaluating cybersecurity governance frameworks for regulatory compliance in emerging digital systems. Computers & Security, 138, 103662.