Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i05.002

OPEN ACCESS

ISSN: 2706-9001 (P)
ISSN: 2707-2584 (O)

Original Research Article

Optimizing Hybrid Cloud Infrastructure for Mission-Critical Government and Enterprise Applications in Saudi Arabia under Vision 2030

Muneer Shaik[1]*
[1]Research Scholar

***Corresponding Author**
Muneer Shaik
Research Scholar

Article History
Received: 06.07.2026
Accepted: 31.08.2026
Published: 07.09.2026

Abstract: Government and enterprise applications increasingly depend on cloud platforms for elasticity, rapid service delivery, analytics and digital integration, yet mission-critical workloads cannot be optimized through a simple public-cloud-first migration. They require deliberate placement across private, public, sovereign and on-premise environments according to service-level objectives, data sensitivity, latency, dependency and recovery requirements. This review examines how hybrid cloud architecture can be optimized for mission-critical applications in Saudi Arabia. It synthesizes literature on multi-cloud orchestration, workload portability, containerized resource management, observability, cybersecurity and resilience, and interprets these findings against Saudi Cloud First policy, Digital Government Authority guidance, Communications, Space and Technology Commission regulations, National Cybersecurity Authority controls and Vision 2030 priorities. The analysis finds that hybrid cloud value depends less on the number of connected platforms than on unified policy, application-aware placement, automated orchestration, end-to-end observability and tested continuity. A Saudi-oriented reference model is proposed in which governance and data classification drive placement decisions, while cloud-native portability, automation and resilience controls sustain service continuity. The review concludes that hybrid cloud can support Vision 2030 digital-government and enterprise goals when architecture is treated as a governed operating model rather than a collection of disconnected infrastructures.

Keywords: Hybrid Cloud, Mission-Critical Applications, Cloud Orchestration, Business Continuity, Cloud-Native, Saudi Arabia, Vision 2030, Digital Government.

1. INTRODUCTION

Cloud computing has become a foundational delivery model for modern digital services because it offers elastic infrastructure, rapid provisioning and access to managed platforms. The NIST definition established the familiar service and deployment models, including public, private and hybrid cloud, while the NIST reference architecture emphasized the roles, controls and interactions required to operate cloud services at scale. Mission-critical applications require a different decision model. Healthcare systems, enterprise resource planning, financial platforms, identity services, government portals and operational systems can carry strict requirements for availability, recovery time, data protection, performance and auditability. Their architecture therefore has to optimize several objectives simultaneously rather than maximize a single variable such as infrastructure utilization.

Hybrid cloud addresses this problem by allowing applications and data to use a controlled combination of private or on-premise resources and external cloud services. Research on multi-cloud orchestration shows that such environments can improve flexibility and service selection, but also introduce interoperability, portability and governance complexity. A systematic review of multi-cloud-native applications similarly identifies availability, security, cost, portability and performance as key non-functional concerns that influence application design and deployment. Hybrid adoption is therefore not merely a procurement choice. It changes how workloads are classified, how components communicate, how failure domains are designed and how operations teams monitor and recover services.

The topic is particularly relevant to Saudi Arabia. National policy has progressively encouraged cloud adoption in government, while current digital-government guidance explicitly recognizes public, private, community and hybrid deployment models and links cloud adoption with productivity, scalability, cost efficiency and business continuity. At the same time, cloud and data-center services operate within national regulatory and cybersecurity requirements. Vision 2030 reporting also places digital infrastructure, whole-of-government platforms and service maturity at the center of the Kingdom's transformation agenda. Consequently, the practical question is not whether mission-critical systems should use cloud, but how hybrid architectures can be governed and optimized so that digital transformation does not weaken service continuity, cybersecurity or data control.

2. Background and Literature Review

Hybrid cloud combines distinct infrastructure domains that remain administratively or technically separate but are connected so that data, workloads or application functions can move or interact across them. The Saudi Digital Government Authority describes hybrid cloud as a composition of distinct cloud services, commonly combining on-premise and off-premise resources, with technology enabling workload or data portability. This is important for mission-critical services because no single hosting model is optimal for every requirement. Highly sensitive data may need tighter control; burst workloads may benefit from public elasticity; legacy platforms may remain on-premise; and disaster-recovery capacity may be distributed to a separate failure domain.

The management layer is decisive. Tomarchio *et al*., reviewed cloud-resource orchestration frameworks and found that multi-cloud operation requires discovery, selection, allocation and management across heterogeneous providers. Alonso *et al*., further show that multi-cloud-native applications create application-level challenges involving architecture, runtime adaptation, DevOps, security and portability. Cloud brokerage research similarly frames heterogeneous services as linked resource-selection and management problems. Federated-cloud research has long highlighted resource discovery, monitoring, allocation and disaster management as core functions.

Cloud-native technologies make hybrid operation more practical. Containers can reduce deployment friction and improve portability, while orchestration systems can place and reschedule components across clusters. However, container resource allocation remains a multi-objective problem involving CPU, memory, latency, cost and service quality. Microservices can isolate application functions and support independent scaling, yet they increase service dependencies and the number of possible failure paths. Reviews of microservice practice and security identify operational complexity, monitoring, authentication, authorization and attack-surface expansion as recurring issues. For mission-critical applications, cloud-native design should improve portability and fault containment.

Resilience is the second major foundation. Application continuity depends on redundancy, but redundancy alone is insufficient if failures cannot be detected or if failover capacity is not validated. Research on anomaly detection and root-cause analysis shows that distributed applications need correlated metrics, traces and logs to localize faults and recover quickly. Saudi digital-government controls likewise emphasize proactive risk management, disaster-recovery planning, technical alternatives and testing of continuity arrangements. These principles suggest that a hybrid architecture is only mission-critical when workload placement, observability, recovery and governance are designed as one operating system.

3. Research Aim, Objectives and Questions

The aim of this review is to identify the architectural and operational practices that can optimize hybrid cloud infrastructure for mission-critical government and enterprise applications in Saudi Arabia. The objectives are to: (1) examine evidence on hybrid and multi-cloud workload placement, orchestration and portability; (2) evaluate resilience, security and observability requirements for critical services; (3) interpret those requirements within Saudi cloud, cybersecurity and digital-government policy; and (4) propose a practical optimization framework aligned with Vision 2030. The review addresses three questions: RQ1:

Which capabilities most strongly determine hybrid-cloud performance and reliability for mission-critical applications? RQ2: How should security, data and continuity constraints shape workload placement? RQ3: What operating model is most suitable for Saudi government and enterprise environments?

4. REVIEW METHODOLOGY

A structured narrative review was used because the research question crosses technical architecture, cloud operations, security, regulation and national digital-transformation policy. Peer-reviewed literature was selected from publisher and index-visible sources associated with IEEE, ACM, Elsevier, Springer, Wiley and other scholarly databases. Search concepts included hybrid cloud, multi-cloud orchestration, cloud brokerage, workload portability, cloud-native applications, container resource allocation, microservice security, observability, disaster recovery and business continuity. Priority was given to systematic reviews, surveys and architecture studies that explain transferable mechanisms rather than vendor-specific product features. Foundational standards were retained where they define widely used cloud concepts.

Saudi policy evidence was drawn from official sources, including the Digital Government Authority, Ministry of Communications and Information Technology, Communications, Space and Technology Commission, National Cybersecurity Authority and Saudi Vision 2030. Sources were included when they directly addressed cloud adoption, data-center regulation, cybersecurity, risk management, continuity or digital-government infrastructure. The synthesis was thematic rather than statistical. Evidence was grouped into five themes: workload placement, orchestration and portability, resilience, security and data governance, and observability/optimization. The final interpretation focuses on design principles that can be applied to mission-critical environments without assuming a specific commercial cloud provider.

5. Thematic Findings and Analysis

5.1 Application-Aware Workload and Data Placement

The first optimization task is application-aware workload placement. Hybrid architecture should begin with a workload and data classification rather than with available infrastructure. A useful placement decision considers business criticality, recovery objectives, latency, data sensitivity, dependency patterns, elasticity, licensing and operational skills. Hybrid-cloud adoption research identifies quality of service and public-cloud security concerns among the most important barriers to adoption. These concerns can be converted into placement criteria: workloads with high sensitivity or tightly coupled legacy dependencies may remain in private or sovereign environments, while stateless digital channels, analytics jobs or burst capacity can exploit external cloud elasticity. Cloud brokerage research supports requirement-driven resource selection across heterogeneous services.

For mission-critical workloads, placement must also account for failure domains. A component should not be distributed across clouds simply because it can be. Distribution is valuable when it reduces a known risk, improves latency, supports regulatory separation or creates recoverable capacity. Otherwise, it may add network dependency and operational complexity. This distinction is essential in enterprise systems where an application, database, storage layer and identity service may have different recovery and performance characteristics. The optimized unit of placement is therefore the service component and its dependency graph, not the application name alone.

5.2 Orchestration, Portability and Cloud-Native Operations

The second theme is orchestration and portability. Hybrid value depends on the ability to deploy, configure and operate workloads consistently across heterogeneous domains. Orchestration frameworks seek to abstract differences among providers and automate resource selection and deployment. Earlier work on portable cloud applications and heterogeneous-cloud orchestration likewise emphasizes model-driven deployment and common descriptions of application components. The MiCADO architecture demonstrates how application-level orchestration can combine microservices, autoscaling and infrastructure management across cloud environments.

In practice, portability should be engineered at several layers. Infrastructure-as-code can standardize networks, virtual machines and policies; container images can standardize application packaging; declarative orchestration can standardize desired state; and CI/CD pipelines can standardize release processes. However, database services, identity systems, proprietary APIs and managed platform features can still create lock-in. Multi-cloud-native research therefore treats portability as a design concern that must be considered during the application lifecycle rather than after deployment. For critical systems, the objective should be controlled portability: enough abstraction to recover or relocate priority components without discarding valuable platform-specific capabilities.

5.3 Resilience, Disaster Recovery and Service Continuity

The third theme is resilience and continuity. Hybrid cloud can strengthen continuity by separating failure domains and maintaining alternate capacity, but this benefit exists only when recovery paths are engineered and tested. Critical applications require explicit service-level objectives, recovery time objectives (RTOs), recovery point objectives (RPOs), dependency maps and failover criteria. Storage replication, backup immutability, alternate connectivity, DNS and identity continuity, and capacity reservation must be designed together. A recovery site that has copied data but insufficient compute, network throughput or authentication services is not a viable continuity architecture.

Distributed cloud-native systems also require rapid detection and diagnosis. Soldani and Brogi show that anomaly detection and root-cause analysis are central challenges in microservice-based cloud applications because failures propagate across interacting services. Unified observability should therefore correlate infrastructure metrics, application performance, logs, traces, security events and change records. For Saudi government services, this operational logic aligns closely with DGA controls that require proactive risk management, continuity planning, technical alternatives, disaster-recovery plans and effectiveness testing. Resilience should thus be measured through successful recovery exercises, not only through nominal redundancy.

5.4 Security, Data Governance and Sovereignty

The fourth theme is security, data governance and sovereignty. Hybrid cloud expands the control surface because identity, network policy, encryption, secrets, logging and configuration must remain consistent across multiple environments. A systematic review of microservice security identifies authentication, authorization, privacy, intrusion detection and service interaction as recurring areas of concern. Multi-cloud security research also highlights the need for unified monitoring and defensive controls across provider boundaries. The practical implication is that security architecture should be centralized in policy but distributed in enforcement. Federated identity, least privilege, segmentation, encryption, key management and continuous posture monitoring need common standards even when workloads run on different platforms.

Saudi regulation makes this dimension especially important. CST's current cloud-service regulations seek to develop the cloud market while defining obligations for providers and users. NCA Cloud Cybersecurity Controls establish security requirements intended to improve cloud-service reliability and resilience. DGA cloud guidance links provider selection and migration to approved data-classification principles. Therefore, optimization cannot treat compliance as a post-deployment audit. Data classification, cybersecurity control mapping and provider eligibility should be inputs to placement decisions before a workload is moved.

5.5 Observability and Continuous Optimization

The fifth theme is observability and continuous optimization. Mission-critical hybrid cloud should operate as a closed control loop: classify, place, observe, evaluate, and rebalance. Resource-management studies show that heterogeneous clouds require ongoing selection and provisioning rather than one-time deployment. In operational terms, dashboards should combine capacity, latency, saturation, error rate, availability, recovery readiness, security status and cost. A change in any one of these indicators can alter the optimal placement of a service.

Optimization should also distinguish steady-state efficiency from resilience headroom. Driving every cluster to maximum utilization can reduce cost but leave insufficient capacity for failover, maintenance or workload bursts. Critical environments need protected reserve capacity and clear priority tiers. Automation can improve this balance by forecasting demand, scaling stateless components, enforcing policies and detecting drift, but high-impact actions should remain bounded by guardrails. Figure 1 summarizes this control-loop model. Its central principle is that hybrid optimization is continuous: placement decisions must be revisited as demand, risk, regulation and application architecture change.

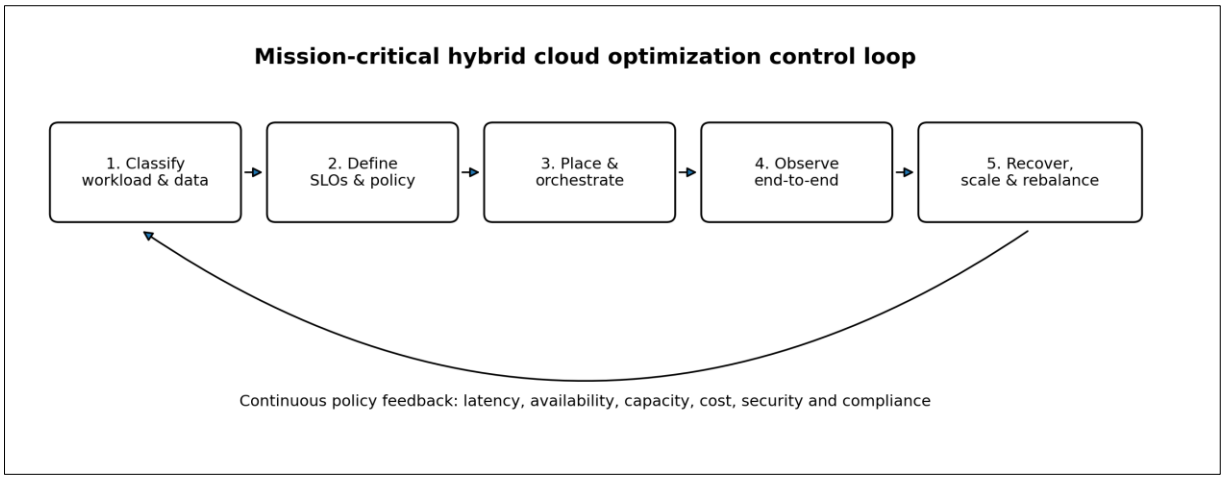

Figure 1: Closed-loop hybrid cloud optimization model for mission-critical applications.

Table 1: Deployment-model trade-offs for mission-critical workloads

Dimension	Private / on-premise	Public cloud	Optimized hybrid approach
Control & data placement	High direct control; suited to tightly governed or legacy systems	Provider-managed control plane and broad managed-service options	Place components according to data classification, criticality and provider controls
Elasticity	Limited by owned/reserved capacity	Rapid elastic scaling	Keep stable systems of record private; burst scalable tiers when policy permits
Portability	High within owned standards but can be hardware/platform dependent	Can be reduced by proprietary managed services	Use containers, IaC and open interfaces for priority recovery components
Resilience	Requires separate internal failure domains and DR capacity	Multi-zone/region options but provider dependency remains	Separate failure domains and test cross-environment recovery paths
Operations	Single estate may be simpler but legacy tooling can fragment visibility	Rich automation and observability within one provider	Unified identity, telemetry, policy and service ownership across domains
Cost logic	Capital/reserved capacity and lifecycle cost	Consumption and transfer cost	Optimize total service cost including resilience headroom, transfer and operations

6. DISCUSSION

Across the literature, a consistent pattern emerges: hybrid cloud succeeds when architectural flexibility is matched by operational discipline. The technology can improve availability, portability and elasticity, but it also multiplies interfaces, policies and failure modes. The relevant optimization target is therefore not 'maximum cloud usage'. It is the best feasible combination of service continuity, security, performance, portability and cost for each workload class. This explains why mature hybrid environments often retain a deliberate mix of private, public and on-premise systems rather than forcing uniform migration.

Application architecture also determines infrastructure choices. Monolithic systems with tightly coupled databases may require replication or virtual-machine mobility, whereas cloud-native services can be placed and scaled at component level. Containers and orchestration increase mobility, yet security and observability must mature at the same time. If service ownership, dependency mapping and telemetry are weak, adding clouds can reduce reliability.

Third, resilience has to be treated as a capacity and dependency problem. Hybrid disaster recovery may fail if alternate environments lack synchronized identities, adequate network bandwidth, required licenses or tested operational procedures. The DGA's continuity controls are significant because they focus attention on risk treatment, technical alternatives and testing. This aligns with research on distributed-cloud failures, where visibility and root-cause analysis are prerequisites for fast restoration.

Finally, governance should be expressed as executable policy. Data classifications, approved provider classes, cybersecurity controls, service-level objectives and placement restrictions should be translated into architecture patterns, pipeline checks and configuration rules. This reduces the gap between policy documents and runtime behavior. It also provides a traceable basis for deciding why a mission-critical component is hosted in a particular environment.

7. Implications for Saudi Arabia and Vision 2030

Saudi Arabia offers a strong policy context for this operating model. The KSA Cloud First Policy established a preference for cloud consideration in new government IT investment and linked cloud adoption to Vision 2030. DGA's government cloud-adoption guideline extends this direction with practical guidance on provider selection, migration, deployment models and continuity, and explicitly recognizes hybrid cloud as a combination of distinct environments. DGA digital-transformation standards further position cloud architecture, risk management, business continuity, whole-of-government platforms and government data as connected dimensions of digital maturity.

The national regulatory environment also supports a more structured infrastructure market. CST's cloud-service regulations and data-center rules aim to improve service quality, transparency, competition and investment while establishing provider obligations. NCA Cloud Cybersecurity Controls provide a national security baseline for cloud services. Together, these sources link technical performance with provider qualification, cybersecurity, data classification and continuity evidence.

Vision 2030 annual reporting shows why this matters at scale. The 2024 report attributes progress in digital government partly to unified government cloud and whole-of-government platforms, while the 2025 report emphasizes advanced digital infrastructure, governance and continued investment in technology. The Ministry's 2025 computing-infrastructure white paper similarly describes cloud policy, data centers and advanced computing as elements of the Kingdom's digital foundation. A practical Saudi reference model is therefore layered: governance and national controls at the top; workload and data classification below; a hybrid infrastructure layer combining approved cloud and retained enterprise platforms; and an operations layer that provides observability, automation, cybersecurity, backup and tested recovery. Figure 2 presents this model.

For enterprises, the same logic applies even where government-specific policy is not mandatory. ERP, healthcare, virtual desktop, banking, industrial and analytics platforms can use hybrid architectures to separate sensitive systems of record from elastic digital services, establish independent recovery domains and modernize legacy estates progressively. Unified service ownership and measurable SLOs should span the application chain.

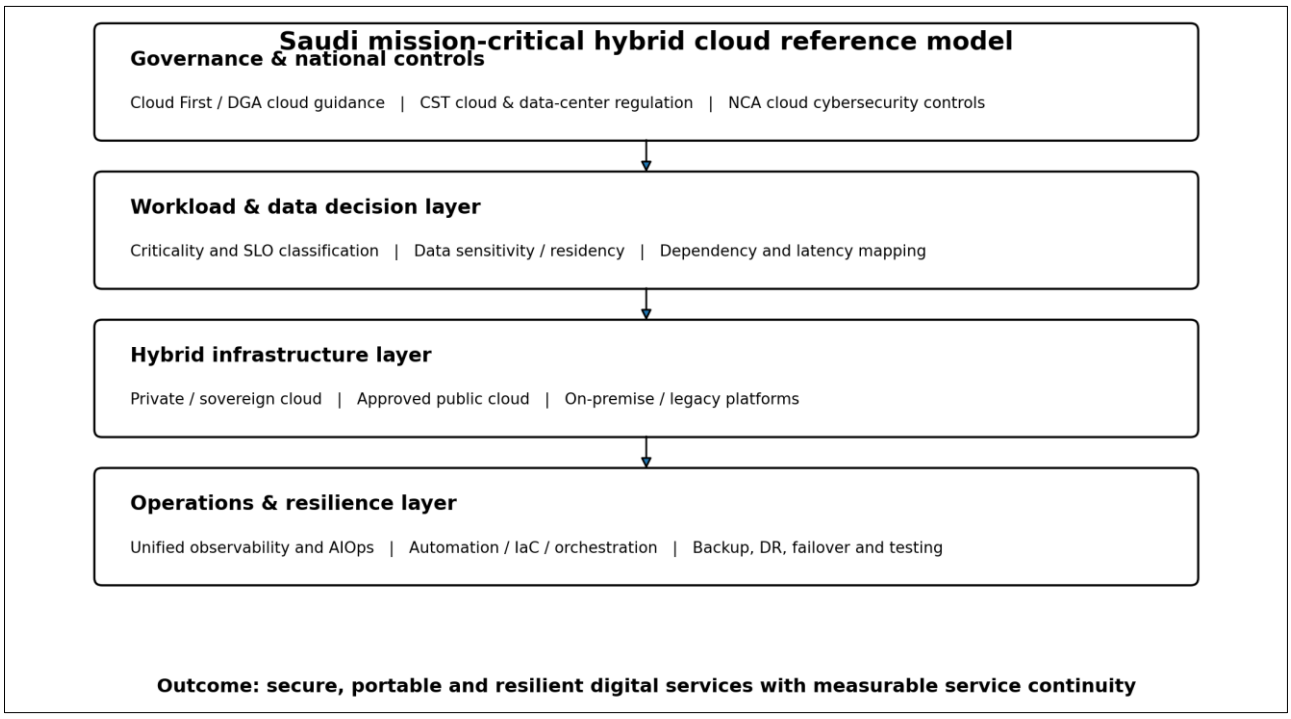

Figure 2: Saudi mission-critical hybrid cloud reference model

Table 2: Optimization objectives, mechanisms and evidence for Saudi mission-critical cloud

Objective	Architecture / operations mechanism	Evidence / KPI	Saudi governance linkage
Availability	Multi-zone or cross-environment redundancy; dependency-aware failover	SLO achievement, MTTR, failover success rate	DGA business continuity and DR controls
Data protection	Classification-led placement, encryption, key management, least privilege	Policy compliance, encryption coverage, access-review findings	DGA cloud guidance; NCA CCC
Portability	Containers, IaC, declarative orchestration, tested restore/migration procedures	Recovery portability test, deployment repeatability	Cloud adoption and provider-selection governance
Performance	Latency-aware placement, local data services, autoscaling and capacity headroom	P95/P99 latency, saturation, error rate, capacity reserve	Digital service quality and cloud architecture standards
Operational resilience	Unified observability, change correlation, anomaly/root-cause analysis	Detection time, change-failure rate, recovery drill results	Risk and business continuity controls
Economic efficiency	Workload right-sizing, tiered storage, selective use of managed services	Unit service cost, unused capacity, transfer cost	Vision 2030 digital-infrastructure efficiency context

8. Challenges and Future Research

Important challenges remain. First, interoperability is still incomplete: providers expose different networking, identity, database and managed-service interfaces, so portability often decreases as applications consume higher-level cloud services. Second, cross-cloud latency and data-transfer cost can undermine architectures that distribute tightly coupled components. Third, policy consistency is difficult when security and configuration controls are implemented through different native tools. Fourth, resilience testing across organizational and provider boundaries can be operationally disruptive.

Future research should evaluate Saudi-specific workload-placement models that jointly optimize data classification, latency, carbon/energy considerations, cost and recovery objectives. Other priorities include AI-assisted cross-cloud observability, automated evidence collection for compliance, policy-as-code for national controls, sovereign-cloud interoperability and quantitative measures of recovery readiness. Research should also examine how unified government platforms and enterprise hybrid clouds can share standards without creating common failure dependencies.

9. CONCLUSION

Hybrid cloud can provide a strong foundation for mission-critical government and enterprise applications in Saudi Arabia, but its value depends on disciplined optimization rather than infrastructure diversity by itself. The literature indicates that successful environments classify workloads and data before placement, engineer portability where it has operational value, automate deployment through common orchestration practices, and maintain unified observability across all failure domains. Security and compliance must be embedded into placement and lifecycle decisions, while resilience must be demonstrated through capacity-aware recovery design and regular testing.

For Saudi Arabia, these principles align with Cloud First policy, DGA cloud-adoption and continuity guidance, CST regulation, NCA cybersecurity controls and the broader Vision 2030 digital-transformation agenda. The proposed reference model therefore treats hybrid cloud as a governed operating model with four connected layers: national and organizational governance, workload/data classification, heterogeneous infrastructure, and continuous operations/resilience. Such an approach can allow organizations to modernize legacy systems, use public-cloud innovation selectively and preserve control over critical services. The most important measure of optimization is not how much infrastructure has moved to cloud, but whether digital services are more secure, observable, portable and recoverable under real operating conditions.

REFERENCES

- P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011. https://doi.org/10.6028/NIST.SP.800-145
- F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture, NIST Special Publication

500-292, 2011. https://doi.org/10.6028/NIST.SP.500-292
- O. Tomarchio, D. Calcaterra, and G. Di Modica, "Cloud resource orchestration in the multi-cloud landscape: a systematic review of existing frameworks," Journal of Cloud Computing, vol. 9, art. 49, 2020. https://doi.org/10.1186/s13677-020-00194-7
- J. Alonso, L. Orue-Echevarria, V. Casola, A. I. Torre, M. Huarte, E. Osaba, and J. L. Lobo, "Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review," Journal of Cloud Computing, vol. 12, art. 6, 2023. https://doi.org/10.1186/s13677-022-00367-6
- S. U. Khan, H. U. Khan, N. Ullah, and R. A. Khan, "Challenges and Their Practices in Adoption of Hybrid Cloud Computing: An Analytical Hierarchy Approach," Security and Communication Networks, 2021, art. 1024139. https://doi.org/10.1155/2021/1024139
- X. Li, L. Pan, and S. Liu, "A survey of resource provisioning problem in cloud brokers," Journal of Network and Computer Applications, vol. 203, art. 103384, 2022. https://doi.org/10.1016/j.jnca.2022.103384
- M. Liaqat, V. Chang, A. Gani, S. H. A. Hamid, M. Toseef, U. Shoaib, and R. L. Ali, "Federated cloud resource management: Review and discussion," Journal of Network and Computer Applications, vol. 77, pp. 87–105, 2017. https://doi.org/10.1016/j.jnca.2016.10.008
- M. Caballer, S. Zala, Á. L. García, G. Moltó, P. O. Fernández, and M. Velten, "Orchestrating Complex Application Architectures in Heterogeneous Clouds," Journal of Grid Computing, vol. 16, pp. 3–18, 2018. https://doi.org/10.1007/s10723-017-9418-y
- T. Kiss, P. Kacsuk, J. Kovács, B. Rákóczi, A. Hajnal, A. Farkas, G. Gesmier, and G. Terstyanszky, "MiCADO—Microservice-based Cloud Application-level Dynamic Orchestrator," Future Generation Computer Systems, vol. 94, pp. 937–946, 2019. https://doi.org/10.1016/j.future.2017.09.050
- D. Petcu, G. Macariu, S. Panica, and C. Crăciun, "Portable Cloud applications—From theory to practice," Future Generation Computer Systems, vol. 29, no. 6, pp. 1417–1430, 2013. https://doi.org/10.1016/j.future.2012.01.009
- D. Berardi, S. Giallorenzo, J. Mauro, A. Melis, F. Montesi, and M. Prandini, "Microservice security: a systematic literature review," PeerJ Computer Science, vol. 8, e779, 2022. https://doi.org/10.7717/peerj-cs.779
- J. Soldani and A. Brogi, "Anomaly Detection and Failure Root Cause Analysis in (Micro) Service-Based Cloud Applications: A Survey," ACM Computing Surveys, vol. 55, no. 3, art. 59, pp. 1–39, 2023. https://doi.org/10.1145/3501297
- J. Soldani, D. A. Tamburri, and W.-J. van den Heuvel, "The pains and gains of microservices: A systematic grey literature review," Journal of Systems and Software, vol. 146, pp. 215–232, 2018. https://doi.org/10.1016/j.jss.2018.09.082
- V. K. Netaji and G. P. Bhole, "A comprehensive survey on container resource allocation approaches in cloud computing: State-of-the-art and research challenges," Web Intelligence, vol. 19, no. 4, pp. 295–316, 2021. https://doi.org/10.3233/WEB-210474
- T. Alyas, K. Alissa, M. Alqahtani, T. Faiz, S. A. Alsaif, N. Tabassum, and H. H. Naqvi, "Multi-Cloud Integration Security Framework Using Honeypots," Mobile Information Systems, vol. 2022, art. 2600712, 2022. https://doi.org/10.1155/2022/2600712
- Digital Government Authority, Kingdom of Saudi Arabia, Guideline for Cloud Computing Adoption by Government Agencies, Document DGA-1-2-5-212, Version 1.0, 2023.
- Ministry of Communications and Information Technology, Kingdom of Saudi Arabia, KSA Cloud First Policy, 2020.
- Communications, Space and Technology Commission, Kingdom of Saudi Arabia, Cloud Computing Service Provisioning Regulations, Version 4, Decision No. 506/1445, 2023.
- National Cybersecurity Authority, Kingdom of Saudi Arabia, Cloud Cybersecurity Controls (CCC-1:2020), 2020.
- Digital Government Authority, Kingdom of Saudi Arabia, Controls of Risk Management and Business Continuity for Digital Government, Document DGA-1-2-5-107, Version 4.0, 2025.
- Digital Government Authority, Kingdom of Saudi Arabia, Digital Transformation Basic Standards, Document DGA-1-2-1-111, Version 4.0, 2025.
- Saudi Vision 2030, Vision 2030 Annual Report 2024, Kingdom of Saudi Arabia, 2025.
- Saudi Vision 2030, Vision 2030 Annual Report 2025, Kingdom of Saudi Arabia, 2026.
- Ministry of Communications and Information Technology, Kingdom of Saudi Arabia, KSA Computing Infrastructure White Paper, 2025.
- Communications, Space and Technology Commission, Kingdom of Saudi Arabia, Data Center Services Regulations and Data Center Service Providers Guide, effective 1 January 2024.