



Hybrid Cloud and Hyperconverged Infrastructure Framework for Digital Transformation in Saudi Organisations

*Mohammad Hassan Qureshi**

Department of Computer Science, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan

Email: hassanqureshi305@gmail.com

ORCID: <https://orcid.org/0009-0008-5999-1124>

*Corresponding author

DOI : <https://doi.org/10.55248/gengpi.07.0926.3033>

ABSTRACT :

Saudi organisations are modernising under strong national expectations for digital government, data value creation, service resilience, and cybersecurity. Yet public cloud adoption alone cannot resolve the combined requirements of legacy integration, workload sovereignty, predictable performance, operational continuity, and rapid innovation. This review develops an evidence-based framework in which hyperconverged infrastructure (HCI) forms a software-defined private-cloud foundation and hybrid cloud provides selective access to elastic public services. A structured integrative review synthesised 30 academic, regulatory, standards, and policy sources published from 2020 to 2025. Evidence was coded against technological, organisational, environmental, governance, security, and value-realisation dimensions. The synthesis finds that the strongest architecture is neither cloud-first in a literal placement sense nor an indiscriminate retention of on-premises systems. It is a policy-led operating model that classifies workloads, separates control and execution concerns, standardises identity and observability, and assigns each application to an HCI, sovereign-cloud, public-cloud, or edge location according to evidence. HCI contributes consolidation, locality, repeatable operations, and recovery, while public cloud contributes elasticity, managed innovation services, and geographic reach. Their combination succeeds only when platform engineering, FinOps, zero-trust security, data governance, vendor-exit planning, and skills development are designed as one transformation system. The proposed framework links national obligations to architecture decisions and measurable outcomes. It offers Saudi ministries, regulated enterprises, universities, healthcare providers, and large private organisations a staged route from fragmented infrastructure to a governed hybrid platform. The review also identifies research needs concerning longitudinal value, energy performance, Arabic-language operations, sovereign-cloud interoperability, and sector-specific empirical validation.

Keywords: cloud governance; digital government transformation; hybrid cloud; hyperconverged infrastructure; Saudi Arabia; sovereign cloud; workload sovereignty; zero-trust security

1. Introduction

Digital transformation is not the purchase of newer infrastructure. It is an organisational redesign in which digital resources change services, operating routines, decision rights, and value creation. Contemporary reviews describe transformation as a systemic process shaped by technology, structure, strategy, and external institutions rather than a sequence of isolated IT projects (Verhoef et al., 2021; Hanelt et al., 2021; Kraus et al., 2022). This distinction is important in Saudi Arabia. Vision 2030 programmes have increased expectations for accessible services, interoperable data, automated decisions, and resilient national platforms, while regulation requires organisations to manage privacy, localisation, cybersecurity, and third-party risk. Infrastructure is therefore both an enabler and a governance boundary.

Cloud computing supports fast provisioning and managed capabilities, but a simple public-cloud migration is rarely suitable for a diversified Saudi organisation. Core applications may depend on tightly coupled databases, specialised appliances, low-latency industrial interfaces, or licensing models that resist refactoring. Sensitive information may require controlled processing and auditable residency. Operational technology, clinical systems, campus platforms, and branch services may also need to continue during wide-area network degradation. Government research consequently presents cloud adoption as an organisational and regulatory programme, not merely a hosting decision (DGA, 2024; World Bank and DGA, 2024). Studies of public-sector adoption similarly show that relative advantage is moderated by security confidence, skills, leadership, procurement, and institutional readiness (Alqahtani and Alshahrani, 2022; Alkhasawneh et al., 2025).

Hyperconverged infrastructure offers a complementary foundation. HCI combines virtualised compute, software-defined storage, networking integration, and centralised lifecycle management on clustered commodity nodes. Capacity can be expanded through repeatable units, and many operational tasks can be expressed as software policies. Recent performance research and network experiments suggest that HCI can reduce

infrastructure fragmentation, although results depend on workload profile, storage design, oversubscription, and failure-domain engineering (Syed, 2023; Ushakov et al., 2023). HCI should therefore not be presented as an automatically cheaper appliance. Its strategic value is that it can make controlled local infrastructure behave more like a cloud platform.

The unresolved question is how Saudi organisations can combine that local platform with public or sovereign cloud services without creating two management silos. Existing literature often examines cloud adoption, digital transformation, security, or HCI separately. A recent Saudi multi-cloud blueprint usefully emphasises tiering and localisation, but its prescriptive design requires a broader synthesis of organisational readiness, workload economics, platform operations, and evidence quality (Mostafa, 2025). A review centred on the hybrid cloud–HCI relationship can connect these fields and replace product-led migration logic with decision rules.

1.1 Aim, objectives, and review questions

The study aims to develop a governance-centred hybrid cloud and HCI framework that supports measurable digital transformation in Saudi organisations. Unlike a blueprint that begins with provider selection, the framework begins with public value, business capability, data obligations, and workload evidence. Four objectives guide the review: to synthesise recent knowledge on hybrid cloud, HCI, and transformation outcomes; to map Saudi regulatory and institutional requirements to technical controls; to identify adoption conditions, risks, and performance measures; and to formulate a staged implementation and research agenda.

Three review questions follow. First, what complementary capabilities do HCI and public or sovereign cloud contribute to Saudi transformation? Second, which governance, security, data, organisational, and economic mechanisms determine whether the combination creates value? Third, how can organisations sequence adoption while preserving service continuity, portability, and regulatory accountability? These questions shift attention from whether cloud is desirable to how placement, control, and learning should operate across a portfolio.

2. Conceptual foundations

2.1 Digital transformation as capability renewal

Digital transformation research consistently distinguishes digitisation of information, digitalisation of processes, and transformation of organisational purpose or operating logic. A cloud-hosted legacy workflow may be digitised without becoming more responsive, integrated, or user-centred. Meta-review evidence shows that credible transformation models connect technology to dynamic capabilities, organisational design, ecosystems, and performance, while also acknowledging disruption and unintended consequences (Reis et al., 2023). For Saudi organisations, infrastructure investment should consequently be judged by time to deploy a service, reliability, policy compliance, data reuse, workforce productivity, and citizen or customer experience rather than by migrated server counts.

Cloud adoption can improve agility and innovation by making resources rapidly accessible and enabling teams to experiment without lengthy procurement cycles. Empirical work links adoption to operational and market performance, but the relationship is mediated by organisational capability and actual use (Khayer et al., 2020). A 2025 systematic review likewise reports benefits across agility, productivity, innovation, and sustainability while warning that outcomes are heterogeneous and often weakly measured (Donat et al., 2025). This implies a value chain: infrastructure standardisation enables platform services; platform services shorten delivery cycles; delivery improvements enable service outcomes. Skipping an intermediate link produces optimistic business cases that cannot be audited.

2.2 Hybrid cloud and the cloud continuum

Hybrid cloud joins controlled private resources with external cloud services through coordinated identity, networking, data, security, and operations. The definition requires more than connectivity. If separate teams provision incompatible environments, duplicate controls, and monitor through unrelated consoles, the organisation has parallel estates rather than a hybrid operating model. The cloud-continuum literature extends the concept from central data centres to edge and fog resources, showing that latency, bandwidth, autonomy, and data gravity influence placement (Hasan et al., 2025). Container orchestration can increase portability, but comparative studies show meaningful differences in scheduling, overhead, recovery, and suitability for resource-constrained nodes (Čilić et al., 2023; Vaño et al., 2023).

Public cloud is strongest where demand is variable, global reach matters, or managed analytics, artificial intelligence, integration, and developer services accelerate outcomes. HCI is strongest where workloads are steady, locality or deterministic latency matters, existing virtualisation is substantial, or disconnected operation is necessary. Sovereign or locally registered cloud can add a third option, subject to contractual and technical verification. The portfolio therefore needs differentiated placement rather than a universal destination. Security reviews of multi-cloud and hybrid environments identify inconsistent identity, configuration drift, exposed interfaces, fragmented logs, and ambiguous shared responsibility as recurrent risks (Ali et al., 2025). More locations increase optionality, but also increase the number of relationships that must be governed.

2.3 HCI as a private-cloud substrate

HCI collapses separate compute and storage administration into a cluster governed through software. This can simplify branch deployments, virtual desktop infrastructure, database consolidation, backup targets, and recovery sites. Standard node patterns also support infrastructure-as-code and repeatable expansion. However, HCI couples resource scaling: adding storage may add unneeded compute, and adding compute may add unneeded storage. Data-reduction ratios, rebuild traffic, fault tolerance, and licensing materially affect usable capacity. Performance claims must therefore be tested with representative workloads rather than vendor reference values.

HCI becomes transformational only when exposed as a service. A self-service catalogue, approved templates, automated policy, service-level objectives, and telemetry convert a cluster into a private-cloud experience. Without them, HCI is simply a consolidated virtualisation refresh. The design must also avoid treating one cluster as a universal failure domain. Management, production, security tooling, backup, and disaster recovery need deliberate separation, immutable recovery paths, and tested restoration. Network research further indicates that software switching and virtual overlays introduce measurable behaviour that architects must evaluate under east–west traffic and failure conditions (Ushakov et al., 2023).

3. Review methodology

The study used a structured integrative literature review because the research question crosses information systems, cloud engineering, cybersecurity, public administration, and Saudi regulation. Integrative reviews permit empirical studies, conceptual papers, technical standards, and authoritative policy documents to be analysed together, while still requiring a transparent search and synthesis process. The protocol followed the reporting logic of PRISMA 2020 where applicable and the review-design guidance of Paul and Criado (2020) and Page et al. (2021). It did not perform a statistical meta-analysis because outcomes, units of analysis, and technical configurations were too heterogeneous.

Searches covered material published from January 2020 through December 2025. Query families combined “hybrid cloud,” “hyperconverged infrastructure,” “HCI,” “cloud continuum,” “digital transformation,” “Saudi Arabia,” “government cloud,” “data localisation,” “zero trust,” and “cloud adoption.” Academic discovery emphasised Scopus- and Web of Science-indexed journal literature, supplemented by IEEE, ACM, ScienceDirect, SpringerLink, and targeted citation chaining. A parallel grey-literature stream covered Saudi authorities, international standards bodies, and development institutions. The 2025 blueprint was treated as a contextual source rather than as evidence of effectiveness.

Sources were eligible when they addressed at least one framework construct: architecture, adoption, governance, security, performance, regulation, organisational capability, or transformation outcome. They also had to provide identifiable authorship, publication date, and sufficient methodological or institutional authority. Product pages, undated commentary, duplicate summaries, sources outside the date window, and claims lacking a traceable basis were excluded. Thirty sources formed the final purposive evidence corpus. This bounded set favours conceptual relevance and source quality over bibliometric exhaustiveness; accordingly, the conclusions are analytical rather than prevalence estimates.

Each source was coded in a matrix using six dimensions: technology, organisation, environment and regulation, governance, cybersecurity and resilience, and realised value. Findings were then compared for convergence, complementarity, and contradiction. Technical claims were triangulated against standards or experimental studies; Saudi legal and policy claims were anchored in primary institutional publications. The synthesis produced design principles, placement rules, adoption stages, metrics, and research gaps. This approach improves reproducibility, but it has limitations: English-language material dominates, proprietary implementation evidence is underreported, HCI scholarship is thinner than cloud scholarship, and fast-changing regulation can outdate specific control mappings.

4. Saudi institutional and regulatory context

Saudi Arabia’s transformation environment combines strong central direction with sector diversity. The Digital Government Strategy promotes integrated, proactive, and efficient services, while government cloud research frames elastic infrastructure as a route to reliability and sustainable service development (DGA, 2021; DGA, 2024). The joint World Bank and DGA account of the Kingdom’s cloud journey emphasises institutional coordination, common platforms, and an orchestrating Government Cloud Office (World Bank and DGA, 2024). This supports a federated model: central guardrails and shared services should coexist with sector-specific workload ownership.

The Personal Data Protection Law and its Implementing Regulations make data lifecycle decisions central to architecture. Organisations need a lawful basis, defined purposes, appropriate protection, processor oversight, and controls for disclosure or transfer (SDAIA, 2021; SDAIA, 2023). Data residency is therefore not a label applied to a data centre. Architects must know where primary data, replicas, backups, logs, support artefacts, encryption keys, and administrative access reside. A service may store records locally while sending telemetry or support data elsewhere. The framework consequently treats data-flow evidence and contractual rights as prerequisites to placement.

Cloud services also operate within sectoral and national cybersecurity expectations. The NCA Cloud Cybersecurity Controls establish requirements for both service providers and tenants, and the updated control set reinforces governance, defence, resilience, and third-party accountability (NCA, 2024a).

Essential Cybersecurity Controls provide the broader organisational baseline (NCA, 2024b). Zero-trust architecture complements these obligations by removing implicit trust based on network location and continuously evaluating identity, device, workload, and policy context (Rose et al., 2020). In hybrid environments, consistent identity and policy are more durable boundaries than a traditional perimeter.

CST cloud-service regulations influence provider registration, customer protection, transparency, and handling of content (CST, 2022). ISO/IEC 27001:2022 adds a certifiable information-security management structure, while Cloud Security Alliance guidance consolidates cloud-specific control considerations across governance, identity, data, workloads, and incident management (ISO, 2022; CSA, 2024). These sources should not be converted into a single undifferentiated checklist. The organisation should maintain a control crosswalk that assigns each obligation to an accountable owner and collects evidence once for multiple assurance purposes.

5. Proposed hybrid cloud–HCI framework

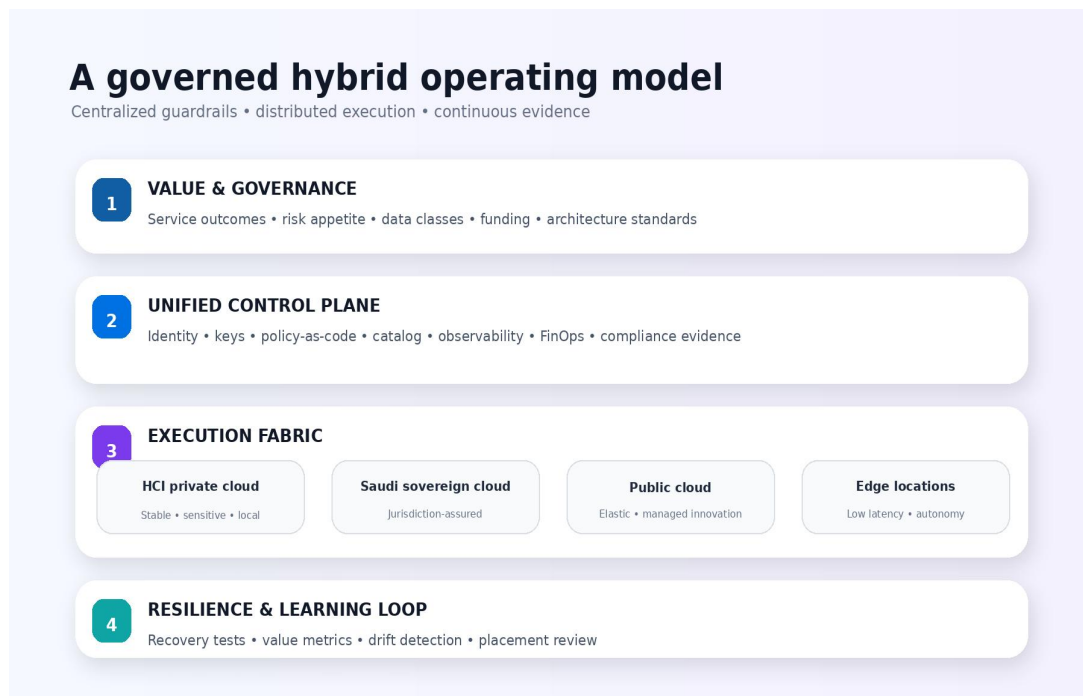


Figure 1. Hybrid cloud–HCI framework for Saudi organisations. Source: authors’ synthesis.

The proposed framework comprises four linked layers. The first is the value and governance layer, where strategy owners define service outcomes, risk appetite, data classes, funding rules, and architecture standards. The second is the unified control plane: identity, keys, policy-as-code, configuration, service catalogue, observability, cost allocation, and compliance evidence. The third is the execution fabric comprising HCI private cloud, Saudi sovereign or registered cloud, public cloud, and edge locations. The fourth is the resilience and learning loop, which tests recovery, measures value, detects drift, and feeds evidence back into placement decisions. The defining principle is centralised guardrails with distributed execution.

Workload placement uses six evidence gates. Business criticality determines acceptable interruption and recovery objectives. Data classification determines permitted locations and processing paths. Technical fit considers latency, dependencies, refactoring effort, hardware affinity, and portability. Economic fit compares a realistic total cost of ownership, including network, licensing, operations, exit, and recovery. Operational readiness tests whether teams can secure, observe, patch, and support the target. Strategic value asks whether a managed cloud capability materially improves the service. A workload moves only when the chosen destination is superior across the weighted decision, not because migration volume is itself a target.

The HCI zone hosts stable, sensitive, locality-dependent, and legacy-compatible workloads. It provides virtual machines, container platforms where appropriate, software-defined storage, local backup staging, and standardised infrastructure services. A sovereign or locally compliant cloud zone accommodates workloads that benefit from cloud operations while requiring specific jurisdictional assurances. Public cloud hosts elastic digital channels, collaboration, development sandboxes using protected data, and managed innovation services where permitted. Edge nodes support sites that need low latency or intermittent autonomy. Data products can span zones only through approved interfaces, tokenisation, encryption, and lifecycle policy.

The unified control plane prevents the architecture from becoming a collection of islands. Workforce and workload identities should originate from governed sources, use phishing-resistant authentication for privileged actions, and receive least-privilege access. Keys and secrets require defined ownership, rotation, and separation from protected data. Policy-as-code should test network exposure, image provenance, encryption, region, backup, logging, and tagging before deployment. A shared telemetry model must correlate events across HCI, cloud, network, applications, and identity. This

implements zero trust as an operating discipline rather than a network product (Rose et al., 2020; Ali et al., 2024).

Portability is selective. Containers, open interfaces, declarative deployment, portable data formats, and automated build pipelines reduce avoidable lock-in, but forcing every managed service into a lowest-common-denominator design destroys its innovation value. The framework distinguishes portable core services from intentionally provider-specific accelerators. For the latter, the owner records business benefit, data implications, replacement options, and exit cost. Cloud-native orchestration research supports containers for heterogeneous placement but also shows that edge constraints and scheduler behaviour must be tested rather than assumed (Čilić et al., 2023; Vaño et al., 2023).

6. Evidence synthesis: benefits, tensions, and conditions

6.1 Agility and service innovation

The combined model can shorten provisioning by replacing bespoke infrastructure requests with approved platform products. HCI supplies rapid local capacity for workloads that cannot move externally; public cloud supplies on-demand environments and managed services. This duality expands the feasible transformation portfolio. The gain, however, depends on developer experience. If teams navigate separate tickets for identity, networking, security review, and cost codes, nominally automated infrastructure will not improve lead time. Platform teams should therefore design reusable “golden paths” for common application types and measure adoption, deployment frequency, and change failure.

Digital transformation reviews caution that technology creates value through complementary organisational change (Verhoef et al., 2021; Hanelt et al., 2021). Product-oriented teams, empowered service owners, iterative funding, and user research are as important as infrastructure. Saudi organisations with centralised decision traditions may need explicit delegation boundaries: central bodies define non-negotiable controls, while service teams choose within approved patterns. This preserves accountability without returning every routine decision to an architecture committee.

6.2 Resilience and performance

HCI can improve local resilience through clustered resources, distributed storage, and standardised recovery, while cloud adds off-site capacity and geographic options. Yet redundancy is not resilience unless failure modes are independent and recovery is exercised. Shared identity, domain-name services, network circuits, or management consoles can become hidden common dependencies. Ransomware can also replicate corruption across highly connected environments. The design therefore requires isolated recovery credentials, immutable copies, clean-room restoration, dependency mapping, and regular scenario tests aligned to service-level objectives.

Performance placement should be empirical. HCI may reduce latency for tightly coupled applications, whereas public cloud may outperform local systems for globally distributed channels or specialised analytics. Cloud-continuum studies show that placing computation nearer data can reduce delay and bandwidth, but distributed orchestration adds coordination and observability costs (Hasan et al., 2025). A benchmark must include peak load, node failure, storage rebuild, encryption, backup windows, and network impairment. Average response time alone conceals tail latency that affects critical services.

6.3 Economics and sustainability

Hybrid economics are often misrepresented as a comparison between hardware purchase and hourly cloud rates. A sound model includes capital, subscriptions, facilities, energy, connectivity, migration, platform engineering, cybersecurity, staffing, support, depreciation, and exit. HCI can improve utilisation and reduce separate storage administration, but high availability consumes capacity and licensing can dominate cost. Cloud can match variable demand efficiently, but idle resources, data transfer, duplicated tools, and unmanaged consumption create waste. FinOps should unite finance, engineering, procurement, and service owners around unit costs such as cost per transaction or protected workload.

Sustainability claims require equal care. Consolidation may reduce server count, and hyperscale facilities may use resources efficiently, yet data replication, AI workloads, network transfer, and premature hardware replacement can offset savings. Recent reviews find that cloud can support organisational sustainability but measurement remains inconsistent (Donat et al., 2025; Merlo and de la Torre, 2025). Saudi organisations should collect energy, utilisation, hardware-life, and carbon-intensity evidence where available, avoiding claims based only on migration volume.

6.4 Security, sovereignty, and operational complexity

Hybrid architecture can strengthen sovereignty by retaining defined workloads and keys under direct control while using external services selectively. It can also worsen security through inconsistent tools and unclear responsibility. The remedy is not to duplicate every control in every zone; it is to define control outcomes and implement zone-specific mechanisms that generate comparable evidence. Central security teams should provide identity, logging, posture rules, vulnerability policy, and incident integration as platform services. Workload teams remain responsible for data use, application security, and recovery validation.

The most difficult risk is operational complexity. Staff must understand virtualisation, distributed storage, cloud networking, automation, containers, identity, cost, and regulation. Outsourcing all knowledge creates dependency; attempting to internalise everything delays progress. A capability model should identify sovereign responsibilities that remain inside the organisation—architecture authority, data ownership, risk acceptance, key decisions, and supplier oversight—while partners can accelerate engineering and operations. Cloud-adoption research in developing-government contexts repeatedly places skills, leadership, governance, and procurement alongside technical factors (Alkhasawneh et al., 2025).

6.5 Procurement and ecosystem governance

Procurement can either reinforce the operating model or fragment it. Traditional tenders often specify equipment quantities and five-year support, whereas a hybrid platform evolves through software releases, consumption, and changing service demand. Requirements should therefore describe outcomes, interfaces, assurance evidence, service levels, data handling, and exit obligations. Bid evaluation should test operating scenarios, including a failed node, a compromised administrator, loss of a cloud connection, restoration of a protected workload, and export of data in a usable format. Demonstrations reveal integration limits that compliance declarations may conceal.

Contracts should allocate responsibility for patching, vulnerability notification, incident cooperation, subcontractors, support access, encryption keys, log retention, deletion, portability, and end-of-service assistance. Pricing schedules need thresholds and unit rates for growth, network transfer, premium support, and recovery capacity. The organisation should retain audit rights and receive evidence in formats that its assurance process can consume. A contractual residency promise is necessary but insufficient when operational metadata, diagnostic bundles, or remote administration follow different paths.

Saudi economic-development objectives add a capability dimension. Local partners can provide Arabic support, sector knowledge, and rapid on-site response, while global providers contribute scale and advanced services. Supplier diversity reduces concentration only if components interoperate and internal teams preserve architecture authority. Otherwise, multiple contracts can create several forms of lock-in at once. Ecosystem governance should assess provider financial health, local staffing, skills transfer, roadmap transparency, interoperability, and concentration exposure at least annually. Exit tests should sample configuration, images, keys, data, and runbooks; a paper exit plan that has never been exercised is not an operational control. This discipline turns procurement from a periodic purchasing event into a continuing mechanism for resilience, learning, and innovation.

7. Implementation roadmap and measurement

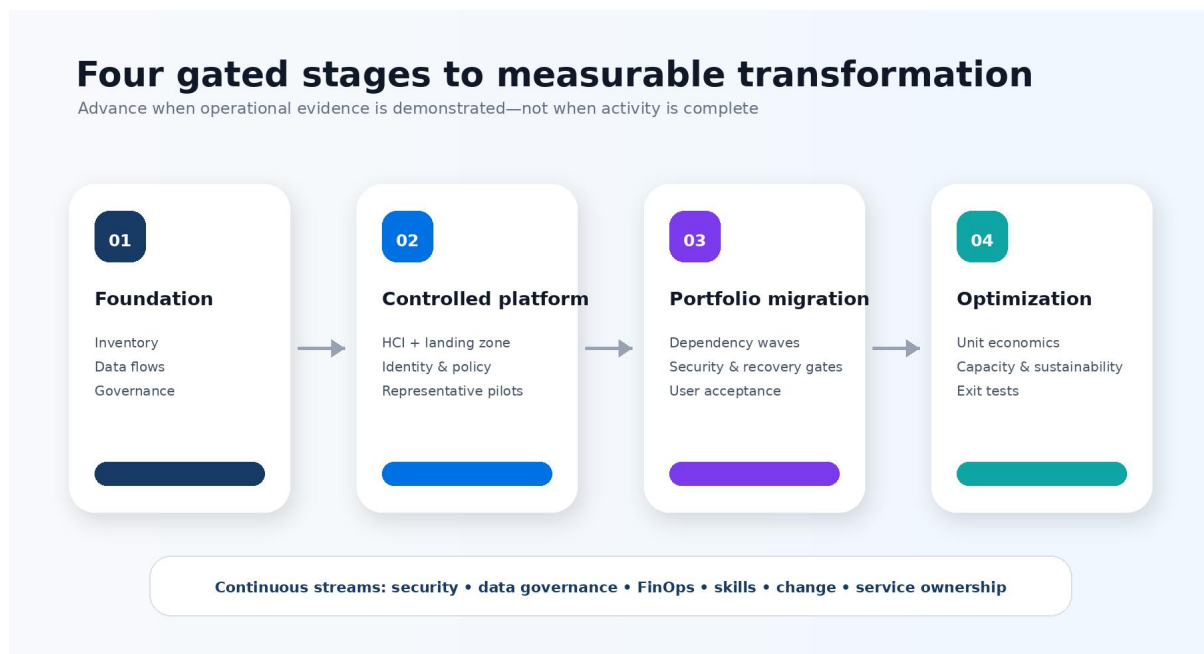


Figure 2. Evidence-gated implementation roadmap. Source: authors' synthesis.

Implementation proceeds through four gated stages. Stage one, foundation, inventories applications, data flows, dependencies, contracts, skills, and current costs. It establishes governance, classification, target principles, identity direction, and a small platform team. Stage two, controlled platform, deploys a minimum viable HCI private cloud and cloud landing zone with common identity, network segmentation, logging, key management, templates, and tagging. Pilot workloads are deliberately low in blast radius but representative enough to test integration and operations.

Stage three, portfolio migration, organises applications into retire, retain, rehost, replatform, refactor, replace, or relocate pathways. Migration waves

follow dependency maps and business calendars. Each wave must pass security, performance, recovery, cost, and user-acceptance gates. Stage four, optimisation, introduces automated placement signals, service-level management, capacity forecasting, unit economics, sustainability measurement, and periodic exit tests. Progress is evidence-based: a stage closes only when its operational criteria are demonstrated.

Change management runs through every stage. Executives sponsor outcomes and resolve cross-unit barriers; a platform product owner manages the roadmap; enterprise architecture maintains patterns; cybersecurity defines control outcomes; data owners approve use and movement; finance leads unit economics; procurement secures audit, portability, notification, and termination rights; and service teams own reliability. Communities of practice and paired delivery convert vendor participation into internal capability. Training should be role-based and assessed through practical operation, not attendance alone.

Table 1. Balanced measurement architecture for hybrid transformation.

Dimension	Indicator	Evidence source	Cadence	Owner
Delivery speed	Median request-to-production lead time	Platform telemetry	Quarterly	Service owner
Reliability	SLO attainment and change-failure rate	Observability platform	Monthly	SRE lead
Recovery	Percentage of critical services passing timed restore	Exercise evidence	Quarterly	Continuity lead
Security	Policy-as-code coverage and critical drift age	Posture system	Monthly	CISO delegate
Economics	Unit cost per transaction or protected workload	FinOps ledger	Monthly	Finance partner
Adoption	Share of new services using approved golden paths	Service catalogue	Quarterly	Platform owner
Value	User satisfaction and time to launch priority services	Service analytics	Semiannual	Business sponsor

Metrics should balance speed, stability, security, economics, compliance, adoption, and value. A single migration percentage invites superficial rehosting. Leading indicators include platform-product adoption, automated-control coverage, deployment lead time, recovery-test success, configuration drift, privileged-access hygiene, forecast accuracy, and staff proficiency. Lagging indicators include service availability, user satisfaction, incident impact, audit findings, cost per transaction, and time to launch a digital service. Every metric needs an owner, baseline, target, data source, and decision it will inform.

Table 2. Illustrative workload-placement decision matrix.

Workload	Dominant evidence	Preferred zone	Required control	Review trigger
Stable core system	Predictable demand; legacy integration	HCI private cloud	High availability; tested restore	Reassess on major release
Sensitive cloud-ready service	Local assurance; managed operations	Saudi sovereign/registered cloud	Residency evidence; key ownership	Annual provider review
Elastic digital channel	Variable demand; internet reach	Public cloud	WAF; autoscaling; protected data paths	Seasonal demand review
Analytics/AI experiment	Specialised managed capability	Public or sovereign cloud	De-identification; spend limits	Promote only after DPIA
Industrial/branch workload	Low latency; intermittent WAN	Edge HCI	Local autonomy; signed updates	Connectivity change
Obsolete duplicate	Low value or redundant capability	Retire/replace	Archive and deletion evidence	Business approval

Governance should also include stop conditions. A migration pauses when data flows are unknown, recovery cannot be demonstrated, expected cost lacks a defensible baseline, or the operating team cannot support the target. A provider-specific service should be rejected when its benefit does not exceed its switching and compliance risks. Conversely, retaining a workload on HCI requires justification when managed cloud would materially improve resilience or service delivery. Symmetric scrutiny prevents both cloud enthusiasm and legacy inertia from becoming policy.

8. Discussion and research agenda

The synthesis reframes hybrid cloud and HCI as an organisational control system. HCI supplies a locally governed execution substrate; cloud supplies elastic and specialised capabilities; the control plane makes them operable as one portfolio; and the learning loop keeps placement aligned with changing evidence. This interpretation explains why infrastructure-only programmes disappoint. Consolidation without self-service preserves queues, cloud without governance multiplies risk, and compliance without automation slows delivery. Transformation occurs when architecture, authority, routines, and measures change together.

The framework extends the reviewed blueprint in three ways. First, it replaces fixed tiers with evidence gates, recognising that classification alone does not determine technical or economic fit. Second, it treats HCI as a platform product rather than merely the Saudi-hosted layer. Third, it makes value measurement, capability transfer, and exit testing explicit. The framework remains consistent with the blueprint's emphasis on localisation and secure routing while avoiding unsupported universal compliance scores or return-on-investment promises (Mostafa, 2025).

For scholarship, the review exposes an evidence imbalance. Digital transformation and cloud adoption have mature conceptual literatures, but independent longitudinal studies of HCI outcomes are scarce. Researchers should compare HCI-only, public-cloud, sovereign-cloud, and hybrid portfolios using service-level and unit-economic measures over several years. Saudi sector studies should test how regulation, procurement, organisational culture, and platform maturity interact in healthcare, education, finance, industry, and government. Such studies need transparent baselines and should distinguish correlation from benefits caused by the architecture.

Five additional questions merit attention. How can policy-as-code express Saudi controls without oversimplifying legal judgment? Which interoperability mechanisms preserve sovereignty while enabling cross-organisation data products? How do Arabic-language operations and local skills markets affect incident response and platform adoption? Under Saudi climatic and energy conditions, when does consolidation reduce whole-life environmental impact? Finally, how should organisations evaluate AI services whose models, prompts, telemetry, and derived data can cross conventional workload boundaries? These questions require collaboration among information-systems scholars, engineers, regulators, economists, and service users.

9. Conclusion

Saudi organisations do not need to choose between public cloud and controlled infrastructure. They need an operating model that uses each deliberately. The reviewed evidence supports HCI as a standardised private-cloud and edge foundation for stable, sensitive, latency-dependent, and legacy-compatible workloads, complemented by sovereign and public cloud for elasticity, managed capabilities, and reach. The combination becomes transformational only through unified identity, policy, observability, data governance, resilience engineering, FinOps, platform product management, and workforce development.

The proposed four-layer framework and staged roadmap translate these requirements into decisions. Strategy and regulation define guardrails; a shared control plane makes them executable; differentiated zones host workloads according to six evidence gates; and continuous measurement corrects drift. This design aligns technical placement with service outcomes and makes assurance part of delivery. It also preserves optionality by distinguishing portable cores from justified provider-specific innovation.

The practical message is disciplined: begin with a verified portfolio and data flows, build a minimum controlled platform, migrate in measured waves, and optimise only after reliability and accountability are demonstrated. Success is not the number of workloads moved. It is the organisation's improved ability to deliver trusted, resilient, cost-aware, and user-centred services while meeting Saudi obligations. Future empirical work should validate the framework across sectors and quantify its longitudinal effects, but the current synthesis provides a coherent foundation for decisions that are too consequential to be driven by fashion or vendor architecture alone.

REFERENCES

- [1] B. Ali, A. I. Awad, and Z. Al-Qudah, "Implementing zero trust security with dual fuzzy intelligent intrusion detection systems for software-defined networking," *Comput. Netw.*, vol. 242, p. 110259, 2024.
- [2] S. Talpur, A. Abro, K. S. Alshudukhi, G. N. Alwakid, M. Humayun, F. Bashir, S. A. Wadho, and A. Shah, "Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies and future directions," *Comput. Secur.*, vol. 157, p. 104599, 2025.
- [3] R. Alkhasawneh, Z. C. Cob, and A. B. A. Latif, "Cloud computing adoption in government organizations in developing countries: A systematic literature review and future research directions," *Int. J. Public Adm. Digit. Age*, vol. 12, no. 1, pp. 1–27, 2025.
- [4] M. Alqahtani and S. Alshahrani, "Core elements impacting cloud adoption in Saudi government organizations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 6, pp. 285–294, 2022.
- [5] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 5, Cloud Security Alliance, 2024.
- [6] Communications, Space and Technology Commission, *Cloud Computing Services Provisioning Regulations*, Riyadh, 2022.

- [7] I. Čilić, P. Krivić, I. Podnar Žarko, and M. Kušek, "Performance evaluation of container orchestration tools in edge computing environments," *Sensors*, vol. 23, no. 8, p. 4008, 2023.
- [8] Digital Government Authority, *Digital Government Strategy*, Riyadh, 2021.
- [9] Digital Government Authority, *Cloud Computing and Its Role in Accelerating Digital Transformation and Its Sustainable Impact in the Government Sector*, Riyadh, 2024.
- [10] V. Donat, C. Haertel, D. Staegemann, C. Daase, M. Pohl, D. Dreschel, D. S. Walia, and K. Turowski, "Examining the impact of cloud computing on organizational performance: A systematic literature review," *Proc. 27th Int. Conf. Enterp. Inf. Syst.*, vol. 1, pp. 375–386, 2025.
- [11] A. Hanelt, R. Bohnsack, D. Marz, and C. Antunes Marante, "A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change," *J. Manag. Stud.*, vol. 58, no. 5, pp. 1159–1197, 2021.
- [12] M. M. Hasan, A. K. M. A. Habib, and M. S. Hossain, "The journey to cloud as a continuum: A review of edge, fog and cloud integration," *Array*, vol. 26, p. 100390, 2025.
- [13] International Organization for Standardization, *Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, ISO/IEC 27001:2022, Geneva, 2022.
- [14] A. Khayer, M. S. Talukder, Y. Bao, and M. N. Hossain, "Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach," *Technol. Soc.*, vol. 60, p. 101225, 2020.
- [15] S. Kraus, S. Durst, J. J. Ferreira, P. Veiga, N. Kailer, and A. Weinmann, "Digital transformation in business and management research: An overview of the current status quo," *Int. J. Inf. Manage.*, vol. 63, p. 102466, 2022.
- [16] T. R. Merlo and N. de la Torre, "Cloud computing's impact on the digital transformation of the enterprise: A systematic review," *Sustainability*, vol. 17, no. 13, p. 5755, 2025.
- [17] M. M. Mostafa, "A multi-cloud design blueprint for Saudi Arabian government entities: Ensuring data localization compliance and cybersecurity in the digital transformation era," *SSRN Electron. J.*, Paper 5330955, 2025.
- [18] National Cybersecurity Authority, *Cloud Cybersecurity Controls*, CCC-2:2024, Riyadh, 2024.
- [19] National Cybersecurity Authority, *Essential Cybersecurity Controls*, ECC-2:2024, Riyadh, 2024.
- [20] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021.
- [21] J. Paul and A. R. Criado, "The art of writing literature review: What do we know and what do we need to know?" *Int. Bus. Rev.*, vol. 29, no. 4, p. 101717, 2020.
- [22] J. Reis, M. Amorim, N. Melão, Y. Cohen, and M. Rodrigues, "Digital transformation: A meta-review and guidelines for future research," *Heliyon*, vol. 9, no. 1, p. e12834, 2023.
- [23] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, 2020.
- [24] Saudi Data and Artificial Intelligence Authority, *Personal Data Protection Law*, Royal Decree No. M/19, Riyadh, 2021.
- [25] Saudi Data and Artificial Intelligence Authority, *Implementing Regulations of the Personal Data Protection Law*, Riyadh, 2023.
- [26] A. A. M. Syed, "Hyperconverged infrastructure for enterprise data centers: Performance and scalability analysis," *Int. J. AI, Big Data, Comput. Manage. Stud.*, vol. 4, no. 4, pp. 29–38, 2023.
- [27] Y. Ushakov, V. Muliukha, A. Kalyuzhny, and Y. Gatchin, "Research of a virtual infrastructure network with hybrid topology," *Eng. Proc.*, vol. 33, no. 1, p. 52, 2023.
- [28] R. Vaño, I. Lacalle, P. Sowiński, R. S-Julián, and C. E. Palau, "Cloud-native workload orchestration at the edge: A deployment review and future directions," *Sensors*, vol. 23, no. 4, p. 4008, 2023.
- [29] P. C. Verhoef, T. Broekhuizen, Y. Bart, A. Bhattacharya, J. Q. Dong, N. Fabian, and M. Haenlein, "Digital transformation: A multidisciplinary reflection and research agenda," *J. Bus. Res.*, vol. 122, pp. 889–901, 2021.
- [30] World Bank and Digital Government Authority, *Cloud First: Strategy and Practices from the Kingdom of Saudi Arabia*, World Bank, Washington, DC, 2024.