Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i03.025

OPEN ACCESS

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

Original Research Article

Data Sovereignty and Regulatory Compliance in Cloud Storage Environments in Saudi Arabia

Asim Badhuralam[1]*
[1]Independent Researcher

***Corresponding Author**
Asim Badhuralam
Independent Researcher

Article History
Received: 23.04.2026
Accepted: 16.06.2026
Published: 18.06.2026

Abstract: Cloud storage has become a core platform for Saudi digital transformation, yet its use now operates within a dense sovereignty and compliance environment shaped by personal data protection, cybersecurity controls, data classification duties, and cloud service regulations. This review examines how Saudi organizations can govern cloud storage without reducing sovereignty to a narrow data localization rule. It argues that sovereignty is a multidimensional capability involving lawful jurisdiction, data location, key custody, operational access, auditability, incident response, vendor accountability, and continuity of critical services. Using a structured integrative review of recent academic, regulatory, and standards literature from 2020 to 2025, the paper synthesizes obligations relevant to cloud storage in Saudi Arabia and proposes a control-oriented framework for regulated workloads. The review finds that the main compliance risks arise from cross-border transfers, hidden metadata flows, privileged administrator access, subcontractor chains, weak classification, unclear shared responsibility, and insufficient evidence for audits. It also finds that effective governance requires data-centric architecture rather than contract-only compliance. Recommended practices include workload classification, Saudi-region hosting where required or justified, encryption with locally governed keys, privacy impact assessment, transfer assessment, immutable logging, contractual audit rights, exit planning, and continuous compliance monitoring. The paper contributes a practical framework that aligns legal, technical, and operational controls for Saudi cloud storage environments while supporting innovation under Vision 2030. Its central conclusion is that compliant cloud adoption is achievable when data sovereignty is treated as a measurable governance system rather than a static storage location.

Keywords: Data Sovereignty, Cloud Storage, Saudi Arabia, Personal Data Protection, Regulatory Compliance, Cybersecurity, Data Governance, Cloud Risk Management.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

1. INTRODUCTION

Saudi organizations are moving large volumes of operational, customer, health, financial, and government data into cloud storage because cloud platforms provide elasticity, managed resilience, rapid provisioning, and integration with analytics services. This transition supports Vision 2030 digital transformation, but it also relocates control from owned infrastructure to distributed service environments where legal jurisdiction, technical administration, metadata processing, and subcontracted operations may cross organizational and national boundaries. Cloud storage therefore raises a distinctive governance problem: the organization may remain accountable for data even when the physical infrastructure, support personnel,

encryption services, and replication logic are controlled by a provider. Recent research on cloud privacy compliance shows that public organizations face recurring difficulties with unauthorized access, loss of confidentiality, weak awareness, lack of trust, legal uncertainty, and loss of control when using public cloud services [1].

Saudi Arabia's regulatory direction has made these questions more urgent. The Personal Data Protection Law establishes obligations for controllers and processors, while its implementing instruments and transfer rules require disciplined handling of personal data, sensitive data, and cross-border disclosure [2-4]. National data governance policies also treat government data as a national asset requiring classification, stewardship, sharing controls, and lifecycle management [5, 6]. In parallel, the National Cybersecurity Authority has issued essential, cloud, and data cybersecurity controls that create minimum cybersecurity expectations for entities and cloud service arrangements [7-9]. The Communications, Space and Technology Commission regulates cloud computing and data center services, including service provider registration and market obligations [10-30]. The result is not a single compliance checklist, but a layered regime that combines privacy, cybersecurity, sectoral governance, contractual accountability, and operational resilience.

This paper addresses that layered challenge by reviewing data sovereignty and regulatory compliance in Saudi cloud storage environments. The review is motivated by three gaps. First, much cloud compliance literature discusses privacy principles or international data transfer in general terms, while Saudi organizations need an operational map that connects legal obligations to storage architecture. Second, data sovereignty is often equated with local hosting, although recent scholarship on digital sovereignty emphasizes control over infrastructure, keys, access, procurement dependencies, and continuity during geopolitical or supplier disruption [20, 21]. Third, many organizations treat compliance as a procurement activity, even though modern cloud systems can conflict with privacy regulation through distributed logging, backups, analytics, and automated processing that are difficult to trace [12]. A review paper is therefore appropriate because the field sits at the intersection of legal doctrine, cybersecurity engineering, cloud architecture, and governance practice.

The aim of the study is to develop a review-based compliance framework for Saudi organizations that use cloud storage for regulated data. The objectives are: to synthesize Saudi and international requirements relevant to cloud storage; to identify recurring sovereignty risks in public, private, hybrid, and multi-cloud deployments; to map those risks to technical, contractual, and organizational controls; and to propose an assurance model that helps organizations prove compliance continuously. The contribution is not a new empirical survey, but a rigorous synthesis that translates dispersed requirements into a coherent decision logic for cloud storage design.

2. METHODOLOGY

This study adopts a structured integrative review methodology suitable for topics where legal instruments, technical standards, and academic findings must be interpreted together. The review focused on literature published between 2020 and 2025, including peer-reviewed studies on cloud privacy, accountability, threat modeling, regulatory compliance, and digital sovereignty; Saudi official regulations and control frameworks; and international standards relevant to cloud security and audit. Sources were selected for direct relevance to cloud storage, data protection, cross-border transfer, cybersecurity controls, data classification, encryption, vendor management, and sovereignty. The attached cloud compliance study was used as a conceptual reference because it links public cloud privacy issues to a threat model and shows how legal compliance depends on routines, contracts, encryption, pseudonymization, and awareness [1].

The review proceeded in four stages. First, regulatory scoping identified Saudi instruments that affect data storage decisions, including personal data protection rules, national data governance policies, cybersecurity controls, and cloud service regulations [2-11]. Second, conceptual scoping identified academic work explaining why cloud-scale systems create compliance friction, including conflicts between GDPR-style principles and distributed storage operations, accountability gaps, data transfer uncertainty, and privacy threat categories [12-17]. Third, the sources were coded into six themes: data classification and residency; cross-border transfer and third-country access; technical confidentiality and key control; provider accountability and subcontracting; organizational awareness and routines; and audit evidence. Fourth, the themes were synthesized into a control framework that emphasizes traceability across the data lifecycle.

The method is deliberately review-based rather than survey-based. This is justified because Saudi cloud compliance is still developing, public case evidence is limited, and many obligations are contained in official instruments rather than empirical datasets. To maintain analytical discipline, the review distinguishes enforceable obligations from good practice, and technical controls from legal

safeguards. It also avoids treating foreign privacy frameworks as directly applicable to Saudi Arabia. Comparative sources are used only where they illuminate recurring cloud governance problems, such as transfer risk, accountability, or lack of user awareness [18-22]. The outcome is a normative and practical synthesis designed for organizations that need to make defensible cloud storage decisions in a changing regulatory environment.

3. Conceptual Foundations of Data Sovereignty

Data sovereignty refers to the capacity of a state, organization, or data controller to ensure that data are governed according to applicable legal, policy, and institutional requirements. In cloud storage, sovereignty is broader than the physical location of a file. A dataset may be hosted in a local region but still be exposed to foreign legal processes, offshore support, remote administration, provider telemetry, replicated backups, or foreign-managed encryption keys. Conversely, an international cloud arrangement may sometimes be lawful if transfer conditions, safeguards, and controls are demonstrably satisfied. Sovereignty should therefore be understood as control over location, access, processing purpose, metadata, encryption, operational dependency, audit, and exit.

This multidimensional view aligns with recent work on digital sovereignty, which treats sovereignty as the ability to make autonomous and accountable digital choices without severing beneficial international cooperation [20, 21]. For Saudi organizations, the practical question is not whether every workload must always remain within national borders, but which workloads require local storage, which can use foreign or regional services under safeguards, and what evidence is needed to prove that the chosen model respects law, cybersecurity controls, and business continuity. A sovereign cloud posture is thus a risk-based operating model, not a slogan.

Cloud storage complicates sovereignty because storage is rarely a single function. Object storage, block storage, file storage, content delivery, backup, disaster recovery, data lake services, logs, encryption modules, identity services, and monitoring tools may all process related data. A customer may encrypt business files but overlook search indexes, access logs, diagnostic telemetry, support snapshots, or machine-learning feature stores. The compliance perimeter is therefore wider than the primary data repository. Studies of cloud privacy show that linkability, identifiability, detectability, disclosure, and policy non-compliance can arise from indirect data processing and not only from obvious database exposure [1-16]. This insight is particularly relevant for Saudi organizations handling identity records, health files, government records, citizen services, or strategic industrial data.

4. Saudi Regulatory Landscape

Table 1: Regulatory and control obligations mapped to cloud storage design decisions

Regulatory source	Primary obligation for storage	Architectural implication	Evidence to retain
PDPL and implementing rules [2,3]	Lawful processing, controller accountability, personal-data security, rights support.	Identify personal data, restrict processing purpose, align retention and deletion with lawful basis.	Processing record, privacy notice, consent or lawful basis, deletion log.
Transfer mechanisms [4]	Conditions and safeguards for disclosure or transfer outside the Kingdom.	Map replication, support access, backup regions, and processor locations before approval.	Transfer assessment, contractual clauses, regional configuration report.
National data governance [5,6]	Classification, stewardship, sharing, lifecycle management, and public-value protection.	Apply class-based hosting and access policies to every repository and derivative artifact.	Data inventory, classification register, owner approval, sharing record.
Cybersecurity controls [7-9]	Minimum governance, defense, resilience, third-party, cloud, and data lifecycle controls.	Use least privilege, logging, encryption, backup, incident response, and supplier assurance.	Control mapping, audit reports, access reviews, incident tests.
Cloud and data-center rules [10-30]	Provider registration, service obligations, market transparency, and data-center governance.	Select providers able to demonstrate Saudi compliance, resilience, portability, and service quality.	Provider registration evidence, service terms, SLA, exit plan.

The Saudi cloud storage compliance environment rests on four interacting pillars. The first is personal data protection. The Personal Data Protection Law requires lawful processing, purpose limitation, data minimization, accuracy, security, rights enablement, and controlled disclosure of personal data [2]. Implementing rules and transfer mechanisms add operational detail, including security measures, controller obligations, processor responsibilities, and conditions for transferring personal data outside the Kingdom [3, 4]. For cloud storage, these obligations mean that controllers must know where personal data reside, why they are stored, who can access them, how long they are retained, and whether any disclosure to foreign jurisdictions or providers is lawful.

The second pillar is national data governance. National data governance policies emphasize that data have lifecycle value and must be classified, managed, shared, retained, and disposed of according to sensitivity and public interest [5]. Data classification policy is especially important because cloud storage decisions cannot be made uniformly for all data [6]. Public, internal, confidential, and highly restricted data should not share the same location, access, encryption, backup, or export rules. Classification also provides the bridge between legal obligations and technical controls. Without accurate classification, a cloud team cannot determine whether a workload requires local hosting, stronger key custody, limited support access, or special approval.

The third pillar is cybersecurity control. The Essential Cybersecurity Controls establish baseline cybersecurity governance, defense, resilience, and third-party requirements for covered entities [7]. The Cloud Cybersecurity Controls extend these expectations to cloud service providers and tenants, making shared responsibility explicit and requiring governance over cloud use [8]. The Data Cybersecurity Controls emphasize protection throughout the data lifecycle [9]. These controls shift cloud storage governance from a narrow privacy issue to an enterprise risk issue involving identity, privileged access, encryption, backup, incident response, vulnerability management, monitoring, outsourcing, and assurance evidence.

The fourth pillar is cloud market regulation. CST cloud and data center regulations organize the provider environment, service categories, registration, and service obligations [10, 11]. This matters because regulated storage depends not only on what a customer configures but also on whether the provider is authorized, transparent, auditable, and capable of supporting Saudi regulatory expectations. Provider selection therefore becomes a compliance control. For sensitive Saudi workloads, procurement should evaluate not only price and functionality but also data residency options, contractual commitments, local support models, breach notification, subcontractor disclosure, portability, and resilience.

5. REVIEW FINDINGS

Table 2: Review synthesis matrix linking sovereignty risks to controls and evidence

Sovereignty risk	Typical cloud-storage trigger	Priority controls	Assurance evidence
Unclassified regulated data	Users or developers create repositories without owner approval.	Mandatory tags, data discovery, storage guardrails, approval workflow.	Inventory report, exception register, classification coverage metric.
Hidden cross-border movement	Replication, failover, telemetry, support snapshots, or analytics exports.	Region policies, transfer assessment, support restrictions, data-flow mapping.	Replication settings, provider commitments, transfer record, flow diagram.
Provider or foreign access	Managed keys, offshore support, lawful access exposure, subcontractors.	Customer-managed keys, privileged access logging, subcontractor disclosure.	Key custody logs, support tickets, audit reports, subcontractor list.
Deletion and retention failure	Backups, archives, cache layers, and legal holds outlive approved retention.	Retention locks, deletion workflows, backup expiry, destruction verification.	Deletion certificate, retention report, archive inventory.
Compliance drift	New cloud services or configuration changes bypass original approval.	Policy as code, posture management, change control, periodic reassessment.	Drift report, control dashboard, reassessment minutes.

The first finding is that classification is the foundation of sovereignty. Organizations that begin with a provider selection exercise often discover compliance problems late, whereas organizations that classify workloads before migration can define permitted regions, encryption requirements, retention periods, and transfer conditions. Classification must include primary data and

secondary artifacts such as logs, metadata, backups, indexes, and exported reports. It should also be dynamic because information can become more sensitive when combined with other datasets or when the status of the data subject changes [1]. Saudi storage governance should therefore treat classification as a continuing obligation, not a one-time migration label.

The second finding is that cross-border transfer risk is not limited to deliberate export. Transfer can occur through replication, failover, support access, administrative tooling, security monitoring, subcontractors, or embedded analytics. International literature on GDPR compliance shows that organizations struggle to determine when a cloud operation constitutes transfer, disclosure, or unauthorized access, especially where cloud providers are subject to foreign surveillance or legal compulsion [18, 19]. For Saudi organizations, Article-based transfer controls and national policy obligations require explicit data-flow mapping before storage architecture is approved [2-4]. Data-flow maps should identify countries, entities, purposes, legal bases, retention periods, technical safeguards, and emergency access scenarios.

The third finding concerns encryption and key custody. Encryption is essential but not sufficient. If the provider controls both encrypted data and encryption keys, encryption may protect against external attack while doing little to reduce provider or jurisdictional access risk. Stronger sovereignty requires customer-managed keys, hardware security modules, split duties, local key administration, key rotation, and auditable key access. However, encryption can reduce cloud functionality when providers need plaintext for search, analytics, indexing, or managed support [1]. Saudi organizations should therefore adopt tiered encryption designs. Highly sensitive storage should use customer-controlled keys and restrict provider access, while lower-risk workloads may use managed encryption if contractual and monitoring safeguards are adequate.

The fourth finding is that shared responsibility remains widely misunderstood. Cloud providers secure the infrastructure, but customers remain responsible for data classification, identity configuration, access policies, retention, lawful purpose, and many application-level controls. Misconfigured storage buckets, excessive privileges, unmanaged service accounts, and weak logging remain customer-side failures even when the provider is technically robust. Cloud cybersecurity controls reinforce this distinction by assigning duties to cloud service providers and tenants [8]. Effective compliance therefore requires a responsibility matrix for each storage service, including backup, logging, encryption, incident notification, vulnerability management, and data deletion.

The fifth finding is that contractual compliance must be evidence-based. Contracts are necessary to define processing roles, audit rights, support locations, subcontractor use, incident timelines, deletion duties, and exit assistance. However, contracts cannot substitute for technical control evidence. Research on accountability in the cloud emphasizes that organizations need mechanisms to verify provider behavior across the data lifecycle [13]. Saudi organizations should require audit reports, control attestations, data residency evidence, support access logs, encryption architecture documentation, deletion certificates, penetration testing summaries, and breach notification procedures. Evidence should be refreshed periodically because cloud services and provider subcontractors change frequently.

The sixth finding concerns organizational awareness. Studies using privacy threat models show that content unawareness and policy non-compliance often arise because employees do not understand data handling rules or the difference between information security, privacy, and IT convenience [1-23]. In Saudi cloud storage, users may upload regulated data to collaboration folders, export reports to unmanaged repositories, synchronize files to foreign regions, or use analytics services without transfer assessment. Training must therefore be role-based. Legal teams need cloud architecture literacy; cloud engineers need privacy and classification literacy; procurement teams need sovereignty clauses; and data owners need approval routines for new storage locations.

The seventh finding is that compliance must be continuous. Cloud environments are programmable and change quickly. A workload that was compliant at migration can become non-compliant when a new region is enabled, a replication rule changes, a provider launches a new telemetry feature, or a developer connects storage to an analytics service. Modern governance therefore requires compliance-as-code, automated policy checks, immutable logging, continuous posture management, and periodic reassessment. International standards support this direction by emphasizing risk management, access control, supplier relationships, logging, cryptographic control, and continual improvement [24-28].

6. Proposed Framework

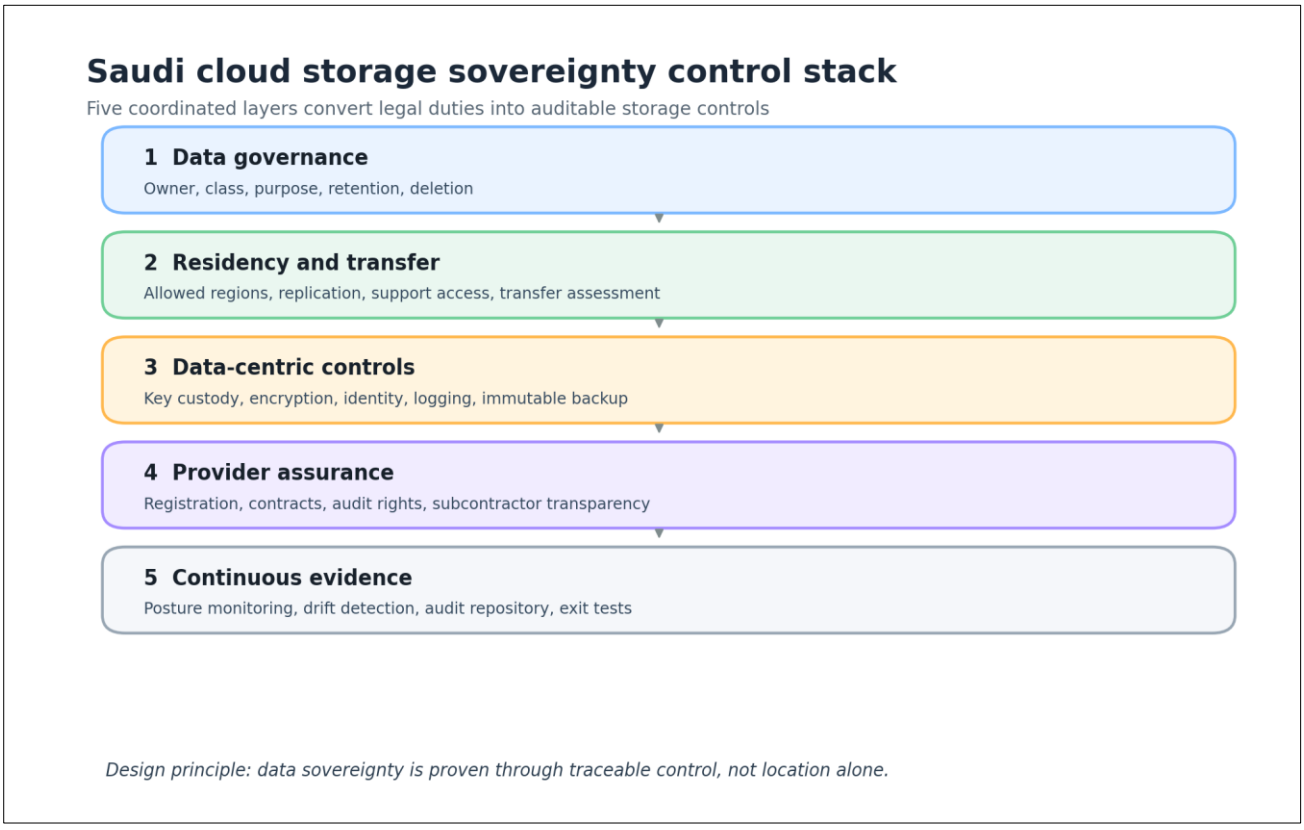

Figure 1: Five-layer control stack for Saudi cloud storage sovereignty and compliance

The proposed Saudi Cloud Sovereignty and Compliance Framework has five layers. Layer one is data governance. Each storage workload must have an accountable owner, classification label, lawful purpose, retention rule, sharing rule, and deletion rule. Data owners should document whether the workload includes personal data, sensitive data, government data, critical business data, or regulated sector data. This layer creates the legal and business context for all technical decisions.

Layer two is residency and transfer governance. The organization should determine whether the workload must remain in the Kingdom, may remain in a Saudi cloud region operated by a global provider, may be hosted in another jurisdiction with safeguards, or must use a private or community cloud. The decision should be recorded in a transfer assessment that considers law, sector requirements, contractual controls, operational access, replication, metadata, support, and emergency recovery. Where transfer is not permitted or uncertainty is high, the architecture should disable foreign replication and restrict support access.

Layer three is data-centric technical control. Storage should be protected through least-privilege identity, customer-managed encryption keys for sensitive workloads, segregation of duties, private connectivity, network isolation, immutable backups, malware scanning, retention locks, tokenization or pseudonymization where useful, and detailed logs. These controls should apply not only to production repositories but also to backups, test copies, data lakes, and analytics exports. A sovereignty architecture that protects the main database while ignoring logs and replicas remains incomplete.

Layer four is provider and contract assurance. Cloud procurement should evaluate provider registration, local data center presence, security certifications, service-level commitments, incident notification, audit evidence, subcontractor transparency, data deletion support, portability, and financial resilience. Contracts should include audit rights, data processing terms, confidentiality obligations, support-location commitments, notification windows, exit duties, and remedies for unauthorized disclosure. Because provider ecosystems evolve, contracts should also require notice of material changes in subcontractors, regions, and service architecture.

Layer five is continuous compliance. Organizations should monitor configuration drift, key access, cross-region replication, public exposure, privileged activity, data export, policy exceptions, and retention violations. Compliance evidence should be

stored in an audit repository mapped to legal obligations and cybersecurity controls. Management should review metrics such as percentage of classified workloads, number of unresolved transfer exceptions, encryption-key ownership, logging coverage, supplier evidence currency, time to revoke access, and verified deletion completion. These metrics convert sovereignty from an abstract principle into measurable operational control.

7. DISCUSSION

The review demonstrates that Saudi cloud storage compliance is not anti-cloud. Rather, it requires more precise cloud adoption. Local regions, domestic data centers, registered providers, and sovereign service features can reduce risk, but they do not automatically solve accountability problems. A locally hosted workload can still fail compliance through poor identity management, unclassified data, excessive administrator access, weak deletion controls, or inadequate audit evidence. Conversely, some lower-risk data may be suitable for broader cloud services if transfer conditions and safeguards are documented. The correct question is therefore not whether cloud storage is allowed, but which storage model is justified for a specific data class and control environment.

A second implication is that compliance teams and cloud teams must be integrated. Legal review alone cannot identify hidden telemetry, replication, key management, or backup flows. Technical review alone cannot interpret lawful basis, data subject rights, regulatory transfer conditions, or public-sector confidentiality obligations. The attached cloud compliance study shows that organizations often rely on contracts while still feeling that they lack full control over provider behavior [1]. Saudi organizations should therefore create multidisciplinary cloud governance boards involving data owners, legal advisers, cybersecurity teams, procurement, enterprise architects, and internal audit.

A third implication concerns innovation. Strict sovereignty requirements are sometimes viewed as slowing digital transformation. The review suggests a more balanced view. Clear classification, transfer assessment, local-key architecture, and compliant provider ecosystems can accelerate adoption because they reduce uncertainty. Organizations that lack a decision framework often delay migration or accept uncontrolled risk. By contrast, organizations that know which workloads can use which storage patterns can migrate faster and more safely. Regulatory clarity, local cloud capacity, and repeatable templates are therefore innovation enablers.

A fourth implication is the need for audit-ready architecture. Regulators and boards increasingly expect evidence rather than verbal assurances. Audit-ready architecture means that every sensitive repository can produce records showing classification, location, access history, key custody, backup location, processor identity, subcontractor status, retention rule, and deletion action. This does not require manual paperwork for every storage event. It requires automated evidence collection and a governance model that links cloud telemetry to compliance obligations.

8. Practical Implications

For Saudi public-sector organizations, the main priority is to align cloud storage with classification, national data policies, and cybersecurity controls before migration. Government data should be classified by sensitivity and public value, and highly restricted datasets should receive stronger residency, encryption, access, and monitoring requirements. Agencies should also avoid uncontrolled use of consumer collaboration storage for official records, because such tools may create unmanaged copies and unclear retention.

For private-sector organizations, especially finance, health, energy, telecommunications, and platform businesses, the priority is to integrate PDPL compliance with enterprise risk management. Personal data inventories should identify storage services, lawful purposes, processors, data subject rights workflows, and transfer exposure. Sensitive customer data should be supported by stronger encryption, role governance, and deletion capabilities. Organizations should treat breach response as a shared responsibility exercise involving providers, processors, legal counsel, and communications teams.

For cloud providers, the opportunity is to offer services that make Saudi compliance easier to evidence. Useful features include Saudi-region commitments, transparent support-location controls, customer-managed key options, sovereign logging, local incident escalation, compliant deletion reports, subcontractor disclosure, and mappings to Saudi cybersecurity controls. Providers that can produce clear audit evidence will be better positioned than providers that merely claim security excellence.

For policymakers and regulators, the review suggests value in practical implementation guidance. Organizations need templates for transfer assessment, data residency decisions, controller-processor clauses, incident notification, and cloud exit planning. They also need clarity on how different frameworks interact. Regulatory convergence does not mean weakening obligations; it means making

obligations easier to interpret and implement consistently.

9. Limitations and Future Research

This paper is limited by its review design and by the evolving nature of Saudi cloud regulation. It does not test the proposed framework through interviews, audits, or case studies, and it does not provide sector-specific legal advice. Publicly available information on actual Saudi cloud storage practices remains limited, so the analysis emphasizes regulatory logic, academic evidence, and control design rather than empirical performance measurement. Another limitation is that international literature often reflects European privacy debates, which must be adapted carefully rather than copied into the Saudi context.

Future research should conduct interviews with Saudi data protection officers, cloud architects, regulators, and procurement leaders to validate the proposed framework. Sector-specific studies are needed for health, banking, education, government platforms, and critical infrastructure. Empirical work should examine whether organizations can produce audit evidence for data location, key access, deletion, and transfer assessment. Further research should also investigate sovereign cloud economics, because excessive fragmentation may increase cost, while poorly governed centralization may increase systemic risk. Finally, technical research should evaluate automated compliance tools capable of discovering regulated data, detecting unauthorized replication, enforcing policy as code, and producing regulator-ready evidence.

10. Assurance Maturity Metrics

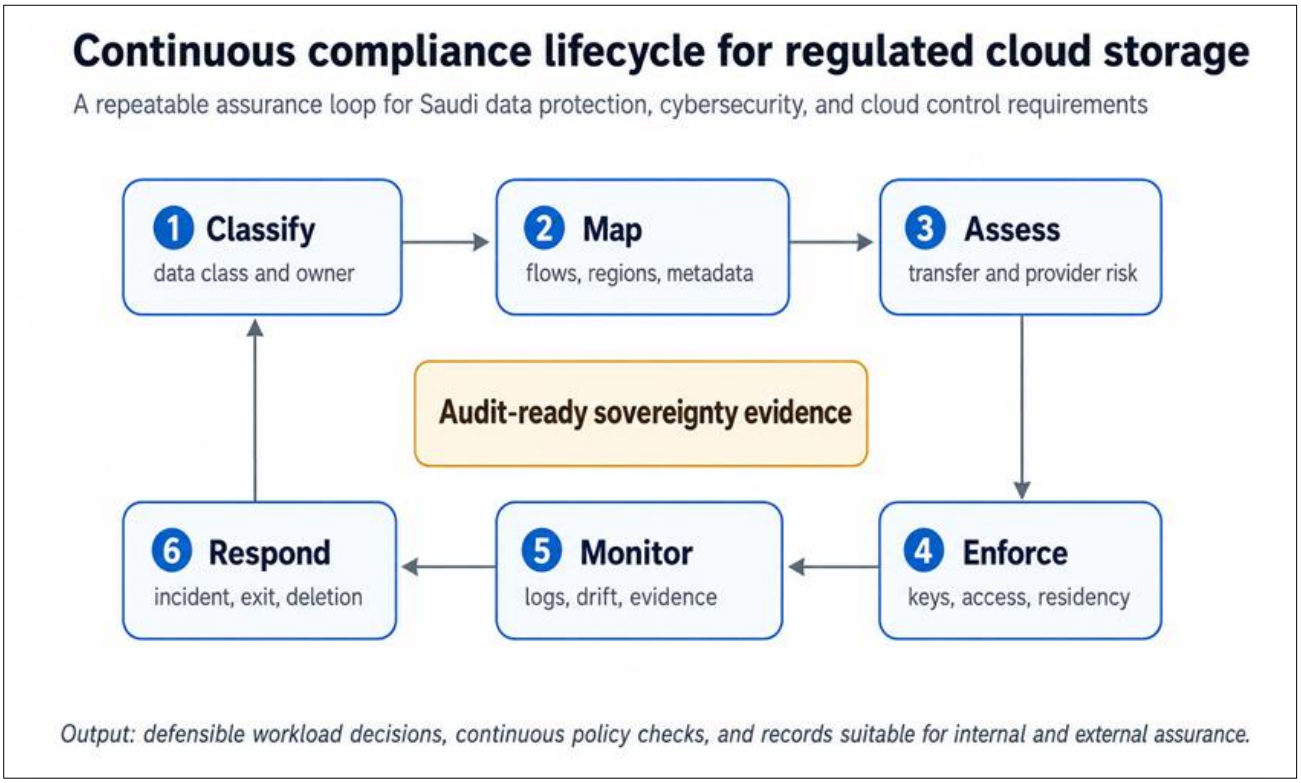

Figure 2: Continuous assurance lifecycle for regulated cloud storage workloads

A compliance framework becomes useful only when it can be measured. Saudi organizations should therefore convert sovereignty expectations into maturity indicators that can be reviewed by executives and auditors. The first indicator is classification coverage, defined as the proportion of storage repositories with an approved owner, data class, retention rule, and permitted hosting pattern. Low coverage indicates that the organization cannot reliably determine which workloads require local residency or transfer assessment. The second indicator is residency assurance, measured by the percentage of regulated repositories with verified region settings, replication controls, backup locations, and documented exceptions. This should include evidence from provider consoles, infrastructure code, and audit reports rather than screenshots alone.

The third indicator is key-governance strength. Mature organizations should be able to show which keys protect each sensitive repository, who can administer them, whether keys are generated and stored under approved custody, when

they were rotated, and whether provider personnel can decrypt data. The fourth indicator is access accountability, measured through privileged access reviews, service-account inventories, conditional access coverage, and unresolved toxic combinations of duties. The fifth indicator is transfer visibility. Each outbound data flow, including analytics exports and support access, should have a lawful purpose, destination, processor identity, and safeguard. The sixth indicator is deletion verifiability. Organizations should not assume deletion merely because an object is removed from a user interface; they should confirm retention locks, backup expiry, archive removal, and provider deletion attestations.

The final indicator is resilience under regulatory stress. A sovereign storage environment should remain accessible during provider outage, legal dispute, incident investigation, or geopolitical disruption. Metrics can include restore success rate, recovery time, alternative access procedures, tested exit plans, and ability to migrate critical datasets to another approved environment. These indicators do not replace Saudi regulatory obligations. They operationalize them by enabling managers to see whether policy is functioning in daily storage operations. They also support continuous improvement because weaknesses can be prioritized according to data sensitivity and business criticality.

An important governance lesson is that maturity should be evaluated at workload level rather than only at enterprise level. A company may have strong cloud policies but weak evidence for a single high-risk repository. Conversely, a small team may operate a well-controlled sensitive workload even when wider organizational maturity is uneven. Workload-level assessment also supports proportionality. Public information, internal collaboration files, confidential contracts, health records, and national security data should not carry identical controls, because over-control can waste resources and under-control can create legal exposure. A practical Saudi model should therefore combine enterprise policy with workload-specific risk decisions. Each decision should record the data class, legal basis, hosting choice, transfer status, key model, support model, recovery arrangement, and evidence owner. When this record is maintained automatically, compliance becomes a living control environment rather than a static approval document. This is the operational meaning of data sovereignty in cloud storage: not isolation, but governed, auditable, and resilient control.

Such discipline gives regulators evidence, gives executives confidence, and gives engineers clear boundaries for secure innovation across expanding Saudi cloud ecosystems and future data services securely.

11. CONCLUSION

Data sovereignty and regulatory compliance in Saudi cloud storage environments require a shift from location-only thinking to control-based governance. Saudi organizations must understand what data they store, which rules apply, where the data and metadata move, who can access them, who controls the keys, how providers are monitored, and what evidence proves compliance. The review shows that Saudi Arabia already has a substantial regulatory foundation through personal data protection rules, data governance policies, cybersecurity controls, and cloud service regulations. The practical challenge is integration.

A mature compliance posture combines classification, residency assessment, transfer governance, encryption and key custody, provider assurance, contractual safeguards, continuous monitoring, and audit evidence. This approach allows cloud storage to support innovation without surrendering accountability. The proposed framework can help organizations choose appropriate storage models, reduce hidden transfer risk, and demonstrate compliance over time. In the Saudi context, sovereignty should be measured by the ability to govern data throughout its lifecycle, maintain lawful and secure control, and preserve national and organizational resilience while benefiting from modern cloud capabilities.

REFERENCES

1. Issaoui, A., Örtensjö, J., & Islam, M. S. (2023). Exploring the General Data Protection Regulation compliance in cloud services: insights from Swedish public organizations on privacy compliance. Future Business Journal, 9, 107. https://doi.org/10.1186/s43093-023-00285-2
2. Saudi Data and Artificial Intelligence Authority. (2023). Personal Data Protection Law. Riyadh: SDAIA.
3. Saudi Data and Artificial Intelligence Authority. (2024). Implementing Regulation of the Personal Data Protection Law. Riyadh: SDAIA.
4. Saudi Data and Artificial Intelligence Authority. (2024). Regulation on Personal Data Transfer Outside the Kingdom and Standard Contractual Clauses. Riyadh: SDAIA.
5. Saudi Data and Artificial Intelligence Authority. (2020). National Data Governance Interim Regulations. Riyadh: National Data Management Office.
6. Saudi Data and Artificial Intelligence Authority. (2020). Data Classification Policy. Riyadh: National Data Management Office.

7. National Cybersecurity Authority. (2024). Essential Cybersecurity Controls ECC-2:2024. Riyadh: NCA.
8. National Cybersecurity Authority. (2024). Cloud Cybersecurity Controls CCC-2:2024. Riyadh: NCA.
9. National Cybersecurity Authority. (2022). Data Cybersecurity Controls DCC-1:2022. Riyadh: NCA.
10. Communications, Space and Technology Commission. (2024). Cloud Computing Services Provisioning Regulations. Riyadh: CST.
11. Communications, Space and Technology Commission. (2024). Data Center Services Regulations. Riyadh: CST.
12. Shastri, S., Wasserman, M., & Chidambaram, V. (2021). How design and operation of modern cloud-scale systems conflict with GDPR. Communications of the ACM, 64(2), 66-73. https://doi.org/10.1145/3378061
13. Jaatun, M. G., Pearson, S., Gittler, F., Leenes, R., & Niezen, M. (2020). Enhancing accountability in the cloud. International Journal of Information Management, 53, 101498. https://doi.org/10.1016/j.ijinfomgt.2016.03.004
14. de Carvalho, M., Prete, C., Martin, Y., Rivero, R., Önen, M., Schiavo, F., Rumín, F., Mouratidis, H., Yelmo, J., & Koukovini, M. (2020). Protecting citizens' personal data and privacy: joint effort from GDPR EU cluster research projects. SN Computer Science, 1, 217. https://doi.org/10.1007/s42979-020-00218-8
15. Robles-Gonzales, A., Parra-Arnau, J., & Forné, J. (2020). A LINDDUN-based framework for privacy threat analysis on identification and authentication processes. Computers & Security, 94, 101755. https://doi.org/10.1016/j.cose.2020.101755
16. Reisinger, T., Wagner, I., & Boiten, E. A. (2022). Security and privacy in unified communication. ACM Computing Surveys, 55(3), 1-35. https://doi.org/10.1145/3498335
17. Diker Vanberg, A. (2020). Informational privacy post GDPR: end of the road or the start of a long journey? International Journal of Human Rights, 25(1), 52-78. https://doi.org/10.1080/13642987.2020.1789109
18. Tracol, X. (2020). Schrems II: the return of the Privacy Shield. Computer Law & Security Review, 39, 105484. https://doi.org/10.1016/j.clsr.2020.105484
19. Rotenberg, M. (2020). Schrems II, from Snowden to China: toward a new alignment on transatlantic data protection. European Law Journal, 26, 141-152. https://doi.org/10.1111/eulj.12370
20. Moerel, L., & Timmers, P. (2021). Reflections on digital sovereignty. EU Cyber Direct Research in Focus Series. https://doi.org/10.2139/ssrn.3772777
21. Misra, S., Sharma, A., & Singh, R. (2025). Trust in digital sovereignty: a review of security, privacy, and regulatory challenges. Public Organization Review. https://doi.org/10.1007/s11115-025-00968-0
22. Aslak Juliussen, B., Kozyri, E., Johansson, D., & Rui, J. P. (2023). The third country problem under the GDPR: enhancing protection of data transfers with technology. International Data Privacy Law, 13(2), 66-84.
23. Jaeger, L., Eckhardt, A., & Kroenung, J. (2021). The role of deterrability for the effect of multi-level sanctions on information security policy compliance. Information & Management, 58(3), 103318. https://doi.org/10.1016/j.im.2020.103318
24. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements. Geneva: ISO.
25. International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: Information security controls. Geneva: ISO.
26. National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53 Revision 5. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.SP.800-53r5
27. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.CSWP.29
28. European Union Agency for Cybersecurity. (2021). Cloud Security for Healthcare Services. Athens: ENISA.
29. World Bank. (2024). Cloud computing in the public sector: strategy and practices from the Kingdom of Saudi Arabia. Washington, DC: World Bank.
30. Organisation for Economic Co-operation and Development. (2025). Cloud computing services provisioning regulations: Saudi Arabia policy initiative. OECD AI Policy Observatory.