Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i03.013

OPEN ACCESS

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

Original Research Article

Cloud-Based Disaster Recovery and Business Continuity for Mission-Critical Data in Saudi Organizations

Syed Imtiyaz[1]*
[1]Independent Researcher

***Corresponding Author**
Syed Imtiyaz
Independent Researcher

Article History
Received: 11.04.2026
Accepted: 01.06.2026
Published: 03.06.2026

Abstract: Saudi organisations are placing mission-critical data in cloud, hybrid-cloud and software-as-a-service environments while national regulation is tightening expectations for data protection, service continuity and cyber resilience. This review synthesises 2020-2025 literature and Saudi regulatory guidance to examine how cloud-based disaster recovery and business continuity can protect essential datasets in government, healthcare, finance, energy, logistics and digitally enabled small and medium enterprises. A structured narrative methodology was used to screen recent peer-reviewed articles, international standards and official Saudi control documents. The review finds that cloud continuity is most effective when recovery is treated as a socio-technical capability rather than a storage service. Important themes include shared accountability across service models, recovery objective engineering, sovereign data governance, automated failover, immutable backup, identity resilience, service-level evidence and continuity exercises. The paper proposes a Saudi-aligned reference model that integrates business impact analysis, multi-region architecture, regulatory mapping, contractual assurance and continuous testing. It contributes a practical research synthesis for scholars and practitioners by clarifying how organisations can balance cloud elasticity with local compliance, supplier concentration, cyberattack recovery and executive oversight. The review concludes that cloud-based recovery can reduce downtime and data loss, but only when governance, architecture and rehearsed operating procedures mature together.

Keywords: Cloud Disaster Recovery, Business Continuity, Mission-Critical Data, Saudi Arabia, Cyber Resilience, Cloud Governance, Regulatory Compliance.

1. INTRODUCTION

Cloud platforms have become central to Saudi digital transformation because they allow organisations to scale computing capacity, deploy services faster and store large operational datasets without building every component internally. Yet the same dependence creates a continuity problem: if a cloud workload, identity service, network route, key vault or managed database is unavailable, core services may stop at national speed. Mission-critical data in this paper means information whose loss, corruption or prolonged unavailability would disrupt public services, patient care, payment settlement, industrial operations, citizen transactions or contractual obligations. Cloud-based disaster recovery therefore cannot be reduced to periodic backup. It must include business impact analysis, system dependency mapping, recovery time objectives, recovery point objectives, legal

constraints, crisis communication and technical recovery validation [2-4].

Recent research shows that cloud recovery decisions are shaped by dependability, elasticity, security, data integrity and shared responsibility. Dependability influences whether organisations trust cloud services for strategic operations [12]. Dynamic risk assessment is also necessary because cloud risk changes when configurations, workloads and suppliers change [5]. Storage integrity remains a recurring challenge because backups that exist but cannot be verified, decrypted or restored are operationally weak [6]. These insights are important for Saudi organisations, where cloud adoption is growing across SMEs and public sector entities while regulators specify cybersecurity, cloud service and personal data transfer controls [14-21].

Saudi Arabia presents a distinctive setting for this review. Organisations must design continuity for a market that encourages cloud services, local data centres and digital government, while requiring careful handling of government data, personal data, cybersecurity controls and third-party risk. The Cloud First policy supports cloud adoption by government entities [19], while CST regulations establish obligations for cloud providers and subscribers [18]. NCA controls define minimum expectations for cloud cybersecurity and essential cybersecurity governance [15-17]. SDAIA regulations add privacy and transfer considerations for personal data [20, 21]. A resilience architecture that ignores this regulatory fabric may be technically elegant but institutionally unusable.

The problem addressed in this paper is therefore not whether cloud can support disaster recovery, but how Saudi organisations can govern and engineer cloud-based recovery for mission-critical data without creating new single points of failure. The review argues that effective continuity requires alignment among four layers: business priorities, cloud architecture, cyber-resilient data protection and regulatory assurance. This alignment is particularly important where organisations rely on managed services, container platforms, serverless functions and cross-cloud integrations, because responsibility for recovery may shift across providers, subscribers and technology partners [3-30].

2. Aim and Objectives of the Study

The aim of this review is to develop a research-informed and Saudi-aligned understanding of cloud-based disaster recovery and business continuity for mission-critical data. Six objectives guide the paper. First, it clarifies the relationship between business continuity and disaster recovery in cloud environments. Second, it identifies recent technical mechanisms that support resilient recovery, including replication, orchestration, fault injection, service-level monitoring and cloud-native deployment patterns. Third, it examines how Saudi regulatory expectations influence architecture, data residency, provider selection and evidence requirements. Fourth, it evaluates governance challenges arising from shared responsibility across infrastructure, platform, software and recovery-as-a-service models. Fifth, it proposes a conceptual reference model for resilient cloud continuity in Saudi organisations. Sixth, it identifies research gaps that can be investigated through future empirical work in Saudi sectors that operate critical data assets.

3. STRUCTURED REVIEW METHODOLOGY

This paper adopts a structured narrative review methodology suitable for an interdisciplinary topic that combines cloud engineering, continuity management, cybersecurity regulation and organisational governance. The search focused on literature and guidance published from 2020 to 2025, reflecting the period in which cloud-native operations, Saudi cloud regulation, cyber resilience and modern continuity standards accelerated. Sources were identified through major academic publishers, standards organisations and official Saudi regulatory portals. Keywords included cloud disaster recovery, business continuity, mission-critical data, cloud resilience, multi-cloud, cloud cybersecurity, Saudi cloud adoption, data integrity, service-level agreement, cyber resilience and personal data transfer.

Inclusion criteria were relevance to cloud recovery, continuity planning, cloud security, Saudi regulation, or mission-critical data governance; publication within 2020-2025; and sufficient conceptual or practical contribution. Exclusion criteria were opinion-only material without traceable authority, studies focused solely on non-cloud physical disaster management, and papers that did not address continuity, recovery, data assurance or cloud governance. Academic papers were assessed for clarity of method, relevance to cloud recovery, sector applicability and contribution to resilience theory or practice. Regulatory and standards documents were assessed for direct applicability to Saudi organisations and for their role in shaping audit evidence, supplier accountability or data protection obligations.

The synthesis proceeded in four steps. The first step separated business continuity from disaster recovery while recognising their overlap. The second mapped technical controls to continuity outcomes, such as lower recovery time, lower recovery point loss, greater availability and stronger data integrity.

The third interpreted Saudi regulatory instruments as design constraints rather than administrative afterthoughts. The fourth integrated the findings into a conceptual model and implementation matrix. This method is transparent, replicable in logic and appropriate for a review paper because it synthesises diverse sources without claiming statistical meta-analysis.

Table 1: Review protocol and analytical logic

Review element	Operational definition used in this paper
Period	Sources published from 2020 to 2025, with emphasis on cloud, continuity, cyber resilience and Saudi regulation.
Source types	Peer-reviewed journal papers, international standards, official Saudi regulatory documents and cloud security frameworks.
Core questions	How can cloud recovery protect mission-critical data, who is responsible, and which controls create evidence of recoverability?
Quality lens	Relevance to RTO/RPO, data integrity, shared responsibility, Saudi applicability, regulatory alignment and practical implementability.
Synthesis approach	Thematic coding across architecture, governance, security, privacy, supplier assurance and organisational maturity.

4. Conceptual Foundations: Continuity, Recovery and Resilience

Business continuity and disaster recovery are often used interchangeably, yet recent scholarship emphasises that they are related but not identical. Business continuity concerns the organisation-wide ability to keep essential services operating or restore them to acceptable levels after disruption. Disaster recovery is narrower and focuses on recovering information systems, infrastructure, applications and data after an incident [2]. Operational resilience extends the discussion by asking whether the organisation can absorb, adapt and learn when disruption exceeds planned assumptions [4]. In cloud environments, these concepts converge because technology platforms mediate nearly every critical process.

For mission-critical data, the most practical continuity question is not where the data is stored, but whether authorised users, applications and automated processes can access trustworthy data during stress. The value of a recovery plan depends on tested restoration, dependency awareness and executive ownership. A cloud backup that is not mapped to a business process cannot assure continuity. Likewise, a continuity plan that ignores database consistency, identity recovery, encryption keys and provider outage modes may fail when invoked. ISO/IEC 27031:2025 is especially relevant because it frames ICT readiness as part of business continuity and explicitly includes external service dependencies such as cloud providers [25].

Cloud architectures create resilience opportunities. Elastic resources can be provisioned on demand, managed databases can replicate across zones, infrastructure-as-code can rebuild environments and observability tools can detect failures quickly. Cloud also creates resilience risks. Misconfigured identity, provider concentration, opaque managed service dependencies, cross-border data constraints, ransomware targeting backups and unavailable control planes can undermine recovery. Multi-cloud and container strategies may reduce vendor dependency, but they also add complexity, inconsistent security models and new authentication paths [29, 30]. The literature therefore supports a balanced view: cloud increases continuity options, but only mature governance converts options into recoverable capability.

5. Saudi Regulatory and Organisational Context

Saudi cloud continuity design is shaped by a layered regulatory environment. NCA Cloud Cybersecurity Controls define minimum cybersecurity requirements for cloud service providers and tenants, including governance, risk management, identity, data protection and resilience themes [15, 16]. ECC 2-2024 strengthens entity-wide cybersecurity governance and connects cyber risk to national digital transformation [17]. CST cloud service provisioning regulations define provider and subscriber obligations, registration expectations and service responsibilities in the Saudi market [18]. These controls are not merely compliance artefacts; they are architectural requirements because they influence data classification, localisation, incident handling, supplier due diligence and contractual evidence.

Personal data adds another constraint. SDAIA regulations require lawful processing, controller accountability and safeguards for transfers outside the Kingdom [20, 21]. For disaster recovery, this means that cross-region replication, backup export, managed support access and forensic copying should be assessed before deployment, not after an incident. The risk is not only legal exposure. Unclear transfer rules can delay recovery if a team discovers during a crisis that replicated data, encryption keys or support logs cannot be used as planned.

Saudi organisations also differ in maturity. Large regulated entities may have enterprise risk teams, security operations centres and local cloud regions available to them. SMEs may adopt cloud services for affordability and agility but lack tested runbooks, contract expertise or specialist recovery skills. Exploratory research on Saudi SMEs indicates that cloud adoption is important for efficiency but still faces knowledge and organisational barriers [14]. A Saudi continuity model must therefore be scalable: it should support advanced automation for mature entities and clear minimum controls for smaller organisations.

6. Cloud-Based Disaster Recovery Architecture

The first architectural principle is data classification. Not all datasets require the same recovery investment. Mission-critical records such as patient medication histories, payment ledgers, identity claims, industrial telemetry and service authorisations require stricter objectives than archival reports. Business impact analysis should assign each data class an RTO, RPO, maximum tolerable downtime, integrity requirement, confidentiality requirement and lawful location. This classification then guides replication frequency, encryption design, backup immutability and recovery sequence.

The second principle is separation of failure domains. A resilient architecture should avoid placing production, recovery copies, management credentials, logging and backup deletion permissions under one compromised identity boundary. Where possible, organisations should use separate accounts, subscriptions or projects for backup vaults, distinct administrative roles, separate key material and limited break-glass procedures. Storage-level integrity research supports the need for verifiable integrity checks, access control and protection against tampering [6]. For cyber recovery, immutable backup and isolated copies should complement, not replace, detection and prevention.

The third principle is orchestration. Cloud recovery improves when infrastructure, configuration, dependencies and data restoration are automated through tested runbooks. Containerisation and multi-cloud patterns can increase portability, but only where images, secrets, policies, monitoring and network routes are reproducible [29]. Serverless platforms and function-as-a-service can reduce infrastructure management, yet security and cold-start or platform dependency concerns should be addressed in recovery planning [9, 10]. Fault injection research is valuable because it tests whether systems remain resilient under realistic component failures rather than ideal laboratory assumptions [8].

The fourth principle is evidence. Boards and regulators need proof that continuity works. Evidence includes recovery exercise results, backup restoration logs, integrity checks, RTO/RPO achievement, supplier attestations, service-level monitoring and incident lessons learned. Blockchain-enabled SLA monitoring has been proposed as one approach to tamper-resistant service evidence [11], while dynamic cloud risk assessment can help teams update risk ratings as environments change [5]. Evidence should be stored in a way that is available during a crisis, not only in the affected platform.

7. Business Continuity Governance and Shared Responsibility

Cloud recovery succeeds when responsibilities are explicit. In infrastructure-as-a-service, the customer usually controls operating systems, application configuration and much of the recovery workflow. In platform-as-a-service and software-as-a-service, the provider controls more of the stack, but the subscriber still owns data classification, access decisions, process continuity, contract requirements and user communication. Recent work on cloud service models shows that accountability and responsibility vary by service and recovery model, making RACI-style allocation useful during procurement and continuity planning [3].

Saudi organisations should therefore include recovery clauses in cloud contracts and supplier assessments. These clauses should specify backup frequency, retention, deletion protection, restoration support, incident notification, data location, subcontractor access, service credits, audit rights, exit procedures and evidence format. They should also define what happens if the cloud provider is available but a customer configuration, identity tenant or integration fails. This distinction is important because provider availability does not guarantee customer service continuity.

Governance should also connect technical recovery with crisis management. ISO 22361:2022 emphasises crisis leadership, decision-making, communication, training and learning [26]. In practice, this means that a database failover is only one part of continuity. Organisations must know who declares an incident, who approves manual workarounds, who communicates with regulators and customers, who authorises emergency access and who decides when to return to normal operation. ISO 22301:2019/Amd 1:2024 further reinforces the need to integrate changing external risks into continuity management [27].

8. Security, Privacy and Data Integrity Risks

Cyberattacks are now a central driver of disaster recovery planning. Ransomware, destructive

malware, DDoS campaigns, insider misuse and credential compromise can make data unavailable even when facilities and cloud regions remain operational. DDoS detection research demonstrates the relevance of cloud-native monitoring and software-defined controls for availability protection [7]. Serverless and managed service research highlights that security boundaries shift when code execution, event triggers and provider-managed components become part of the recovery path [9].

Identity resilience deserves special attention. If privileged accounts, single sign-on, multi-factor devices or key management services fail, teams may be unable to restore applications even when backups are intact. NIST SP 800-53 Rev. 5 and NIST CSF 2.0 both support governance, protection, detection, response and recovery outcomes that can be mapped to cloud continuity [23, 24]. ISO/IEC 27001:2022 and CSA CCM v4 provide further control structures for access control, logging, supplier management and incident readiness [22-28]. The practical implication is clear: recovery designs should be tested under scenarios where identity, keys or administrator workstations are impaired.

Privacy must be engineered into recovery. Backup copies often contain the most complete version of organisational data, making them attractive targets and raising obligations for retention, transfer and destruction. Saudi personal data transfer rules require risk assessment and safeguards when data is transferred outside the Kingdom [20]. Therefore, recovery teams should record where backup replicas reside, who can access them, how encryption keys are managed, and how data subjects or regulators would be informed if backup data were exposed.

9. Proposed Saudi-Aligned Reference Model

Figure 1 presents the proposed reference model. The model has three planes. The data and workload plane protects applications, databases, backup copies, keys and access paths. The continuity orchestration plane coordinates runbooks, replication, failover, exercises and observability. The governance and assurance plane aligns policies, contracts, audit evidence and risk ownership. This layered design reflects the finding that cloud disaster recovery is a governance and engineering capability, not a single tool purchase [1-8].

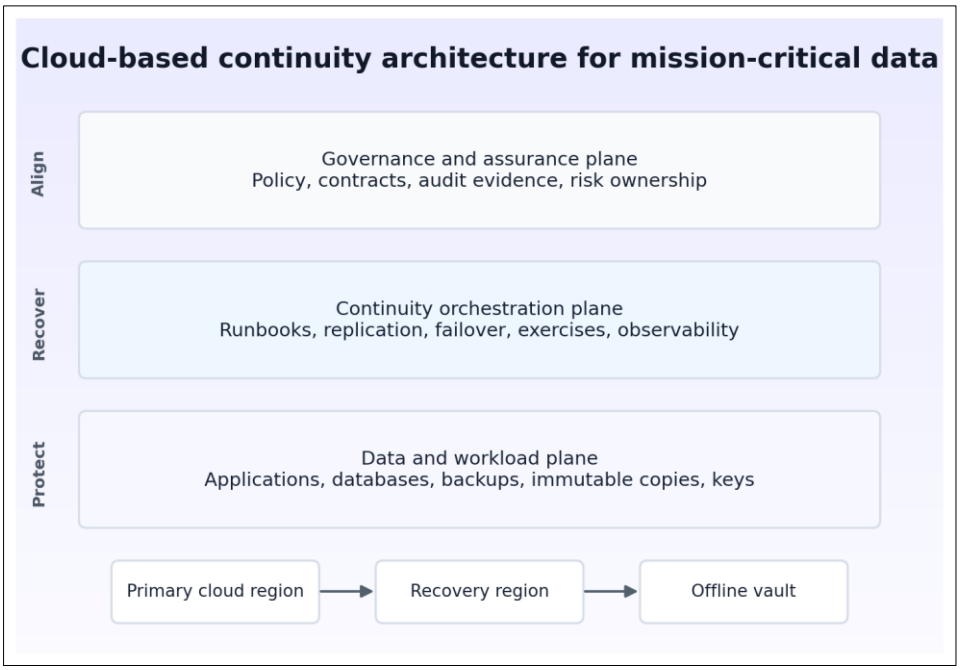

Fig. 1: Saudi-aligned cloud continuity architecture for mission-critical data.

The model begins with executive sponsorship and criticality mapping. Each mission-critical service should have a named business owner, technology owner, security owner and recovery coordinator. The team should document upstream and downstream dependencies, including identity, network, third-party APIs, payment gateways, data warehouses, customer messaging and reporting obligations. A recovery sequence should then be defined, because restoring every system simultaneously may consume scarce bandwidth, people and administrative attention.

The second stage is architecture selection. Options include backup-and-restore, pilot light, warm standby, active-active regional deployment, SaaS-native recovery, and recovery-as-a-service. Backup-and-restore is cheaper but may miss aggressive RTO targets. Warm standby and active-active designs reduce downtime but increase cost,

complexity and synchronisation risk. Hybrid models may be suitable when Saudi data residency or operational technology constraints require local processing while cloud is used for protected copies, analytics or emergency capacity [13-18].

The third stage is continuous validation. The organisation should test restoration of randomly selected datasets, execute failover exercises, simulate identity loss, verify integrity hashes, review provider reports and update runbooks after every material change. Predictive analytics and automated recovery can support mature environments, but they should not remove human accountability. Table 2 summarises the key control domains required for cloud-based disaster recovery and business continuity in Saudi organisations, linking each recommended practice to the type of evidence that should be retained for governance, audit and recovery assurance.

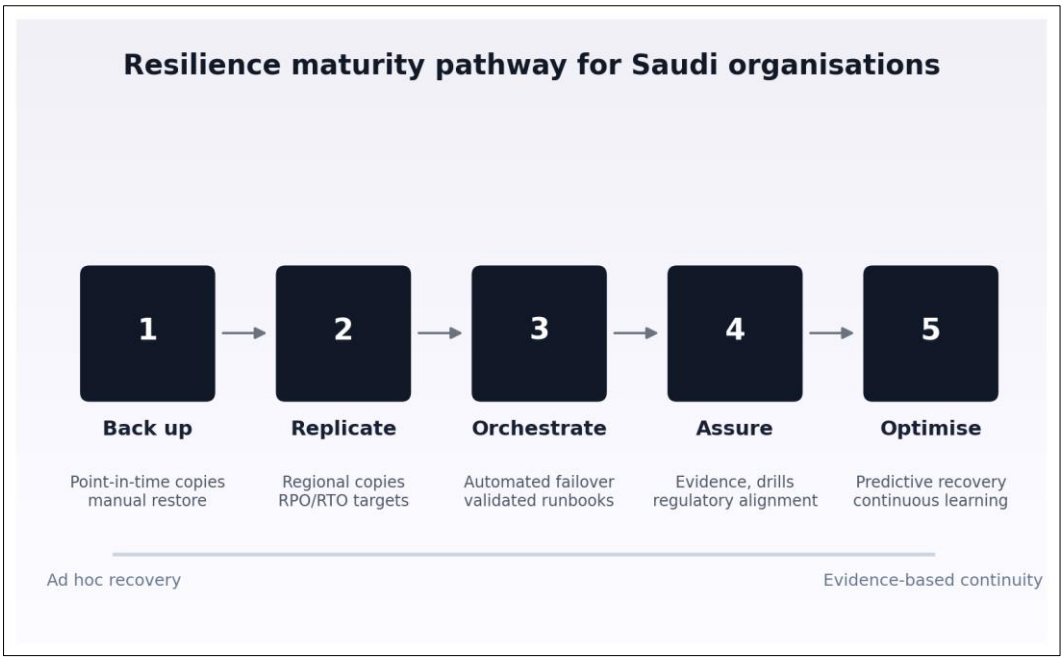

Fig. 2: Resilience maturity pathway from basic backup to evidence-based continuity.

10. DISCUSSION

The review shows that Saudi organisations can gain significant resilience from cloud-based recovery, but the highest value comes from disciplined integration. Cloud elasticity reduces the need for duplicate physical capacity, yet it does not decide which processes matter most. Cloud replication reduces data loss, yet it may replicate corruption if integrity controls are weak. Cloud automation accelerates failover, yet it may accelerate mistakes if code, credentials or network assumptions are wrong. Cloud providers offer mature controls, yet subscribers remain accountable for configuration, data classification and continuity outcomes [3-22].

The Saudi context intensifies these lessons. National regulation encourages secure cloud adoption while expecting entities to manage cyber risk, cloud tenant responsibilities and personal data safeguards. For boards and executives, the central question should shift from "do we have backups?" to "can we prove that critical services can continue within approved tolerances under credible disruption scenarios?" This question forces alignment between risk appetite, budget, architecture and assurance.

A second discussion point is supplier concentration. Using one major provider can simplify skills, tooling and contracts, but may create dependence on one control plane. Using multiple providers can increase bargaining power and recovery options, but may introduce inconsistent identity, monitoring, security and operational models [29, 30]. The review suggests that multi-cloud should be adopted only when the organisation can fund standardisation, automation and specialist skills. Otherwise, a well-designed single-cloud or hybrid architecture with isolated backups and tested exit procedures may provide stronger practical resilience.

A third issue is recovery culture. Continuity cannot be outsourced entirely because cloud recovery depends on internal decisions about priorities, risk tolerance and acceptable manual workarounds. Organisations should train cross-functional teams, rehearse crisis communication, and include business users in exercises. Mature recovery culture treats failed exercises as useful evidence, not

embarrassment. Such learning orientation is consistent with resilience literature that emphasises adaptation and continual improvement [4-26].

11. Research Gaps and Future Directions

Several gaps remain. First, empirical studies of Saudi cloud recovery maturity are limited, especially across healthcare, logistics, education, energy and SMEs. Second, more research is needed on how Saudi entities interpret data localisation and personal data transfer requirements during emergency recovery. Third, few studies measure the true cost-performance trade-off between warm standby, active-active and recovery-as-a-service models in local cloud regions. Fourth, there is scope for simulation studies that combine cyberattack scenarios, provider outage, identity failure and regulatory reporting timelines. Fifth, human factors deserve more attention because recovery delays often arise from unclear authority, communication breakdown or insufficient rehearsal rather than absent technology.

Future research could develop sector-specific maturity instruments, collect anonymised recovery exercise data, compare RTO/RPO attainment across architectures, and evaluate how contracts allocate responsibility in Saudi cloud procurement. Researchers could also examine how artificial intelligence operations tools support predictive recovery while preserving accountability. Such work would benefit practitioners by moving the field from broad recommendations to evidence-based design patterns suitable for Saudi organisational realities.

12. Managerial Implications

Managers should treat cloud disaster recovery as a strategic investment linked to service obligations, reputation and regulatory compliance. The first practical step is to identify crown-jewel datasets and map them to services, owners and tolerance levels. The second is to compare current recovery capability with regulatory expectations from NCA, CST and SDAIA. The third is to require suppliers to provide recovery evidence rather than generic availability promises. The fourth is to test restore processes quarterly for critical datasets and at least annually for full service failover. The fifth is to keep crisis communication templates, emergency contacts and decision thresholds available outside the affected environment.

Table 2: Control matrix for cloud-based recovery and business continuity

Control domain	Recommended practice for Saudi organisations	Evidence to retain
Data classification	Classify mission-critical datasets by RTO, RPO, sensitivity, residency and service dependency.	Approved BIA, data register, recovery tier map.
Cloud architecture	Use separated failure domains, protected backup vaults, tested replication and documented recovery sequence.	Architecture diagrams, restore logs, failover test reports.
Identity resilience	Protect privileged accounts, break-glass access, MFA recovery and key management from the production blast radius.	Access reviews, emergency account tests, key recovery records.
Supplier governance	Define RACI responsibilities, data location, incident notice, support access and exit arrangements in contracts.	Signed contracts, provider attestations, SLA evidence.
Privacy and localisation	Assess backup replicas, support logs and transfers under Saudi personal data and cloud regulations.	Transfer risk assessments, safeguards, retention decisions.
Continuous assurance	Run exercises, record lessons, update runbooks and report residual risk to executives.	Exercise minutes, action trackers, board risk reports.

For SMEs, the recommended starting point is modest but disciplined: enable managed backups, protect administrator accounts, use immutable retention where available, document restore steps, verify restores, and understand where data is stored. For large enterprises, the priority is integrated assurance across business continuity, security operations, cloud engineering, legal, procurement and executive risk committees. In both cases, the strongest continuity posture is one that produces evidence before an incident and calm coordination during an incident.

Implementation should follow a phased roadmap. Phase one is discovery: identify business services, data owners, data flows, legal constraints, existing backups, administrator roles and third-party dependencies. This phase should produce a recovery register rather than a generic asset list, because recoverability is attached to services and processes. Phase two is stabilisation: remove obvious weaknesses by enabling central logging, multifactor authentication, backup immutability, retention locks, documented restore procedures and emergency communication channels. Phase three is engineering: define the target pattern for each service, such as backup-and-restore, pilot light, warm standby or active-active operation, and implement it through repeatable infrastructure code. Phase four is assurance: conduct scenario exercises, measure

results, record gaps and report residual risk. Phase five is optimisation: add predictive monitoring, automated remediation and cost-aware placement once the basic capability is reliable.

Measurement should also be standardised. RTO and RPO are necessary but insufficient because they can be reported as aspirations rather than demonstrated outcomes. Saudi organisations should measure recovery success rate, restoration integrity, mean time to declare an incident, mean time to assemble the crisis team, percentage of critical dependencies covered by runbooks, percentage of backups restored during testing, privileged-access recovery time, and evidence availability during a simulated platform outage. These metrics translate technical recovery into managerial language. They also help procurement teams compare providers through evidence instead of marketing claims. For example, a provider may advertise high availability while the organisation still lacks rapid recovery because identity, domain name services, encryption keys or application secrets are not included in the tested scenario.

Scenario design is another practical requirement. Exercises should cover more than regional outage. Useful scenarios include ransomware with attempted backup deletion, accidental mass data corruption, loss of a privileged administrator, failure of a managed identity tenant, unavailability of a cloud control plane, failed replication caused by network misconfiguration, provider support delay, and a legal decision to stop cross-border data movement. Each scenario should define trigger conditions, decision owners, technical actions, business workarounds, communication steps and post-incident learning. Such exercises reveal hidden dependencies and encourage teams to reduce manual improvisation. They also create evidence for auditors because the organisation can show what was tested, what failed, what was fixed and what remains outside risk appetite.

Cost management should not be separated from resilience. Some workloads justify active-active deployment, but others may be better served by immutable backup and rapid rebuild. The correct decision depends on business impact, transaction rate, data sensitivity and the cost of downtime. A tiered portfolio prevents two common mistakes: under-protecting crown-jewel services and over-engineering low-value workloads. It also supports executive decision-making because leaders can see how spending changes expected recovery performance. In Saudi organisations, this tiering should be reviewed whenever regulations, cloud regions, supplier contracts or business processes change, since each change may alter the balance between cost, performance and compliance.

Finally, people remain decisive. Cloud tools can automate failover, but people approve crisis posture, communicate with stakeholders, interpret legal duties and manage exceptions. A continuity programme should name alternates for every critical role, maintain contact details outside the affected platform, and train teams to use recovery consoles under stress. Legal, procurement, cybersecurity, business operations and communications teams should be included in exercises, because recovery decisions are rarely purely technical. When these roles are rehearsed together, the organisation moves from a document-based plan to a practised capability.

A further consideration is interoperability with national and sector platforms. Many Saudi services depend on shared identity, payment, messaging, geospatial, logistics or regulatory gateways. Recovery planning should therefore include interface-level continuity, not only internal application recovery. If a critical external gateway is unavailable, the organisation needs preapproved manual workarounds, queueing mechanisms, customer notices and reconciliation procedures. Where automated retries are used, engineers should ensure that recovery traffic does not overwhelm downstream services after restoration. This point is especially relevant for high-volume public transactions and healthcare operations, where delayed data exchange can create safety, financial and reputation impacts. Continuity planning should also address evidence retention for these integrations, including API logs, message acknowledgements, reconciliation reports and exception approvals. These records help prove that data remained complete and accurate even when processing was delayed. They also support root-cause analysis and claims management when responsibility is shared across multiple providers. In short, mission-critical continuity is an ecosystem problem: each organisation controls only part of the service chain, but it remains accountable for understanding the chain before disruption occurs.

This discipline turns cloud recovery from emergency improvisation into accountable, auditable and operationally realistic continuity for services that citizens, patients, customers and regulators expect to remain dependable during severe disruption.

Accordingly, Saudi organisations should treat recovery design as continuous governance, not as a one-time migration milestone. The practical measure of success is the ability to restore verified data, operate priority services, communicate decisions, and demonstrate compliance evidence

under pressure. This position suits entities with different maturity levels because it starts with classification, ownership and testing before advancing toward automation, multi-region operations and predictive resilience. It also reduces the risk of overbuying technology without rehearsing people, processes and supplier obligations. In this sense, cloud continuity becomes a living organisational discipline that connects digital transformation to trust, accountability and national service reliability.

13. CONCLUSION

Cloud-based disaster recovery and business continuity are essential for Saudi organisations that depend on mission-critical data. The review demonstrates that cloud platforms provide powerful tools for replication, automation, elasticity and monitoring, yet resilience depends on governance, regulatory alignment and tested execution. Saudi organisations must design recovery around critical services, legal data obligations, shared cloud responsibilities and credible disruption scenarios. The proposed reference model offers a structured way to align the data plane, continuity orchestration plane and governance plane. Its central message is that recoverability must be engineered, contracted, rehearsed and evidenced. When these elements mature together, cloud recovery can support national digital transformation while protecting the trust, availability and integrity of essential Saudi services.

REFERENCES

- Alwakeel A.M. Adaptive edge-fog healthcare networks: a novel framework for emergency response management. Journal of Cloud Computing. 2025;14:48. https://doi.org/10.1186/s13677-025-00784-3.
- Sawalha I.H. Views on business continuity and disaster recovery. International Journal of Emergency Services. 2021;10(3):351-365. https://doi.org/10.1108/IJES-12-2020-0074.
- Stamenkov G. Cloud service models, business continuity and disaster recovery plans, and responsibilities. International Journal of Organizational Analysis. 2025;33(3):437-451. https://doi.org/10.1108/IJOA-12-2023-4127.
- Galaitsi S.E., Pinigina E., Keisler J.M., Pescaroli G., Keenan J.M., Linkov I. Business continuity management, operational resilience, and organizational resilience: commonalities, distinctions, and synthesis. International Journal of Disaster Risk Science. 2023;14:713-721. https://doi.org/10.1007/s13753-023-00494-x.
- Behbehani D., Komninos N., Al-Begain K., Rajarajan M. Cloud Enterprise Dynamic Risk Assessment (CEDRA): a dynamic risk assessment using dynamic Bayesian networks for cloud environment. Journal of Cloud Computing. 2023;12:79. https://doi.org/10.1186/s13677-023-00454-2.
- Goswami P., Faujdar N., Debnath S., Khan A.K., Singh G. Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability. Journal of Cloud Computing. 2024;13:45. https://doi.org/10.1186/s13677-024-00605-z.
- Songa A.V., Karri G.R. An integrated SDN framework for early detection of DDoS attacks in cloud computing. Journal of Cloud Computing. 2024;13:64. https://doi.org/10.1186/s13677-024-00625-9.
- Al-Said Ahmad A., Andras P. Scalability resilience framework using application-level fault injection for cloud-based software services. Journal of Cloud Computing. 2022;11:1. https://doi.org/10.1186/s13677-021-00277-z.
- Marin E., Perino D., Di Pietro R. Serverless computing: a security perspective. Journal of Cloud Computing. 2022;11:69. https://doi.org/10.1186/s13677-022-00347-w.
- Bouizem Y., Dib D., Parlavantzas N., et al. Integrating request replication into FaaS platforms: an experimental evaluation. Journal of Cloud Computing. 2023;12:94. https://doi.org/10.1186/s13677-023-00457-z.
- Khan K.M., Arshad J., Iqbal W., Abdullah S., Zaib H. Blockchain-enabled real-time SLA monitoring for cloud-hosted services. Cluster Computing. 2022;25:537-559. https://doi.org/10.1007/s10586-021-03416-y.
- Song C.H., Sohn Y.W. The influence of dependability in cloud computing adoption. The Journal of Supercomputing. 2022;78:12159-12201. https://doi.org/10.1007/s11227-022-04346-1.
- Ozen F., Souri A. Cloud-based disaster management architecture using hybrid machine learning approach in IoT. Multimedia Tools and Applications. 2024;83:72357-72370. https://doi.org/10.1007/s11042-024-18333-6.
- Alamri N., Alzahrani S. Navigating the clouds: an exploratory research of cloud computing adoption in Saudi Arabia's small and medium enterprises. Engineering, Technology and Applied Science Research. 2024;14(6):17859-17869. https://doi.org/10.48084/etasr.8435.
- National Cybersecurity Authority. Cloud Cybersecurity Controls (CCC-1:2020). Riyadh: NCA; 2020.
- National Cybersecurity Authority. Cloud Cybersecurity Controls (CCC-2:2024). Riyadh: NCA; 2024.

- National Cybersecurity Authority. Essential Cybersecurity Controls (ECC 2-2024). Riyadh: NCA; 2024.
- Communications, Space and Technology Commission. Cloud Computing Services Provisioning Regulations, Version 4. Riyadh: CST; 2023.
- Digital Government Authority. Cloud First Policy. Riyadh: DGA; 2023.
- Saudi Data and AI Authority. Regulation on Personal Data Transfer Outside the Kingdom. Riyadh: SDAIA; 2024.
- Saudi Data and AI Authority. Implementing Regulation of the Personal Data Protection Law. Riyadh: SDAIA; 2023.
- Cloud Security Alliance. Cloud Controls Matrix and CAIQ v4.0. Seattle: CSA; 2021.
- National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations: SP 800-53 Revision 5. Gaithersburg: NIST; 2020. https://doi.org/10.6028/NIST.SP.800-53r5.
- Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST; 2024. https://doi.org/10.6028/NIST.CSWP.29.
- International Organization for Standardization. ISO/IEC 27031:2025 Cybersecurity - Information and communication technology readiness for business continuity. Geneva: ISO; 2025.
- International Organization for Standardization. ISO 22361:2022 Security and resilience - Crisis management - Guidelines. Geneva: ISO; 2022.
- International Organization for Standardization. ISO 22301:2019/Amd 1:2024 Security and resilience - Business continuity management systems - Requirements - Amendment 1. Geneva: ISO; 2024.
- International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO; 2022.
- Waseem M., Ahmad A., Liang P., Akbar M.A., Khan A.A., Ahmad I., Setala M., Mikkonen T. Containerization in multi-cloud environment: roles, strategies, challenges, and solutions for effective implementation. Journal of Systems and Software. 2025;230:112558. https://doi.org/10.1016/j.jss.2025.112558.
- Reece M., Lander T.E. Jr., Mittal S., Rastogi N., Dykstra J., Sampson A. Emergent insecurity of multi-cloud environments. CoRR. 2023;abs/2311.01247. https://doi.org/10.48550/arXiv.2311.01247.