© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1718374

Oracle Database Migration, High Availability, And Disaster Recovery Strategies in Hybrid Cloud Environments for Saudi Enterprises

SYED IMTIYAZ

Abstract- ***Saudi enterprises are modernizing mission-critical Oracle estates under two pressures: faster digital delivery and stronger resilience under regulatory, operational, and cyber risk. Hybrid cloud is attractive because it allows sensitive databases to remain on premises or in controlled deployments while enabling cloud-based scale, automation, geographic separation, and managed recovery options. Yet migration projects often underperform because cutover planning, high availability design, and disaster recovery architecture are treated as separate workstreams. This paper presents a structured review of 2020-2025 literature, standards, and vendor documentation on Oracle database migration, high availability, and disaster recovery in hybrid cloud settings relevant to Saudi enterprises. A PRISMA-informed review protocol defined scope, screened sources, and synthesized evidence across migration methods, Oracle Maximum Availability Architecture patterns, Oracle RAC, Oracle Data Guard, Zero Downtime Migration, Oracle Database Azure, and Saudi governance controls. The review finds that successful programs follow an integrated continuity pipeline: classify workloads and residency obligations first, choose the target topology second, select a migration path with explicit rollback, engineer local availability at the primary site, and then map disaster recovery and cyber recovery controls to measured RPO and RTO targets. The paper contributes a Saudi-focused synthesis, two design figures, and two decision tables that translate recent evidence into implementation guidance suitable for a review article aligned to Springer or Elsevier conventions.***

Keywords: Oracle Database; hybrid cloud; migration; high availability; disaster recovery; Oracle RAC; Oracle Data Guard; Saudi enterprises.

I. INTRODUCTION

Oracle databases are still used for payment rails, government services, ERP systems' key modules, billing systems, and operational analytics in Saudi Arabia. Such applications will hardly be lifted and shifted since they need to ensure high availability, security, performance, residency, continuity, and compliance. At the same time, migration to hybrid cloud seems like a promising step. Enterprises will retain total control over their critical assets and enjoy benefits from cloud regions, distributed cloud, and multicloud to gain flexibility, automation, geographical redundancy, and alternative disaster recovery strategies [2-4,15,30]. For Saudi organizations, the issue is not whether or how to migrate but how to do it effectively and reliably. The problem gets even more significant with comprehensive continuity considerations.

The migration could look like the best decision from the technical standpoint, but it might be unacceptable from a business point of view due to absence of proper failover procedures, unknown recovery time, and low-level recovery capabilities related to cybersecurity. As defined in maximum availability architecture in Oracle, availability refers to an architectural practice including requirements analysis, fault domains management, validation, and testing [5-7]. However, as per regulations on cloud computing cybersecurity in Saudi Arabia, special attention should be paid to access control, logging, localization, resiliency, and accountability [22-25].

As a result, the processes of migration, local high availability, disaster recovery, and cybersecurity recovery should be addressed in an integral way of practices and policy. Recent Oracle multicloud architectures add new dimensions to the discussion. Oracle Cloud Infrastructure, Exadata Cloud@Customer, distributed cloud models, and Oracle Database@Azure all represent different ways of modernizing Oracle database estates while preserving Oracle database semantics, operations, and availability characteristics [2-4,15-21,30]. In this paper, Oracle Database@Azure is treated only as an

optional Oracle multicloud pattern for organizations already standardized on Microsoft application or analytics ecosystems. The primary focus remains Oracle database migration, local high availability, disaster recovery, cyber recovery, and Saudi governance alignment in OCI-centered and hybrid Oracle environments. Selecting Oracle database architecture implies deciding on potential scenarios of failures and operating model as well. This paper will discuss the continuity principles which should be taken into account in Oracle database migration in hybrid cloud architecture. Migration, local high availability, and disaster recovery will be viewed as connected decisions which should be made according to concrete recovery goals and national policy directives. In this connection, the following research questions will be studied within the literature review framework: Which Oracle database migration architectures could provide chances for controlled downtime and rollback capability? Which hybrid cloud architectures for high availability and disaster recovery could meet realistic recovery goals? How could the principles of governance and validation promote resilience of Saudi enterprises? It should be emphasized that while this paper complies with the standard research paper format (section numbering), it deviates from the empirical studies expected by the journal with regards to articles as indicated below.

1.1 Aim of the Study

The aim of the paper is to conduct a literature review of contemporary scholarly research on Oracle database migration, high availability, and disaster recovery to create recommendations for Oracle database architecture in Saudi organizations from the viewpoint of resilience via modernization.

1.2 Objectives of the Study

The objectives of the paper are to review the most advanced Oracle database architecture in hybrid cloud environment regarding both business and regulatory perspectives; analyze various Oracle database migration architectures in terms of downtime, rollback capability, operability, and functionality; consider Oracle RAC, Data Guard, Active Data Guard, and Far Sync in relation to local high availability and regional disaster recovery; examine cybersecurity and cloud regulations in Saudi Arabia in relation to Oracle database migration and disaster recovery; and elaborate recommendations for implementation of Oracle database architecture.

II. REVIEW METHODOLOGY

The current article represents a structured review. It was designed and conducted according to PRISMA 2020 reporting framework that offers an effective way to establish scope, selection logic, and synthesis boundaries [1]. The evidence base included peer-reviewed scholarly publications as well as primary vendor-specific sources such as Oracle, Microsoft, and Saudi governmental agencies. The source hierarchy was deliberate as the vendor guides typically deal with the issues specific to Oracle products like Data Guard redo transport, RAC features, and Zero Downtime Migration procedure.

Peer-reviewed literature, in its turn, provides useful insights concerning migration governance, legacy migration complexities, and fault-tolerance considerations [26-29]. Specifically, the current review used the search time window 2020-2025 for the reason of the client request as well as recent Oracle hybrid cloud developments. The keywords were numerous variations containing Oracle database migration, Oracle Cloud Infrastructure, hybrid cloud, high availability, disaster recovery, Oracle RAC, Oracle Data Guard, Active Data Guard, Zero Downtime Migration, Exadata Cloud@Customer, Oracle Database@Azure, Saudi cloud legislation, Essential Cybersecurity Controls, and Cloud Cybersecurity Controls. The articles of interest involved implementation guidance, clarification of trade-offs concerning migration or resiliency, or definition of relevant governance requirements [5-25]. As for the filtering process, it allowed discarding irrelevant material due to falling outside the search time window; lacking any relevant information despite having marketing nature; repetition; lack of specificity, and lack of consideration of either architectural or governance aspects. Given the practical implementation-oriented focus of the topic, meta-analysis was not considered as a research tool within this study. Instead, a thematic synthesis across five categories was done: deployment topology, migration technique, control of high availability, disaster recovery plan, and governance obligation.

Every piece of evidence was then evaluated based on decision value regarding fault domains, rollback possibilities, recovery objectives, and compliance considerations. As a result, the synthesized output was presented in two figures and two tables intended for architecture workshops. The latter utilizes two-stage empirical methodology relying on interviews, survey data, and structural equation modeling to identify migration key factors [26]. This method does not suit the present paper due to its type.

Nevertheless, it serves a good example of disciplinary and academic style, whereas the methodology was modified according to current findings.

III. STRATEGIC DRIVERS AND CONSTRAINTS IN SAUDI HYBRID CLOUD ADOPTION

“Hybrid cloud remains attractive for Oracle deployments owing to the following reasons. First, it presents a balance of two extremes: complete outsourcing and unregulated public cloud migration. The official Oracle cloud migration guidance mentions hybrid and distributed transformations as part of the coherent transition of people, processes, and technologies, but not of the hosting decisions [2].

It is particularly true of Saudi Arabia as their databases will most likely be linked to applications and reporting. In accordance with Oracle definitions, hybrid and distributed cloud migrations are preferred by companies due to their benefits of enhanced performance, greater control, and better location fit [3,4,30]. As for the peer-reviewed literature, it corroborates the fact stated above. Thus, Shirvani et al. state that finding the right migration strategy is often accompanied by complex considerations of technical readiness, costs, risks, uncertainties, and decision-making structures [26]. Althani emphasizes several issues in terms of legacy migration including resistance to change, reengineering, interdependencies, and skills mismatch among the team members [29]. All these facts complicate Oracle cloud migration in Saudi Arabia even more as it influences database, middleware, network, cybersecurity, procurement, and business continuity teams. However, if considering compliance with governance obligations, options become limited. First, in accordance with Saudi ECC 2-2024 and CCC 2:2024, the organizational role structure in terms of cybersecurity, assets, event logging, access control, and cloud security requirements must be independently verifiable during assessment and cannot only be documented [22,23]. Second, Saudi cloud law and its amendments determine cloud services and customer content, as well as impose restrictions on storing and transferring government-related data [24,25]. Therefore, there is a need to choose the architecture that enables tracing, segregation of duties, and generating evidence for recovery purposes. As regards Oracle cloud, the implications of the above discussion become clear.

First, hybrid cloud migration begins with workload assessment. Residency sensitivity, latency tolerance, connection tightness, rate of changes, and impact of downtime are the important criteria for Missing full stop: “database sorting. Organizations that are extremely sensitive to residency or depend significantly on Oracle applications, Oracle E-Business Suite, or tightly coupled Oracle databases should prioritize OCI-centered deployment, Exadata Cloud@Customer, or Oracle distributed cloud models rather than treating public cloud relocation as the default path [4,21,30]. Oracle Database@Azure may be considered only where enterprise applications, identity services, or analytics are already standardized on Azure and low-latency Oracle database integration is required [15-20].

IV. ORACLE MIGRATION STRATEGIES FOR HYBRID CLOUD ENVIRONMENTS

The migration strategy is a key factor when it comes to migration in hybrid cloud environments, as it determines the time needed to execute cutover, the possibility of rolling back the operation safely, the way in which the data will be synchronized, and the operational evidence available. Under the current Oracle migration guidance, migration strategies are grouped into physical, logical, and restoration options [12-14].

Furthermore, the Oracle ZDM migration tool offers several migration paths in the form of a coherent strategy [12-14]. Physical migration using Oracle Data Guard is the most robust option for migrating

valuable Oracle systems, as the migration process features constant synchronization with the backup environment due to the use of Data Guard. The approach implies the continuous synchronization with the fall-back environment and shipping of the redo. That is why ZDM migration gives an opportunity to validate the target environment using a realistic load before promoting it in a brief cutover period [12-14].

It must be noted that the strengths of this approach do not stop at the low amount of downtime, as they also include disciplined proof of pre-checks, continuous replication health visibility, compliance with encryption regulations, and post-cut-over cleanup. Considering that internal audits are quite common in Saudi Arabia, the audit trail provided by physical migration could be just as important as the downtime.

From a logical standpoint, the physical migration method is appropriate in cases where there are no transformation needs and conflicting requirements regarding the replication of data. Otherwise, various logical migration techniques can be applied. Their weakness consists in the high level of complexity involved in detecting conflicts, implementing supplemental logging, applying validation rules, and making the resynchronization of the replicated database possible when multiple write paths exist or when the database schema is being updated [13,15].

For this reason, logical migration must be chosen only when its advantages are essential. Finally, migration based on backup and restore is also a good solution for projects that accept some amount of downtime and require no complex transformation operations. These migration strategies tend to be easy to understand but carry a risk at the implementation stage due to unknown speed of backing up and restoring, storage capabilities, and validation processes. The general idea in Oracle migration guidance is that these strategies could be improved using incremental catch-ups, seeding the target system before migration, and full test restores [12-14]. Nonetheless, they do not compete with synchronous standby strategies' ability to perform rollbacks in mission-critical workload migrations. In conclusion, it must be emphasized that the strategy of migration should be developed alongside continuity analysis. There are four questions that have to be answered one by one: What amount of downtime can be tolerated? What rollback functionality is required? What level of data loss tolerance should be achieved? Finally, what capacity and expertise could be dedicated to migration validation? Then, the selected strategy must be able to answer these questions.

Physical ZDM migration would be the best option in situations where some downtime within the range of a few minutes is acceptable. Otherwise, the strategy must be chosen based on the transformation needs, with logical migration or physical migration preferred accordingly.

The restore migration is implemented in less critical tiers. Non-database factors also play an important role in migration readiness in the sense that network throughput, name resolution, integration with organizational directories, encryption key management, performance monitoring, and application behavior could become critical. In accordance with the Oracle migration advice, cloud adoption readiness is dependent on the maturity of the organization's processes [2]. This is the main reason behind the frequent failure of even well-designed migration processes. While database migrations are often executed successfully, there might be some unexpected issues that affect the result.

Figure 1. Hybrid-cloud reference architecture for Oracle migration, availability, and disaster recovery in Saudi enterprises.

Table 1. Oracle migration options for hybrid cloud.

Migration	Primary mechani	Typical	Strengths	Key watch

path	sm	downtime		points
ZDM physical migration	Standby build plus redo apply and controlled switchover	Minutes to low hours	Strong rollback, high fidelity, repeatable automation	Version compatibility, network quality, encryption prerequisites
Logical replication migration	Change capture and apply to transformed target	Minutes	Supports transformation and selective cutover	Conflict handling, logging overhead, reconciliation effort
Backup and restore migration	RMAN or service-based restore to cloud target	Hours to days	Simple pattern and clear source preservation	Longer cutover, restore validation, throughput bottlenecks
Data Pump or object-level migration	Schema export-import with object remapping	Hours to days	Useful for restructuring and selective objects	Not suitable for strict continuity targets
Phased mixed migration	Combination of physical, logical, and restore methods by tier	Variable	Matches diverse estate realities	Governance complexity and inconsistent runbooks

V. HIGH AVAILABILITY ARCHITECTURE AT THE PRIMARY SITE

Migration alone does not provide robustness. After a workload is migrated to the hybrid target, the primary site must endure hardware failures, node crashes, software-related issues, and planned outages without causing any noticeable business interruptions. Oracle recommendations on building high availability consider this level of protection a first line of defense against downtime. Oracle RAC is a technology that helps deal with this issue through clustering and node tolerance [7,8]. Oracle RAC allows services to survive instance failures through load distribution among clustered nodes. The major benefit of Oracle RAC is achieved when the enterprise becomes capable of handling its complex operation process. However, one should not see Oracle RAC as an answer to all questions about high availability.

Although it provides a lot of protection against unexpected and planned local events, it does not solve the problem of disaster recovery. This notion is highlighted in Oracle MAA guides – although local high availability decreases the probability of local interruption, Oracle Data Guard and other similar technologies help resist those events that lie beyond the local fault domain [5-7,10,11]. Therefore, the most powerful architecture for Tier 1 Saudi workloads should include both Oracle RAC for fault tolerance locally and a dedicated server for disaster recovery. Primary site availability should also address maintenance engineering issues. Oracle high availability guidelines note that gray failures, partial failures, or poor maintenance practices tend to cause the most disturbing outages [7]. Therefore, rolling patching, moving services, managing connections, tracking performance issues, etc., should be as important as having redundant hardware. The issue receives extra importance in the context of migration to hybrid clouds when operations become more complicated. Cloud-managed services may relieve the organization from a lot of tasks, but they cannot remove the necessity of testing applications' behavior under circumstances of partial or full disconnects and role changes. Exadata Cloud Customer seems to be the best solution to gain all benefits of the cloud environment under strict corporate governance.

Oracle documentation states that Exadata Cloud Customer makes it possible to enjoy Oracle RAC and Active Data Guard availability guarantees without transferring hardware infrastructure to the cloud service provider's territory [21]. The solution can be used in Saudi enterprises to support data-sensitive and low-latency workloads, which require managed and automated cloud-based operations. Moreover, Exadata Cloud Customer is suitable as the intermediary phase in hybrid transformation to gain operational benefits before deploying disaster recovery on public cloud servers. The key recommendation to make is that the issue of primary site availability should be analyzed from the perspective of services. One should learn how sessions failover, how services start, how patches are applied, what signs indicate abnormal workload or performance lag, how end-user performance is estimated, and others. Otherwise, availability will be nothing more than topology.

VI. DISASTER RECOVERY AND CYBER RECOVERY IN HYBRID AND MULTICLOUD ENVIRONMENTS

Disaster recovery takes place when an outage lies beyond the territory of the primary site. Oracle Data Guard is the base technology here because it creates and maintains one or several replica databases to serve as a backup in the case of catastrophic damage of or corruption within the main server [9-11]. The decision to make is whether to use asynchronous or synchronous transport of redo logs.

The former option is better suited for regional and nationwide recovery, but it sets the bounds for the value of RPO that needs to be accepted knowingly. However, synchronous transport provides better performance because it guarantees zero data loss and faster failover if possible [18,19].

As stated in Oracle availability guidelines, disaster recovery should involve several fault domains instead of building a single remote replica. Redo logs can be delivered to the nearest standby database for immediate failover and later be transported to regional standby for further redundancy [10,11,18,19].

Such approach proves itself effective in designing Saudi enterprise architecture because it divides the goals of fast recovery and large-scale redundancy into two separate steps. In the case when fast restoration is the goal, close-region standby is needed. A distant standby is required to protect the enterprise from wider disasters. Figure 2 and Table 2 reflect this logic.

An additional disaster recovery pattern, relevant mainly in multicloud environments, is Oracle Database@Azure. This pattern is discussed in recent Oracle and Microsoft documentation as a reference option for organizations that already operate important application or analytics workloads in Azure [15-20]. It should not be interpreted as the primary implementation path for all Saudi enterprises. For Oracle-centered estates, OCI, Exadata Cloud@Customer, Oracle Data Guard, Active Data Guard, and distributed cloud models remain the more natural starting points for continuity design. Where Oracle Database@Azure is selected, network connectivity, DNS configuration, identity management, zone and region redundancy, governance ownership, and failover orchestration must be planned in advance [17].

Far Sync and fast-start technologies provide another way to enhance disaster recovery process by reducing the penalties for synchronous commitment. They also guarantee that database is safe from faults inside the zone or region [20].

Oracle Database@Azure architecture documentation states that such options allow overcoming the disadvantages associated with commit lag by applying Far Sync combined with zone/region-specific standbys. These options may not be required for every database but should be included in case of very valuable transactional activities that require high resilience and fast failover. An example of such applications could be financial clearing services, governmental applications, and telecommunication charging systems.

One should remember that cyber recovery must be taken into consideration in addition to classic disaster recovery. Modern attacks are likely to target not only primary database and applications but also backup

© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1718374

servers, credential storages, and failover pathways. Consequently, the design goal moves from providing availability to restoring even under hostile conditions.

Oracle BCDR and resilience guides state that the enterprise needs detailed disaster recovery plans, secure and isolated backup repositories, and regular failover testing [17,18]. From the point of view of Saudi enterprise, it implies use of immutable or logically-protected backups, restricted access to credential storages, and additional security measures for restoration. Standby database is responsible for protecting the company from downtimes and some types of data corruption, but it cannot solve the problem of cyber recovery. Therefore, the architecture of cyber recovery should be built on top of replication with backups and failover testing. The message to managers is quite clear – disaster recovery should be initially defined through values of RPO and RTO, after which technical requirements can be set. In cases when managers ask to provide the best possible DR without setting measurable targets, the resulting architecture is likely to be too expensive and inconsistent. Conversely, when a particular service has been estimated as having RTO less than 30 minutes and RPO less than 1 minute, it narrows down the options of architectural decisions to a few advanced solutions including local/distant standby, broker automation, and regular failover testing.

Figure 2. RPO-RTO decision map for Oracle continuity patterns in hybrid cloud.

Table 2. Availability and disaster recovery patterns mapped to recovery objectives.

Pattern	Typical target	Indicative RPO	Indicative RTO	Best-fit use case
Single-site RAC	Local node and instance failures	Zero within site	Seconds to minutes	Tier 1 workloads needing local continuity but not site DR
RAC plus local standby	Site-local HA plus zone-level recovery	Near zero to seconds	Minutes	Critical services needing rapid failover inside one metro or cloud region
Primary plus remote physical standby	Regional or datacenter disaster recovery	Seconds to minutes	Minutes to under one hour	Regulated production systems with moderate distance
Local standby plus regional standby	Layered zone and region protection	Seconds locally; minutes remotely	Fast local failover; broader regional recovery	Large enterprises balancing speed and resilience
Far Sync plus remote standby	Low-data-loss remote resilience	Near zero	Minutes	High-value transaction systems where commit protection matters
Standby plus immutable backup tier	Cyber recovery and rollback confidence	Depends on backup cadence	Hours to planned restore window	Ransomware-conscious systems requiring clean recovery evidence

VII. ALIGNMENT OF ORACLE RECOVERY GOVERNANCE IN SAUDI ARABIA

Oracle resiliency frameworks need to be clear about governance considerations as well. The ECC 2-2024 and CCC 2:2024 explicitly point out the necessity to tie together cybersecurity accountability and architectural decisions. Privileged access management, logging, change management, third-party risk management, encryption practices, and incident response all affect migration and recovery architectures directly [22,23]. For example, it is essential that such critical components as key material, standby administration credentials, backup accounts, and failover authorizations be segregated in the way that no operator or vendor is able to exercise de facto control over the whole recovery process.

It also becomes relevant to consider the categorization of cloud services, treatment of customer content, and limitations related to government-generated data and cross-border data transfers imposed by the Saudi regulatory regime governing the use of the cloud [24,25]. While in most cases a non-government enterprise will not face these challenges, nevertheless, the procurement process, residency evaluation, and architecture certification will reflect these requirements in the terminology used. Hybrid cloud architectures without clearly marked borders in terms of data location, applicability of each vendor's SLA, and regions for failover purposes cannot be considered mature. Such practical mapping of control points can be made through the migration and continuity lifecycle.

Before the migration process starts, enterprises must validate data classification, target destination for migration, cryptography setup, and roles necessary for successful cutover. During migration activities, it is essential to monitor logging of privileged operations, to ensure that tested and documented rollback strategies exist, and to protect standby and/or backup mechanisms. Once in the steady state, one must validate replication lag, perform backup testing, validate compliance with patch scheduling, and monitor administrative actions. During testing, it is necessary to collect relevant data about failovers and restoration procedures in accordance with the needs of internal audit and cybersecurity governance committees. Document-based approach works well for both compliance and technical excellence.

VIII. DISCUSSION AND IMPLICATIONS FOR PRACTICE

Based on the literature analysis, one may say that there is at least one major conclusion which can be derived here: architecture quality plays a much more important role than choice of cloud service when it comes to success of Oracle modernization efforts. Organizations that succeed are those which follow the proper sequence of making decisions: workloads must be classified first, targets must be quantified, topology choices must be considered, and finally, migration strategies decided. On the contrary, those organizations which fail often reverse this logic:

starting with platform or tool selection and building the resilient architecture after. This is yet another reason why hybrid cloud architecture remains strategic in today's Oracle environment. Given the existence of Exadata Cloud Customer, Oracle Database Azure, and other solutions provided by the distributed cloud model, there is no more black-and-white decision between cloud or on-premises infrastructure anymore [3,4,15,21,30].

Now one may select many different ways of allocating computation resources, storage spaces, and recovery capabilities across several control domains. This is good, but without standards for migration runbook creation, nomenclature, monitoring, and testing procedures, there will be chaos. A Saudi enterprise will deploy numerous topologies, but still, it will do it according to established rules. Here we have three main recommendations for practitioners. First, migration governance boards must demand rollback planning for all activities associated with database migration. Second, it is imperative that continuity targets must be defined only by test results and not claims made by vendors in their brochures. Finally, it is necessary to allocate budget for cyber recovery since mere backup and standby will not help restore the Oracle estate in the case of a cyberattack.

All three are absolutely critical from the standpoint of business continuity, governance, and potential outage impacts. Scholars' task is to develop benchmarking

procedures for Oracle architectures. At present, there is hardly any public dataset that allows comparison of actual RPOs, RTOs, failover variation rates, and recovery certainty for hybrid Oracle cloud estates. This topic deserves particular attention as far as further research goes: if possible, one must compare Exadata Cloud Customer, OCI-region architecture, and Oracle Database Azure under comparable fault and governance conditions.

CONCLUSION

The reliability of Oracle database in hybrid clouds should be planned in terms of overall architectural approach to its consistent operations, not through separate infrastructure planning steps. New research results show that the best results can be obtained by combining workload classification, unique aspects of Saudi governance, migration, availability in Saudi Arabia, disaster recovery in Saudi Arabia, and recovery of cybersecurity in one architectural solution [5-25]. Physical ZDM migration with rollback-ready synchronization emerges as an optimal approach for mission-critical databases, and the RAC, Data Guard, Active Data Guard, and Far Sync form the base of layered continuity solutions.

Oracle Database@Azure and Exadata Cloud@Customer introduce new possibilities, but make architecture an obligatory component of the process under challenging conditions.

REFERENCES

[1] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021;372:n71.

[2] Oracle. Oracle Cloud Infrastructure Cloud Adoption Framework. Oracle Documentation. 2024.

[3] Oracle. What Is Hybrid Cloud? Use Cases, Pros and Cons. Oracle. 2024.

[4] Oracle. Distributed Cloud Services. Oracle. 2024.

[5] Oracle. Oracle Maximum Availability Architecture (MAA). Oracle. 2025.

[6] Oracle. MAA Best Practices for the Oracle Cloud. Oracle. 2025.

[7] Oracle. High Availability Overview and Best Practices for Oracle Database 23. Oracle Documentation. 2024.

[8] Oracle. Oracle Real Application Clusters Administration and Deployment Guide, 21c. Oracle Documentation. 2022.

[9] Oracle. Active Data Guard. Oracle. 2024.

[10] Oracle. Oracle Data Guard Concepts and Administration, 23ai. Oracle Documentation. 2024.

[11] Oracle. Configure and Deploy Oracle Data Guard. Oracle Documentation. 2024.

[12] Oracle. Zero Downtime Migration. Oracle. 2024.

[13] Oracle. Zero Downtime Migration 21.5. Oracle Documentation. 2024.

[14] Oracle. Zero Downtime Migration 21.5 Release Notes. Oracle Documentation. 2024.

[15] Oracle. Oracle Database Service for Azure. Oracle. 2024.

[16] Oracle. Oracle Database@Azure is Gold Maximum Availability Architecture Endorsed. Oracle. 2024.

[17] Microsoft. Business Continuity and Disaster Recovery for Oracle Database@Azure. Microsoft Learn. 2025.

[18] Oracle. Implement Disaster Recovery with Local and Regional Standbys on Oracle Database@Azure. Oracle Architecture Center. 2025.

[19] Oracle. Implement Disaster Recovery with Multi-Region Standby on Oracle Database@Azure. Oracle Architecture Center. 2025.

[20] Oracle. Learn About Deploying Active Data Guard Far Sync on Oracle Database@Azure. Oracle Architecture Center. 2025.

[21] Oracle. Exadata Cloud@Customer. Oracle. 2024.

[22] National Cybersecurity Authority. Essential Cybersecurity Controls (ECC 2-2024). Saudi Arabia. 2025.

[23] National Cybersecurity Authority. Cloud Cybersecurity Controls (CCC 2:2024). Saudi Arabia. 2025.

[24] Communications, Space and Technology Commission. Approval on the Update of the Cloud Computing Service Regulatory Framework, Version 3. Saudi Arabia. 2023.

[25] DLA Piper. Saudi Arabia Releases Version 3 of Its Cloud Computing Regulatory Framework. 2021.

[26] Hosseini Shirvani M, Amin GR, Babaeikiadehi S. A decision framework for cloud migration: a hybrid approach. IET Software. 2022;16(6):603-629.

[27] Campelo RA, Casanova MA, Guedes DO, Laender AHF. A brief survey on replica consistency in cloud environments. Journal of Internet Services and Applications. 2020; 11:1.

[28] Rehman AU, Aguiar RL, Barraca JP. Fault-tolerance in the scope of cloud computing. IEEE Access. 2022; 10:63422-63441.

[29] Althani B. Migration challenges of legacy software to the cloud: a socio-technical perspective. Cogent Business & Management. 2025;12(1):2503421.

[30] Oracle. Hybrid Cloud Services. Oracle. 2024.