ORACLE

Achieving Zero Data Loss in Indian Banking

With Oracle Maximum Availability Architecture (MAA)

July 2026, Version 1.0

Public

ORACLE

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

All Oracle product capabilities described herein are based on Oracle Maximum Availability Architecture (MAA) documentation (Oracle AI Database 26ai High Availability Overview and Best Practices) and may be subject to change. Statistical data are sourced from publications of the Reserve Bank of India and the National Payments Corporation of India.

ORACLE

Table of contents

1. Executive Summary 4
2. Data Loss Risk in Indian Banking 4
2.1 The Scale of the Challenge 4
2.2 Regulatory Framework 4
2.3 Types of Failures in Mission-Critical Banking Databases 4
2.4 How Oracle MAA Addresses These Types of Failures 5
3. Oracle MAA Reference Architecture Tiers 6
3.1 Banking Tiers Mapped to MAA Architecture 6
3.2 What Zero Data Loss Means Technically 6
3.3 Recommended Target Architecture 6
4. Oracle Data Guard — The Zero Data Loss Engine 7
4.1 Why Transport Mode Matters 7
4.2 Why Protection Modes Matter 8
4.3 Why Automatic Failover Matters 8
5. Zero Data Loss Architecture Patterns 9
5.1 RTT Zones and Transport Modes 9
5.2 Zone A/Zone B — Platinum MAA Target: Remote Standby 10
5.3 Zone C — Platinum MAA Target: Multiple Standby Databases (Pattern 1) 11
5.4 Zone C — Platinum MAA Target: Active Data Guard Far Sync (Pattern 2) 12
5.5 Choosing Between Pattern 1 and Pattern 2 13
6. Network Architecture for Redo Transport 13
7. Zero Data Loss Configuration Checklist 14
8. Phased Implementation Roadmap 15
9. Conclusion 15
References 16

ORACLE

1. Executive Summary

Every payment confirmed, every settlement recorded, and every account balance updated depends on a resilient database platform that preserves committed transactions through server, storage, network, and site-wide failures. In India's digital banking economy, the Unified Payments Interface (UPI) processed 185.8 billion transactions in FY 2024–25, while Real-Time Gross Settlement (RTGS) accounted for 69% of national payment value in CY 2024. There is no acceptable threshold for losing a committed transaction.

Oracle Maximum Availability Architecture (MAA) is Oracle's prescriptive framework for achieving the highest levels of availability, data protection, and disaster recovery for mission-critical Oracle AI Database deployments. This technical brief applies MAA principles to the Indian banking sector, where the scale and velocity of digital payments make zero data loss a baseline architectural requirement, not an aspiration.

For Indian banks, the Reserve Bank of India's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI/2023-24/107) requires at least half-yearly disaster recovery drills for critical information systems, establishes Board-level IT oversight, and asks regulated entities to prioritize minimal Recovery Time Objective (RTO) and near-zero Recovery Point Objective (RPO). The Oracle AI Database deployments underpinning core banking systems, payment switches, settlement engines, and fraud-detection platforms must therefore be architected to protect every committed transaction across the failure scenarios addressed by the architecture.

For Tier-0 and Tier-1 banking workloads, this paper positions Gold MAA as the minimum data-protection foundation. For banks running or upgrading to Oracle AI Database 26ai on Oracle Exadata, a fully implemented Platinum MAA architecture using Oracle Real Application Clusters (RAC) and Oracle Active Data Guard is the recommended target for more stringent recovery objectives. For qualifying workloads requiring extreme availability, Diamond MAA provides two options: Oracle GoldenGate 26ai active-active replicas, each running Oracle AI Database 26ai with Oracle RAC on Exadata and Active Data Guard; or Oracle Globally Distributed AI Database 26ai with native Raft replication.

All guidance in this paper is aligned with Oracle AI Database 26ai High Availability Overview and Best Practices and the applicable RBI regulatory framework.

2. Data Loss Risk in Indian Banking

2.1 The Scale of the Challenge

India's digital payments infrastructure operates at extraordinary scale. In CY 2024, payment systems collectively processed over 20,849 crore transactions worth ₹2,830 lakh crore. RTGS alone carried ₹1,938 lakh crore, representing 69% of total value. UPI reached a record 20.01 billion transactions in August 2025.

These mission-critical databases operate at national scale. A lost commit in a settlement engine creates an unreconcilable gap; a lost commit during an RTGS cut-off window delays high-value interbank settlements; and a lost commit in fraud detection means an alert that never fires.

2.2 Regulatory Framework

Three RBI instruments establish resilience, recovery, security, and data-location requirements relevant to Indian banks:

Instrument	Key Data Protection Requirement
RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023 (RBI/2023-24/107	Regulated entities should prioritize minimal RTO and near-zero RPO for critical information systems. Disaster recovery drills for critical information systems must be conducted at least half-yearly. Relevant IT, business-continuity, information-security, and cyber-recovery policies require Board approval and Board-level IT Strategy Committee oversight.
Storage of Payment System Data circular (RBI/2017-18/153; DPSS.CO.OD. No.2785/06.08.005/2017-18)	The entire data relating to payment systems must be stored in systems located only in India.
Cyber Security Framework in Banks, 2016(DBR.No.BP.BC.92/21.04.048/ 2015-16)	Banks must establish a dedicated cybersecurity policy and controls covering continuous monitoring, system activity logging, audit trails, incident detection, response, recovery, and cyber-crisis management.

The Digital Personal Data Protection Act (DPDPA) 2023 establishes additional obligations relating to personal-data security and breach notification, subject to the applicable commencement provisions. Together, these requirements reinforce the need for resilient architectures that can meet each bank's approved RPO, RTO, security, and recovery objectives.

2.3 Types of Failures in Mission-Critical Banking Databases

Mission-critical banking databases face six recurring data-protection and recovery risks. If not addressed, these risks can cause data loss, corruption, extended recovery, or failure to meet recovery objectives. They can surface during production incidents and disaster recovery exercises:

- Silent replication gaps: Operations performed with NOLOGGING can omit sufficient redo to reproduce affected data blocks on a standby database. The exposure may remain unnoticed until validation, recovery, or role transition.
- Storage-level silent corruption: A storage subsystem can return stale or incorrect data without raising an immediate error. Without database-aware detection, validation, and independent recovery copies, corruption can remain undetected until the affected data are read or recovery is attempted.
- Distance-driven replication trade-offs: Synchronous redo transport can provide zero-data-loss protection while a qualified standby remains synchronized, but it adds network and standby I/O latency to the commit path. Geographic distance is therefore an important design and testing consideration.
- Backup and recovery exposure: Recoverability beyond the latest backup depends on the availability and integrity of redo, the configured retention period, and the recovery architecture. Archived redo and real-time redo protection can reduce this exposure.
- Human error propagation: A mistaken bulk delete, table truncation, or schema change can be applied to physical standby databases as part of normal redo apply. Flashback, restore points, backups, and, where appropriate, delayed apply provide recovery options within their configured retention and operational limits.
- Untested recovery posture: A disaster recovery architecture that has not been exercised under representative conditions has unverified recovery capability. RBI directions therefore require periodic DR drills for critical information systems.

2.4 How Oracle MAA Addresses These Types of Failures

Oracle MAA provides a prescriptive, field-validated framework that maps directly to each of these failure categories. Rather than requiring banks to architect data protection from first principles, Oracle MAA delivers proven design patterns built for the world's most demanding Oracle AI Database deployments.

Type of Failure	How Oracle MAA Addresses It
Silent replication gaps	FORCE LOGGING and appropriate logging controls reduce exposure to NOLOGGING operations. Data Guard validation and monitoring help identify unrecoverable or unsynchronized data before a role transition.
Storage-level silent corruption	Oracle Active Data Guard detects supported physical block corruption and can automatically repair a corrupt block using a valid copy from the standby. Exadata background disk scrubbing and RMAN validation provide additional proactive coverage.
Distance-driven replication trade-offs	SYNC, FASTSYNC, nearby standby, and Far Sync patterns allow banks to balance transaction durability, commit latency, and geographic protection. Representative workload and failure testing remains required.
Backup window exposure	Standby protection, archived redo, and, where deployed, Zero Data Loss Recovery Appliance real-time redo protection reduce exposure beyond the latest backup. Recoverability depends on the retained and validated recovery data.
Human error propagation	Flashback Database, restore points, backups, and optional delayed apply support point-in-time recovery within configured retention, redo availability, and recovery limits.
Untested recovery posture	Planned switchovers and recovery exercises enable banks to validate procedures, application behavior, and recovery objectives while meeting RBI DR-drill requirements.

3. Oracle MAA Reference Architecture Tiers

Designing for zero data loss requires coordinated decisions across three layers: the application layer, which should be configured and tested to maintain service continuity; the infrastructure layer, which must provide sufficient bandwidth, latency, and storage performance; and the database layer, where the Oracle MAA protection architecture is implemented. No single layer is sufficient on its own.

The Oracle MAA tiers provide validated patterns for unplanned outages, including corruption, component failure, and site outages, as well as planned maintenance and migrations. These patterns are documented in Oracle AI Database 26ai High Availability Overview and Best Practices [1]. In Oracle Cloud, many MAA configuration and lifecycle practices are built into the managed platform services.

3.1 Banking Tiers Mapped to MAA Architecture

The table below illustrates how MAA tiers can map to representative banking workload classifications. Individual banks should confirm the mapping through business-impact analysis, approved RPO and RTO, and application-specific risk assessment.

Banking Tier	Representative Systems	Target Data-Loss Tolerance	Recommended MAA Tier	Indicative Gold Baseline RTO (Local/DR)
Tier-0	CBS, RTGS, NEFT, UPI switch, settlement engines	Zero	Gold minimum; Platinum recommended target for Oracle AI Database 26ai on Oracle Exadata deployments that satisfy all Platinum requirements; Diamond for qualifying workloads requiring extreme availability	Under 60 seconds / Under 5 minutes

Banking Tier	Representative Systems	Target Data-Loss Tolerance	Recommended MAA Tier	Indicative Gold Baseline RTO (Local/DR)
Tier-1	Internet and mobile banking, ATM switch, fraud and AML systems, card management	Zero to near-zero	Gold minimum; Platinum recommended target for Oracle AI Database 26ai on Oracle Exadata deployments that satisfy all Platinum requirements	Under 60 seconds / Under 5 minutes
Tier-2	Branch back-office, CRM, loan origination, regulatory reporting	Minutes (recoverable)	Silver	Seconds to minutes / Hours
Tier-3	Dev/test, archival, data warehouse, training	Hours (acceptable)	Bronze	Minutes to hours / Days

Note: The Tier-0 and Tier-1 RTO values shown in the table reflect the Gold MAA service-level baseline. A fully implemented Oracle AI Database 26ai Platinum architecture targets more stringent local and regional recovery times.

3.2 What Zero Data Loss Means Technically

Within a defined failure scope, zero data loss means that committed transactions remain recoverable after a protected failure while the architecture is operating in its required synchronized state.

For Oracle AI Database, this outcome is achieved by synchronously protecting the redo required to recover committed transactions on a qualified standby before acknowledging the commit. When the configured protection conditions are met, Oracle Data Guard synchronous redo transport can provide an RPO of zero for the protected failure scope. This capability supports the RBI objective of minimal RTO and near-zero RPO for critical information systems.

The outcome also depends on infrastructure and operating state. Protection mode, redo transport, and Fast-Start Failover (FSFO) establish the intended behaviour, while network round-trip time (RTT), available bandwidth, and standby write performance influence commit latency and synchronization. Congestion or an unavailable standby can degrade performance or cause the configuration to leave its synchronized protection state, depending on the selected protection mode.

3.3 Recommended Target Architecture

For the banking workloads considered in this paper, Gold MAA is the minimum architecture recommended for Tier-0 and Tier-1 systems requiring zero or near-zero data loss. Gold combines Oracle Real Application Clusters for compute-layer resilience with Oracle Active Data Guard for database and site protection. Synchronous redo transport may be implemented directly or through a suitable near-DR intermediary, based on topology, performance testing, and the required failure scope.

For banks running or upgrading to Oracle AI Database 26ai on Oracle Exadata, a fully implemented Platinum MAA architecture using Oracle RAC and Oracle Active Data Guard is the recommended target. It builds on the Gold data-protection foundation with Oracle Exadata, Fast-Start Failover, appropriately placed standby databases, backups, and the prescribed MAA application and operational practices.

The deployed architecture—not the database release or platform alone—determines the MAA tier. A configuration on a non-Exadata platform, or one that does not satisfy all prescribed Platinum requirements, remains Gold MAA. For Oracle Database 19c, Platinum MAA requires Oracle Exadata and Oracle GoldenGate in addition to the underlying MAA data-protection foundation.

For the most demanding Tier-0 workloads, Diamond MAA provides two extreme-availability approaches: Oracle AI Database 26ai on Oracle Exadata with Oracle GoldenGate 26ai active-active replication and an MAA-hardened GoldenGate Hub; or Oracle Globally Distributed AI Database 26ai with native Raft replication [17]. The appropriate

option depends on application architecture, data distribution, consistency requirements, and failure-isolation requirements.

4. Oracle Data Guard — The Zero Data Loss Engine

Oracle Data Guard is the core data-protection technology for the Gold and Active Data Guard-based Platinum patterns described in this paper. It maintains physical standby databases by transmitting redo for logged database changes from the primary database to one or more standby databases.

The central design question is how to protect the redo required to recover a committed transaction on a standby before the application receives commit confirmation. The answer depends on redo transport, protection mode, standby state, and the behavior selected when transport is interrupted.

4.1 Why Transport Mode Matters

Banking workloads differ in latency sensitivity, business impact, and approved data-loss tolerance. High-value settlement workloads may prioritize the strongest durability even when it adds commit latency. Customer-facing workloads may require a different, risk-approved balance between latency and protection. Reporting or downstream systems may permit a bounded recovery window.

Oracle Data Guard provides three transport modes, each representing a deliberate trade-off between protection strength and the latency added to database commits:

Transport Mode	How It Works	Zero Data Loss?	Latency Impact	Recommended For
Synchronous (SYNC AFFIRM)	Waits for standby to write redo to disk	Yes, while a qualified standby is synchronized	Highest	Tier-0: CBS, RTGS, settlement engines
Fast Synchronous (FASTSYNC)	Waits for standby memory receipt only	Yes for primary-only failure; residual risk for certain concurrent failures	Lower	Tier-1: Internet/mobile banking, ATM, fraud and AML
Asynchronous (ASYNC)	Primary does not wait; redo shipped in background	No guarantee	Minimal	Systems where some data loss is acceptable

Note: Oracle MAA performance data in [15] provides representative examples of synchronous transport impact. Actual impact varies with workload characteristics, application concurrency, network RTT, and standby I/O performance. Every deployment should validate peak workloads before selecting a transport mode.

4.2 Why Protection Modes Matter

Transport mode determines how redo is sent. Protection mode determines what happens to the primary database if the standby becomes temporarily unavailable — for example, during a network interruption or a planned maintenance window. Oracle Data Guard provides three protection modes:

Protection Mode	Transport	Zero Data Loss Guarantee	Recommended For
Maximum Protection	Synchronous	Zero data loss; the primary stops if it cannot maintain the required synchronized protection	Settlement engines where absolute zero data loss outweighs availability risk
Maximum Availability	Synchronous or Fast Synchronous	Zero data loss while at least one qualified standby is synchronized; the primary may continue unprotected if synchronization is lost	CBS, UPI, internet and mobile banking

Protection Mode	Transport	Zero Data Loss Guarantee	Recommended For
Maximum Performance	Asynchronous	No zero-data-loss guarantee; exposure depends on transport and apply lag	Systems that can tolerate some data loss

4.3 Why Automatic Failover Matters

For workloads with stringent recovery-time objectives, automated failover is an important part of the architecture. Manual failover introduces detection, decision, and execution time that can extend an outage even when the standby contains all required redo.

Fast-Start Failover (FSFO) allows Data Guard broker to initiate failover to a designated standby without a manual command. The observer and target standby evaluate connectivity and protection state before failover. Maximum Protection and Maximum Availability can provide automatic zero-data-loss failover when the target is synchronized; Maximum Performance uses the configured lag limit. Recovery time depends on the threshold, database topology, and application reconnection behavior.

Note: For detailed Oracle Data Guard configuration guidance, refer to [1]. For synchronous transport tuning and performance characterization, refer to [15].

5. Zero Data Loss Architecture Patterns

Protecting transactions across geographic distance requires careful network and standby design. RTT between the primary database and the synchronous endpoint is an important input, together with workload behavior and the approved protection objective.

The following patterns provide the Gold MAA data-protection foundation and qualify as part of the Oracle AI Database 26ai Platinum architecture only when deployed on Oracle Exadata with all prescribed Platinum requirements.

5.1 RTT Zones and Transport Modes

The following zones are practical planning bands used in this paper. They are not formal Oracle product limits, and every deployment must be validated under representative peak workloads and failure conditions.

Zone	RTT	Transport Guidance	Indian DC Example	Architecture
A	0–2 milliseconds (ms)	Evaluate SYNC/AFFIRM; validate at peak load	Mumbai - Navi Mumbai	See Figure 2
B	2–5 milliseconds (ms)	Benchmark SYNC/AFFIRM; consider FASTSYNC only after evaluating its failure-scope exposure	Mumbai - Panvel (near-metro)	See Figure 2
C	> 5 milliseconds (ms)	Validate direct synchronous transport; otherwise evaluate near-DR Pattern 1 or Pattern 2	Mumbai - Pune / Hyderabad	See Figures 3 and 4

Zone A (0–2 ms) generally offers the best conditions for direct synchronous transport with lower commit-latency impact. Application testing remains required.

Zone B (2–5 ms) can also support direct synchronous transport but commit-latency impact is typically more visible. Oracle documentation cites RTT above approximately 2 ms as an example where SYNC impact can increase [1]. SYNC AFFIRM and FASTSYNC should be evaluated against the required failure model and peak workload.

Zone C (>5 ms) represents higher-latency paths common in many cross-city deployments. Direct synchronous transport may still be feasible for some workloads, but banks should evaluate a nearby standby or Active Data Guard Far Sync endpoint when direct commit latency does not meet requirements.

Note: Transport mode is selected from the required durability, failure scope, protection mode, and measured performance. RTT informs whether the synchronous endpoint should be the remote standby or a near-DR intermediary. City names are illustrative, and measured results take precedence over the planning bands.

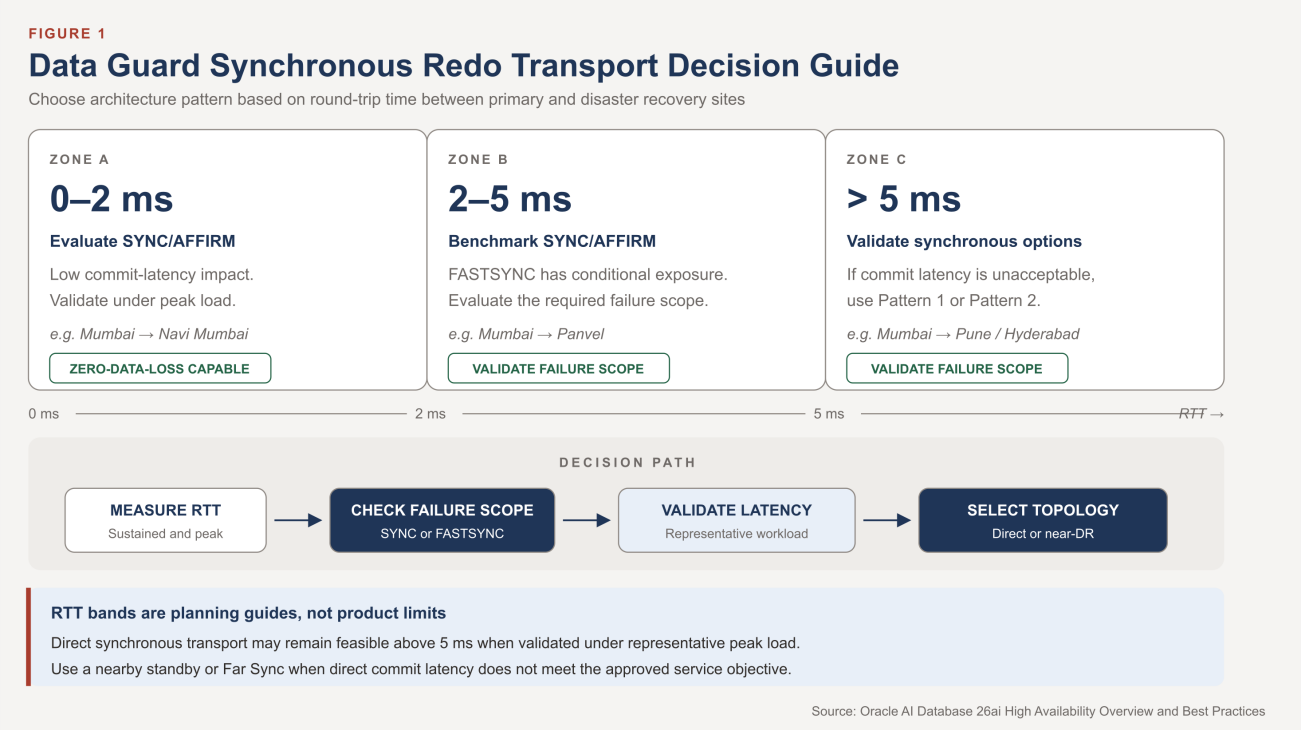


Figure 1 — Data Guard Synchronous Redo Transport Decision Guide (illustrative RTT planning bands)

5.2 Zone A/Zone B — Platinum MAA Target: Remote Standby

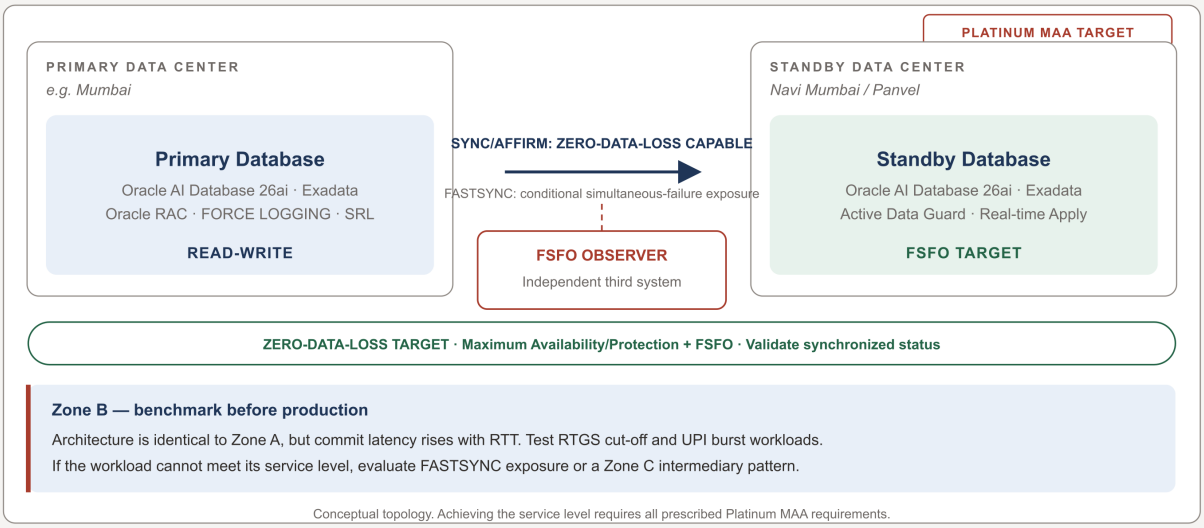
When measured RTT and workload testing support direct synchronous transport, use SYNC/AFFIRM with an appropriate protection mode to provide zero-data-loss protection within the defined failure scope while a qualified standby remains synchronized. FASTSYNC can reduce commit-latency impact, but it introduces potential data-loss exposure during certain simultaneous failures and should be selected only after evaluating and approving that risk. Active Data Guard can provide real-time read-only access, subject to licensing and workload requirements, while Fast-Start Failover automates qualified failover.

For Zone B, the topology can remain the same as Zone A, but testing under representative peak workload is essential. If SYNC AFFIRM does not meet the approved performance objective, evaluate FASTSYNC and obtain approval for its failure-scope trade-off before selecting a near-DR intermediary pattern.

FIGURE 2

Zone A/Zone B — Platinum MAA Target: Remote Standby

26ai on Exadata · Direct synchronous redo transport · Fast-Start Failover



Source: Oracle AI Database 26ai High Availability Overview and Best Practices

Figure 2 — Zone A/Zone B: Platinum MAA Target with Remote Standby

5.3 Zone C — Platinum MAA Target: Multiple Standby Databases (Pattern 1)

When direct synchronous transport to the remote DR site does not meet commit-latency requirements, Pattern 1 places a full standby at a nearby site. Redo is sent synchronously to that standby, providing zero-data-loss protection for the defined failure scope while the standby remains synchronized. The nearby standby cascades redo asynchronously to the remote DR standby, whose regional RPO depends on transport and apply lag. FSFO can target the nearby standby. The remote standby may also be configured as an FSFO candidate, subject to the selected protection mode, permitted lag, and successful Data Guard broker validation.

The nearby standby can run Active Data Guard for read offload. Transparent Application Continuity (TAC) can mask many planned and unplanned interruptions by replaying eligible in-flight work after reconnection. TAC requires supported clients, correctly configured services, replay-compatible requests, and representative failover testing; some requests may not be replayable and can still return an error to the application.

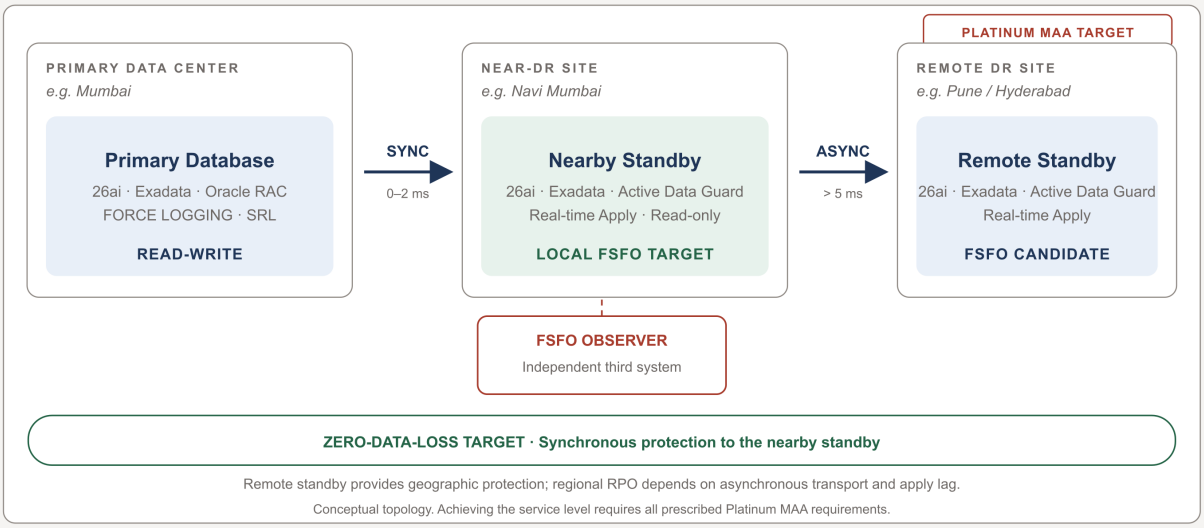
Note: Application testing is essential before enabling TAC in production to validate behavior under failover conditions. For configuration guidance, refer to [1].

Pattern 1 provides a full local failover target and can support sub-minute recovery when the complete database and application stack are configured and validated accordingly. If a regional event affects both the primary and nearby standby, the remote standby provides geographic recovery, with RPO determined by asynchronous transport and apply lag.

FIGURE 3

Zone C — Platinum MAA Target: Multiple Standby Databases

26ai on Exadata · Local synchronous protection · Remote geographic recovery



Source: Oracle AI Database 26ai High Availability Overview and Best Practices

Figure 3 — Zone C Pattern 1: Platinum MAA Target with Multiple Standby Databases

5.4 Zone C — Platinum MAA Target: Active Data Guard Far Sync (Pattern 2)

Pattern 2 places an Active Data Guard Far Sync instance at the near-DR site. This lightweight intermediary has a control file and standby redo logs but no data files. Oracle Data Guard sends redo synchronously to the Far Sync HA pair, which forwards it asynchronously to the remote standby. The remote standby can be the FSFO target. The Far Sync HA pair and alternate redo-transport routes must be configured so that the intended protection level can be maintained, or any degradation controlled, when a Far Sync instance or transport path becomes unavailable.

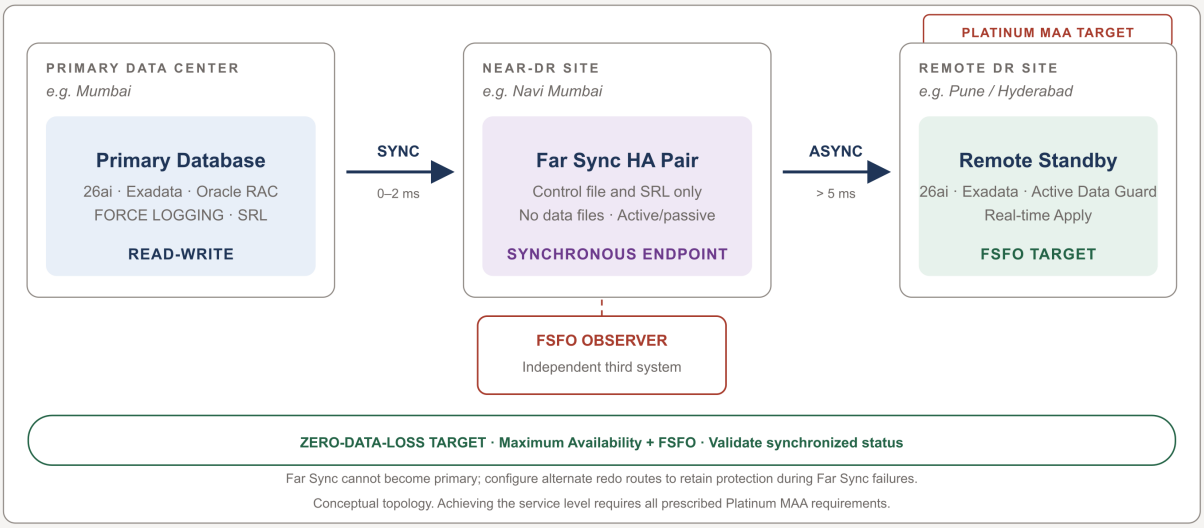
Advantages include a smaller near-site footprint, the ability to offload redo encryption and compression from the primary, and support for multiple remote destinations from a synchronous endpoint. Validate destination limits and configuration requirements against the applicable Oracle release documentation.

Key limitation: A Far Sync instance cannot become a primary or serve queries because it has no data files. Failover targets the remote standby, and RTO is affected by redo apply progress, role transition, and application reconnection.

FIGURE 4

Zone C — Platinum MAA Target: Active Data Guard Far Sync

26ai on Exadata · Local Far Sync acknowledgement · Remote Active Data Guard standby



Source: Oracle AI Database 26ai High Availability Overview and Best Practices

Figure 4 — Zone C Pattern 2: Platinum MAA Target with Active Data Guard Far Sync

5.5 Choosing Between Pattern 1 and Pattern 2

Both patterns can provide zero-data-loss protection within their defined failure scope and required synchronized state. Pattern 1 prioritizes local failover and read offload; Pattern 2 prioritizes a smaller near-site footprint and remote failover.

Priority	Pattern 1 (Nearby Standby)	Pattern 2 (Far Sync)
Local failover	Yes; sub-minute RTO to local standby	No; failover must target the remote standby
Read offload	Strong; nearby standby serves queries	Limited; only remote standby
Near-site footprint	Full database; higher storage cost	No data files; minimal cost
Encryption/compression offload	Primary handles redo processing	Far Sync can offload from primary

6. Network Architecture for Redo Transport

Oracle MAA network recommendations are documented in [1] and [15]. The controls below should be applied according to topology, workload, protection mode, security policy, and measured performance.

Core network design practices:

- Redo traffic capacity: Provide sufficient, predictable bandwidth and latency for peak redo volume. A dedicated interface or appropriately isolated quality-of-service path is strongly recommended where other traffic could cause contention. Congestion can increase commit latency and can affect synchronized protection state, depending on the protection mode.
- Diverse WAN paths: Use physically independent network paths where the availability objective requires protection from a single carrier, cable, device, or routing failure. Validate failover behavior for each path.

- TCP buffer tuning: Size send and receive socket buffers for high-latency, high-bandwidth paths. Oracle recommends a minimum socket-buffer value of 3 × the Bandwidth-Delay Product (BDP), and recommends validating the result with oratcptest [1].

Performance-sensitive configuration:

- Session Data Unit (SDU) = 65535: Oracle testing shows that the maximum SDU can improve synchronous redo-transport performance. Configure it for the relevant Oracle Net connection in tnsnames.ora and listener.ora; do not apply it universally.
- LOG_BUFFER: Use a minimum of 256 MB for asynchronous Data Guard transport. For databases with Flashback Database enabled, the general Oracle MAA minimum is 128 MB; when both recommendations apply, use the higher applicable value.
- Transport encryption: Protect WAN redo traffic according to the bank's approved security architecture and applicable RBI requirements. Oracle Net native encryption and TLS provide supported encryption options with different configuration and certificate-management considerations. For TLS configuration, use the Oracle Database Security Guide [16] and validate the protocol version permitted by organizational policy.

Conditional configuration:

- Redo transport compression: Consider compression when WAN bandwidth is the binding constraint. Compression reduces network traffic but adds CPU overhead, requires the applicable license, and may offer limited benefit for encrypted or poorly compressible redo. Validate the trade-off with representative workloads.

Note: Oracle provides the oratcptest utility for measuring redo transport network capacity. Refer to MOS Doc ID 2064368.1 for detailed usage.

7. Zero Data Loss Configuration Checklist

This checklist combines foundational Data Guard controls with recommended and conditional MAA practices. Apply each item according to the selected protection mode, failure scope, Oracle release, platform, licensing, and approved recovery objectives:

1. Foundational: When zero-data-loss protection is required, configure at least one qualified synchronized Data Guard destination using SYNC/AFFIRM with an appropriate protection mode. FASTSYNC may be considered only after evaluating and accepting its potential exposure during certain simultaneous failures. Additional remote destinations may use ASYNC according to the architecture and approved RPO.
2. Foundational: Enable FORCE LOGGING on production databases protected by a physical standby.
3. Foundational: Configure correctly sized standby redo log groups on primary and standby databases.
4. Foundational for 26ai guidance: Set DB_LOST_WRITE_PROTECT = AUTO on primary and standby databases.
5. Foundational for 26ai guidance: Set DB_BLOCK_CHECKSUM = TYPICAL. Set DB_BLOCK_CHECKING = MEDIUM on standby databases; evaluate MEDIUM or FULL on the primary only after performance testing.
6. Recommended for stringent RTO: Configure Fast-Start Failover and high-availability observers using MAA placement guidance.
7. Conditional: Evaluate a nearby standby or Far Sync intermediary when direct synchronous transport does not meet latency, availability, or failure-scope requirements.
8. Conditional: Use Zero Data Loss Recovery Appliance or Oracle Database Zero Data Loss Autonomous Recovery Service when the backup, cyber-recovery, and real-time redo-protection requirements justify it.
9. Recommended: Enable Flashback Database on primary and standby databases for reinstatement and recovery from supported logical errors, with retention sized to the recovery objective.

10. Conditional: Use Flashback Data Archive for selected tables that require long-term historical tracking, subject to policy, retention, storage, and licensing requirements.
11. Performance: Use LOG_BUFFER = 128 MB minimum with Flashback Database and 256 MB minimum with asynchronous transport; use the higher applicable value. On Linux, apply USE_LARGE_PAGES = ONLY where supported and correctly provisioned.
12. Recommended for faster role transitions: Use Bigfile Tablespaces for new designs and reduce excessive data-file counts. Evaluate migration of existing tablespaces against operational risk and maintenance requirements.
13. Regulatory validation: Conduct DR drills for critical information systems at least half-yearly. RBI guidance requires the alternate site to operate as primary for a sufficiently long period covering at least one full working day.

Note: For detailed implementation steps, refer to [1], [3], [4], and [15].

8. Phased Implementation Roadmap

The following roadmap translates the target architecture in Section 3.3 into phased adoption, allowing each bank to progress according to workload criticality, existing platform, and operational maturity.

Note: Achieving application transparency at the Platinum tier requires the prescribed client configuration, Application Continuity or Transparent Application Continuity practices, and validation under representative failover conditions. Oracle Database 19c deployments that use Oracle GoldenGate require the corresponding application considerations.

Phase	Target	Key Milestone
0	Bronze MAA baseline: backups, FORCE LOGGING, monitoring, and recovery validation	Data-protection foundation established
1	Silver MAA: Oracle RAC for compute-layer high availability; Oracle Exadata recommended but not required	Instance and server-level resilience established
2	Gold MAA, local: Active Data Guard with synchronous transport to a nearby standby	Zero-data-loss-capable protection established and validated for the defined failure scope
3	Gold MAA, geographic: add a remote standby using direct ASYNC transport, or use a Far Sync topology with SYNC transport to the near-DR Far Sync endpoint and ASYNC forwarding to the remote standby	Geographic disaster recovery established
4	Optional, risk-based enhancement: deploy Zero Data Loss Recovery Appliance or Recovery Service with real-time redo protection	Backup exposure reduced and cyber-recovery posture strengthened
5	Platinum MAA: upgrade to Oracle AI Database 26ai on Oracle Exadata and implement the fully prescribed Oracle RAC and Active Data Guard-based Platinum configuration	Zero or near-zero RPO and RTO for mission-critical workloads
6	Diamond MAA: select either Oracle AI Database 26ai on Oracle Exadata with Oracle GoldenGate 26ai active-active replication and an MAA-hardened GoldenGate Hub, or Oracle Globally Distributed AI Database 26ai with native Raft replication	Extreme-availability architecture established for qualifying Tier-0 workloads

Phase 6 is an optional architecture branch rather than a mandatory continuation of Phase 5. Qualifying Tier-0 workloads can choose the Diamond MAA option that best fits their application architecture and data-distribution model.

At the Platinum tier, Oracle AI Database 26ai Data Guard rolling upgrades using DBMS_ROLLING can provide a path to near-zero-downtime database upgrades without requiring Oracle GoldenGate, provided the prescribed standby architecture and operational requirements are satisfied.

9. Conclusion

India's digital banking infrastructure depends on database architectures that preserve committed transactions across local and regional failures.

Oracle MAA gives Indian banks a structured way to translate workload criticality, network latency, regulatory expectations, and recovery objectives into a resilient database architecture. The appropriate Gold, Platinum, or Diamond design should be selected according to the required RPO and RTO and validated under representative conditions.

In India's digital banking economy, every committed transaction must persist. Oracle MAA provides the engineering framework to design and validate for that outcome.

For implementation guidance, consult the Oracle MAA documentation referenced in this paper, or engage with Oracle's MAA team for architecture review and deployment planning. Additional resources are available at oracle.com/goto/maa.

References

1. Oracle MAA — Oracle AI Database (Oracle AI Database 26ai High Availability Overview and Best Practices)

2. Oracle MAA Blog — Diamond Tier

3. Configure and Deploy Oracle Data Guard, DB 26ai

4. Oracle MAA Gold — ADG Far Sync Reference Architecture

5. Oracle Real Application Clusters

6. Oracle Active Data Guard

7. RBI/2023–24/107 IT Governance Master Directions

8. RBI Storage of Payment System Data

9. RBI Cybersecurity Framework 2016

10. RBI Annual Report 2024–25

11. RBI Payment System Report H1 2025

12. NPCI UPI Product Statistics Aug 2025

13. Oracle MAA Product Page

14. DPDPA 2023

15. Best Practices for Synchronous Redo Transport — Data Guard and Active Data Guard

16. Oracle Database Security Guide — Configuring Transport Layer Security Encryption

17. Oracle Globally Distributed AI Database — Using Raft Replication

ORACLE

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle