

CASE STUDY

Leading Bank cuts
Disaster Recovery RTO
& RPO
across 280
applications by
more than 50%

About the Client

This is a leading Indian multinational private sector bank headquartered in Mumbai, offering a comprehensive range of financial products to retail and corporate customers. Founded in 1955, it is one of India's "Big Four" banks, operating a large network of branches and ATMs, with a strong emphasis on digital banking and global presence.

Key Aspects of ICICI Bank

Headquarters: Mumbai, India

Founded: 1955

Standing: One of India's "Big Four" banks

Global Presence: 19 countries, including subsidiaries in the UK, Canada, and Russia, and branches in the US, Singapore, Bahrain, and Hong Kong

Services & Products: The bank offers a wide range of services including commercial banking, mortgages, credit cards, investment banking, life and non-life insurance (via subsidiaries), and wealth management.

Digital Innovation: The bank is known for its pioneering role in digital banking in India, with its Mobile Banking app offering extensive functionality.

Key Subsidiaries: Life Insurance, General Insurance, Securities, and the Bank's Venture arm.

Performance: In 2025, the bank reported high levels of profitability, maintaining a strong position in the Indian financial sector. The bank serves millions of customers through its extensive network and is known for its strong focus on technological advancements.

Client Challenges

- The bank was missing a Disaster Recovery (DR) plan for their business and core service application environment.
- The bank had difficulty managing the complex heterogeneous IT infrastructure supporting their applications.
- The Bank has a multi data center approach with Two Site and Three Site architectures — Three DCs at Hyderabad, One DC at Jaipur, Two DCs in Mumbai, one in Oracle Cloud, and one in Azure Cloud — which makes it difficult to perform multiple DR drills and DR tests across sites for the designated applications.
- Lack of visibility on DR infrastructure and the readiness of DR to take over the role of primary.
- The client also required DR automation to reduce the RTO of their applications spread across branches and minimize the dependency on SMEs for conducting DR activities.
- The bank needed a unified dashboard to view all applications from a single window.
- The bank was missing ISO compliance on reports as per RBI guidelines.
- They needed a DR automation tool that could adhere to their stringent security policies while achieving these objectives.

Our Solution

- Implementation of Continuity PatrolTM orchestrated the recovery of applications at the DR site using customized recovery plans.



- Successfully configured 280 applications used by the bank running on approximately 6,900 VMs on IBM AIX, HP-UX, Oracle Solaris, and VMware platforms for disaster recovery, with Windows, AIX, Solaris, and RHEL operating system environments.
- Replication systems used included Native DB Log Shipping for Oracle, Oracle RAC, MSSQL NLS, MSSQL Always ON, PostgreSQL streaming replication, and MongoDB Replica Sets, with approximately 390 DBs in total.
- Successful configuration of Switchover/Switchback workflow for Application and Database tier in Continuity PatrolTM.
- Alert notification through Email & SMS.
- Successful Switchover and Switchback for in-scope applications & database tier during drills, within agreed RPOs: 0-30 min for Tier 0, 1-30 min for Tier 1, 2-120 min for Tier 2, and 1 to 3 days for Tier 3.
- RPO reduction of more than 50%.
- ISO 22301 standard DR drill reports for audit and compliance.
- Visibility into the availability of various applications through Unified Monitoring Console.
- Integration with Active Directory and ARCON for authentication.

Unique Achievements

- Authentication and approval mechanism was achieved which is called as Four Eye Principal by integrating with Infoblox DNS, Arcos UI6, Digital Multifactor Authentication platform which provides OTP and enabling Maker Checker functionality.
- Data pointing changes, initially manual, are now automated through Continuity Patrol, improving RTO.
- DNS change automation substantially reduced dependency on the network team.
- Load balancer changes are automated through Continuity Patrol, improving RTO and avoiding manual intervention during DR drills.
- Also configured bunker site recovery with Zero Data Loss (ZDL).



Results and Benefits to Business

- Reduced overall RTO by more than 50%
- Dependency on SMEs was considerably brought down.
- TCO optimization achieved by reducing the number of resources required to conduct DR drills.
- Faster availability of applications through single-click automated DR processes.
- ISO 22301 standard DR drill reports and RPO SLA reports.
- Better visibility of application service availability via dashboard.



Key Metrics

280

APPLICATIONS
ONBOARDED TO
CONTINUITY
PATROLTM

6,900 VMs

UNDER AUTOMATED
DR ORCHESTRATION

390 DBs

ACROSS MULTIPLE
REPLICATION
TECHNOLOGIES

50%+

REDUCTION IN RTO &
RPO

READY FOR YOUR OWN SUCCESS STORY?

Get in touch with our automation experts and learn how you can fast-track your digital transformation initiatives.

mktg@ptechnosoft.com

+91 - 020 - 6687 8300

About Perpetuuiti

Perpetuuiti empowers people and businesses alike. We deliver the world's most-comprehensive and urbane automation platforms making work more human. Our platforms deliver leading-edge automation solutions for modernizing resiliency management, and turbocharging the performance of your applications, IT and business operations at speed and scale to drive exponential efficiencies.

For more information, visit www.ptechnosoft.com