

GDPR Compliant Private Cloud architected and delivered for a Global Top 10 Bank

Highly available Private cloud for a Premier Global bank

Delivered a private cloud for their banking operations that could be leveraged to create new business frontiers, as well as optimize the organization for agility and compliance by implementing the right mix of strategy, technology, and knowledge.

About the Client

10+

Operations in 10+ countries

200

Year

Old legacy

Personal Banking, Business Banking and Specialist Banking operations in 10+ countries

The client is a global premier bank and one of the oldest banks in the world that has been known to embrace technological innovations in their pursuit of customer service excellence. As one of the largest banks in the world, they emphasized on being ahead of the curve to ensure that they retain a competitive advantage over new-age Fintech rivals.

Moreover, there was increased scrutiny on customers PII – (Personal Identifiable Information) related data management and security. GDPR was about to come into effect, which would mean new rules and safe guards to be factored in for such a data-intensive institution.

The Challenge

Infrastructure Modernization with Assured Scalability

The bank has a large number and variety of financial products and services that mandated technology infrastructure to look beyond a traditional solution approach. Additionally, they aimed to undertake modernization as an opportunity to overhaul their systems, improve transparency and accountability, ensure complete and comprehensive compliance with all applicable regulations existing currently, or in the future. The bank's on-premises infrastructure was becoming obsolete, and migrating to cloud was their need of the hour.

The bank wanted to embrace a private cloud that could deliver performance at scale with cutting-edge technology. It needed support for integration of some of the legacy assets and applications from their primitive data center components.

Fulfilled Data Residency & Accelerated Compliance

Applicability of new Regulations such as GDPR and stronger data privacy laws required an agile and constant compliance systems that are geared to meet demands of fiduciary linked regulatory guidelines . The cloud solution would have to be geared towards the future as well, with capabilities that could evolve in sync with compliance upgradations along with integration with banking existing Information Security Management System.

Cyber Resiliency & Rights of Data Subjects

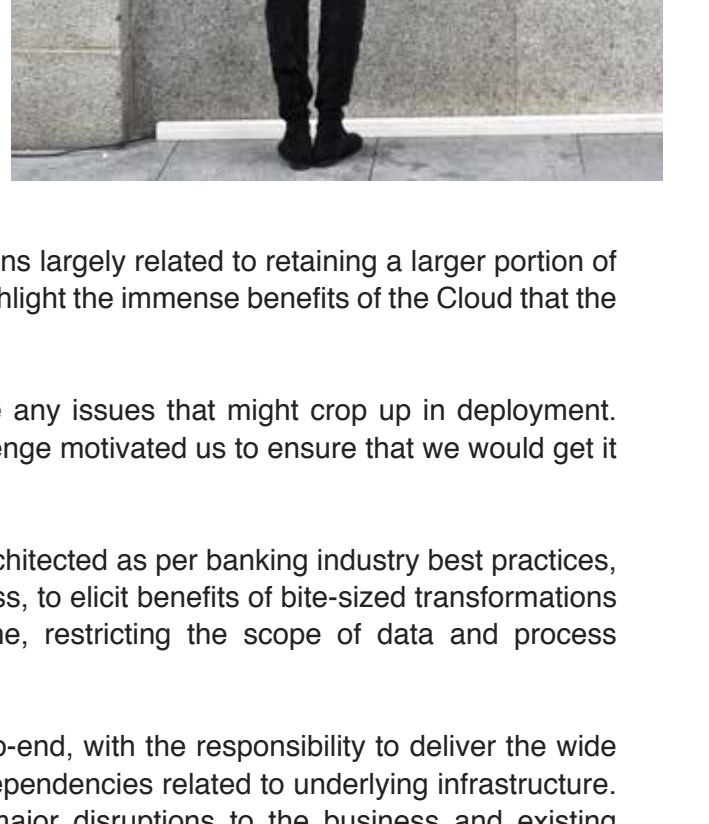
The bank was concerned about the possibilities of data breaches, so security had to be at the heart of the solution. Protecting client data was their top priority but Perimeter-to-Edge security with a castle-and-moat concept would not be right approach to protect the crown jewel and bringing the resiliency in the overall cyber security posture. The model envisioned providing rapid and secure user access while complying with the strict security and regulatory mandates that govern the financial services vertical for the data subjects.

Aiming for an Always-On Environment

While 100 per cent availability may not yet be a practical goal, banks strive to get as close to this as possible. At a time when competition is high, consumers have more choice than ever with an inclination for a digitally immersed ecosystem which can give them a frictionless experiences. The market is eventually open both for an established legacy players and for new challengers that can promise a more digital-first approach to personal banking. It will not take much time for consumers to transfer their loyalties to another provider if they feel they aren't getting the level of service they expect, and 24x7 availability is now a minimum requirement for customers.

The client wanted an Active-Active cluster between two sites in order meet the business objectives, typically made up of at least two nodes, both actively running the same kind of service simultaneously for all productions workloads. The main purpose was to achieve load balancing that would distribute workloads evenly across all nodes and secondly to prevent any possibilities single node from getting overloaded or failed. As there are more nodes available to serve, there will also be a marked improvement in throughput and response times.

The bank was interested in offering a more responsive level of service to customers without training staff. All in all, they wanted to upgrade their legacy systems to more effectively gather, analyse and contextualize a wide range of data.



The Solution

Built on Trust Principles

SECURITY, INTEGRITY, CONFIDENTIALITY, PRIVACY AND AVAILABILITY

Banks would usually deploy on-prem solutions for reasons largely related to retaining a larger portion of controls with them. Conversely, Cloud4C was able to highlight the immense benefits of the Cloud that the client could leverage, and pass on to their customers.

Each aspect of the migration was examined to resolve any issues that might crop up in deployment. There was no room for error at any point, and this challenge motivated us to ensure that we would get it 'First Time Right'.

Our teams focused on delivering a solution that was 'Architected as per banking industry best practices, Delivered Right'. We focused on each step of the process, to elicit benefits of bite-sized transformations which include mitigating risk by reducing delivery time, restricting the scope of data and process conversions, and minimizing liability for the bank.

The Cloud4C team handled the complete project end-to-end, with the responsibility to deliver the wide range of requirements for different functionalities and dependencies related to underlying infrastructure. The project was meticulously executed without any major disruptions to the business and existing ecosystem. The solution stood the values of Strategy-to-operations cutting across all phases of design, build, test, implementation, and migration with a point of accountability, and transparency in our project management approach.

Our project team were involved with the stakeholders since inception to seek consensus towards the milestones to be achieved. We started with a reference architecture that outlined the fundamental components that would be required to build and integrate the various solution building blocks delayed over a dedicated private cloud. This includes laying out the physical infrastructure, computation capabilities, network and storage resources, OS requirements, service and technology management requirements, and even the virtualisation resources.

Once the client approved the architecture, we moved on to detailing the features and functions of each aspect of the architecture. We carried out a thorough analysis of the bank's existing infrastructure to build a seamless solution.

The overall solution was made possible with applied innovation at some major steps of the project. Here are some of the ways in which the Cloud4C team achieved this:

Devising a Futuristic Transformation

Cloud4C delivered a GDPR compliant Always-ON private cloud to ensure strong protection of information - A private cloud that can be set up on demand, guaranteeing the client a higher isolation and a robust military grade security standards which can meet current and future requirements with modularity for integrations for advanced technologies should there be business needs in future. We focused on creating multi-availability zones, equivalent to hyperscalers platform from big-tech.

An Active-Active cloud POD - point of deployment was achieved for applications with databases running on SQL and Oracle while the Web servers were enabled to work with an ubiquitous load balancing feature supported through Global Server Load Balancing (GSLB). Central bank and data privacy guidelines were met by incorporating the right security controls and tools.

Once the client approved the architecture, we moved on to detailing the features and functions of each aspect of the architecture. We carried out a thorough analysis of the bank's existing infrastructure to build a seamless solution.

The overall solution was made possible with applied innovation at some major steps of the project. Here are some of the ways in which the Cloud4C team achieved this:

Compliance Readiness & Security Postures

From a regulatory requirement perspective, it was imperative to adopt data privacy principles to adhered across the data lifecycle encircling around CSU-SAD (CREATE STORE USE – SHARE ARCHIVE DESTROY). Key security controls like data encryption, masking and obfuscation for PII related attributes link to data subjects phone numbers, affinities, relationship status, DOB, address, etc. To be GDPR compliant, privacy experts from our Governance Risk & Compliance (GRC) team were involved to set the right directions

The highly confidential nature of datastore required that it remain inaccessible even to developers with admin privileges. Even while running routine troubleshooting tasks, the system was designed to have a high-level secure database masking mechanism while transmitting data from the production environment to any lower security environment.

The Cloud4C Private Cloud solution eliminated this risk with data masking and obfuscation techniques and creating a cryptographic encryptions hashed through a asymmetric Public and Private set of key pairs

Migration of Sensitive Data Workloads

The bank had a Hadoop data processing unit that would have to be accessed by the new Private cloud environment for content. These are two different environments at different locations, and the data is PII data which required the highest integrity and security at both the database level as well as during transmission.

We implemented transparent encryption at the database network layer, not between IP to IP, but from the Application Server to the Database Server. We established a secured protocol encryption mechanism that let them scoop data from the production environment to the Hadoop system in a completely secure manner, with certificate control.

Cloud4C assumed the responsibility of seamlessly migrating business-critical applications without affecting the client's banking operations while ensuring GDPR compliance at every step. Continuous vulnerability scans and detection of open areas and exposures were integral to maintaining the integrity of the business data during the migration process and thereafter.

Achieve Continuous Availability: Bringing RPO/RT0 to near Zero

The client was especially concerned about the recovery options from the private cloud. Cloud4C provided an active primary database and a secondary database that is on standby. The client had a target of activating the secondary database within one hour, but we were able to achieve it in few minutes.

Our solution design principle has ensured to have a seamless application delivery and channels for the applications hosted , irrespective of whether the primary or the secondary database is in use.

Key Accelerators

Dedicated Banking practice at Cloud4C

- Cloud4C helps banks of all sizes deliver innovative cloud-based solutions to accelerate their digital transformation journey and leverage cutting-edge technology to become more agile, strategic and customer-focused.
- Cloud4C has a Banking practice with certified cloud experts across Solution, Pre-Sales, Sales and Service Delivery teams dedicated for Banking Transformation and Migration projects.
- Regulatory approved security stack with 40+ Security controls tailored specifically for banks
- Successfully serving 78 banks today, including 6 of the Global Top 20 banks
- Total ownership – Single SLA delivered at application login
- Compliance to local data residency and sovereign norms in 50 global locations
- End-to-End Cloud journey ownership including IT modernization and Migration

Cloud4C Private Cloud for Financial Services

- With 12 years of proven experience in this vertical, Cloud4C is a pioneer in end-to-end migration of mission-critical instances on to a private cloud environment.
- We develop security and compliance-ready framework to deploy and migrate existing workloads in private environment from our in-country cloud PODs present across 25 countries and 50 locations.
- For any client, we can have 2 sites in each country, one for In-country Primary and another for In-country DR
- We support and maintain 50,000+ instances and 250+ private cloud setup for enterprises globally to help accelerate their business transformations.

Information Security Compliance Ready Portfolio

The ever-evolving regulatory requirements in different regions or countries can be very challenging for banks. The Cloud4C solution complies with distinct data localization laws to eliminate disruptions to the operations. The cloud infrastructure is built on a robust architecture with high availability, disaster recovery, and backup. We ensure transparency and dependable implementation by strictly adhering to data sovereignty laws.

High-level Architecture for Client Bank on Cloud4C Private Cloud

Results

99.99%

Uptime with cost effective and resilient solution

100%

Adherence to Compliance requirements

SUCCESS

In all emergency drills, Load Testing and Vulnerability Management

10X

Accelerated execution of batch jobs

ZERO

Data loss during migration and thereafter

ZERO

Data breaches and no major outages till date

ACE

All Central Bank's audits

INNOVATION

Fostering innovation by timely execution of CRs

REDUCED

Complexity of improving Application performance