Leading Kyrgyz Bank achieves 2-day audit turnaround & 20% IT savings with RackCorp

Private cloud with sovereign data handling, pre-mapped controls, and automated operations built for regulated banking

Executive Summary

A leading retail and SME bank in the Kyrgyz Republic shifted core digital and payment services to RackCorp to improve service continuity, tighten control ownership, and reduce operational friction. RackCorp delivered sovereign private cloud on its hypervisor, segmented networking, managed backup and recovery, and integrated security operations that aligned with the bank's governance model. Cutovers were staged to protect settlement windows and busy periods while capturing logs for audits.

Client Snapshot

A leading Kyrgyz Bank with a national footprint, retail and SME focus. The scope of transformation included core banking, payments and cards, digital channels, data services, and support systems.

The bank wanted to stabilise key services, reduce change risk for its regulated workloads, and be ready for internal audit checks. As well as create a secure base for new products and adopt evolving technologies.

- Platform strain during peaks & limited options for controlled scale & failover
- Gaps in control, ownership & audit evidence for access & change
- Clearer rules needed for personal data handling & external interconnects
- Payments & card flows needed predictable paths during settlement periods

Why RackCorp?

The bank discovered RackCorp through a trusted partner referral by DataTime followed by structured evaluation sessions. RackCorp was chosen for its local regulatory alignment, private connectivity, clear shared responsibility, and predictable commercials. RackCorp's hypervisor with private cloud model, bank-grade runbooks, and audit artefacts fit the bank's business needs.

RackCorp Solution

RackCorp provided a private cloud with segmented virtual networks, policy-driven storage, managed backup and disaster recovery, web protection and DDoS controls, and a managed security operations service. Control mapping, logging, and evidence packs were prepared to support regulator and internal audit reviews and to align personal data handling with bank policy.

Core Methodology

Architecture & security

- Regions and continuity: Primary region serving the Kyrgyz market with a secondary site for continuity per the bank’s recovery plan
- Network: Private address space, tiered segmentation, private service endpoints, and controlled partner peering
- Identity and access: Bank identity provider integration, multi-factor for admins, least privilege roles, and a break-glass process with full audit
- Data protection: Encryption at rest and in transit, customer key options, key rotation policy, and immutable backup copies with restore drills
- Observability: Metrics, logs, traces, synthetic tests, and standard dashboards for operations and audit review

Implementation

- Assessment and pilot runs preceded incremental deployments for payments, channels, and core services
- Data movement used replication and checkpointed cutovers with rollback points
- Issues found during pilots were resolved through tuning, runbook adjustments, and access clean-ups and retests

Key features in use

- Private compute on the RackCorp hypervisor with reserved capacity options
- Private interconnects and policy-based firewalls for bank and partner systems
- Automated backups with retention policies and regular restore exercises
- Web application protection and DDoS controls for public channels
- 24x7 security operations with alert triage and incident workflows

Business Impact

- **99.99% uptime ensured** uninterrupted settlement and card processing
- **40–50ms average latency** improved real-time payments and customer experience
- **Audit prep reduced from weeks to 2 days** with mapped controls and evidence packs
- **20–25% IT cost savings** through optimized infrastructure and automation
- **30% faster release cycles**, fewer rollbacks, and steadier change windows
- **60% fewer incidents** requiring manual intervention

Future Outlook

Planned next steps include selective container adoption, SIEM uplift, and deeper alert triage. The bank will leverage RackCorp’s support for growth in analytics and fraud controls.

Contact us today to learn more about how we can help streamline your cloud operations with ease and at affordable cost!

sales@rackcorp.com

www.rackcorp.kg

RackCorp
SECURE CLOUD