kyndryl

Elevating regulatory compliance as part of cloud migration

North American Bank | Banking

Business opportunity

In the heavily regulated financial services industry, banks risk reputational damage, financial penalty and an impaired ability to conduct business if an auditor reports non-compliance. Sarbanes Oxley (SOX) reporting legislation, for example, and essential payment standards like Payment Card Industry Data Security Standard (PCI DSS) require regular audits.

During a recent audit, this large bank's independent auditor identified and reported security risks, lapses in best practices, misconfigurations and other issues in the bank's migrated cloud workloads. The auditor mandated that the bank resolve the issues within a specific timeframe to maintain regulatory compliance.

To meet the auditor's deadline, the bank's Board of Directors imposed rigorous new change management requirements for the IT team.

Technical challenge

The source of the risks identified in the audit were primarily associated with the bank's two security frameworks. As part of migrating workloads to 3000 Amazon Web Services (AWS) servers, the bank set up controls modeled on their on-premises security framework. However, that framework was not easy to adapt to a Cloud Native Application Protection Platform (CNAPP), which uses AWS services to define, monitor and enforce security controls in customer tenancies. As a result, events in the bank's cloud workloads were inadequately monitored, measured and managed.

An added challenge: though the bank was building a cloud security engineering team, they were still closing the CNAPP skills gaps.

To meet the auditor's deadline, the bank needed a partner who could create integrated visbility into their cloud workloads, and apply expertise with CNAPP configurations and iterations to adjust security controls related to issues flagged in the audit.

Our solution

Together, the bank and Kyndryl reconfigured and optimized use of the Orca Cloud Native Application Protection Platform (CNAPP) on AWS. The team custom-configured many of the essential security controls and enabled Identity and Access Management to support the 11,000 employees who have the option to work remotely.

For all cloud workloads, the team remediated risks, vulnerabilities and deviations from security policies. As part of that work, the team streamlined monitoring across a previously siloed organization with fragmented views. They integrated the bank's custom ServiceNow platform with the Orca CNAPP, configuring it to autogenerate and assign tickets on policy-triggering events.

What progress looks like

Within hours of going live, the solution delivered a full asset inventory, automatically classified sensitive data, and measured the entire AWS environment against financial regulations.

Other specific benefits so far include:

- Compliance with key industry regulations and standards:
  - → Financial reporting (SOX)
  - → Online payment systems (PCI DSS)
  - → Security posture (FFIEC, ISO 27001)
- Each security event directly tied to the specific control violated, expediting understanding and resolution
- ServiceNow automation that routes every high-priority alert into the correct workflow, captures remediation evidence, and builds a gapless audit trail
- Support for remote work that maintains all security and compliance controls

What's your next digital business challenge?

Let's tackle it together. →

Meet the team

Kenneth Moten
Associate Director,
Cybersecurity Resiliency
Kyndryl

Mirza Baig
Director, Customer Enterprise Architect
Kyndryl

Pat St. Jean
Associate Director,
Cybersecurity Engineering
Kyndryl

kyndryl