kyndryl | aws

# Elevating regulatory compliance as part of cloud migration

North American Bank | Banking

## Business opportunity

In the heavily regulated financial services industry, a bank risks reputational damage, financial penalty, and an impaired ability to conduct business if they are found non-compliant, for example, with Sarbanes Oxley (SOX) reporting legislation, or essential payment standards like Payment Card Industry Data Security Standard (PCI DSS).

In an annual audit, this large bank's auditor identified and reported security risks, lapses in best practices, misconfigurations, and other issues in migrated cloud workloads. The auditor mandated the bank to resolve the issues within a specific timeframe. The bank's board prioritized the mandate and closely monitored the IT organization's progress towards meeting the deadline.

## Technical challenge

The source of the risks identified in the bank's audit were mainly due to gaps between two security frameworks. As part of migrating workloads to 3000 AWS servers, the bank set up controls modeled on their on-premises security framework. However, that framework was not easily adaptable 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 bank was building a cloud security engineering team, at the time they completely lacked experience with CNAPPs.

To meet the auditor's remediation deadline, and remain in compliance with demanding financial industry regulations, the bank needed a partner with the technical expertise with CNAPP configurations and integrations who could first bring the bank's cloud workloads into integrated visibility. From there, the team could identify and fix issues related to specific security controls.

## Our solution

Together, the bank and Kyndryl conducted discovery workshops to define the AWS services to monitor in an Orca CNAPP, the bank's chosen platform built on AWS infrastructure. About 30% of the security controls for AWS services were immediately ready to track in the CNAPP. For the many other controls, the team had to develop custom configurations.

The team identified risks, vulnerabilities, misconfigurations and deviations from security policies in the bank's cloud workloads. They integrated the bank's custom ServiceNow implementation into the Orca CNAPP and configured it to autogenerate and assign tickets based on policy-triggering events. Vulnerability analysts then worked to resolve the issues and close their assigned tickets.

The team steadily resolved overlaps between the bank's existing monitoring tools and the Orca CNAPP, streamlining the view across a previously siloed organization with fragmented views.

Identity and access controls were integrated into the CNAPP to support the 11,000 employees who have the option to work remotely.

Finally, the team integrated the CNAPP with AWS Guard Duty for a holistic threat management and security control solution with situational awareness of sensitive data and governance to enforce best practices and mitigate risks as the business grows.

## The power of partnership

Based on an ongoing partnership with Amazon, the Kyndryl team provided a regulatory compliance solution through deep knowledge of the AWS cloud platform and services and expertise in cybersecurity architecture and engineering.

Amazon Web Services included in the solution:

**Orca Cloud Native Application Protection Platform** on AWS for security controls that govern compliance with industry regulations

**Amazon GuardDuty** for threat detection and management

**Amazon S3** for scalable storage solutions

**Amazon EC2** for flexible computing capacity

Within just a few hours of go-live, **Orca Cloud Native Application Protection Platform** on AWS delivered a full asset inventory, automatically classified sensitive data, and measured the entire AWS environment against financial regulations—including PCI DSS, FFIEC, SOX, and ISO 27001. The platform did not simply highlight issues such as overly permissive IAM roles or unencrypted data stores. It tied each finding directly to the specific control it violates (such as PCI DSS req 7 "Least Privilege," and req 3 "Protect Stored Data"). Two-way integration with ServiceNow routed every high-priority alert into the correct workflow, captured remediation evidence, and enforced SLA deadlines—building an airtight audit trail in the process.

Executive dashboards now give leadership real-time visibility into AWS risk exposure and trending, empowering proactive decisions rather than reactive firefighting. The net result: audit readiness is a by-product of day-to-day operations, proven with traceable, regulator-ready evidence.

## What progress looks like

The bank established a new security control framework for cloud workloads that satisfied mandated remediations and also can grow with their business and the IT estate's evolving security posture. Cloud security and compliance results so far include:

- Compliance with SOX and PCI DSS regulatory requirements.
- Adherence to ISO 27010 standards for transferring confidential information.
- 50% reduction in potential breaches by predicting and remediating high severity vulnerabilities in a development environment before deploying security controls in production.
- Streamlined redundant tools into a single security control framework (Orca CNAPP).
- Support for remote work that maintains security and compliance controls.

## Meet the team

**Kenneth Moten**
Associate Director, Cybersecurity Resiliency, Kyndryl

**Mirza Baig**
Director, Customer Enterprise Architect, Kyndryl

**Pat St. Jean**
Associated Director, Cybersecurity Engineering, Kyndryl

What's your next digital business challenge? Let's tackle it together.

Start a conversation. →

kyndryl | aws