SPHERE

Global Bank Meets Access, Compliance, & Audit Obligations

GOVERNANCE

CASE STUDY

THE CLIENT

- Global Bank
- 85K Employees
- 17M Clients
- 1,200 Locations

THE ENVIRONMENT

- 3M IT Assets
- 500+ Applications
- 10K+ Platform Integration Points

THE BACKGROUND

This Canadian headquartered global bank was struggling to meet identity and access governance, compliance, and audit obligations. Inconsistent and ineffective access controls were applied across the organization resulting in significant control issues across Unstructured Data, Privileged Access, and Identity Access Management (IAM).

While access governance policy and standards were defined centrally, controls were designed and operated at a departmental level resulting in disparate and independent approaches to achieve the control objectives. The result was a catalogue of audit and control issues around access management.

THE CHALLENGE: DECENTRALIZED MANUAL REPORTING

Each department or platform team provided identity and access management reporting independently and invariably leveraged different views of source data. This resulted in varying degrees of accuracy and the inability to build a consolidated view of access controls, putting the organization at significant risk.

The institution deployed diverse technology to extract information regarding roles, users, and entitlements—each with differing mechanisms and limitations. The decentralized approach and broad range of technologies involved and deployed globally resulted in significant manual effort and overheads placed on technology teams.

Numerous tools had been deployed to solve various security systems; however, these operated in silos and no system existed to aggregate and unify the organization's identity and entitlement data. These factors presented a significant opportunity to drive efficiencies and create capacity in the technology teams.

THE SCOPE

Working with the customer, SPHERE defined a global operating model for identity and access governance which incorporated a centralized reporting platform using SPHEREboard. The objective was to deliver consistent, accurate and automated reporting at scale across a broad scope of technologies throughout the bank.

These technologies included, but were not limited to:

- > Active Directory
- > Workday
- > Custom ownership and membership catalogs
- > Mainframe platforms
- > UNIX infrastructure
- > Windows infrastructure
- > CyberArk
- > Tanium
- > ServiceNow
- > BeyondTrust
- > Hi-PAM

The involved systems and technologies underpinned many critical business processes and applications at the bank. It was key to ensure the stability of these processes and applications was not impacted by any integrations with SPHEREboard. The SPHERE team worked closely with the bank's architects, platform engineers, and change managers to deliver robust and sustainable integrations ensuring the stability and continuous availability of in-scope platforms.

Central to this was SPHEREboard's distributed server architecture, enabling the platform to process large datasets quickly and efficiently from multiple regions and locations within the client environment.

THE SOLUTION

SPHERE approached the client's governance challenges with people, process, and technology surrounding Identity Hygiene.

People	SPHERE experts worked closely with key bank stakeholders to establish the right governance approach and perform technical integrations and remediation campaigns.
Process	SPHERE established a strong governance framework which clearly identified roles and responsibilities with senior executives accountable for deployment and adoption.
Technology	SPHEREboard was deployed into the environment to provide a centralized integration point and reporting platform.

The SPHEREboard deployment was a highly scalable and flexible Identity Governance & Administration (IGA) discovery, sanitization, and unification platform that was able to eliminate gaps between the existing system and organization structure. Using SPHERE's "only capture metadata" approach, it collected the necessary data for the client's governance needs without impacting target systems. SPHERE leveraged its unique crowd sourcing ownership model to identify true owners rather than assumed owners of client's platforms, accounts, and data assets.

SPHERE delivered a technology-enabled service to remediate the client's security and governance challenges. Organizational structures and team dynamics inhibited collaboration on governance issues. SPHERE proposed an all-encompassing governance program that balanced every team's primary concerns. SPHERE also leveraged senior executives in the organization to campaign for organizational-wide acceptance of the overall strategy.

THE APPROACH

To aggregate and normalize data across the platforms within their environment, SPHERE developed and proposed a technology-enabled managed services process to agree on identity governance, perform discovery, and build the solution:

Identity Governance Strategy | **Source Data Discovery & Analysis** | **Data Cleanup & Risk Remediation**

Identity Governance Strategy

Through a series of stakeholder interviews, SPHERE gained an understanding of the existing gaps and governance needs and developed a strategy to address the broad range of stakeholder needs.

Once the strategy was developed, SPHERE solicited support from senior executives within the organization to evangelize the process throughout the company. SPHERE built individualized Target Operating Models for each team providing a path forward that aligned to the bank's overall strategy. The Target Operating Models gave each team the guardrails to align with other stakeholders during the project and beyond.

Source Data Discovery & Analysis

Working directly with individual stakeholder teams, SPHERE identified how platforms could expose entitlements and user data, leveraging existing discovery tools where possible, and building custom integrations where not. Data was extracted into SPHEREboard and relationships were mapped between accounts and across multiple platforms.

To ensure data integrity, SPHERE developed a data source management process to coordinate the many connectors, reports, feeds, and API calls. The data sources were analyzed for two independent factors: data quality issues and data security issues.

Data Quality

SPHERE's analysis of the data, feeds, and outputs identified inconsistencies, inaccuracies, formatting issues, and completeness. Common issues included:

- Inconsistent or missing unique identifiers
- Mismatched data
- Incorrect effective entitlements
- Incompatible data format

SPHERExperts used this analysis to make recommendations for each individual data quality issue and agreed a plan to address.

Data Security

SPHERE reviewed the organization's policies, processes, and industry best practices to complete a gap analysis of accounts and entitlements.

SPHERE identified major security issues across the estate including open access, as well as "needle in the haystack" issues including non-standard access and segregation of duties concerns.

SPHEREboard's risk profiler was used to create actionable reports, enabling the prioritization of risks and an understanding of the remediation effort. SPHERE delivered team-specific visibility and actionable intelligence, enabling technology owners to gain insights into data quality and security issues including:

> Open Access

> Direct Permissions

> Excessive Access

> Elevated Privileges

> Privilege Account Control Gaps

> Ungoverned Local Accounts

> Unmodified Default Accounts

> Privileged Personal IDs

> Improper/Hidden Access Mechanisms

> Ungoverned Provisioning Events

> Extradepartmental Access

Data Cleanup & Risk Remediation

SPHERE worked with each technology owner to create a customized feed cleanup and risk remediation plan. Remediation was driven through SPHEREboard's Asset Review Module to expedite the owner outreach, improve response times, and automate remediations.

Owner Outreach

Remediation campaigns were automated through the SPHEREboard Asset Review Module with automated emails performing platform-specific surveys.

Each survey was personalized to the recipient, presenting them with the data quality issues, risk ownership, and remediation options. Remediation was performed based on the owner responses.

To accelerate owner response rates, SPHERE implemented a dual-escalation approach:

1. Unresponsive owner managers were copied on the third reminder email
2. Business Information Security Officers were leveraged to follow up with managers

Leveraging this dual-escalation approach improved owner response rates by more than 350% over the manual processes used before SPHERE was engaged.

Data Cleanup

SPHERE worked with platform owners to create a feed standard which platform teams could adhere to. Source data feeds were tailored to meet the feed standard with custom ETL (Extract Transform and Load) processes.

SPHERE introduced a common information model to be applied to all source feeds to ensure consistency across all technology platforms. Our SPHERE experts worked with the technology owners to remediate root cause data quality issues to ensure sustainability and accuracy.

Risk Remediation

SPHERE leveraged its Virtual Worker technology to provide automated remediation and integration with the bank's existing change control processes. This resulted in reduced remediation efforts from technology teams and increased capacity within the teams to focus on existing and future access governance issues across the organization.

Tech-Enabled Managed Services

After remediating the highest risk security issues and cleansing data quality concerns, SPHERE began to separate comingled data feeds into their distinct IAM components. ETL processes generated account, entitlement, and function objects for each platform which were then loaded into SPHEREboard. Logic was built to combine account data from multiple platforms feeds to enrich the feed of each individual platform. SPHERE employed a software delivery mindset to create production-ready, long-term, maintainable code for each platforms' data feeds. SPHERE also provided detailed documentation to the IAM team on the integration points with SPHEREboard that leverage existing connectors pulling in the platform data feeds.

THE OUTCOME

As a result, the client was left with long-term, sustainable, enterprise-level data integrations across multiple technology platforms. The IAM team received clear and simple integration points where they could ingest platform data to increase coverage of access permissions for ongoing and annual certification campaigns. The security team received the risk reporting and remediation they needed to meet compliance requirements while the platform teams were freed from tedious feeds management and sanitization processes.

SPHERE's approach in applying process, people, and technology to address the client's access governance control issues ensured the delivery of sustainable and effective controls to better protect the bank's customers and overall reputation.

Leveraging the proprietary SPHEREboard platform along with tech-enabled managed services, the client was able to remediate access governance control gaps across a broad range of stakeholders and technologies, thereby providing repeatable and accurate visibility of identities and entitlements across their environment.