SPHERE

CASE STUDY

Resolving Audit Failures: Strengthening Data Access Controls

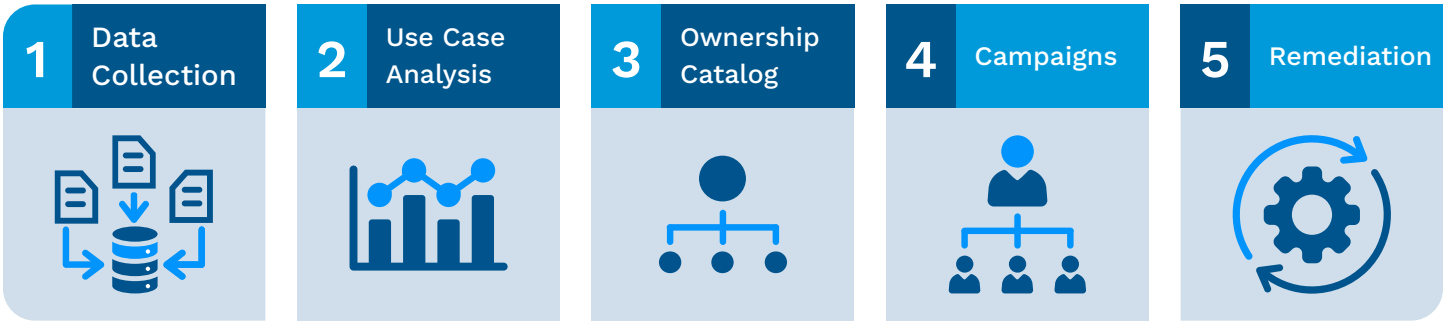
In one of the largest investment banks in the world, a high visibility audit revealed inappropriate access to project and application shares. Board-level stakeholders were made aware of the failed audit and the severity of the findings required immediate remediation of the access control issues. The investment bank first attempted to resolve the issues with internal tools and resources, but this attempt proved unsuccessful. SPHEREboard for Data was deployed to accelerate the remediation of these issues and reduce risk.

The Client

- Global Investment Bank
- 50,000 +Employees
- 100+ Offices
- 40+ Countries
- 1 Billion Permissions
- 600 Million Folders
- 250 Billion Files
- 500+ Servers

The Process

To remediate the inappropriate access to project and application shares, SPHEREboard leverages automation across these:



It was equally important to build a sustainable and repeatable process to ensure that the remediated shares remain compliant as per the defined policies and standards, and any new violations are highlighted with near immediate resolution.

The Challenge: Data Collection

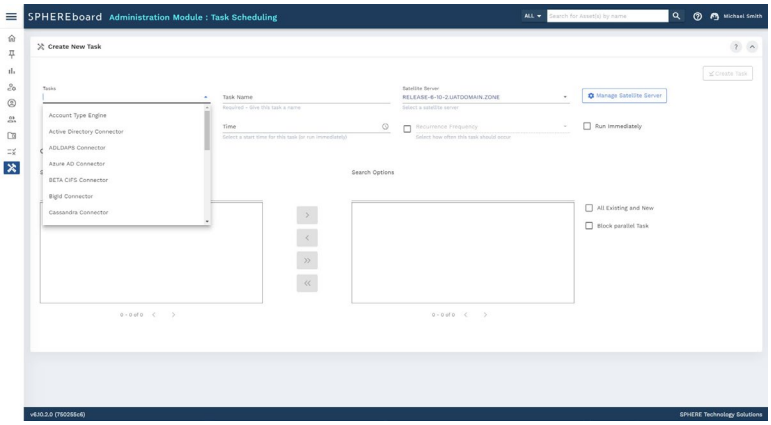
The client leveraged internally developed tools to scan storage devices on their network. However, process failures and limited functionality resulted in poor coverage and data inaccuracies.

Additionally, due to the combination of legacy and new storage devices within the environment, many different and nuanced data collection requirements were needed. The client also desired to take advantage of high-confidence datasets already in place, so that the necessary data could be incorporated into the source feeds to enable accurate analysis of the unstructured data environment.

It was also important to build a sustainable and repeatable process to ensure that the remediated shares remain compliant as per the defined policies and standards and that new violations are identified and immediately resolved including the root cause of the violation.

The SPHERE Solution

SPHEREboard first collected all existing datasets and determined the inaccuracies and data quality issues in these systems. The necessary adjustments were presented to senior leadership and changes made to provide a complete and holistic inventory of all data within the scope of the engagement. Additionally, all other books of record were integrated for accompanying data discrepancies.

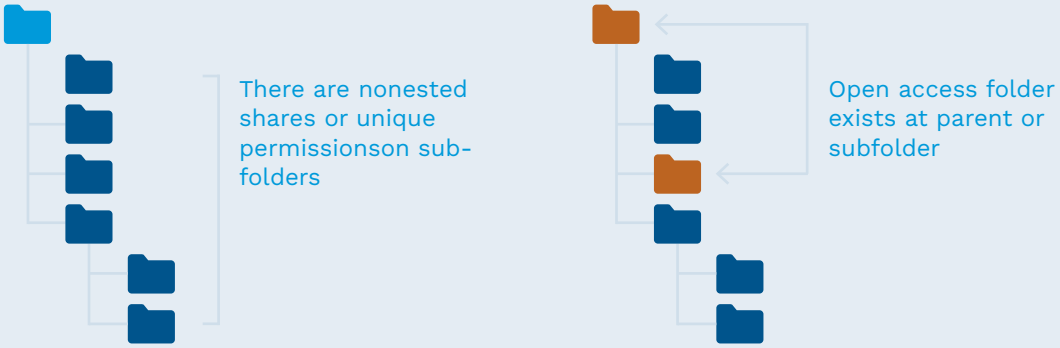


Next, connectors and feed ingestors were deployed to gather the data continuously and processed into SPHEREboard. Additional referential data sources to add context to the permissions information were also deployed. This included multiple HR feeds, as well as four different books of record used across varying business areas for Active Directory group data and unstructured data ownership information. This provided the client for the first time a holistic and complete inventory of shared data and permissions across their storage services.

Within the first 30 days, SPHEREboard was able to demonstrate that the incumbent processes covered only ~10% of the entire estate and the client was unaware of the extent of the missing data and control gaps. Additionally, data collection shifted from a one-time exercise to a scheduled and recurring refresh process.

The Challenge: Use Case Analysis

The customer understood that there were likely many configurations of shares, folders and permissions that will be problematic from a standard automated remediation perspective and these needed to be investigated more precisely. Below is an example of a common scenario the customer knew would be troublesome; open access buried inside a folder structure where the permissions deviated across parent and child folders.



In addition, the customer understood that different processes for remediating different use cases was important to understand and flexibility into how remediation steps were configured was paramount. This includes whether the shares were actively being used versus likely to be stale, as well as, whether the shares were used in the traditional file sharing scenario versus potentially integrated to an application workflow. Finally, the ability to overlay security risks and violations was of key to remediation prioritization. The extent of these scenarios and metrics related to these concepts were also unknown.

The SPHERE Solution

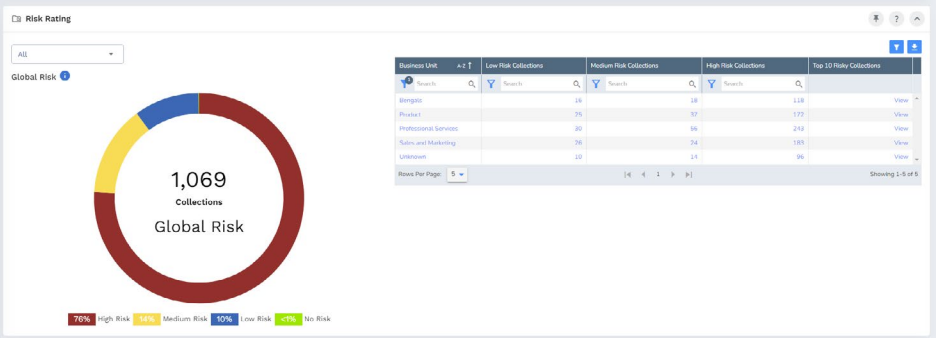
SPHEREboard's ability to collect all feed source data, referential data and existing books of record came first. This information was normalized and enabled the client to leverage analytics and metadata to categorize the file share data, identify in-scope shares and establish for each share whether it was used for user data or application data.

Next, SHEREboard's engines provides deep insights into:

- Open Access
- Excessive Access
- Inappropriate Access
- Direct Permissions
- Stale Data
- Inheritance

As these metrics were compiled, summarized views of Risk Rating was provided to the customer. SPHEREboard also identified various scenarios that were known to be nuanced and created additional complexity. These included:

- Shares with subfolders not inheriting from the parent and with different permissions
- Shares with a subfolder where the owner is different than the parent
- Shares where the SPHERE service account does not have permissions
- Shares with corrupt files or folders



Knowledge is power. By leveraging SPHEREboard, complex and nuanced risks were assessed and where appropriate remediation was directed to automated workflows to address issues or, in several small cases, manual remediation was undertaken. This approach ensured the stability and continuity of storage services and the customer remained unaffected.

The Challenge: Ownership Catalog

The client had missing and/or conflicting ownership across CMDB and other books of record meaning they were unable to align data to specific business areas with any accuracy. This resulted in the business areas inability to report Key Risk Indicators across their respective areas and subsequently unable to understand the risks they were carrying. In addition to ownership identification, SPHERE was engaged to provide controls and subsequent control assurance that Ethical Walls were in place and operating effectively. Concerns had been raised regarding the exposure of Investment Banking / M&A data potentially residing in unstructured data repository where Ethical Wall controls were not enforced. This was a critical deliverable that was top of mind for Audit and IT Executives.

The SPHERE Solution

SPHEREboard provides numerous pre-built methodologies that can be leveraged for assigning ownership across the file shares. This includes, but is not limited to, understanding home drives and the associated owner, reviewing AD groups that had access and their associated owners, reviewing the majority manager and/or majority department to deduce likely ownership, etc. In addition, there were a number of manual efforts made by the client in regard to the ownership catalog that were incorporated into the analysis. A total of 8 different methods were used in an incremental approach, and ownership was assigned to 95% of active shares.

Mapping owners to business units and departments was a key milestone enabling summarized metrics to be shared with Business Information Security Officers (BISOs), Help Desk, Change Management, etc. Additionally, a significant amount of Investment Banking owned data was discovered in areas where it should not be. This resulted in emergency data migration and establishing automated controls to identify reoccurrence of the issue and the process at fault.

The Challenge: Owner Outreach

Due to the varying ownership catalogue methods, it was critical to confirm ownership and allow cataloged owners to confirm, reassign or alert if this was unknown. This could be a prime opportunity to also allow confirmed owners to seamlessly provide feedback on who should or should not have access to the file shares they owned.

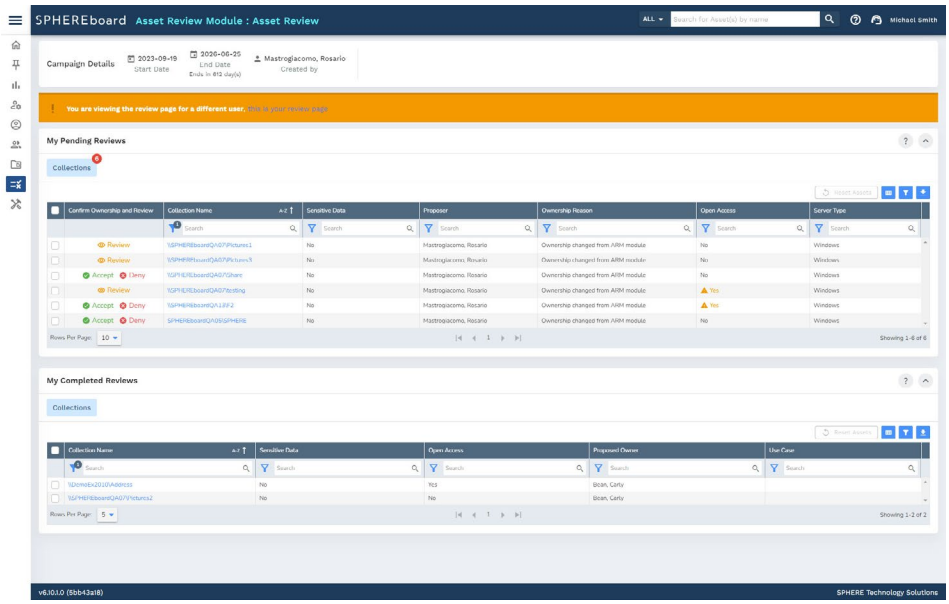
The client also had an understanding that owner outreach to areas of the bank that are considered sensitive must be handled delicately. These required very specific language, conservative frequencies of reminders and defined escalation procedures related to unresponsiveness. At the same time, the client felt comfortable taking a more aggressive approach on file shares that potentially contained very sensitive and confidential data i.e. HR folders, along with file shares used by back office functions i.e. IT. The ability to cater to different scenarios was highly sought after in the final solution.

The SPHERE Solution

SPHERE used the ownership data within the SPHEREboard Asset Review Module (ARM) to campaign with these accurate data owners with actionable intelligence for upcoming remediations.

SPHEREboard's flexibility allowed for multiple iterations of campaigns which were based on the various dissections of ownership and requirements defined by the client. These campaigns were aligned with Corporate Communications policies and processes, ensuring that language and format options were factored into the campaigns. Different automated escalation paths to deal with unresponsive owners, and different tones based on title and region, were implemented.

Additionally, the customer stressed 'certification fatigue' by the end users could become an issue. More specifically, there were too many variations of surveys and questionnaires with varying formats and workflows, and this became a nuisance for the data owners who constantly had to learn a new system and interpret the verbiage presented to them. To solve this, SPHERE leveraged customization options within the Asset Review Module (ARM) to mimic the most used system, so the end user community was mostly unaware that this was a new system reaching out to them for various confirmations and information.



The Challenge: Remediation

The client required prompt remediation activities immediately after owners provided their responses. Prior internal approaches were very manual and there was a significant delay between owner's responses on who should or should not have access, and the accompanying permission changes. This resulted in key personnel losing access to data during ad hoc remediation attempts.

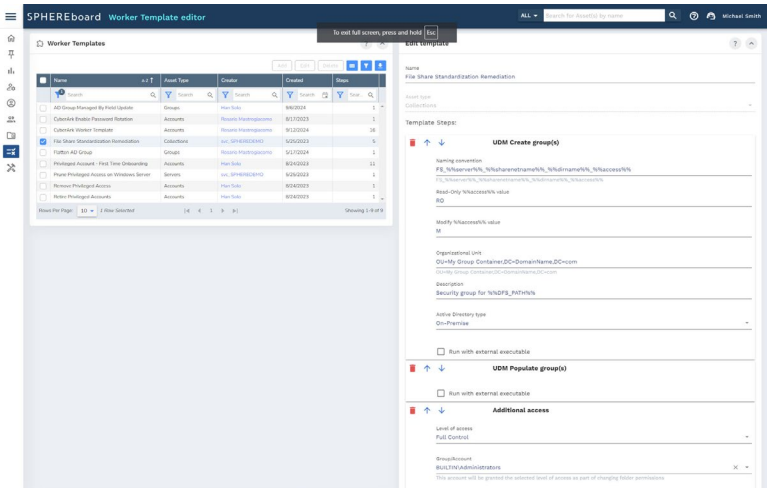
Also, as with most of our engagements, the client required SPHEREboard to integrate with their existing provisioning and entitlement management processes and tooling. This was necessary to ensure all books of record were in sync and mimicked the source of truth that SPHEREboard presented.

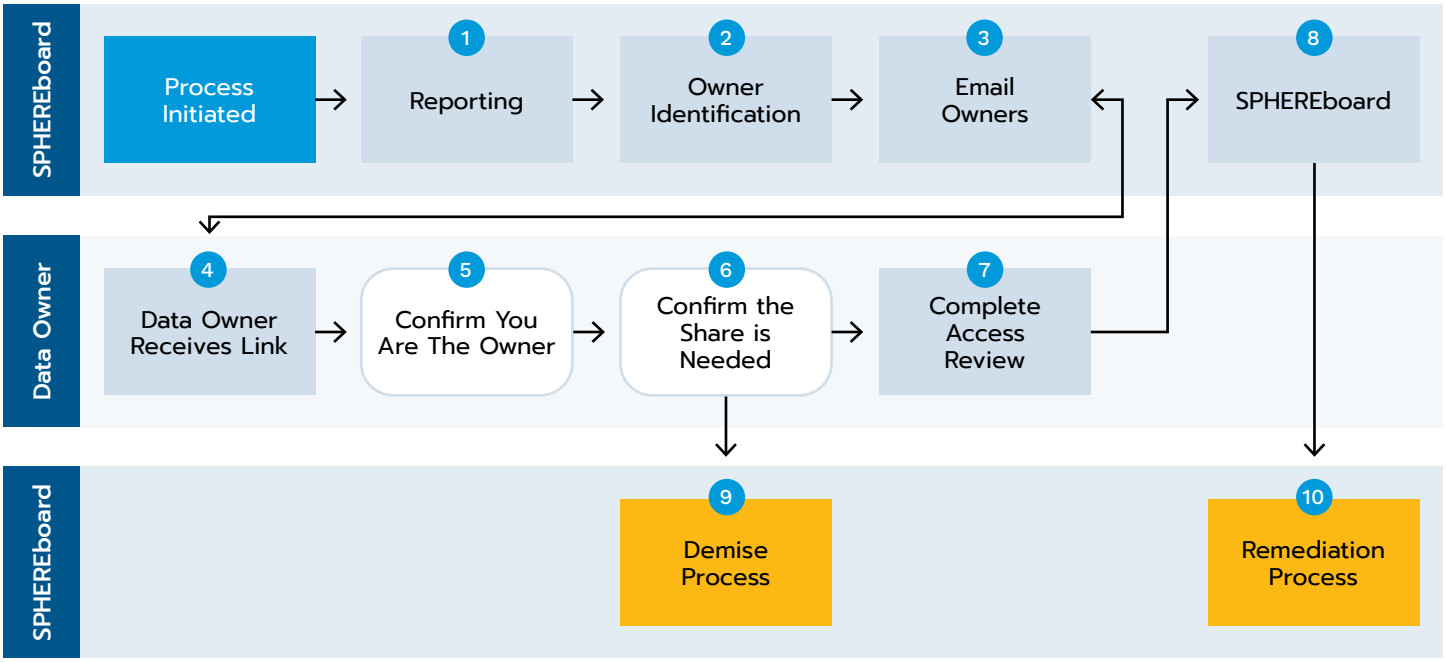
Finally, Audit requirements stated that all file shares must now follow policies related to a standardized set of entitlements.

The SPHERE Solution

Since internal policies and requirements presented some specific requirements of the overall remediation process, SPHEREboard's ability to be highly customized was leveraged. This was essential to ensuring the audit findings were resolved with limited friction and minimized risk of business disruption.

Additionally, a distributed architecture at a regional level for scalability and to meet local compliance requirements was deployed.





The functionality of SPHEREboard's Virtual Worker platform was used to make API calls, connect to necessary source systems and maintain accuracy in the system itself, for:

- Group creation, deletion, and membership modification
  - Add users to standard AD groups
  - Remove users from the standard AD groups
  - Remove non-standard users from the standard AD groups
  - Remove heavy nested groups
  - Leverage standardized existing groups when they exist
- Ownership changes
- Permission changes – including standardizing all permissions throughout directory structure
- Logging for audit and reporting

All of this occurred with pre-change and post-change reports for simple rollback and the maintenance of these details for future internal audit requirements.

Finally, to attain the desired end state regarding permissions standardization as per documented policies, SPHEREboard was successfully embedded into their processes and remediated with these policy assurances:

- Read-only and a read-write group for each share
- Free of heavy and circular nesting
- Removal of access for stale shares
- Updates applied to all the various books of record
- Monthly reporting of shares ready for migration off expensive storage

The result was standardized access, which was applied holistically across the environment, removing nested permission, correcting inheritance across the folder hierarchy, resolving technical issues i.e., broken ACLs that impede ongoing reporting, and ensure all security issues are resolved.

Conclusion

Through SPHEREboard, the client was able to reduce risk immediately due to remediation of many of their access control challenges. In additional to fast discovery and effective remediation, SPHEREboard was able to help the client provide periodic reports regarding the resolution of their outstanding access control issues, which resulted in a reduction in the severity of the audit.

All of this allowed for immediate risk reduction reduction and sustainability for long-term value.

The result: reduced risk, no more failed audits due to access governance, and a more effective process for ongoing management of access control.

About SPHERE

SPHERE is the global leader in Identity Hygiene. We are dedicated to reshaping modern identity programs by embedding this foundational fabric, enabling organizations to quickly reduce risks. We work through an identity lens that protects an organization's accounts, data, and infrastructure. Our solutions deliver immediate time-to-value by leveraging automation to discover, remediate and secure identities, now and forever.

Driven by our core values of passion, empathy, and authenticity, our vision drives us to continually innovate, helping our clients to sleep better knowing their attack surface is drastically reduced, thwarting the plans of bad actors every single day.

We're ready to help you address your Identity Hygiene and security challenges. To find out more about SPHERE and our solutions, please visit www.sphereco.com.

