

Building a Foundation for RBAC



Case Study

Client Profile

- Premier investment company in the US offering more than 300 mutual funds, retirement services, discount brokerage services, estate planning, wealth management and life insurance.
- Strong commitment to continuous improvement, state-of-the-art technology and unparalleled customer service.
- Responsible for innovations that are standards in the industry today.
- The company reinvests a substantial portion of its revenue each year back into technology to deliver new products and services to investors.

Key Challenges

- Like most organizations the need to comply with both government regulations and internal security audit controls.
- The client identified the need to implement a Role Based Access Control (RBAC) model to address the internal audit findings.
 - The company had a well-defined process to handle the disabling and deleting of user accounts upon termination, but the challenge was giving existing users and provisioning new users the correct access for their job responsibilities.
 - Transferred users had entitlements that were carried over from their previous job function.
 - For a new user, the process was to create one by mirroring an existing account. This often resulted in the new user gaining extra access rights.
 - There was no complete and efficient process to review user entitlements.

Solution

The client required a tool which provided comprehensive role engineering and role management functionalities.

Simeio Solutions was brought onboard to utilize the leading role management technology to assist the organization in the creation of roles.

Simeio Solutions was able to define enterprise and departmental roles across three platforms and 88 applications. Once users were assigned to roles the client was able to leverage the Role vs. Actual Analysis feature to identify any entitlement that was not required for a user.

Additionally, the client was able to empower the Business Unit/Manager representatives to certify/revoke user entitlements. This was done using the glossary feature, which allows technical entitlement names to be replaced by business-friendly terms.

Implementation Highlights

Building The Identity Warehouse

The global user information was imported into the Identity Warehouse from an authoritative source maintained by the client for its users. The RBAC system received nightly feeds from the authoritative source to import data for approximately 5,000 global users which were part of two business units.

The system was then configured to receive data feeds from three platforms -- Active Directory Services, UNIX and Top Secret/Mainframe. Additionally, the RBAC system received data feeds from 88 applications classified as tier A and B (high priority Applications) by the client. These data feeds were used to build account information for the global users.

Role Mining

Simeio Solutions used a hybrid approach for role mining. Users were grouped by 'Managers' and mining was conducted for each group. Initial mining was carried out across the three major platforms to identify clusters of users based on their entitlements. Roles were created based on the mining results.

As the next step, the roles which were created based on the three platforms were extended to add attributes from the additional 88 Tier A & B applications. This was accomplished by utilizing the role entitlement discovery process. During this phase, entitlements were added to a role based on certain correlation percentage among the users that belonged to the particular role.

Simeio Solutions worked with the business unit representatives to review the entitlements that are part of each role and users assigned to the role. Business unit representatives, with the help of subject matter experts within their group, decided the final composition of the role.

Additionally, auxiliary roles were defined for entitlements which were not part of the main role. A parent-child relationship was then established between the main role and the auxiliary role.

Business Unit representatives signed off on the Roles and 'Role Owners', who would become responsible for any changes made to the role(s) definitions, were identified. Based on the exception reports generated from the RBAC system, business unit representatives initiated the clean-up process to remove all the extra accesses each user had.

Glossary definition

Subject matter experts from the client and Simeio Solutions worked together to define glossary for over 10,000 different access levels across the three major platforms.

Outcome

- The role engineering process resulted in the creation of 267 roles for 3,700 employees and contractors (230 Employee roles and 37 Contractor roles). The 267 roles were created across three platforms (Active Directory, UNIX and Mainframe) and 88 applications.
- Business-friendly descriptions are now available for 85% of the entitlements across the three platforms and 88 applications. This was achieved in one month.
- User entitlement clean-up process was initiated based on user exception reports resulting in over 3,000 account deletions in Unix and removal of AD groups that were no longer used.
- The advanced features in the RBAC system were used to create roles, assigning entitlements to roles and identifying exceptions between user's current access and existing access.
- The role mining and role entitlement discovery capabilities were utilized to define roles in a significantly shorter timeframe than compared to the manual process that was previously used.

Next Step

- The client is actively working with the RBAC system to export the defined and approved roles into their existing homegrown provisioning application.
- Future plans will be to integrate the RBAC system with a leading provisioning system.
- The client has also expanded the scope to include additional departments, platforms and applications to define roles, which will continue to improve operational efficiencies.

About Simeio Solutions:

West Coast operations
3900 Kilroy Airport Way
Suite 270
Long Beach, CA 90806
Fax: (562) 424-3800
Phone: (562) 424-3600
Visit us at www.simeiosolutions.com

East Coast operations
Hoboken Business Center,
50 Harrison Street, Suite 314
Hoboken, NJ 07030
Phone: (201) 239-1700
E-mail: info@simeioolutions.com