IAM Automation to Achieve
Key Business Objectives

Industry – Financial Services

About the Client

The client is a publicly traded, full-service bank operating over 150 branches across New Jersey and New York.

IAM Initiative Goals

» Centralize and automate IAM
» Timely access provision & de-provision
» Scalable and sustainable data format and quality
» Standardized policies across IAM environments
» Establish governance, accountability, and visibility

Background

The client lacked a centralized Identity and Access repository, policies, and standards. Their access review and provisioning process was manual and not scalable to support business growth. There was also a lack of roles' definition outside of retail banking to be able to enable enterprise wide RBAC. Data quality and format was a concern where it was not scalable nor sustainable. Managing IAM for most organizations is a challenge and the client would be experiencing the same had they chosen to go in-house to achieve their goals. The client wanted to onboard a provider who would manage IAM end to end and help achieve the goals the bank had set for itself – both for security and for the business.

Technical Challenges

» Lack of centralized Identity and Access repository
» Non-scalable and manual access review and provisioning process
» Lack of roles' definition outside of retail banking
» Input data format and quality not sustainable or scalable.
» Manual management of requests and fulfilment.
» Lack of audit trails.

Business Challenges

» Lack of enforcement in terms of policies and standards across IAM environment.
» Need for common policy and process standards across bank through automation.
» Delayed provisioning and de-provisioning of access.
» Unable to provide joiner day 1 access and de-provision access for leavers in a timely manner.
» Unable to transition access timely for movers, leading to mis-management of movers/transfers and causing delays.

Approach

With Simeio's Managed Services for IAM, the client was able to manage and improve management of identities and access using one central IGA repository.

» Create and maintain a single IGA repository of identities and accounts.
» Streamlining processes
» Provision timely and accurate joiners, movers and leavers
» Put better governance structure
» Reduce audit findings
» Mitigate security risks of over provisioning.
» Keep access in check by conducting access certifications

The Solution

IAM Automation

- Application Onboarding - Established factory onboarding methodology for automated onboarding of applications
- Access Governance – Through scheduled timely and automated certifications. Policy driven access control enforcement.
- User life cycle Management - Provisioning & Deprovisioning of user lifecycle events of Joiner, Mover and Leavers
- Auxiliary Use Cases - Leave of Absence, Return, Title changes & other misc. cases.
- Governance & Monitoring - Governance, risk and compliance monitoring and dashboards.
- User driven or on- demand requests - Proactive processes to support user driven or on-demand requests.
- Least privilege model adoption and auditability.
- Optimize Password Management processes.
- Reporting and auditing analytics and user behavior profiling.
- Positive outcomes for SOX and regulatory reviews and audits.
- Role-based access control and provision/de-provision for multiple departments.
- Established ETL process for application data consumption.
- Non-employee employment verification campaigns.

IGA Management:

- Provisioning of users to Active Directory and mailbox connected birthright security groups using Saviynt Platform.
- Managing user lifecycle (JML) based on the client's rules configured in the system.
- Simeio team will monitor the IGA solution and open, respond and assist in coordination with product teams towards resolution of open tickets assigned towards the Saviynt platform.
- Simeio team will be responsible to update connection, resolve connection related issues, etc. if an already on-boarded application fails connection.
- Assist with monitoring of the jobs, respond to alerts in case of job failures etc.
- Update runbook and manage day-to-day maintenance tasks.

The Solution

Enhancement

- Development tasks included were integrating additional application using flat files and/or OOTB connectors.
- Development of new workflow(s) for newer systems, or assisting with re-doing, if required, current workflows.

- Developing communication templates and configuring schedulers.
- Efforts for requirement gathering, development, QA/testing, UAT with the client migration to environments and documentation.

Impact

In the first year of this project implementation, Simeio successfully completed the Go-live for the Saviynt platform on the Simeio Cloud. This was followed by the integration with ADP and Active Directory as authoritative sources. Simeio managed and automated the user lifecycle for leavers (voluntary and ASAP) and for joiners as well as, movers, conversions, and auxiliary use cases were automated. Over 4000 J-M-L tasks were automated that provided audit history while saving costs and improved efficiency. Timely terminations ensured access is taken away in time to mitigate security risks with any non-terminated accounts.

4000+
J-M-L Tasks
Automated

75%
less man hours to prepare, launch & complete Certifications IGA platform automation

Why Simeio

The client found a unique and strategic partner in Simeio with its comprehensive suite of enterprise Identity and Access Management ("IAM") capabilities. Simeio enabled the clients with better, faster, economical and effective IAM, in comparison to what the organization would have achieved building solutions on their own or "in-house".