

Identity Management Solution for Robust Security and Audit Readiness

Client Overview

One of the largest financial services institutions in the Sultanate of Oman with over 150 branches in the region, 4000+ employees, and a strong presence in corporate banking, personal banking, investment banking, islamic banking, treasury, private banking and asset management.

The Business Situation

The banking firm handles massive amounts of sensitive data and transactions every day, and felt it imperative to have complete visibility and control over employee IT access. The organization was also keen on addressing the Business, IT, Audit and Operational issues relating to Identity Governance, in order to fulfill regulatory compliance mandates. The primary objectives of the Identity Management program were:

- Comprehensive insight into user accounts and privileges
- Enforcement of role-based access policies, in alignment with compliance requirements
- Automation of Joiner-Mover-Leaver (JML) processes for faster provisioning and better risk management
- Workflows and Reporting to support identity governance and internal audit functions
- Automated techniques for data quality control

The Solution

Long 80 performed an exhaustive analysis of the workflows and relationships between the applications and the 4000+ users, and determined the number, complexity, criticality, and business impact of the applications, systems and databases that needed to be onboarded. With this information, and a detailed evaluation of their current risk posture, SailPoint's IdentityIQ solution was recommended to streamline and automate their identity governance processes. Over 30 applications including Banking, HRMS, Fraud Monitoring, SIEM, and IVR were integrated with the IAM platform. Role-based access control - including Role Lifecycle Management and Periodic Role Attestation - was designed & implemented. The solution was architected to support processes like Access Reviews, Certifications and Remediation. Custom reporting capabilities were built, and ready-to-audit documentation was made available across the IAM lifecycle (on-boarding, off-boarding, job change & transfer).

Challenges

-  Lack of visibility into user accounts and privileges
-  All-round inefficiencies, provisioning delays and security & compliance vulnerabilities due to manual JML processes
-  Insufficient support for compliance and internal audit functions
-  Inadequate reporting capabilities
-  Data quality issues due to manual conservation techniques

Solution Highlights

-  Integration of IdentityIQ with 30+ applications including HRMS & SIEM
-  Automation of JML processes
-  Role-based access control
-  Automated workflows for routine processes like decommissioning dormant/orphaned accounts
-  Proactive identification/remediation of access controls to eliminate security vulnerabilities
-  Centralized auditing & audit-ready documentation to support identity governance
-  Enhanced framework for automated reporting across the IAM lifecycle

Solution Outcomes

-  Unified risk view due to integration of IdentityIQ with 30+ applications
-  Process efficiencies, robust security & improved regulatory compliance through automation
-  50% reduction in TAT for access requests
-  Improved UX due to quicker sign-ons
-  Effective identity lifecycle management
-  Strengthened risk management & data quality conservation through proactive approach
-  Drastic reduction in time for audits
-  Enhanced governance - 360° view for processes like Access Reviews
-  Holistic visibility and deep insights through reports