CASE STUDY

A Public Sector Bank

Overview

The client is Indian nationalised bank under the ownership of Ministry of Finance, Government of India with its head office located in New Delhi. As of 31 March 2020, the bank has 1526 branches which are widely spread across India, and 25 zonal offices located all over India.

As a result of the growth of new banking products, the bank required a strategic technology plan to implement new systems over the period. Identity management was a key aspect of this reorganization.

The client approached ProcessIT Global, to implement a full IDAM stack across their entire organisation, hoping to boost productivity— while untethering employees from a traditional office setting. Also, being able to manage identities, roles, accesses from one single platform, would reduce the user dependency on system administrators.

Challenge

Below were some salient customer pain points

Hierarchical access rights: The client was facing a hard time managing role-based provision of access to its critical resources. As the client operates within a critical and highly impactful data environment, it was a necessity to ensure data security within the organization.

Single-Sign-On: Users were required to remember three to five usernames and passwords and log into the bank's systems one-by-one, which was time-consuming. For the employees it was very difficult to deal with multiple credentials for each of their applications, and they needed a unified platform that allows their users to access the resources and governs their access at the same time

Solution

Strategic implementation of Identity Manager and Access Manager was done by PITG to meet the client's needs.

Implementation of Identity Manager to manage user on-boarding, all usernames and passwords on the network, employing password management policies such as password strength assignment, periodic password change, and password blocking after several failed attempts, and user offboarding.

Implementation of Access Manager to provide single sign-on access to all web-based applications with multi-factor authentication via tokens.

Implementation of Identity Governance to manage hierarchical access rights based on their position in the company.

Results

Successful implementation of the solutions in the client's environment secured it from the vulnerabilities controlled in an efficient manner.

Improved security: The solution improved overall security standards inside the organization. Password management is more tightly regulated.

Access governance: Hierarchical access rights ensured that employees can only access information, which directly corresponds to their role

Reduced dependency: self-service portal allows users to reset their own forgotten passwords and it resulted in significant reductions in the administrative workload of its IT team.