Ideation phase
Define the problem statements

Date:2 november 2025

Team id: NM2025TMID00414

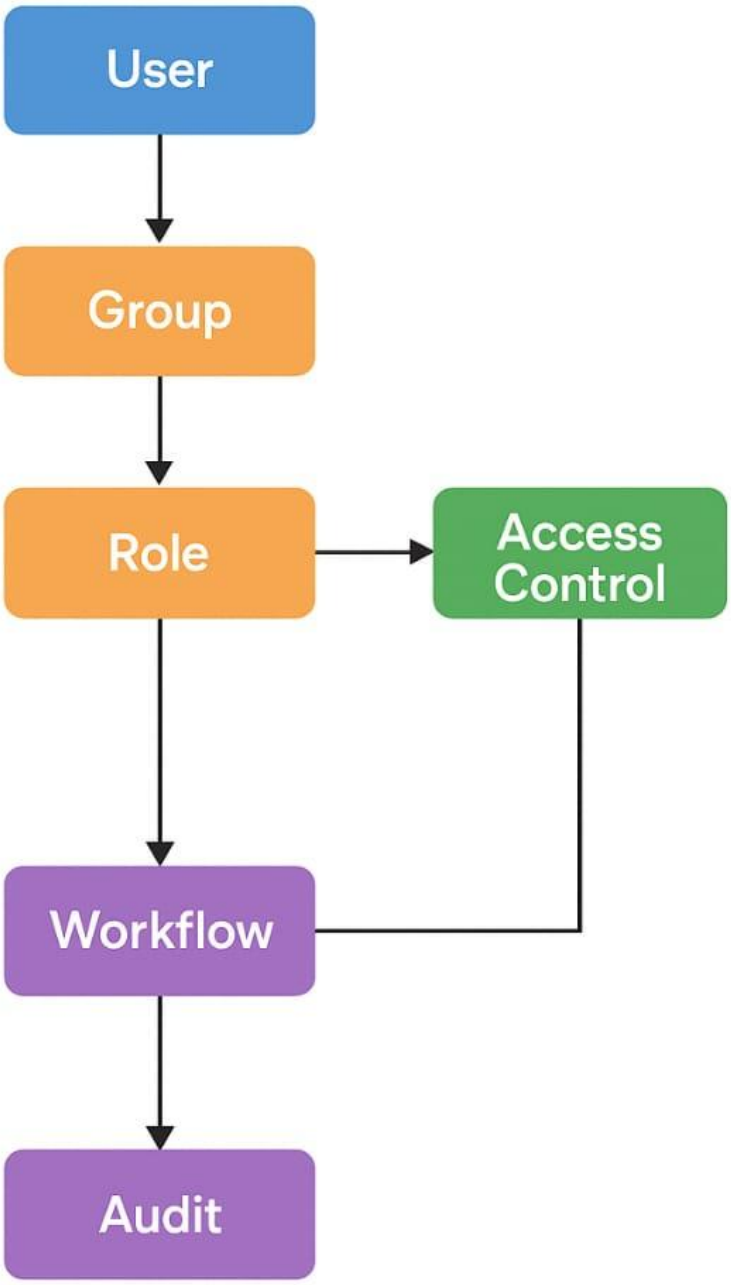
Project name: optimizing user, group, and role management with access control and work flows

Customer problem statement template:

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” focuses on solving inefficiencies in how organizations manage user identities, roles, and permissions across systems. Currently, user and role management is largely manual, leading to errors, security risks, and delays in onboarding and access approvals. Customers face challenges such as unclear role definitions, inconsistent access control, lack of automation in approval workflows, and limited visibility into who has access to what.

The goal is to create an automated, centralized solution that streamlines user, group, and role management with clear access policies and integrated workflows. This system will automate user provisioning and deprovisioning, enforce role-based access control, and provide audit trails for compliance. As a result, organizations can reduce manual effort, strengthen security, accelerate access approvals, and ensure full visibility and accountability in access management processes.

Optimizing User, Group, and Role Management with Access Control and Workflows



Problem Statement 1: Inefficient Manual Access Management

Description:

In many organizations, user account creation, role assignment, and access revocation are handled manually by IT administrators. This process is time-consuming, prone to errors, and creates bottlenecks in onboarding and offboarding employees.

Example:

When a new employee joins the company, the IT team manually creates accounts across multiple applications (email, CRM, HR software). Sometimes, the user receives incorrect permissions or experiences delays of several days before all required access is granted. This leads to productivity loss and inconsistent access records.

Problem Statement 2: Lack of Centralized Role-Based Access Control (RBAC)

Description:

Organizations often lack a centralized system to manage user roles and permissions. As a result, access rights are assigned inconsistently, making it difficult to ensure security and compliance across departments.

Example:

A marketing manager may still retain admin access to financial data after moving to a different department because no automated workflow exists to update or revoke old permissions. This increases the risk of unauthorized data access and audit non-compliance.