# Ideation Phase

# Define problem statement

| | |
|---|---|
| Date | 2-10-2025 |
| Team ID | NM2025TMID07413 |
| Project Name | Optimizing User, Group, and Role Management with Access Control and Workflows |
| Marks | 2 Marks |

## Customer problem statement template

Organizations often struggle with managing a growing number of users, groups, and roles across multiple systems. Manual processes for assigning permissions, approving access, and handling onboarding or offboarding can lead to delays, human errors, and security vulnerabilities. Without a centralized access control system, administrators find it difficult to maintain consistency in role assignments, track user activities, and ensure

compliance with data protection standards. This lack of efficiency not only increases operational costs but also exposes the organization to potential risks such as unauthorized access or data breaches.

To address these challenges, there is a need to develop an automated and optimized system for user, group, and role management integrated with access control and workflows. Such a solution would streamline access provisioning, enforce role-based permissions, and automate approval processes, ensuring both security and productivity. By implementing workflow automation and centralized monitoring, organizations can enhance data protection, reduce administrative overhead, and maintain compliance with industry regulations. This approach enables secure collaboration and efficient governance across all user levels.

## Problem and solution table with example

| S.No | Problem | Description | Proposed Solution | Example |
|---|---|---|---|---|
| 1 | Manual User Management | Adding, modifying, or removing users manually is time-consuming and error-prone. | Implement automated workflows for user onboarding and offboarding. | When a new employee joins, the system automatically creates an account and assigns roles |

| | | | | |
|---|---|---|---|---|
| | | | | based on their department. |
| 2 | Inconsistent Role Assignments | Different users may have access to resources beyond their needs, increasing security risks. | Use Role-Based Access Control (RBAC) to assign permissions according to specific roles. | A marketing employee only gets access to campaign data, not finance reports. |
| 3 | Lack of Centralized Control | Managing users across multiple systems creates confusion and inefficiency. | Develop a centralized dashboard for user, group, and role management | Admins can view and modify all user permissions from one control panel. |
| 4 | Delayed Access Approvals | Manual approval processes slow down workflow and reduce productivity. | Automate access approval workflows with predefined rules and notifications. | Access requests automatically route to the department head for quick approval. |
| 5 | Poor Audit and Compliance Tracking | Difficulty in tracking access changes leads to non-compliance with security regulations. | Enable automated audit logs and reporting features. | System generates monthly access reports for compliance review. |
| 6 | Security Vulnerabilities | Unused or outdated accounts may still have access to sensitive data. | Implement automatic deactivation policies for inactive accounts. | If a user is inactive for 60 days, their account is automatically disabled. |

This table clearly connects each problem with its solution and provides a real-world example, making it easy to understand how the project will improve efficiency, security, and compliance in user and role management.

## Problem statement 1

Organizations face difficulties in efficiently managing users, groups, and roles due to manual access control processes and lack of automation. This leads to security risks, inconsistent permission assignments, delays in onboarding and offboarding, and challenges in maintaining compliance. There is a need for an optimized system that automates user and role management, integrates access control workflows, and ensures secure, efficient, and compliant operations across all departments.

## Problem statement 2

In many organizations, managing user access, group permissions, and role assignments is a complex and time-consuming process. The absence of centralized control and automated workflows often results in unauthorized access, duplicate accounts, and delayed approvals. These inefficiencies not only reduce productivity but also increase the risk of data breaches and non-compliance with security regulations. Therefore, an integrated solution is needed to streamline user, group, and role management with automated access control and approval workflows to enhance security and operational efficiency.