Ideation Phase

Define the Problem Statements

Date	1 NOVEMBER 2025
Team ID	NM2025TMID00309
Project Name	Optimizing User, Group, and Role Management with Access Control and Workflows
Maximum Marks	2 Marks

Customer Problem Statement :

Organizations face challenges in efficiently managing user access rights, group memberships, and role assignments within ServiceNow due to manual processes, fragmented controls, and lack of automation. This results in security risks, inconsistent access, increased administrative overhead, and difficulties maintaining compliance. The project aims to solve these problems by streamlining and automating access management through structured roles, groups, and workflows that ensure secure, scalable, and auditable user access aligned with organizational policies.

Customer Problem	Solution
Manual and error-prone user access management	Automated workflows for user, group, and role assignment
Security risks due to inconsistent access control	Robust role-based access control rules
High administrative overhead	Centralized role and group management
Compliance and audit challenges	Regular access audits and governance workflows
Delayed user onboarding and offboarding	Workflow-driven automation for onboarding/offboarding

Example:

Problem Statement (PS)	I am (Customer)	I'm trying to	But	Because	Which makes me feel
PS-1	IT Administrator	Manage user roles efficiently	Manual role assignments are error-prone	It causes inconsistent access	Concerned about security
PS-2	Security Officer	Ensure compliance	Frequent manual audits are time-consuming	System lacks automation	Frustrated

✅ **Problem Statement PS 1:**

IT administrators are responsible for managing user access and role assignments within ServiceNow. When the process relies heavily on manual intervention, it often leads to errors and inconsistencies in granting roles, which can create security vulnerabilities. This lack of automation makes administrators concerned about maintaining secure, accurate, and up-to-date access controls for all users.

✅ **Problem Statement PS 2:**

Security officers need to ensure the organization remains compliant with internal policies and regulatory requirements. However, the current system's manual approach to user access audits is time-consuming and prone to oversight. The absence of automated tools for monitoring and auditing user roles frustrates these officers, as it increases the risk of non-compliance and makes thorough, timely reviews difficult.