Ideation Phase

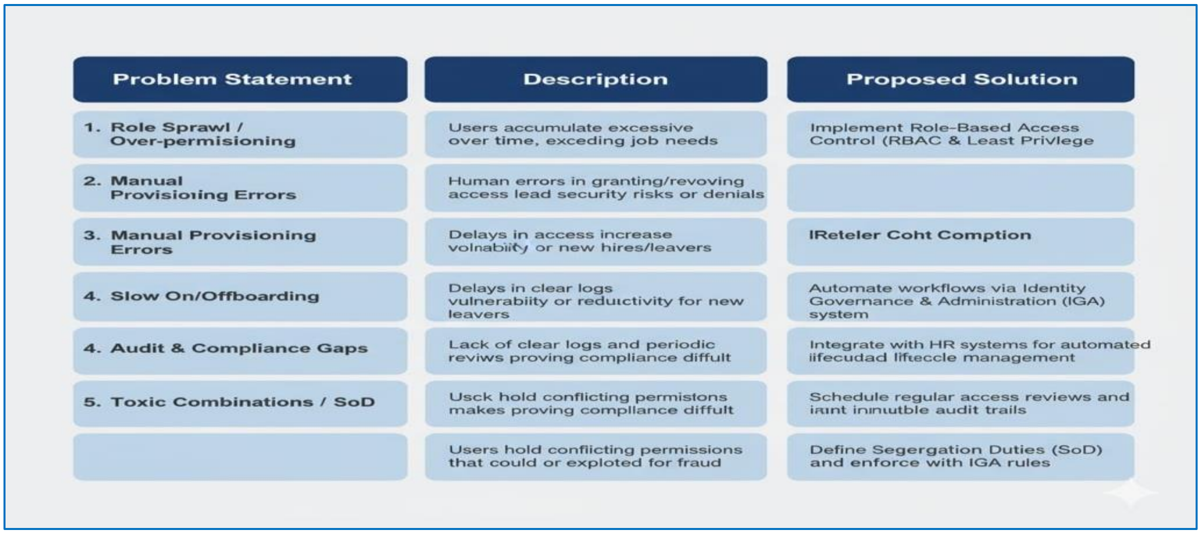
Define the Problem Statements

Date	31 October 2025
Team ID	NM2025TMID06082
Project Name	Optimizing user, group and role management with access control and workflow
Maximum Marks	2 Marks

Customer Problem Statement Template:

The customer faces significant challenges in managing users, groups, and roles across multiple systems due to manual processes and inconsistent access control practices. The lack of automation in provisioning, approval workflows, and role assignments leads to inefficiencies, increased administrative workload, and potential security risks. These issues often result in delays during onboarding and offboarding, limited compliance visibility, and greater exposure to data breaches.

To address these challenges, the customer seeks to implement an integrated access control and workflow management solution that automates user provisioning, enforces role-based permissions, and provides real-time monitoring. This optimization aims to enhance operational efficiency, ensure data security, and maintain consistent governance across the organization's digital ecosystem.



Problem Statement	Description	Proposed Solution
1. Role Sprawl / Over-permisioning	Users accumulate excessive over time, exceding job needs	Implement Role-Based Access Control (RBAC & Least Privlege
2. Manual Provisioıing Errors	Human errors in granting/revoving access lead security risks or denials	
3. Manual Provisioning Errors	Delays in access increase volnabiity or new hires/leavers	IReteler Coht Comption
4. Slow On/Offboarding	Delays in clear logs vulnerabiity or reduıctivity for new leavers	Automate workflows via Identity Governance & Administration (IGA) system
4. Audit & Compliance Gaps	Lack of clear logs and periodic reviws proving compliance diffult	Integrate with HR systems for automated iifecudad lifteccle management
5. Toxic Combinations / SoD	Usck hold conflicting permistons makes proving compllance diffult	Schedule regular access reviews and iaınt inmutble audit trails
	Users hold conflicting permissions that could or exploted for fraud	Define Segergation Duties (SoD) and enforce with IGA rules

Example:

Problem Statement (PS)	I am (Customer)	I'm trying to	But	Because	Which makes me feel
PS-1	A System Administrator	Assign user roles efficiently	The process is manual and inconsistent	There's no centralized access control or automation	Frustrated and overworked
PS-2	A Compliance Manager	Review user access across departments	Data is scattered and outdated	There's no workflow for periodic access reviews	Concerned about security risks

Problem Statement PS-1:

As a system administrator, I am trying to assign and manage user roles efficiently across various departments. However, the process is mostly manual and inconsistent due to the absence of centralized access control and workflow automation. This results in delays, errors, and repetitive work, leaving me frustrated and overworked.

I need an integrated solution that automates role assignment, enforces access rules, and ensures compliance while reducing administrative effort.

Problem Statement PS-2:

As a compliance manager, I want to review user access and permissions across multiple systems to ensure compliance and data security. However, the current process relies on outdated, scattered data and lacks a structured workflow for periodic access reviews. This creates risks of unauthorized access and audit failures, making me concerned about overall security. I need an automated workflow that streamlines access reviews, enforces accountability, and maintains up-to-date records for compliance reporting.