Project Design Phase

Proposed Solution

Date: 1 NOVEMBER 2025

Project Name: *Optimizing User, Group, and Role Management with Access Control and Workflows*
Maximum Marks: 2 Marks

Proposed Solution Template:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	In enterprise systems like ServiceNow, managing users, groups, and roles manually leads to inconsistent permissions, security risks, and inefficient workflows. There is no automated process to ensure correct access control or role synchronization.
2.	Idea / Solution Description	Implement automated workflows and access control mechanisms that manage user creation, group membership, and role assignment dynamically. These workflows ensure that changes in user roles are automatically reflected across the system while enforcing security policies through Access Control Lists (ACLs).
3.	Novelty / Uniqueness	The solution integrates **workflow automation**, **role-based access control**, and **real-time synchronization** within ServiceNow without relying on external tools. It brings together automation and compliance under a single, scalable framework.
4.	Social Impact / Customer Satisfaction	It reduces administrative workload, minimizes access-

		related errors, and ensures that employees receive the correct access promptly. This improves operational efficiency, data security, and user satisfaction.
5.	**Business Model (Revenue Model)**	Though not a direct revenue model, the solution leads to **cost savings** by reducing manual maintenance, improving accuracy, and lowering risks of security breaches — resulting in more efficient IT governance.
6.	**Scalability of the Solution**	The design can be extended to other modules like **Change Management, Asset Management, or HR workflows**. It also supports scalability for large enterprises with multiple departments or complex role hierarchies.

Solution Description:

To optimize user, group, and role management in ServiceNow, the proposed solution introduces **automated workflows** that assign, update, and revoke roles and access permissions based on predefined rules.

When a user is added or moved to a new group, the workflow automatically updates their access privileges and role mappings. **Access Control Lists (ACLs)** are used to enforce security boundaries and ensure that each user only accesses the data relevant to their role.

This solution eliminates manual dependency, enhances compliance, and ensures faster onboarding/offboarding processes. By combining workflow automation with robust access control, the system achieves improved **efficiency, consistency, and data security** across the organization.