Project Design Phase
Solution Architecture

Date	01 Nov 2025
TeamID	NM2025TMID09058
ProjectName	Optimizing User Group and Role Management with Access Control and Workflows
MaximumMarks	4 Marks

Solution Architecture

Goals of the Architecture:

- Automate and streamline user group and role management in ServiceNow.
- Enforce access control policies using ACLs and approval workflows.
- Maintain data integrity and prevent unauthorized role changes or deletions.
- Reduce manual intervention in access provisioning and revocation.

Key Components:

- sys_user table: Stores user profiles and related details.
- sys_user_group & sys_user_role tables: Maintain group memberships and assigned roles.
- Flow Designer workflows: Handle role assignment approvals and notifications.
- Access Control Rules (ACLs): Restrict unauthorized modifications to user and role records.
- GlideRecord scripts (Script Includes / Business Rules): Validate existing assignments and enforce logic before updates or deletions.
- Notifications and Audit Logs: Track and log every change to ensure compliance.

Development Phases:

1. Create test users and groups (e.g., IT Support, HR Team).
2. Assign roles to users via groups (e.g., “Incident Manager,” “Catalog Approver”).
3. Design approval workflow in Flow Designer for new role assignments or access elevation requests.
4. Implement ACLs and validation scripts to prevent unauthorized access changes.
5. Test scenarios for valid and invalid role changes, workflow approvals, and blocked operations.

Solution Architecture Description

The solution architecture is designed to enhance access governance and automation within the ServiceNow platform by optimizing how user groups and roles are managed. Instead of relying on manual updates, the architecture integrates Flow Designer workflows, Access Control Lists (ACLs)**,** and GlideRecord-based validations to enforce secure, policy-driven access control.

When a role or group assignment request is initiated, Flow Designer triggers an automated approval process that validates user eligibility, existing assignments, and potential role

conflicts. The GlideRecord logic checks relationships within the sys_user, sys_user_group, and sys_user_role tables to ensure that no unauthorized modifications occur.

If the system detects violations—such as conflicting roles, insufficient permissions, or unauthorized escalation—the operation is automatically blocked, and the admin is notified through the ServiceNow notification engine**.**

This architecture leverages native ServiceNow components, requiring no external integrations, making it both secure and easily scalable. It minimizes manual monitoring, ensures access consistency across modules, and strengthens organizational compliance and accountability through automated workflows and audit tracking.

Example-Solution Architecture Diagram: