Project Design Phase
Solution Architecture

Date	01 Nov 2025
TeamID	NM2025TMID07955
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 within ServiceNow.
- Enforce access control policies through ACLs and approval workflows.
- Maintain data integrity by preventing unauthorized role modifications or deletions.
- Minimize manual intervention in access provisioning and revocation.
- **Key Components:**
- **sys_user table:** Stores user profiles and related information.
- **sys_user_group** and **sys_user_role tables:** Manage group memberships and assigned roles.
- **Flow Designer workflows:** Automate approval processes for role assignments and send notifications.
- **Access Control Rules (ACLs):** Restrict unauthorized edits or deletions of user and role records.
- **GlideRecord scripts (Script Includes / Business Rules):** Validate existing assignments and enforce logic before performing updates or deletions.
- **Notifications and Audit Logs:** Record and monitor every change to ensure compliance and accountability.
-

Development Phases:

1. **Create test users and groups:** Set up sample users and groups such as *IT Support* and *HR Team* for testing purposes.
2. **Assign roles via groups:** Allocate roles to users through groups, for example, *Incident Manager* or *Catalog Approver*.
3. **Design approval workflow:** Use Flow Designer to create an approval workflow for new role assignments or access elevation requests.
4. **Implement ACLs and validation scripts:** Configure Access Control Lists and GlideRecord-based validation scripts to prevent unauthorized access modifications.
5. **Test scenarios:** Execute tests for valid and invalid role changes, approval workflows, and blocked operations to ensure proper functionality and security enforcement.

Solution Architecture Description

The solution architecture is designed to strengthen access governance and automation within the ServiceNow platform by streamlining the management of user

groups and roles. Rather than depending on manual updates, it 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 automatically triggers an approval process that verifies user eligibility, reviews existing assignments, and detects potential role conflicts. The GlideRecord logic cross-checks relationships within the sys_user, sys_user_group, and sys_user_role tables to ensure that no unauthorized modifications occur.

If any violations are detected—such as conflicting roles, insufficient permissions, or unauthorized privilege escalations—the system automatically blocks the operation and alerts the administrator via the ServiceNow notification engine.

Built entirely using native ServiceNow components, this architecture requires no external integrations, ensuring both security and scalability. It reduces the need for manual monitoring, maintains consistent access control across modules, and enhances organizational compliance and accountability through automated workflows and comprehensive audit tracking.

Example-Solution Architecture Diagram: