Phase 3: Project Design

DATE	2 NOVEMBER 2025
TEAM ID	NM2025TMID04324
PROJECT NAME	Optimizing User, Group and Role Management with Access Control and Work Flows

3.1 Introduction:

This project focuses on optimizing User, Group, and Role Management in the ServiceNow platform through effective use of Access Control and Workflow automation.
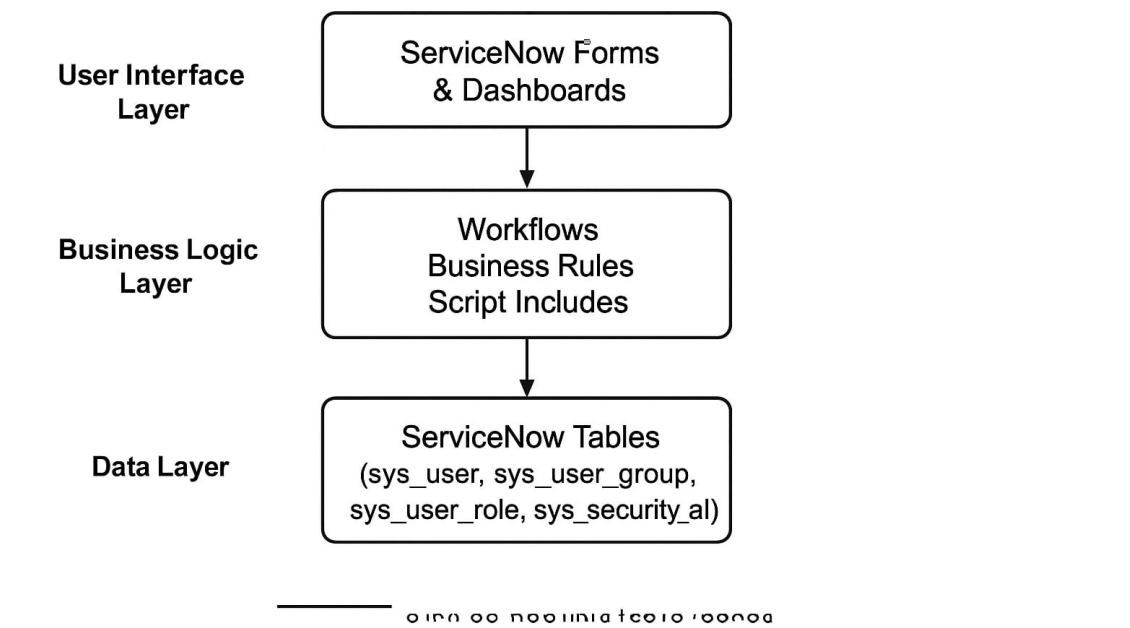
The goal is to create a secure, scalable, and automated system for handling user permissions, group memberships, and role assignments efficiently.

By integrating Access Control Lists (ACLs) and custom workflows, the system ensures that the right users have the right level of access to resources while maintaining compliance with organizational policies.

It minimizes manual administrative work, reduces errors, and enhances visibility into how access is granted and maintained across the platform.

3.2 System Architecture Diagram Description:

System Architecture Diagram Description
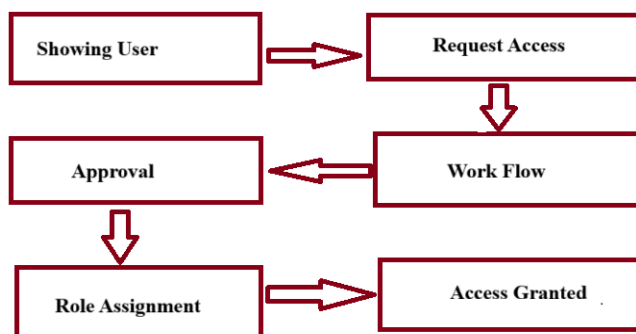
User Interface Layer → ServiceNow Forms & Dashboards

Business Logic Layer → Workflows / Business Rules / Script Includes

Data Layer → ServiceNow Tables (sys_user, sys_user_group, sys_user_role, sys_security_al)

The system follows a **3-tier architecture**:

Layer	Description
User Interface Layer	Provides forms and dashboards for managing users, groups, and roles.
Business Logic Layer	Contains workflows and business rules for automating approvals and access updates.
Data Layer	Stores user, group, role, and ACL information in ServiceNow tables

Working Flow:

- Administrator or Manager submits a request to create or update a user, group, or role.

- The workflow engine triggers approval or provisioning processes automatically.

- Once approved, Business Rules and ACLs validate the request and apply the updates.

- The system reflects the updated access permissions and sends notifications to the user.

3.3 Use Case Diagram Description:

Actor	Use Case
Administrator	Create, modify, and assign users, groups, and roles.
Manager	Request access changes, approve or reject workflow requests.
User	View assigned roles and access permissions.
System (ServiceNow)	Validate ACLs, trigger workflows, and update records automatically.

Primary Actor: Administrator

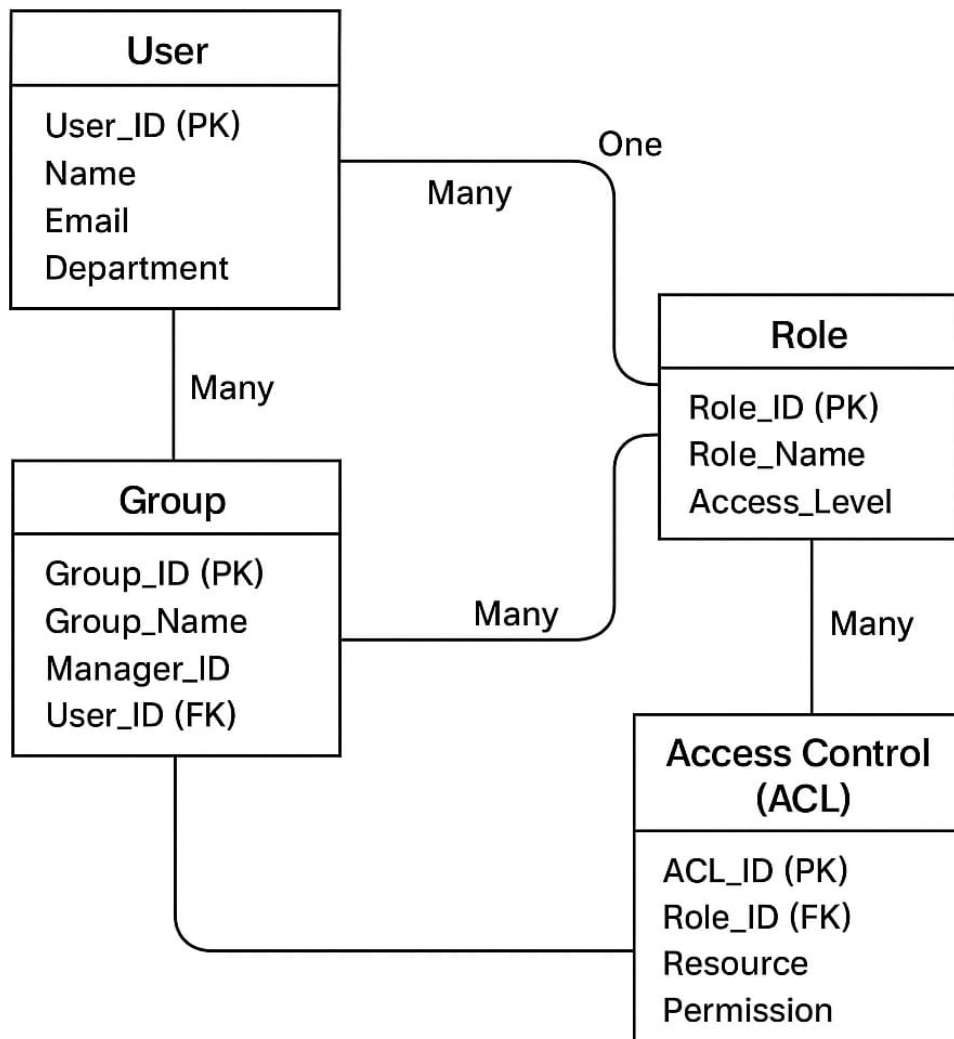**System:** ServiceNow platform

3.3 ER (Entity-Relationship) Diagram:

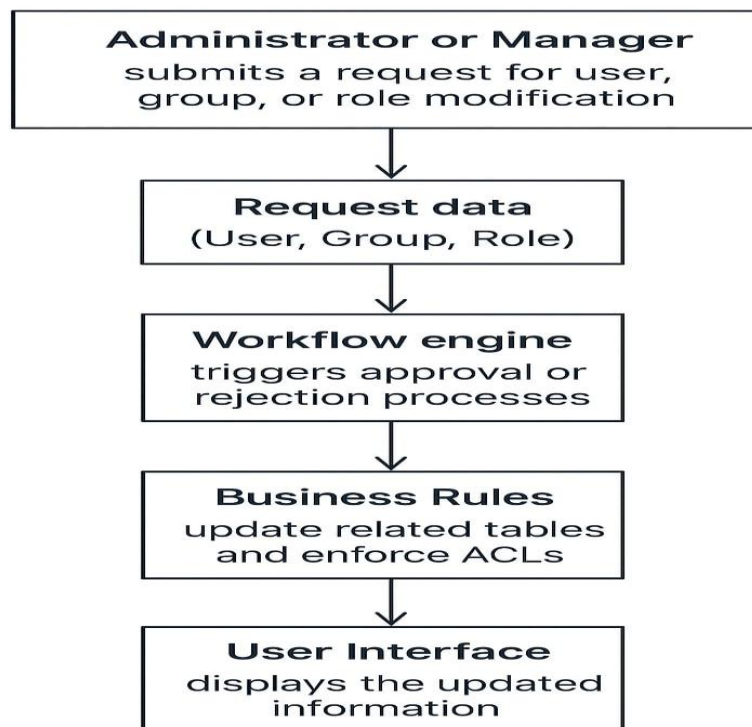| Table Name	Fields	Relation
User	User_ID (PK), Name, Email, Department, Role_ID (FK)	Many Users can be assigned to one Role
Group	Group_ID (PK), Group_Name, Manager_ID, User_ID (FK)	Many Users can belong to multiple Groups
Role	Role_ID (PK), Role_Name, Access_Level	One Role can be linked with many Users and Access Controls
Access Control (ACL)	ACL_ID (PK), Role_ID (FK), Resource, Permission	Defines access rules for each Role on specific Resources

Relationship:

User → Role: Many-to-One (Each user belongs to one role; a role can have many users).

User ↔ Group: Many-to-Many (A user can be in multiple groups, and a group can contain many users).
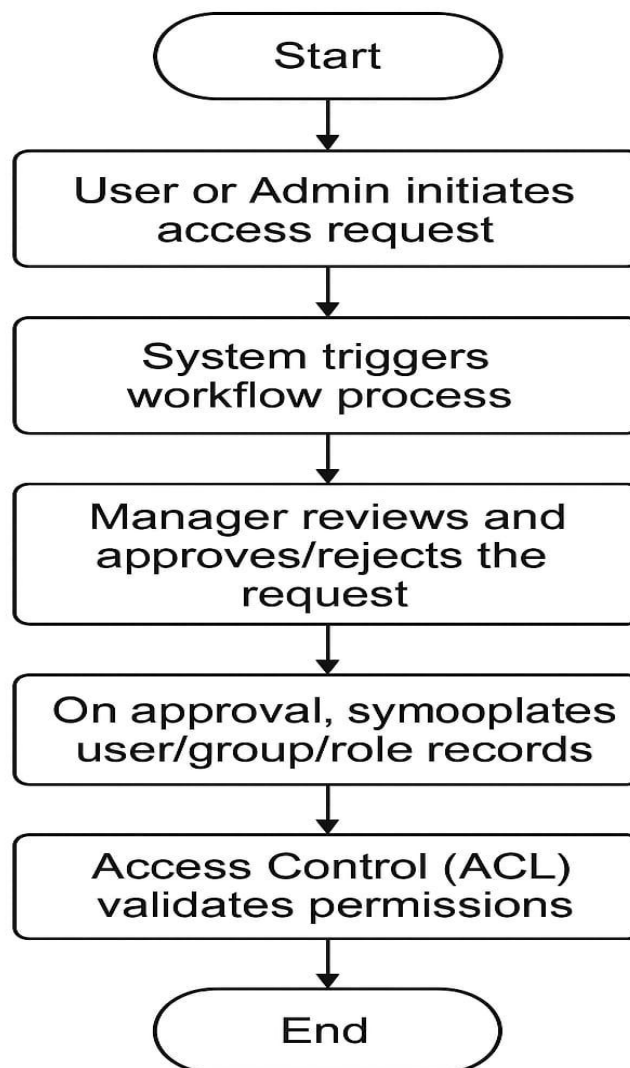
Role → Access Control: One-to-Many (Each role can have multiple access permissions defined through ACL).

Data Flow Diagram (DFD – Level-0):

Step	Action
1.	Admin or Manager submits request for user/group/role update.
2.	Workflow Engine receives and processes the request.
3.	Approval Process triggered automatically.
4.	Business Rules update respective ServiceNow tables.
5.	Business Rules update respective ServiceNow tables.
6.	System sends notification to requester.

3.6 Workflow Diagram Description

```
        ┌───────────┐
        │   Start   │
        └───────────┘
              │
              ▼
   ┌─────────────────────┐
   │ User or Admin initiates│
   │   access request    │
   └─────────────────────┘
              │
              ▼
   ┌─────────────────────┐
   │  System triggers    │
   │  workflow process   │
   └─────────────────────┘
              │
              ▼
   ┌─────────────────────┐
   │ Manager reviews and │
   │ approves/rejects the│
   │      request        │
   └─────────────────────┘
              │
              ▼
   ┌─────────────────────┐
   │ On approval, symooplates│
   │ user/group/role records │
   └─────────────────────┘
              │
              ▼
   ┌─────────────────────┐
   │ Access Control (ACL)│
   │ validates permissions│
   └─────────────────────┘
              │
              ▼
        ┌───────────┐
        │    End    │
        └───────────┘
```

1. Start
2. User or Admin initiates access request
3. System triggers workflow process
4. Manager reviews and approves/rejects the request
5. On approval, system update's user/group/role records
6. Access Control (ACL) validates permissions
7. Notification sent to requester
8. End

3.7 Summary:

This project design ensures efficient and secure management of users, groups, and roles within the ServiceNow platform. By integrating Access Control Lists (ACLs) and automated workflows, the system simplifies administrative tasks, enforces security policies, and reduces manual errors.

- The architecture enables:

- Streamlined access management

- Automated approval processes

- Role-based permission enforcement

- Real-time data consistency and scalability