

Project Design Phase

Solution Architecture

Date	29 October 2025
Team ID	NM2025TMID07101
Project Name	Educational Organisation Using ServiceNow
Maximum Marks	4 Marks

Solution Architecture:

Goals of the Architecture

- Implement a **centralized and secure access control system** for managing users, groups, and roles.
- Ensure **automated workflow validation** during creation, modification, and removal of user permissions.
- Maintain **data consistency** and prevent unauthorized access or misconfigured role assignments.
- Reduce manual administrative effort through **workflow-based automation** and dependency checks.
- Enable **real-time synchronization** of access updates across integrated systems.

Key Components

- **User Management Module** – Handles creation, modification, and deactivation of user accounts.
- **Group and Role Repository** – Stores hierarchical role relationships and access policies.
- **Access Control Engine (RBAC System)** – Enforces permissions and access boundaries dynamically.
- **Workflow Automation Module** – Manages approval flows for user and role requests.
- **Audit and Logging Layer** – Captures all access changes, workflow actions, and system events.
- **Notification System** – Sends real-time alerts to users and administrators on access updates or approvals.

Development Phases

1. **User and Role Setup** – Define sample users, groups, and roles within the system.
2. **Workflow Creation** – Configure approval workflows for adding, updating, or revoking access.
3. **Access Control Implementation** – Apply Role-Based Access Control (RBAC) logic with dependency checks.
4. **Integration and Testing** – Test all modules by simulating access requests, approval flows, and conflict scenarios.

5. **Validation and Monitoring** – Ensure the system maintains security, compliance, and accurate access tracking.

➤ Solution Architecture Description

The **solution architecture** is designed to optimize and automate the entire lifecycle of user, group, and role management.

It integrates **workflow automation** with **access control logic** to ensure secure and compliant operations within enterprise systems.

Whenever a user is added or modified, the system automatically checks their group and role dependencies before applying access permissions. A **workflow approval** process is triggered for any access change, ensuring that only authorized managers can approve modifications.

The **Access Control Engine** validates every transaction using **Role-Based Access Control (RBAC)** principles, preventing redundant or conflicting permissions. Each action—whether it's role assignment, access update, or user deactivation—is recorded in an **audit log** for transparency and traceability.

This architecture reduces administrative workload, enhances organizational security, and ensures consistency across departments. It provides an **end-to-end automated framework** for managing access with high reliability, scalability, and accountability.

Optimizing User, Group, and Role Management with Access Control and Workflows

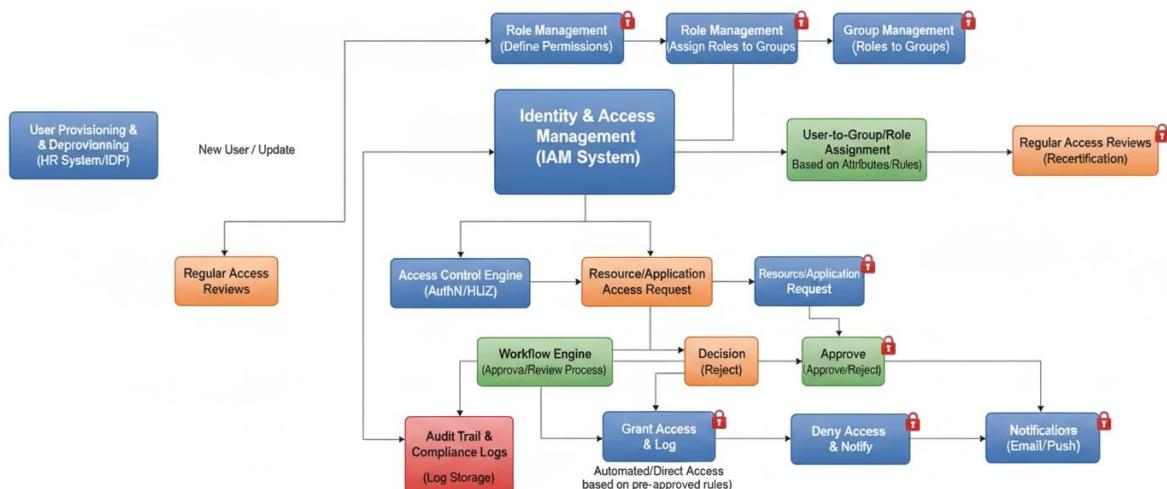


Figure 1: Architecture and Data Flow of User, Group, and Role Management System

Description of Data Flow:

1. **User/Administrator Request:** A user initiates a request for new access or role modification.
2. **Validation Layer:** System checks existing permissions, dependencies, and access policies.
3. **Workflow Engine:** Request passes through multi-level approval workflows.
4. **Access Control Engine:** After approval, permissions are applied or revoked dynamically.
5. **Audit & Logging:** All events are recorded for compliance and monitoring.
6. **Notification:** Alerts are sent to both requesters and administrators regarding status updates.