Project Design Phase
Solution
Architecture

Date	1 NOVEMBER 2025
Team ID	NM2025TMID00309
Project Name	Optimizing User, Group, and Role Management with Access Control and Workflows
Maximum Marks	4 Marks

Solution Architecture

The solution architecture is designed to transform the previously manual and error-prone process of managing user access into a governance-focused, automated lifecycle within the ServiceNow platform.

Architectural Goals

The primary goals of this architecture are to automate the entire Request-to-Provisioning lifecycle, strictly enforce the Role-Based Access Control (RBAC) model, and ensure 100% compliance and auditability for every access decision. This fundamentally reduces administrative overhead and eliminates security risks associated with manual provisioning.

Key Architectural Components

This architecture strategically combines several native ServiceNow features to achieve its goals:

1. Service Catalog: This acts as the single, centralized front door for all access requests, ensuring standardization and necessary data collection upfront.

2. Flow Designer / Workflow Engine: This is the core automation layer. It orchestrates the entire process, handling the sequential routing of the request for approvals and triggering the provisioning actions.

3. Approval Engines: The workflow routes requests for multi-level approval to the appropriate stakeholders (typically the Manager and the Application Owner), enforcing defined Service Level Agreements (SLAs).

4. Data Model Enforcement: The solution enforces the Role-Based Access Control (RBAC) principle by ensuring that permissions (Roles) are assigned to Groups (sys_user_group table), and users are then dynamically added to these groups. This simplifies maintenance and makes audits straightforward.

5. Automation Scripting (Integration): Upon final approval, a script automatically provisions the access by adding the user to the correct Group record in the system.

6. Access Control Lists (ACLs): These remain the enforcement layer, ensuring that the roles inherited by the user correctly and precisely grant only the specific permissions needed (Create, Read, Update, Delete) for the relevant forms and data—enforcing the Principle of Least Privilege.

Summary of the Flow

In summary, the architecture shifts access management from a series of manual handoffs to a reliable, zero-touch workflow. The process starts with a standardized request that automatically triggers a complex, secure approval routing. Only upon securing all required governance sign-offs does the system execute the access provisioning itself, logging every step to create an immutable audit trail. This design guarantees both speed for the user and comprehensive control for the security team.

Example - Solution Architecture Diagram: