Ideation Phase

Brainstorming & Idea Prioritization

Date	01 November 2025
Team ID	NM2025TMID05884
Project Name	Optimizing User, Group, and Role Management with Access Control and Workflows
Maximum Marks	4 Marks

Project Overview:

This guided project focuses on enhancing and automating the management of users, groups, and roles within an organization using ServiceNow. The objective is to create a streamlined process that ensures secure, efficient, and compliant access control across the enterprise.

The project begins by analyzing the existing manual or semi-automated access management process to identify inefficiencies such as role duplication, delayed access approvals, and lack of visibility in user-role assignments. It then introduces a structured workflow for managing user creation, group membership, and role assignments through automation and clear governance policies.

Key components include dynamic form behavior to capture relevant user details, automated workflows for access approvals, and access control rules to ensure that users only receive permissions appropriate to their role. The configuration also includes audit and tracking mechanisms for compliance and security monitoring.

The project concludes with a test scenario validating the access control workflows — ensuring that user creation, group assignment, and role management operate seamlessly with proper approval and audit tracking.

1. Brainstorming

Goal:
To design an automated and secure system for managing users, groups, and roles — ensuring efficient access provisioning and governance.

Key Questions to Explore:

1. How can we automate the process of adding users, assigning groups, and managing roles?

2. What access control mechanisms ensure users have only the necessary permissions?
3. How can approvals and audits be automated and recorded efficiently?
4. How do we ensure changes are trackable and compliant with governance policies?
5. Can we provide role-based workflows to handle different departments automatically?
6. How can we simplify the administrator's job while maintaining security?

Brainstormed Ideas:

1. Use dynamic forms to collect user, department, and role information automatically.
2. Implement approval workflows based on role sensitivity (e.g., admin roles require higher-level approval).
3. Create audit records for every role or group change.
4. Use Access Control Lists (ACLs) to restrict form fields and operations.
5. Automate email notifications for approvals, rejections, and access provisioning.
6. Maintain all configurations in update sets for deployment and rollback tracking.

2.Idea Listing

Functional Ideas

1. Create a **User Management Catalog Item** or form for new user/group/role requests.
2. Add **dynamic visibility** for role and group fields based on selected department or user type.
3. Implement **approval hierarchy** for access requests (e.g., Manager → Admin → Security).
4. Include a **review and revoke** access option for administrators.
5. Provide **audit reports** for tracking user and role changes.

Technical Ideas

1. Use **Catalog Client Scripts** for dynamic field control and validation.
2. Apply **UI Policies** for conditional visibility, mandatory fields, and read-only behavior.

3. Implement **Workflows / Flow Designer** for automated approvals and provisioning.
4. Configure **Access Control Rules (ACLs)** to restrict data access per user role.
5. Maintain **Update Sets** for configuration tracking and deployment governance.
6. Integrate with **User and Group tables** to ensure real-time updates.

3. Grouping

Group	Ideas Included	Purpose
User Experience (UX)	**Dynamic form fields, auto-filled user data, simplified request process**	**To make the process intuitive and user-friendly**
Access & Security Control	**ACLs, approval hierarchy, role-based restrictions**	**To ensure security and proper access governance**
Technical Configuration	**Client scripts, UI policies, workflows**	**To enable backend automation and rule enforcement**
Governance & Compliance	**Update sets, audit records, documentation**	**To ensure transparency, tracking, and compliance**
Testing & Validation	**End-to-end scenario testing for different roles and access types**	**To confirm functionality and eliminate errors**

4. Action Planning

Phase	Task	Expected Output
Requirement Gathering	Identify key user types, groups, and roles; define access rules and approval structure	Approved requirement document and access matrix
Design	Design the user management form and define field dependencies (e.g., department → available roles)	Finalized form layout with dynamic logic

Phase	Task	Expected Output
Development & Configuration	Configure forms, apply UI Policies and Client Scripts, set up ACLs	Functional form with security and dynamic behavior
Workflow & Automation Setup	Build automated workflows for approval, notification, and provisioning	Automated access workflow with triggers and validations
Testing & Validation	Test for multiple user roles, approval chains, and access restrictions	Validated and verified access control system
Deployment & Governance	Move configurations to production and maintain documentation for audit	Production-ready solution with compliance and traceability

5. Idea Prioritization

Priority Level	Idea	Reason for Priority	Expected Impact
High	Implement automated workflows for user and role approvals	Reduces manual approvals and delays	Faster processing and improved governance
High	Configure Access Control Rules (ACLs) for role-based restrictions	Ensures data security and prevents unauthorized access	Strengthened security and compliance
High	Dynamic form fields based on department or user type	Makes the form user-friendly and prevents data errors	Improved user experience and accuracy
Medium	Add audit tracking and logging for user-role changes	Ensures accountability and traceability	Enhanced transparency and compliance
Medium	Automate email notifications for approvals and completions	Keeps stakeholders informed in real-time	Better communication and workflow clarity
Medium	Include reset and review access options for administrators	Provides flexibility for managing user access	Easier maintenance and updates
Low	Display role descriptions and access levels dynamically	Adds extra clarity but not critical to core workflow	Enhanced usability for end users

Priority Level	Idea	Reason for Priority	Expected Impact
Low	Integrate cost or licensing information for premium roles	Useful for governance but can be added later	Financial tracking and budget control