

# Ideation Phase

## Brainstorm & Idea Prioritization – Define the Problem Statements

**Date:** 31 October 2025

**Team ID:** C4B8E28377A600AAD9D4711008669C91

**Project Name:** *Optimize User, Group, and Role Management with Access Control and Workflow*

---

### Introduction

In modern organizations, user, group, and role management are critical for ensuring operational security, data integrity, and workflow efficiency. When access controls are poorly structured, it often leads to unauthorized actions, data exposure, and workflow bottlenecks.

Our project aims to **optimize user, group, and role management** within the **ServiceNow** platform through **automated workflows and granular access control mechanisms**. By integrating role-based access, approval automation, and system auditing, the project enhances transparency, accountability, and security while minimizing manual errors.

---

### Step 1: Team Collaboration and Problem Statement Selection

- The team initiated a **collaborative ideation session** to explore practical problems faced in project and system management environments.
  - Each member proposed challenges related to access permissions, approval delays, and data accountability.
  - After multiple discussions and evaluations, the team finalized the problem statement: **“Optimizing User, Group, and Role Management with Access Control and Workflow”** because it directly addresses core enterprise pain points — *unclear roles, security risks, and inefficient workflow handling*.
- 

### Step 2: Brainstorming, Idea Listing, and Grouping

The team conducted a detailed brainstorming session to gather diverse ideas that could improve user access, security, and workflow performance.

Every member contributed technical and functional ideas, which were later categorized into relevant improvement areas.

### **Initial Ideas Generated:**

- Introduce **approval workflows** for access or role changes.
- Enable **automatic reassignment** of tasks or templates when users change roles.
- Maintain **comprehensive audit logs** for every user activity.
- Prevent **deletion of users** currently assigned to active workflows.
- Implement **Role-Based Access Control (RBAC)** for precise permission handling.
- Introduce **dashboard monitoring** for access analytics and system health.

### **Grouped under Major Categories:**

#### **1. Access Control Improvements**

- Role-Based Access Control (RBAC)
- Prevention of unauthorized access and deletions

#### **2. Workflow & Automation Enhancements**

- Approval workflows for access changes
- Automated task reassignment

#### **3. Security & Audit Management**

- Activity logging and monitoring
- Audit trail for all role and user modifications

---

### **Step 3: Idea Prioritization**

Each idea was assessed based on **feasibility, implementation time, impact, and organizational value**.

After evaluation, the following key ideas were prioritized for implementation:

<b>Priority Idea</b>	<b>Purpose / Benefit</b>
<b>Prevent user deletion if assigned to active workflows</b>	Ensures data consistency and avoids disruption in ongoing processes.

<b>Add approval workflows for role or access changes</b>	Improves accountability and prevents unauthorized privilege escalation.
<b>Automate task or template reassignment</b>	Maintains workflow continuity when team structures change.
<b>Maintain detailed audit logs of all user activities</b>	Enhances system transparency and traceability for compliance.
<b>Implement Role-Based Access Control (RBAC)</b>	Provides secure and scalable access management.

---

## Conclusion

The brainstorming and prioritization process helped the team transform abstract ideas into structured, actionable solutions.

By focusing on automation, security, and auditability, the proposed project ensures a **robust, scalable, and secure framework** for managing users, roles, and workflows in ServiceNow.

This ideation phase establishes the foundation for all subsequent development and testing phases, aligning with the project's core objective — *enhancing efficiency and accountability through smart access management*.