**Ideation Phase**

**Brainstorm & Idea Prioritization**

|  |  |
| --- | --- |
| Date | 31/10/2025 |
| Team ID | FA133F5B1F9199AA1A74FE9CA69D277A |
| Project Name | Optimizing User, Group, and Role Management with Access Control and Workflows |
| Maximum Marks | 4 Marks |

This project demonstrates a solution to automate user, group, and role management within organizations. It leverages workflow automation and access control mechanisms to ensure that requests for access and role assignment are processed quickly and consistently, minimizing security risks and administrative delays.

The implementation begins by digitizing all user provisioning, access requests, group assignments, and approvals. Workflow automation tools or custom engines process these requests end-to-end, verifying compliance policies and automatically updating permissions and audit logs. Scenarios include onboarding a new employee, changing departmental roles, or revoking access when an employee leaves, all handled seamlessly without manual intervention.

This system eliminates manual tracking of permissions, reduces errors, and provides a clear authorization trail. Automated test cases validate that users receive only appropriate permissions based on rules set by the organization, ensuring continuous security and operational efficiency.

**Step-1: Team Gathering, Collaboration and Selecting the Problem Statement**

The team identified challenges caused by manual handling of user and access management. Frequent delays, permission inconsistencies, and audit gaps prompted the group to address automation of user provisioning and access controls.

Through collaborative discussions, the following problem statement was defined:

"To automate user, group, and role management with integrated access control workflows, ensuring secure, efficient, and compliant operations across organizational systems.

**Step-2: Brainstorm, Idea Listing and Grouping**

Team members contributed a range of ideas, including:

* Centralized dashboards for managing groups and roles
* Policy-driven RBAC models
* Automated approval and provisioning workflows for access control
* Real-time audit logging and reporting​

Ideas were grouped into three areas:

* Automation Tools: Custom workflow engines, external automation suites
* Security & Access Control: Policy definition, RBAC, audit compliance
* User Experience: Self-service portals, intuitive request processes​

This ensured all aspects of the proposed solution—technical, security, and usability—were covered, and dependencies between ideas were identified.​

Action planning followed, with roles assigned as:

* Workflow Developer: Solution logic and automation implementation
* Documentation Specialist: Reports, technical diagrams, and user guides
* QA Analyst: System validation and testing​

Development milestones and a clear timeline ensured efficient progress.

**Step-3: Idea Prioritization**

After grouping, the most effective and scalable concept was selected: centralized and automated management of users, groups, and roles using RBAC and digital workflow automation.​

Selection criteria included:

* Feasibility: Easily achievable using workflow engines and RBAC, with no need for external integrations in early phases
* Impact: Substantial reduction in errors, manual effort, and potential security breaches
* Scalability: Expandable to new departments, roles, and compliance requirements as the organization grows​

Focusing on this approach enables the organization to streamline user access, enforce consistent security policies, and maintain transparency through detailed audit logs.