Project Design Phase-II
Solution Requirements (Functional & Non-Functional)

Date	29 October 2025
Team ID	NM2025TMID00560
Project Name	Optimizing User, Group, and Role Management with Access Control and Workflows
Maximum Marks	4 Marks

Functional Requirements

The proposed system focuses on **automating user, group, and role management** through **workflow-based approvals** and **access control enforcement**.

Below are the detailed functional requirements for the system.

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	**User Management**	Admin can create, update, or deactivate users through a centralized interface.
		System validates user details and assigns default roles and groups upon creation.
FR-2	**Group and Role Assignment**	Admins can add or remove users from groups dynamically.
		The system automatically updates related permissions when group or role changes occur.
FR-3	**Access Control Validation**	The system enforces **Role-Based Access Control (RBAC)** to prevent unauthorized operations.
		Validation ensures users only access modules or data relevant to their assigned roles.
FR-4	**Workflow Automation**	Access or role modification requests trigger workflow approval processes.
		The workflow routes requests to designated managers or approvers for validation.

FR-5	**Audit and Logging**	Every change (user, group, or role) is recorded in the system audit logs.
		Logs include user ID, timestamp, and action performed for compliance tracking.
FR-6	**Notification and Alerts**	Notifications are automatically sent to users and administrators after workflow approval or role modification.
		Alerts are triggered in case of failed validations or access rejections.

Non-Functional Requirements

The non-functional requirements ensure that the system performs efficiently, securely, and reliably in various operational environments.

NFR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	The interface should be simple and intuitive for administrators to manage users, groups, and roles efficiently.
NFR-2	**Security**	Only authorized administrators can create or modify access controls. All operations should be validated through secure authentication and role-based restrictions.
NFR-3	**Reliability**	The system must ensure consistent behavior in user-role synchronization, avoiding conflicts or redundant access permissions.
NFR-4	**Performance**	Workflow execution and access validation must be processed quickly (within milliseconds) to ensure smooth user experience.
NFR-5	**Availability**	The system should remain accessible 24/7 to authorized users and automatically recover from temporary downtimes.
NFR-6	**Scalability**	The solution must handle thousands of users, roles, and workflows without affecting system performance.
NFR-7	**Auditability**	All access-related activities should be traceable, allowing compliance verification through detailed logs and reports.
NFR-8	**Interoperability**	The system should integrate with external directories (e.g., LDAP, Azure AD) for identity and access synchronization.