Requirement Analysis: Access Control Optimization Project

I. Functional Requirements (FR)

These define the specific functions the ServiceNow solution **must** perform to meet the project's goal of automation and optimization.

ID	Requirement Category	Description	Source (User Story)
FR-1.0	**Role Management**	The system **must** allow an **Admin** to define, edit, and deactivate custom **Roles** for different user groups.	USN-01
FR-2.0	**User Provisioning**	The system **must** automatically **assign default roles** and permissions to new users upon group assignment.	USN-02
FR-3.0	**Group Management**	The system **must** allow an **Admin** to add or remove users from **Groups** and automatically map group membership to a set of permissions.	USN-02
FR-4.0	**Workflow & Approval**	The system **must** support the creation of custom, workflow-driven approval processes for role and group assignments.	USN-03
FR-5.0	**Access Control (RBAC)**	The system **must** enforce **Role-Based Access Control (RBAC)**, ensuring users can only access resources explicitly granted by their assigned roles and groups.	Architectural Detail
FR-6.0	**Auditing & Logging**	The system **must** log all key access changes, including role assignment, group modification, and approval actions, for compliance.	Architectural Detail
FR-7.0	**Testing**	The system **must** allow a **Tester** to validate approval logic and access restrictions before deployment.	USN-04

II. Non-Functional Requirements (NFR)

These define criteria that judge the operation of the system, not its specific functions.

ID	Requirement Type	Description
NFR-1.0	**Performance**	The **role and group assignment** process, including all automated workflows, **must complete** within **5 seconds** of a request submission.
NFR-2.0	**Security**	All access assignment requests **must** be channeled through an **approval workflow** before becoming effective, enforcing a principle of least privilege.
NFR-3.0	**Usability**	The interface for **Admins** to manage roles, groups, and workflows **must be intuitive and easily navigable** within the ServiceNow platform.
NFR-4.0	**Reliability**	The core access control features (RBAC) **must maintain 99.9% uptime** to prevent service disruptions from access failures.
NFR-5.0	**Compliance**	The system **must** provide features for **audit compliance**, specifically retaining access logs for a minimum of 90 days.

III. Stakeholder Needs Addressed

This analysis directly addresses the core **Problem-Solution Fit**:

- **Security Vulnerabilities:** Addressed by **FR-5.0 (RBAC)** and **NFR-2.0 (Approval Workflow)**.
- **Time-Consuming Manual Process:** Addressed by **FR-2.0 (Automated Provisioning)** and **FR-4.0 (Workflow Automation)**.
- **Centralization/Error-Prone:** Addressed by using a single platform (**ServiceNow**) and implementing **FR-3.0 (Group Management)**.