Requirement Analysis

Solution Requirements(Functional & Non-Functional)

Date	1 NOV 2025
Team ID	NM2025TMID00759
Project Name	Optimizing User, Group, and Role Management with Access Control and Workflows
Maximum marks	4 marks

1. Introduction

The main objective of this project is to optimize the administration of users, roles, and groups in the ServiceNow platform, while ensuring proper access control through Access Control Lists (ACLs). Organizations often face difficulties in managing complex user hierarchies, role assignments, and group memberships, which can result in unauthorized access or administrative inefficiencies. The proposed solution aims to simplify these processes, automate role and group assignments, enforce access control, and provide auditing and reporting capabilities.

2. Problem Statement

Currently, user, role, and group management in ServiceNow can be time-consuming and error-prone due to manual operations and overlapping responsibilities. Without proper ACL enforcement, users may gain unauthorized access to sensitive modules or data. These inefficiencies can lead to security risks, compliance issues, and increased administrative workload. Therefore, a streamlined solution is necessary to ensure proper access, reduce errors, and provide transparency through audit logs and reporting.

3. Solution Objectives

The proposed solution will achieve the following objectives:

- Provide administrators with an efficient interface to create, update, and delete users, roles, and groups.

- Ensure that roles are assigned correctly, and users have access only to authorized resources.
- Automate group memberships and role assignments to minimize manual errors.
- Implement ACLs to enforce security policies at the module and record levels.
- Maintain detailed audit logs and enable administrators to generate reports on user activity, role assignments, and access attempts.

4. Functional Requirements:

The system shall allow administrators to manage users, roles, and groups seamlessly. Administrators must be able to add new users, modify existing user details, and delete obsolete users. Similarly, roles must be created, updated, and deleted as per organizational requirements, with appropriate permissions attached to each role. Group management should support creation, updating, and deletion of groups, with the ability to assign roles to groups and manage group memberships. Access control must be enforced based on roles and group membership using ACL rules. Notifications should be generated for critical actions, and the system should maintain logs for all administrative and access-related activities. Reporting functionality should enable administrators to track user activity, role assignments, group memberships, and ACL changes efficiently.

5. Non-Functional Requirements:

The solution must be user-friendly, providing administrators with an intuitive interface for managing users, roles, and groups. Security is paramount; only authorized personnel should perform administrative actions or access sensitive modules. The system must reflect changes in real time, maintaining accuracy and reliability. Audit logs and reporting capabilities must meet organizational compliance standards. The solution should be robust, minimizing errors and preventing unauthorized access.

6. Data Flow Description:

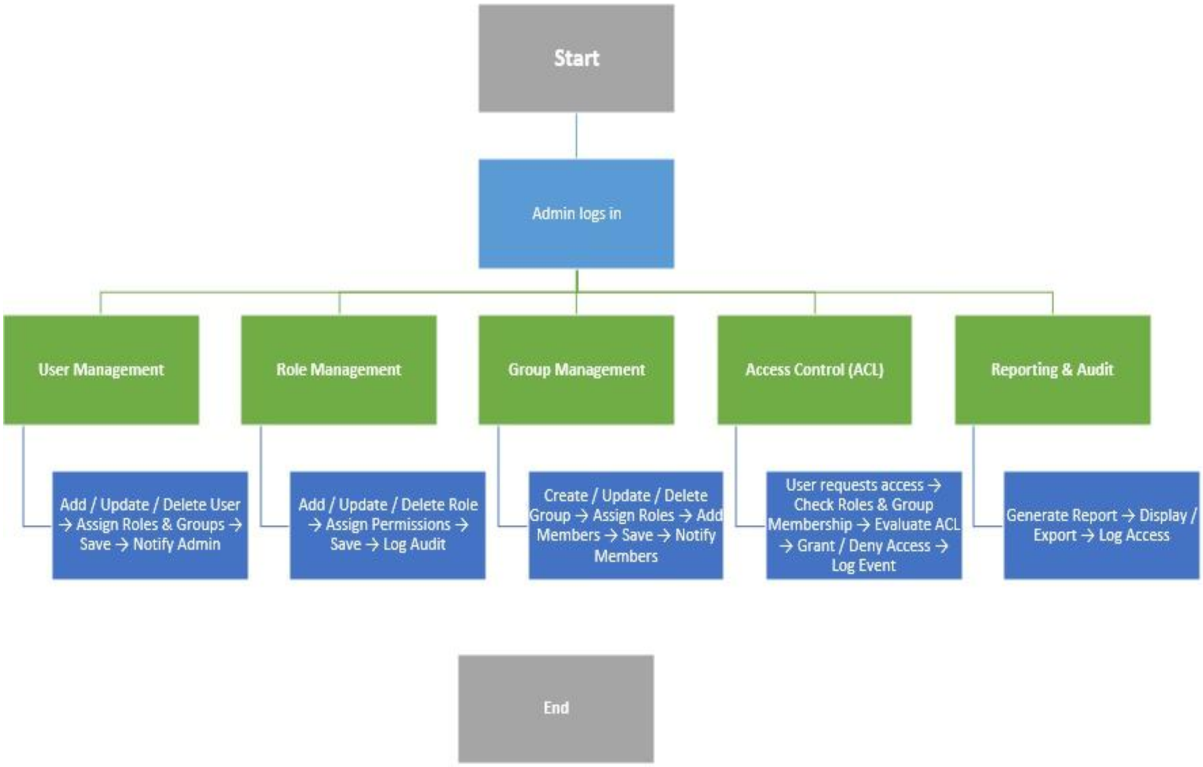
In this solution, the flow of data begins with administrative actions such as creating, updating, or deleting users, roles, and groups. These actions update the respective data tables within the system, and confirmation or notification is sent to the administrator. Users interact with the system by requesting access to modules or data. The system evaluates these requests against role assignments, group memberships, and ACL rules. Access is granted if the user has the required permissions, and denied otherwise, with each event logged for auditing purposes. This data flow ensures that access control is strictly enforced, while administrators remain informed of all activities within the system.

7. User Stories:

The solution is designed around the needs of administrators and users. From the administrator's perspective, the system should enable seamless management of users, roles, and groups, minimizing manual effort and errors. Administrators should be able to generate reports that provide visibility into role assignments, user activity, and ACL changes. From the user's perspective, the system should enforce access control, ensuring that each user can only access authorized modules and data, thereby maintaining security and compliance. These user stories provide a clear understanding of system functionality from both administrative and user viewpoints.

8. Conclusion:

This Solution Requirements Document defines the necessary requirements to optimize ServiceNow user, role, and group management along with ACL enforcement. By addressing administrative efficiency, security, and compliance, the proposed solution provides a framework for implementing a robust and reliable system. The data flow and user story descriptions ensure that the system’s behavior is well understood, serving as a foundation for subsequent design and development phases.


Start
Admin logs in
User Management
Role Management
Group Management
Access Control (ACL)
Reporting & Audit
Add / Update / Delete User → Assign Roles & Groups → Save → Notify Admin
Add / Update / Delete Role → Assign Permissions → Save → Log Audit
Create / Update / Delete Group → Assign Roles → Add Members → Save → Notify Members
User requests access → Check Roles & Group Membership → Evaluate ACL → Grant / Deny Access → Log Event
Generate Report → Display / Export → Log Access
End