Optimizing User, Group, and Role Management with Access Control and Workflows in service now

SOLUTION REQUIREMENTS:

Date	02:11:2025
Team ID	NM2025TMID07577
Project name	Optimizing User, Group, and Role Management with Access Control and Workflows in service now
Maximum marks	4 marks

Here are the Solution Requirements for optimizing User, Group, and Role Management (UGRM) with Access Control and Workflows in ServiceNow, categorized by functional area derived from the Problem-Solution phase.

Functional Requirements (What the System Must Do)

These requirements ensure the platform achieves the goals of automation, standardization, and security.

1. User and Data Management Requirements

- FR1.1: Automated Onboarding: The system must automatically create a new user record in the `sys_user` table immediately upon receiving a "New Hire" status from the integrated HRIS/IdP.
- FR1.2: Automated Offboarding: The system must immediately deactivate the user record and revoke all associated roles and group memberships upon receiving a "Terminated" status from the HRIS/IdP.
- FR1.3: Manager Data Integrity: The user record must maintain an accurate and current Manager field synchronized daily from the IdP/HRIS for workflow approvals.
- FR1.4: Single Source of Truth: All updates to core user attributes (Name, Email, Department) must be driven exclusively by the IdP/HRIS integration, preventing manual override.

2. Group and Role Management Requirements

- FR2.1: Group Classification: The `sys_user_group` table must be extended with a mandatory Classification field (e.g., Security, Assignment, Reporting) to enforce group standardization.
- FR2.2: Role Assignment Governance: The system must enforce that all security roles are assigned only to groups, not directly to individual user records, except for documented "break-glass" accounts.
- FR2.3: Role Definition Clarity: Every defined role must have a clear, concise Description of its purpose and the entitlements it grants.
- FR2.4: Role Hierarchy Utilization: The solution must utilize the ServiceNow Role Hierarchy functionality to consolidate permissions and minimize role sprawl.

3. Access Request Workflow Requirements

- FR3.1: Centralized Request: A single Service Catalog Item (SCI) must be the exclusive entry point for requesting new roles and group memberships.
- FR3.2: Dynamic Approval Routing: The access request workflow must dynamically route the request for approval based on the Risk Level or Group Owner associated with the requested entitlement.

- FR3.3: Automated Fulfillment: Upon final approval, the workflow must automatically execute a script to update the `sys_user_grmember` table, making the change effective without manual intervention.
- FR3.4: Real-Time Status: The Service Portal must display the real-time status and identify the current approver for any pending access request.

4. Access Control (ACL) and Security Requirements

- FR4.1: Principle of Least Privilege: All ACLs must be designed to grant the minimum necessary access required for a role to perform its function.
- FR4.2: ACL Optimization: The solution should minimize the use of complex scripted ACLs in favor of simpler, role-based conditions to improve performance.
- FR4.3: Access Recertification: The system must implement a mechanism (e.g., Access Certification module) to trigger quarterly attestations for all high-risk group memberships by the designated Group Owner.
- FR4.4: Unauthorized Access Alerting: The system must generate a high-priority incident and an email alert if a security-classified role is assigned outside of the defined approval workflow.

Non-Functional Requirements (How the System Performs)

These requirements ensure the solution is stable, maintainable, and performs well.

- NFR5.1: Performance (ACL): The average response time for loading records protected by the new ACL structure must not exceed 3 seconds under peak concurrent load.
- NFR5.2: Performance (Sync): The scheduled IdP/HRIS synchronization job must complete within its designated maintenance window (e.g., 2 hours) and not overlap with business hours.
- NFR5.3: Auditability: All changes to group membership, role assignments, and ACL definitions must be logged and readily auditable for a minimum of three years.
- NFR5.4: Maintainability: All custom scripts, workflows, and integrations must be documented with clear comments and follow established organizational coding standards.