Optimizing User, Group, Role Management with Access Control and Workflow using ServiceNow

Team ID : NM2025TMID02249
Team Size : 3
Team Leader : M Deepak Roshan
Team member : L Kumara Pandiyan
Team member : R Dhanush Kumar

Table of Contents

1. Executive Summary
Provide a concise overview of the goals: reduce risk, enforce least privilege, automate onboarding/offboarding, ensure compliance, and make role/group management scalable in ServiceNow.

2. Objectives & Scope
- Centralize identity and access management in ServiceNow.
- Automate user lifecycle events.
- Implement role-based access controls and table/field-level ACLs.
- Integrate workflows for approvals and provisioning.- Provide audit trails and reporting.

3. Prerequisites
- ServiceNow admin access with elevate role.
- Flow Designer, Access Control, LDAP/AD integration (if applicable).
- Knowledge of target systems (HR, AD, Cloud). - Test instance for development and testing.

4. Design Principles
- Least privilege by default.
- Role hierarchy and separation of duties.
- Role naming convention (area_role_level, e.g., FIN_Approver_RW).
- Use groups to aggregate roles for teams.
- Document everything and maintain change logs.

5. User Lifecycle Management
5.1. User Onboarding (step-by-step)
- Trigger: HR system record or manual request.
- Use Flow Designer to create user record in sys_user.
- Assign default groups/roles based on job profile.

- Provision external systems via integrations (AD, Azure, Okta). - Send welcome notification with next steps.

5.2. User Updates
- Track attribute changes via Business Rules or Flows.- Reevaluate group/role assignments on job change.

5.3. Offboarding
- Trigger immediate deprovisioning on termination.
- Revoke access, disable user, remove group memberships.- Retain sys_user record for audit; log actions.

6. Group Management Best Practices
- Use purpose-based groups (Team_Analytics, Team_HelpDesk).
- Avoid granting roles directly to users; prefer groups.
- Use dynamic groups where possible (attributes-based). - Document group owners and periodic review dates.

7. Role Design and Assignment Strategy
- Create coarse-grained roles for business functions; combine for fine-grained access.
- Role attributes: name, description, owner, allowed_grantors.
- Implement role lifecycle similar to users.
- Avoid role explosion — consolidate where safe.

8. Access Control (ACL) Strategy & Implementation
- Use table-level and field-level ACLs.

- ACL creation steps (example for 'task' table):

1. Navigate: System Security > Access Control (ACL).
2. Click Elevate role.
3. New -> select Table: task, Operation: read/create/update/delete.
4. Condition/Script: Use scripts for complex rules (gs.hasRole('x')).
5. Test using impersonation.

- Use "requires role" rows for complex compound requirements.
- Use script includes for reusable ACL logic.
- Document exceptions and temporary access workflows.

9. Workflow & Approval Flows (Flow Designer)
- Build Flows for onboarding/offboarding, role request approvals, and access reviews.

- Example Flow steps:

1. Trigger (record created or Service Catalog request).
2. Evaluate role mapping logic.
3. Create approval actions (Manager, Security).
4. On approval: add user to group and assign roles.
5. Notify stakeholders and log entry in audit table.

- Use subflows for reusable logic (provisioning, notification).

10. Automation & Onboarding/Offboarding
- Integrate with HR feeds (CSV, REST) for authoritative events.
- Use ServiceNow IntegrationHub spokes for AD/Azure/Okta provisioning.- Schedule periodic access reviews and recertification campaigns.

11. Testing & Validation
- Maintain a testing matrix for ACLs, roles, and flows.
- Use impersonation and automated tests to validate ACL logic.- Use synthetic users to test provisioning pipelines.

12. Monitoring, Audit & Reporting
- Create dashboards for active users, roles per user, and ACL changes.

- Capture sys_audit and syslog entries for critical changes.
- Schedule reports for access reviews and segregation-of-duties violations.

13. Change Management & Governance - Use
scoped apps for custom logic where possible. -
Create a governance board for role approval.
- Implement change requests for ACL or role modifications.

14. Templates & Scripts (Examples)
- Sample Flow Designer pseudocode for onboarding.
- Business Rule example to sync attribute changes.

- **Sample ACL script snippet:**

(Provide example script in appendix)

15. Checklist & Runbook
- Pre-deployment checklist: backup, test plan, owner sign-off.
- Runbook: step-by-step for emergency revocation, role rollback.

16. Appendix: Sample ACL creation steps (ServiceNow)
- Detailed step-by-step (click sequence), sample scripts, testing steps.

17. References
- ServiceNow documentation, IntegrationHub, Flow Designer guides.

End of document.