

Team Members With NM ID

Dheenadhayalan S B59931360F549E58ABD42775F0231F9C (Team Lead)

Ashok M F4674176332D5FFB3124FBB8CB1F7AB4

Deva R D3A5BEB76D26F14BC014DE1101CA8B40

Project Title: Access Control Implementation for Project Table

1. Project Overview

This project focuses on **Access Control Implementation for Project Table**, designed to address the need for controlled data access and security within the project management system. The goal is to deliver a comprehensive solution by leveraging **role-based access control (RBAC)**. Through this project, we aim to enhance **data security**, **operational efficiency**, and **compliance** while supporting the long-term objectives of project management and organizational governance.

2. Objectives

Business Goals

- Ensure **data security** by restricting access to sensitive information.
- Improve **role-based control mechanisms** to simplify user management.
- Enhance **auditability** through well-defined access control levels.

Specific Outcomes

- Deployment of a table with proper access controls applied.
- Creation of user roles with specific permissions.
- Validation of data security by restricting sensitive fields and actions.

3. Key Features and Concepts Utilized

- **Role-Based Access Control (RBAC):** Implementing different access levels based on user roles.
- **Field-Level and Table-Level ACLs:** Restricting user actions and field visibility.
- **High-Security Role Elevation:** Adding elevated privileges for specific use cases.
- **Impersonation Testing:** Verifying access control by simulating different user roles.

4. Detailed Steps to Solution Design

Data Models

- **Project Table Fields:**

- Budget
- Total Expenses
- Project Name

User Roles and Permissions

- Users Created:
 - **Product Manager**
 - **Employee Management**
- Roles Defined:
 - **u_project_user** (Product Manager)
 - **Employee Role** (Employee Management)

Access Levels Configured

- **Table-Level ACL:** Restricting read access for employees to sensitive tables.
- **Field-Level ACL:** Limiting visibility of **Budget** and **Total Expenses** fields based on roles.

Documentation with Screenshots

- Entity Relationship Diagrams (ERD) for the Project Table.
- User and role configuration pages.
- ACL creation and implementation screenshots.

5. Testing and Validation

Testing Approach

- **Unit Testing:** Verify that each field and table-level access control works as expected.
- **User Interface Testing:** Ensure proper visibility and restricted access on the front end for each user role.

6. Key Scenarios Addressed by ServiceNow in the Implementation Project

- **Use Case 1:** Product Managers can view and edit all fields in the Project Table.
- **Use Case 2:** Employees have restricted read-only access and cannot see sensitive fields like Budget and Total Expenses.

- **Use Case 3:** Role elevation enables administrators to validate security setups.

7. Conclusion

Summary of Achievements

- Successfully implemented **role-based access control** for the Project Table.
- Restricted sensitive data fields like **Budget** and **Total Expenses** for non-privileged users.
- Validated the setup through rigorous testing, ensuring compliance with organizational security policies.

Future Prospects

- Extend access control mechanisms to other tables and modules.
- Implement dynamic role assignments for scalable user management.