Team Members with NM ID:

SRINITHI V 582B098CE31B1FC84D540EBE74EA2A5C (Team Lead)
SNEHA PRIYAA J S 5B1747F503499E081F3479A97B1265CC
PRIJEESHA P AE475990122E9D1830449933FEBE609B
KIRUTHIKA K 956FA98B083B5F6BF6B4068FCFA481B1

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

a. **Role-Based Access Control (RBAC):** Implementing different access levels based on user roles.

b. **Field-Level and Table-Level ACLs:** Restricting user actions and field visibility.

c. **High-Security Role Elevation:** Adding elevated privileges for specific use cases.

d. **Impersonation Testing:** Verifying access control by simulating different user roles.

4. Detailed Steps to Solution Design

Data

Models

a. **Project Table Fields:**

    b. Total Expenses

    c. Project Name

    d. Budget

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

a. **Unit Testing:** Verify that each field and table-level access control works as expected.

b. **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

a. **Use Case 1:** Product Managers can view and edit all fields in the Project Table.

b. **Use Case 2:** Employees have restricted read-only access and cannot see sensitive fields like Budget and Total Expenses.

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

7. Conclusion

Summary of Achievements

a. Successfully implemented **role-based access control** for the Project Table.

b. Restricted sensitive data fields like **Budget** and **Total Expenses** for non-privileged users.

c. Validated the setup through rigorous testing, ensuring compliance with organizational security policies.

Future Prospects

d. Extend access control mechanisms to other tables and modules.

e. Implement dynamic role assignments for scalable user management.