Access Control for Project table

1.Project Overview:

The ServiceNow Product Manager aims to customize the Project table to hide certain fields from the employees under their supervision, specifically those with the "Employee Management" user. This customization will ensure that these employees can focus solely on the fields accessible to them.

2.Objective:

- To restrict some field visibility for employees on the Project table .
- To enhance safety between Product management and employee management.

Specific Outcomes:

- Create a project label in the table.
- Create two users product management and employee management and assign respective roles for them.
- Create ACL by elevating to higher security and test them with 3 sample names to see whether they appear in the employee side.

3.Key Features and Concepts Utilized

Access Control Lists:

restrict user access to specific data based on defined conditions. They are applied at the row level (record) and field level (column).

Table-Level Security:

Allows you to specify who can read, create, update, or delete records in a table.
Controls who can view or modify individual fields within a record. This is managed using field-level ACLs.

Elevated Privileges:

Temporary elevated privileges can be granted to users when they need access beyond their normal role. The "Elevate Roles" feature can provide access like security admin temporarily

Implicit and Explicit Permissions

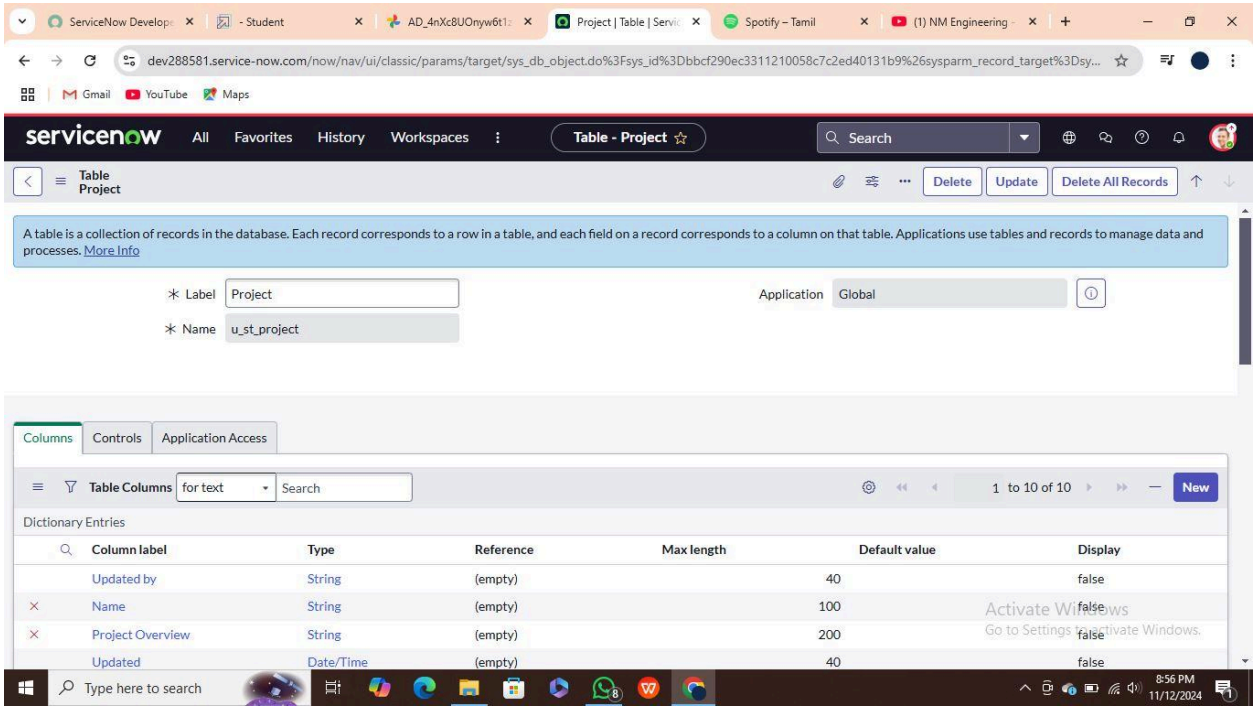
Implicit Permissions: Automatically granted based on the context (e.g., users with ITIL roles can access incident records).
Explicit Permissions: Defined by specific ACL rules or user role assignments.

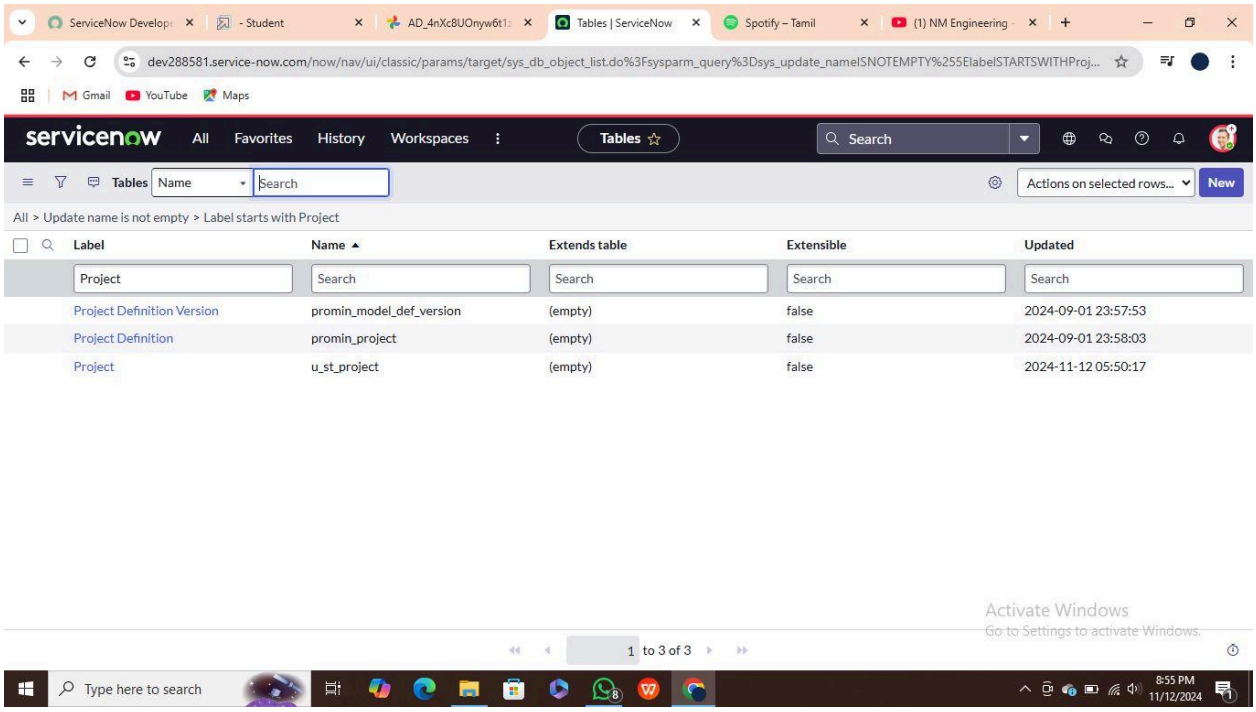
4.Detailed Steps to Solution Design

Implementation

Activity-1 : Create project

1.Open ServiceNow
2.Open “Tables” >> New
3.create table name as project
4.Fill the details
5. Click on submit





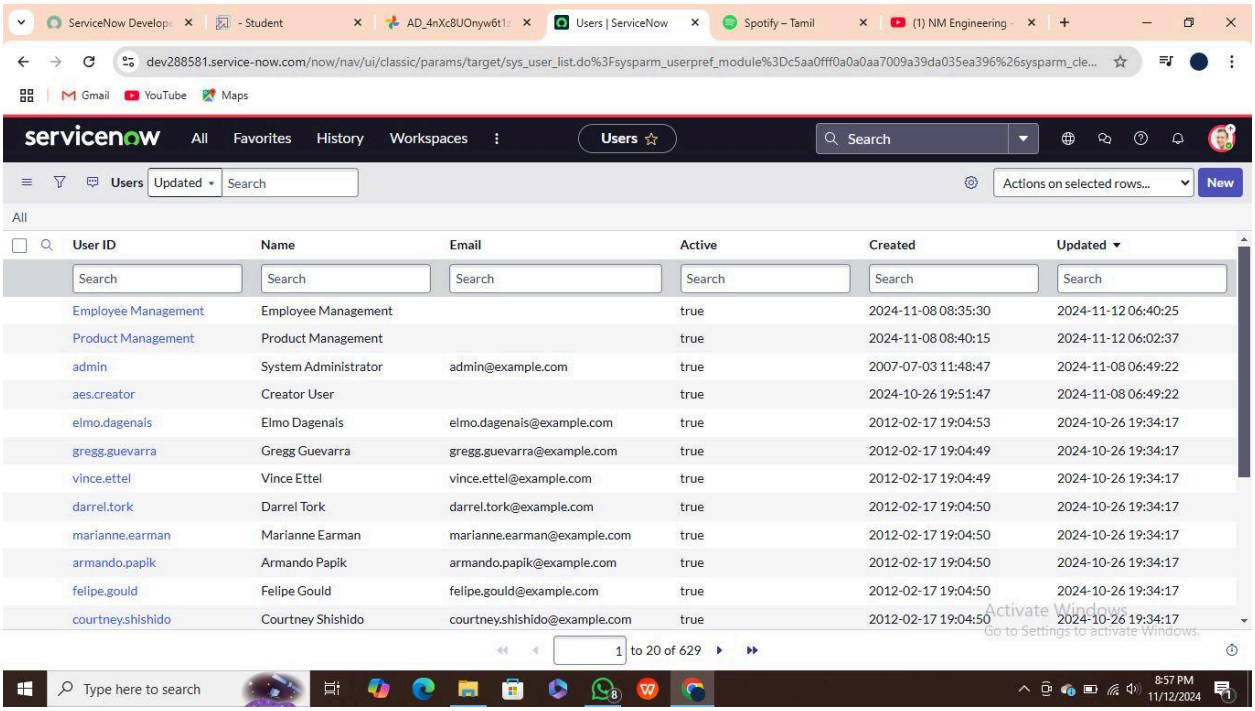
Activity-2 : Create Users

1.Open User >> New.

2.Create Two Users Product Manager and Employe Management.

3.Open Role >>New

4.Create Employee Role.



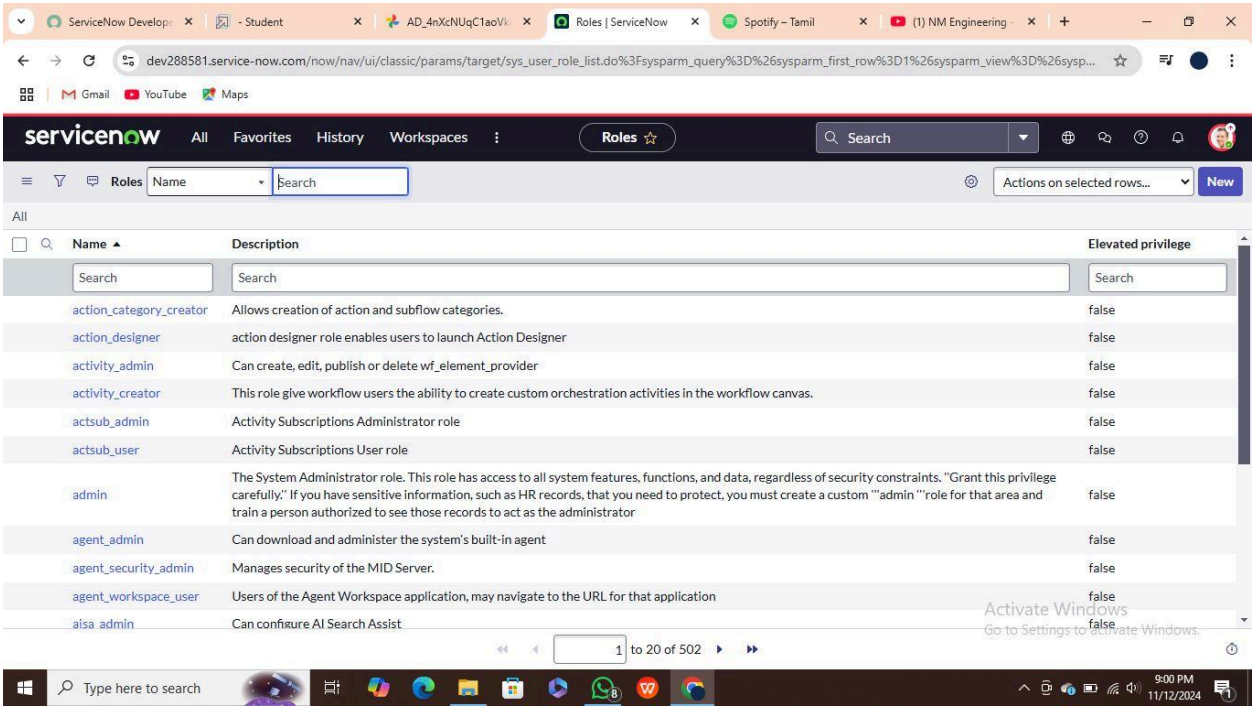
Activity-3 : Assign roles

1.Go to the Project table >> Controls

2.copy the role name from the table.

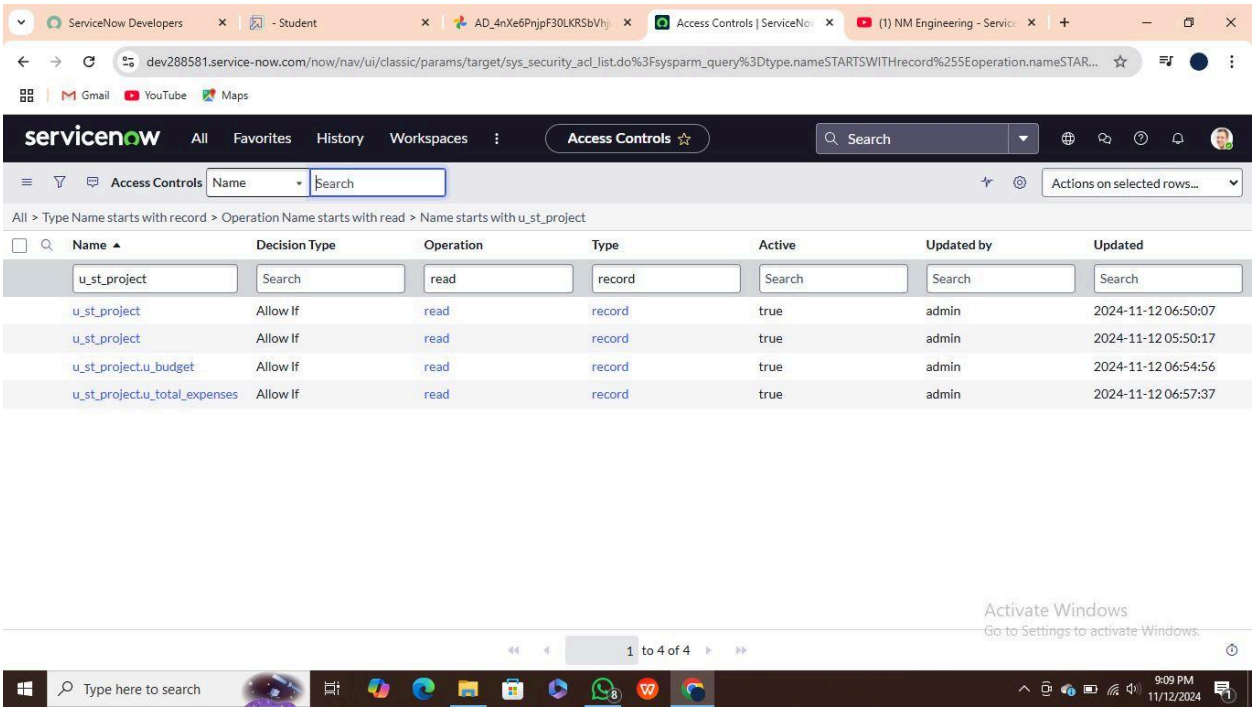
3.Go to Employe Management User

4. Add role : Employe role to it.



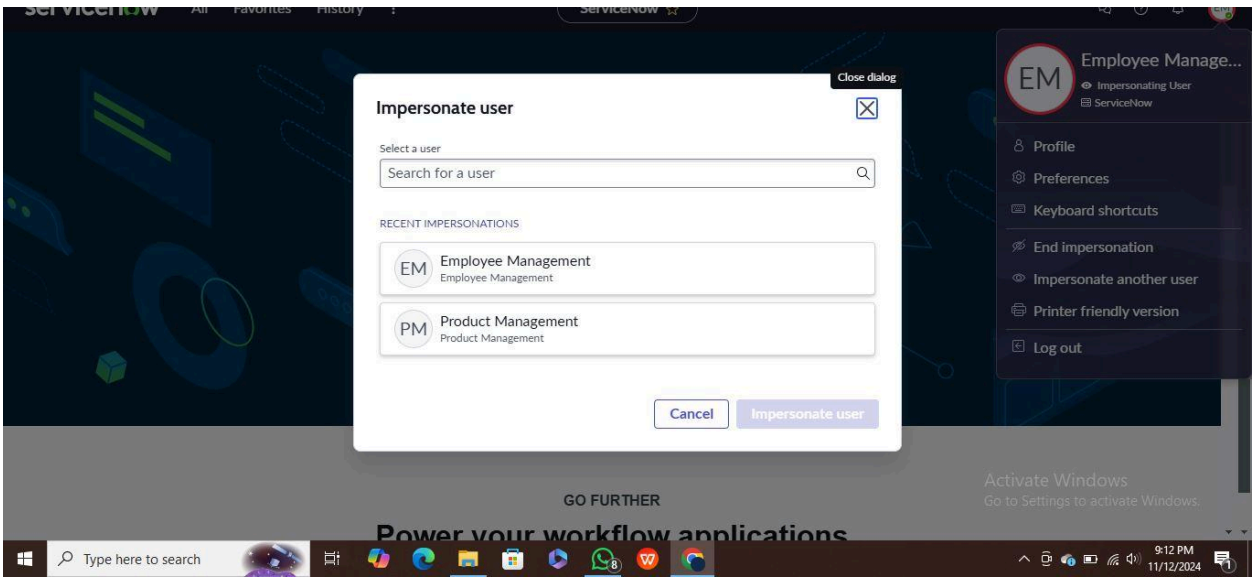
Activity-4 : Access Control List

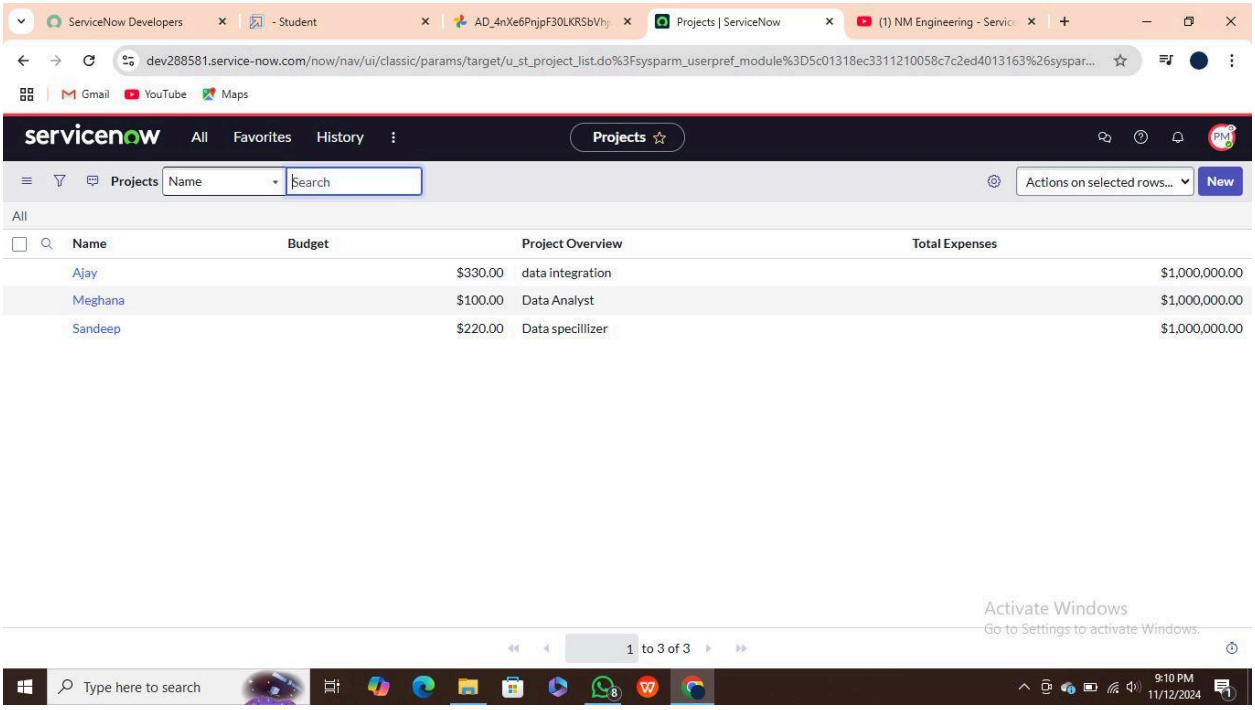
1.Click on the Profile avatar >> Elevate Role >> Grant the high security
2.Search & Open ACL >> New
3.Fill the details
4.Create Read Operation Table Level ACL(none) on Employee role and Save
5.Fill the details and Create Read Operation Field Level ACL(Budget)
6.Create Read Operation Field Level ACL(Total Expenses) on role: u_project_user and Save

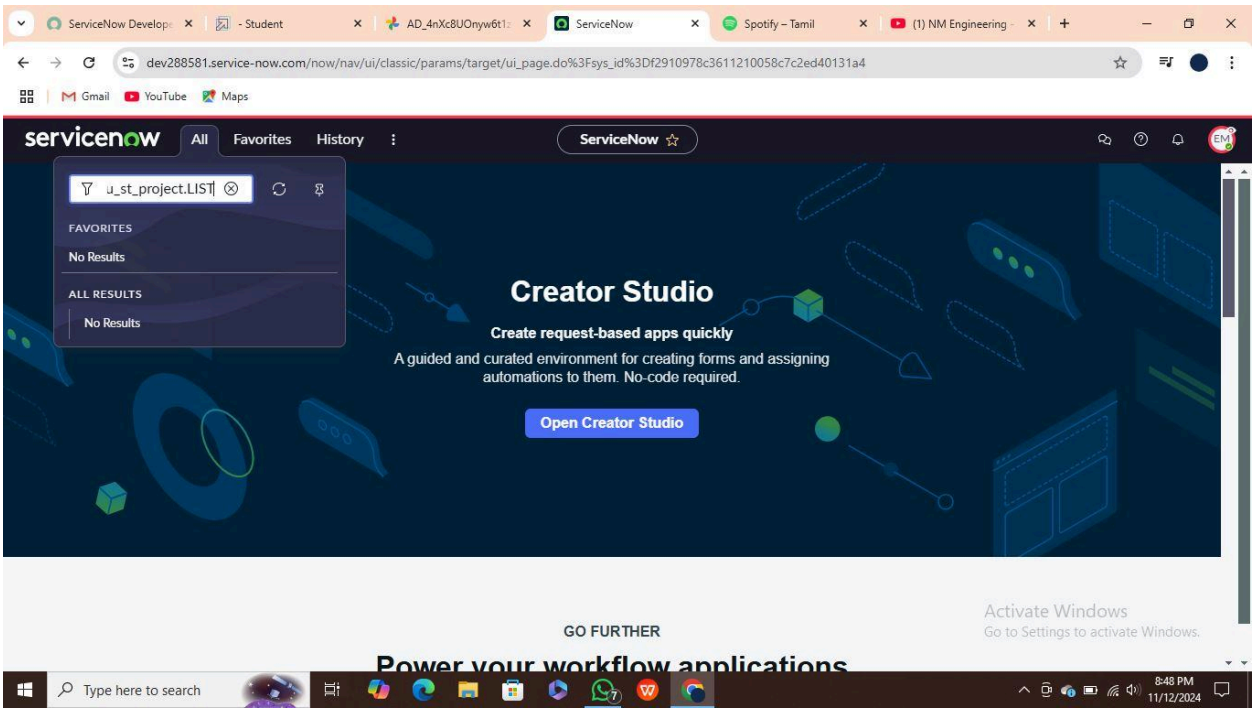


Activity-5 : Impersonate User

1. Impersonate User >> Product Management.
2. All >> Project >> New
3. Create 3 Records with any details .





- 

5.Testing and Validation

Purpose : Ensure that the data entries are not visible from the Employee side

Methodology:

Impersonate the user to Employee management and check for the table project.

- After creating tables and generating roles .
- The data will be entered in the table from the Product management and by elevating the role to higher security the access control list.

6. Key Scenarios Addressed by ServiceNow:

1.IT Service Management (ITSM)

- Streamlines the process of managing IT incidents, enabling quick resolution and minimizing the impact on business operations. Users can log incidents through the self-service portal or automatically through monitoring systems.
- Helps identify the root causes of recurring incidents to prevent future occurrences, improving service reliability.

2.Security Operations (SecOps)

- Identifies and prioritizes vulnerabilities in the IT environment, automating remediation processes to reduce exposure to threats.
- Integrates with external threat intelligence feeds to provide context to security incidents, helping analysts make informed decisions.

3.Governance, Risk, and Compliance (GRC)

- Manages policies and ensures compliance with regulations by automating assessments and monitoring controls.
- Identifies, assesses, and mitigates risks across the organization, enabling proactive risk management and decision-making.
- Streamlines the audit process by automating evidence collection, tracking, and reporting, ensuring efficient and effective audits.

4.Project Portfolio Management (PPM)

- Manages the entire project lifecycle, from planning and resource allocation to execution and reporting, improving project delivery and efficiency.
- Optimizes resource allocation across projects based on skills, availability, and demand, maximizing productivity.
- Prioritizes and manages incoming business demands, aligning them with strategic goals and resource availability.

5.Vendor Management

- Tracks vendor contracts, performance metrics, and compliance, helping organizations manage their relationships with external suppliers effectively.
- Monitors vendor performance against SLAs and other metrics, providing insights to improve vendor selection and performance management.

Conclusion

After switching to the Employee management we won't be able to see the project name under all projects sections . Thus confirms the creation of an Access Control List in the project .We can ensure that some fields(Budget,Total Expenses) visibility is restricted for employees on the Project table.