TASK 1: Define Roles and Permissions Problem: Create a simple table mapping roles to basic permissions.

What is the Roles and Permission problem?

A “Roles and Permission problem” occurs when the system has flaws while assigning permissions to the users based on their roles (job functions or group). This leads to issues like unauthorized access to sensitive data, a lack of necessary access to the legitimate users and complex permission management which can further lead to security breaches, inefficiencies, poor user experience, and compliance risks.

What are Roles and Permissions?

Roles are predefined groupings of permissions that are assigned to users or groups of users. Permissions are the specific actions a user can perform within a system, such as viewing, editing, or deleting data.
Roles and permissions are a way to manage access control by defining who can do what and access what data within a system.

RBAC

Role-based access control (RBAC) is a model for authorizing end-user access to systems, applications and data based on a user’s predefined role.
Components of RBAC are:

- Roles: Predefined job functions or titles within an organization
- Permissions: Specific actions that a role is authorized to perform on a resource
- Users: Individuals assigned to roles.
- Sessions: Temporary associations between users and roles.
- Resources: Digital assets for which users are granted permission to use

Roles Definition

Owner:
Highest level of access with full administrative control. They are system founders or organization heads.
Target users are University IT Directors, Security Chiefs

Admin:
Administrative access with operational control but limited organizational changes.
Target users are Campus Security Managers, Facilities Directors

Analyst :
Responsible for reviews and data analytics. They have limited modification capabilities since they are read-focused roles.
Target users are Data Analysts, Researchers

Roles Permission Table

Roles	Create	Read	Update	Delete
Owner	✓	✓	✓	✓
Admin	✓	✓	✓	✗
Analyst	✗	✗	✓	✗

Principle of Least Privilege

Above table follows the Principle of Least Privilege as each role is granted only the minimum permissions necessary to perform their job functions:

- The Owner has full control (CRUD) as the system's top-level authority.
- The Admin can create, view, and update resources but are not allowed to delete them.
- The Analyst has read-only access since their role is to review reports and analytics, not to modify system data.