1. **Objective**:

To provide a secure and efficient framework for managing user access rights to applications using Role-Based Access Control.

**Key Goals**:

Enable users to request new access rights or modify existing roles.

Allow supervisors or authorized users to approve or manage roles for other users.

Provide a user-friendly interface for self-service and delegated role management.

Ensure security and compliance by maintaining an audit trail of role changes.

1. **Key Features :**
   1. Role Management:

Users can request to add or remove roles for themselves or others.

Supervisors or authorized users can approve or deny role requests.

* 1. Self-Service and Delegated Access:

Users can select themselves or another person for role management.

Supervisors can manage roles for their team members.

* 1. Audit and Compliance:

All role changes are logged for audit purposes.

Provides transparency and accountability for access rights.

* 1. User-Friendly Interface:

Intuitive screens for selecting users, roles, and submitting requests.

Clear workflows for requesting and approving role changes.

1. **User Interface Flow**
   1. Screen 1: User Selection

Option 1: Select yourself to manage your own roles.

Option 2: Select another user (e.g., a team member) to manage their roles.

Input: Search or select user from a list. (\*\*how read user from AD? Or can we copy all Capsugel user to Postgres\*\*)

* 1. **Screen 2: Role Management**

**Application -> role**

**Add Role: Select from a list of available roles.**

**Remove Role: Deselect or remove existing roles.**

**Submit Request: Send the request for approval.**

* 1. Screen 3: Approval Workflow

Supervisors or authorized users receive a notification.

They can approve or reject the role change request.

Notification is sent back to the requester.

* 1. Screen 4: Audit Log

View a history of all role changes (who, what, when).

Filter by user, role, or date range.