**Permission Model References:**

1. Activity driven authorization over Role driven authorization:  
   <https://lostechies.com/derickbailey/2011/05/24/dont-do-role-based-authorization-checks-do-activity-based-checks/>
2. About Design Pattern – Every organization have different permission model so not sure if we can have some design patterns around it.

<http://stackoverflow.com/questions/300359/best-design-for-a-user-role-management-system>

Once we have common understanding after reading the above references, we can decide what are the roles and permissions applicable for our project.

**Types of Roles in our system:**

* Site Admin – Super Admin – System Admin
  + This role belongs to us as we maintain the application under which we may have multiple tenants / multiple societies that are registered with us and using our solution in a shared mode.
  + This role should have access to all the societies and their members and should have full access on complete system.
* Tenant Admin – Society Admin
  + This role belongs to admin of a particular society i.e. Chairman or Secretary who has full access to manage the data within their society.
* Tenant Supervisor – Society Co-ordinator
* Members – Society Members – End users.