IAM works on the principle of Authorisation and Authentication. When it comes to authentication, azure concept used in this one is groups, where the users are divided into necessary groups and are provided the access. But when authorisation comes, there is a concept in azure known as roles. Read-only, access VM roles, etc are created.

To create a resource for IAM, there is something called MS Entra ID.

Search for entra ID on the search bar of Azure UI and create an ID. After creating the ID login with those credentials and you will see that the new user doesn’t have any permissions to create anything in the environment. To get permissions for the user, we need to login through the previous account and grant.

You can assign roles by clicking on the user and navigate to assigned roles. You will some see default roles but you can create as well. To create your own role, go to roles and administrators where you can create custom roles.

Also give on how to create identity from the creation of resource groups and also give commands on how can that be accessed from CLI