1. What is the need of IAM?
   IAM is required for high level of data protection in AWS. It provides security by enabling us to create users and groups to securely control the services for user authentication and allow or deny access to AWS resources.

2. If I am a non tech person, how will you define policies in IAM
   Policies in AWS IAM is like a document which includes sets of permissions in it. You can add that policy to any user to whom you want to grant permissions defined in it.
   Policy contains information like- who can access which AWS resources, what actions that user can take, when they can be accessed.

3. Please define a scenario in which you would like to create your own IAM policy.
   I will create my own IAM policy when I want to add it into single user or group. For example, when a new employee joins a company, I want to give him ec2 full access only for specific period. Then I will create own policy defining required time span and add it to employee.

4. Why do we prefer not using root account?
   Root user is powerful who has access to everything and can hide all their actions. Lack of security by which system might get affected due malicious software downloads. Mistakes done by root user affects the entire system. It is recommended not to use root account for the tasks that does not require all the powers of root.

5. How to revoke policy for IAM user?
   Revoking policy is as simple as adding it. Go to IAM users' section, select a user for whom the policy should be revoked, select the policy you want to revoke, then delete/remove it.

6. Can a single IAM user be a part of multiple policy via group and root? How?
   Single IAM user can be part of multiple groups and policies attached to it. We cannot add IAM policies for root user to restrict access to resources.