## Darshan Nikam Date: 23/02/2024

***IAM Roles***

**An IAM role is like a special access pass that you give to specific individuals (or in the case of AWS, to other AWS services or resources). Instead of giving out individual keys to each resource, you create roles with certain permissions. These permissions determine what that role (or pass) allows the person (or service) to do within AWS.**

**For example, you might create a role that allows someone to access only the storage area (like S3 buckets) but not the database or computing areas. This way, you can control who has access to what parts of your AWS resources, keeping everything secure and organized. Roles can be assigned to users, applications, or even other AWS services, allowing them to perform specific tasks or access certain resources within your AWS environment.**

**IAM roles can be attached to several entities, including:**

* **IAM Users: You can assign IAM roles to individual users within your AWS account. This allows those users to assume the permissions and access provided by the role in addition to their own permissions.**
* **IAM Groups: Roles can be attached to IAM groups. When you add a user to a group, they inherit the permissions associated with the group, including any roles attached to it.**
* **AWS Services: Certain AWS services, such as Amazon EC2 (Elastic Compute Cloud) instances or AWS Lambda functions, can assume IAM roles. This allows the services to perform actions on your behalf securely.**
* **External Users and Applications: IAM roles can also be assumed by external users and applications using temporary security credentials provided by AWS STS (Security Token Service). This is often used for cross-account access or for granting permissions to third-party applications.**

**When you create an IAM role, you define the permissions it grants and specify the trusted entities (such as users, groups, or AWS services) that can assume the role. Then, you attach policies to the role to define the specific permissions granted to those entities when they assume the role. Finally, you can attach the role to the appropriate entity within your AWS environment, depending on your use case.**