When services of multiple organizations are maintained within the same geographical location

Segregation roles carried out by IAM with **Google Cloud**

**Role types**

There are three types of roles in IAM:

* **Basic roles**, which include the Owner, Editor, and Viewer roles that existed prior to the introduction of IAM.
* **Predefined roles**, which provide granular access for a specific service and are managed by Google Cloud.
* **Custom roles**, which provide granular access according to a user-specified list of permissions.

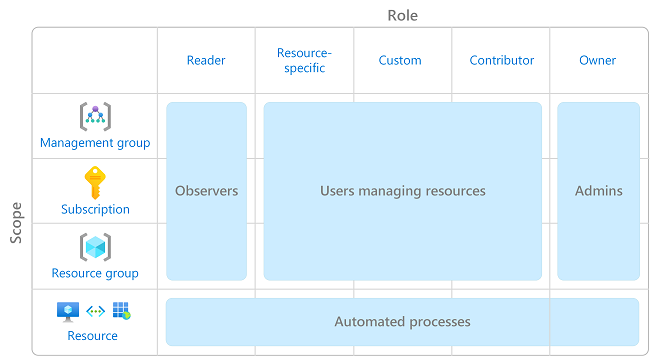
Segregation roles carried out by IAM with **AWS**

AM roles are of 4 types, primarily differentiated by who or what can assume the role:

* Service Role
* Service-Linked Role
* Role for Cross-Account Access
* Role for Identity Provider Access

Segregation roles carried out by IAM with **Azure**

The four key roles that I want to introduce you to are **contributor, owner, reader, and user access administrator**. The contributor role is used to grant full access to manage all Azure resources.



**Components of IAM**

* Users
* Roles
* Groups
* Policies

**Services By IAM**

* Identity management
* Access management
* Federation
* [RBAC/EM](https://www.geeksforgeeks.org/role-based-access-control/)
* Multi-Factor authentication
* Access governance
* Customer IAM
* API Security
* [IDaaS – Identity as a service](https://www.geeksforgeeks.org/identity-as-a-service-idaas-as-a-cloud-based-service/)
* Granular permissions
* Privileged Identity management – PIM (PAM or PIM is the same)