BeSA

Week 5

4th June, 2022

Agenda

1. AWS IAM

2. Architecting for Security

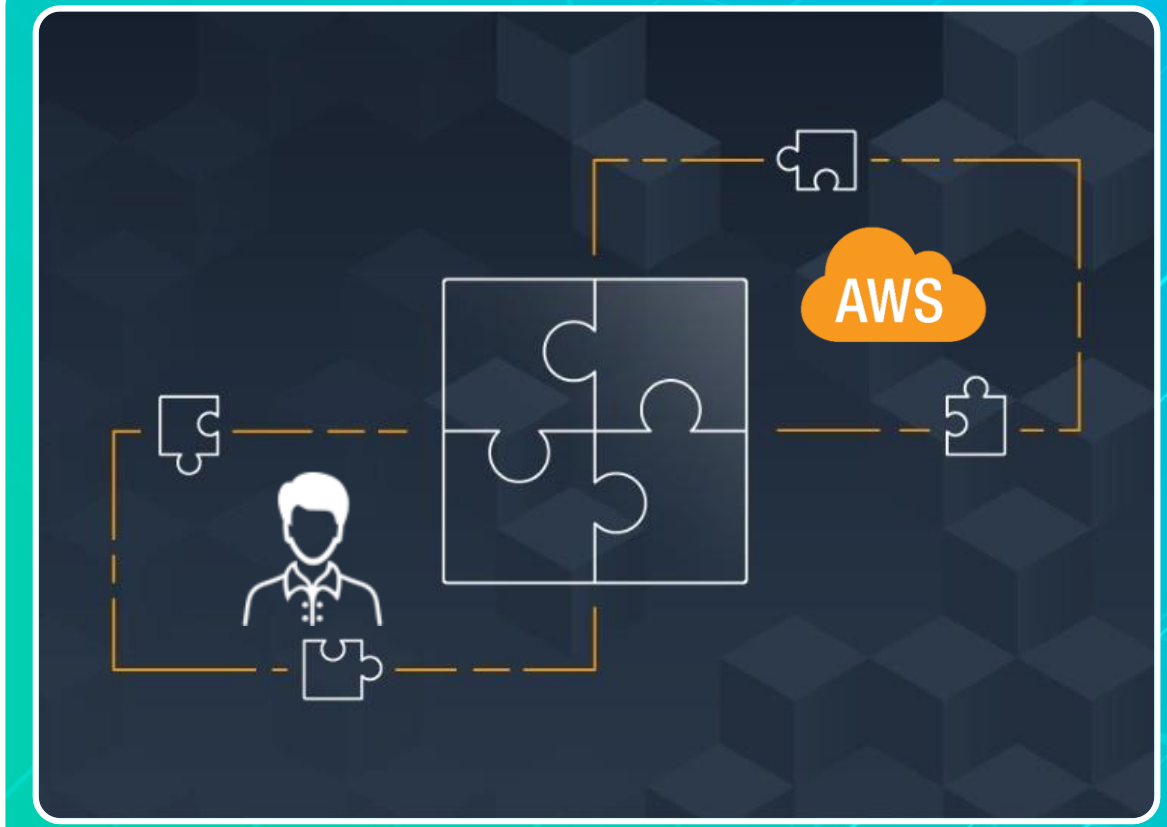
   - Alex

3. Create your own 6 months cloud learning plan

   - Prasad

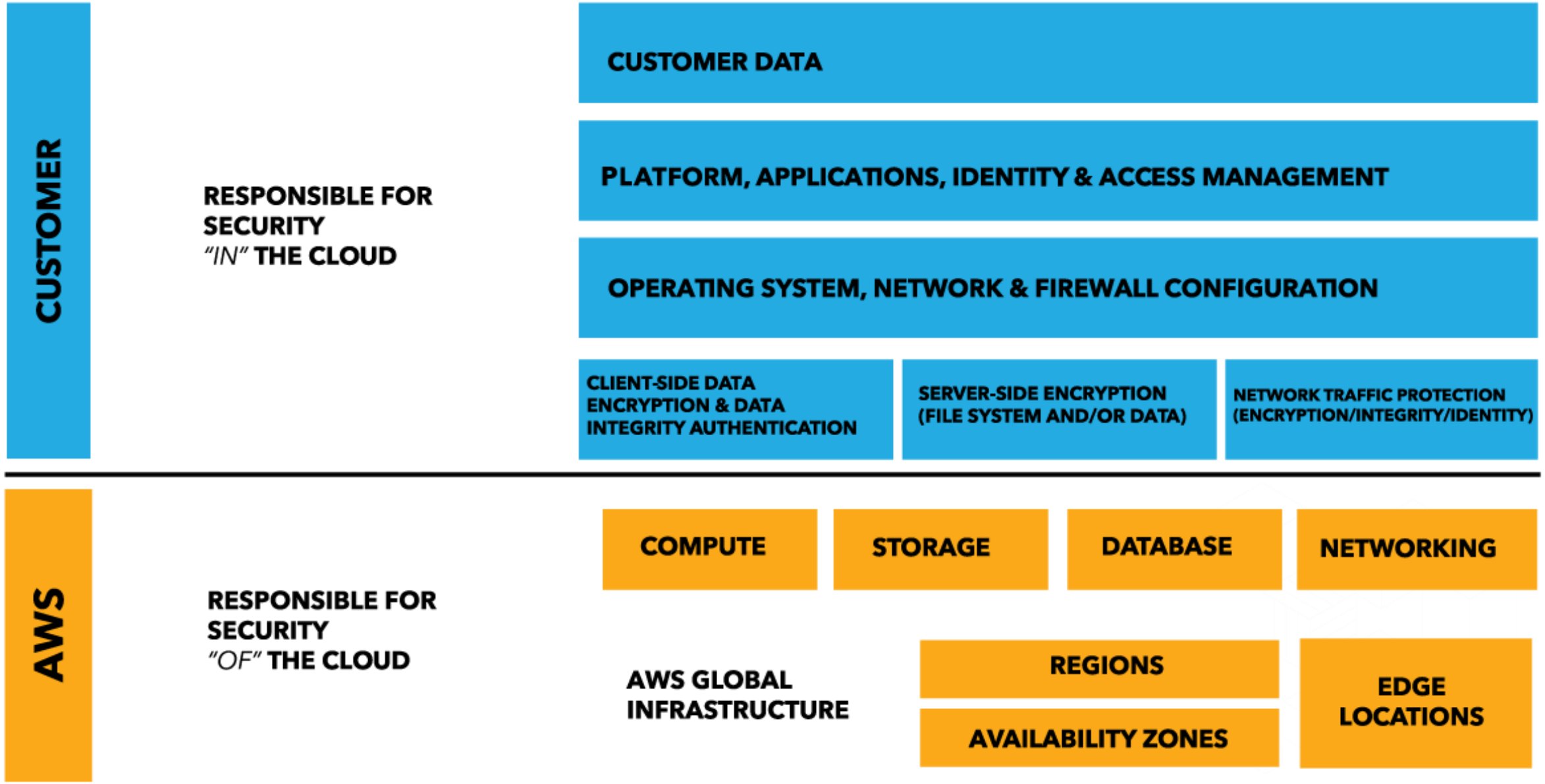
Identity and Access Management (IAM)

AWS Identity &
Access Management

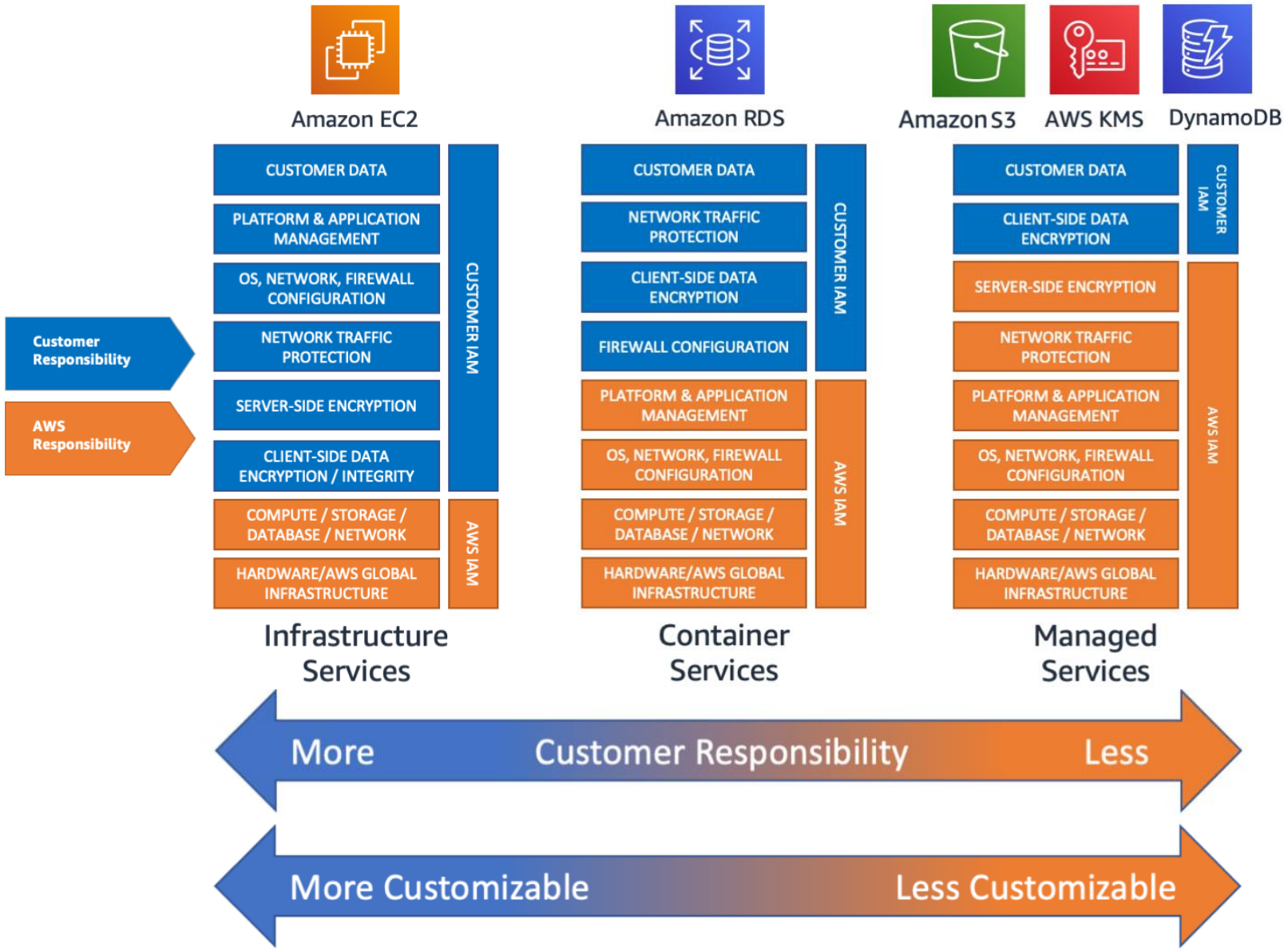


Shared Responsibility Model

AWS Shared Responsibility Model



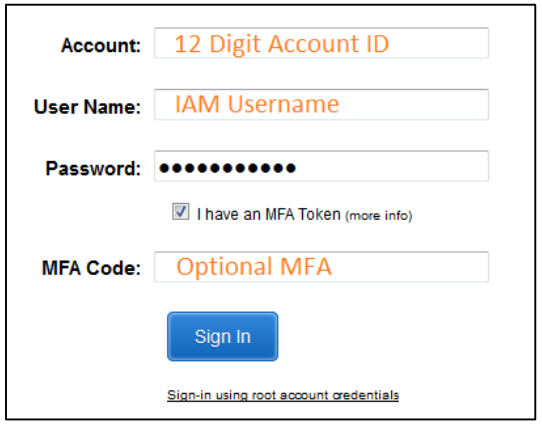
AWS Shared Responsibility Model



AWS Identity & Access Management (IAM)

Accessing AWS Services

IAM Username and Password

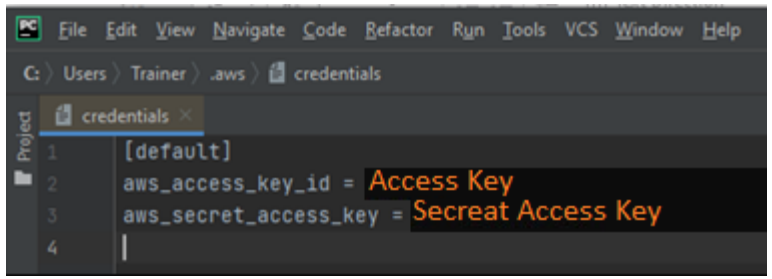


AWS Management Console

Access Key and Secret Access Key

```
C:\Users>aws configure
AWS Access Key ID [None]: Access Key
AWS Secret Access Key [None]: Secreat Access Key
Default region name [None]: Region
Default output format [None]: JSON / Text / Table
```

AWS Command Line Interface

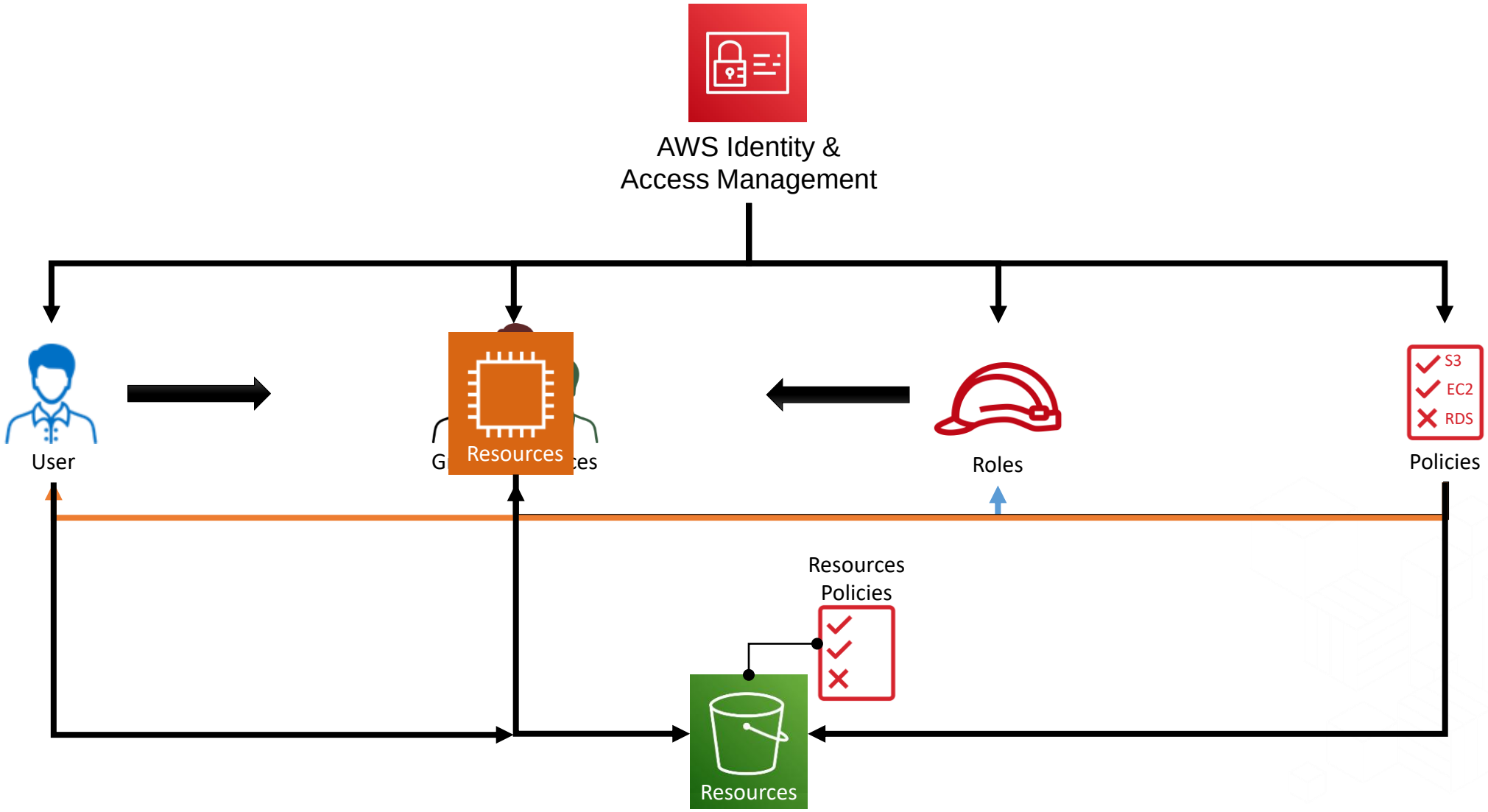


AWS Tools and SDKs

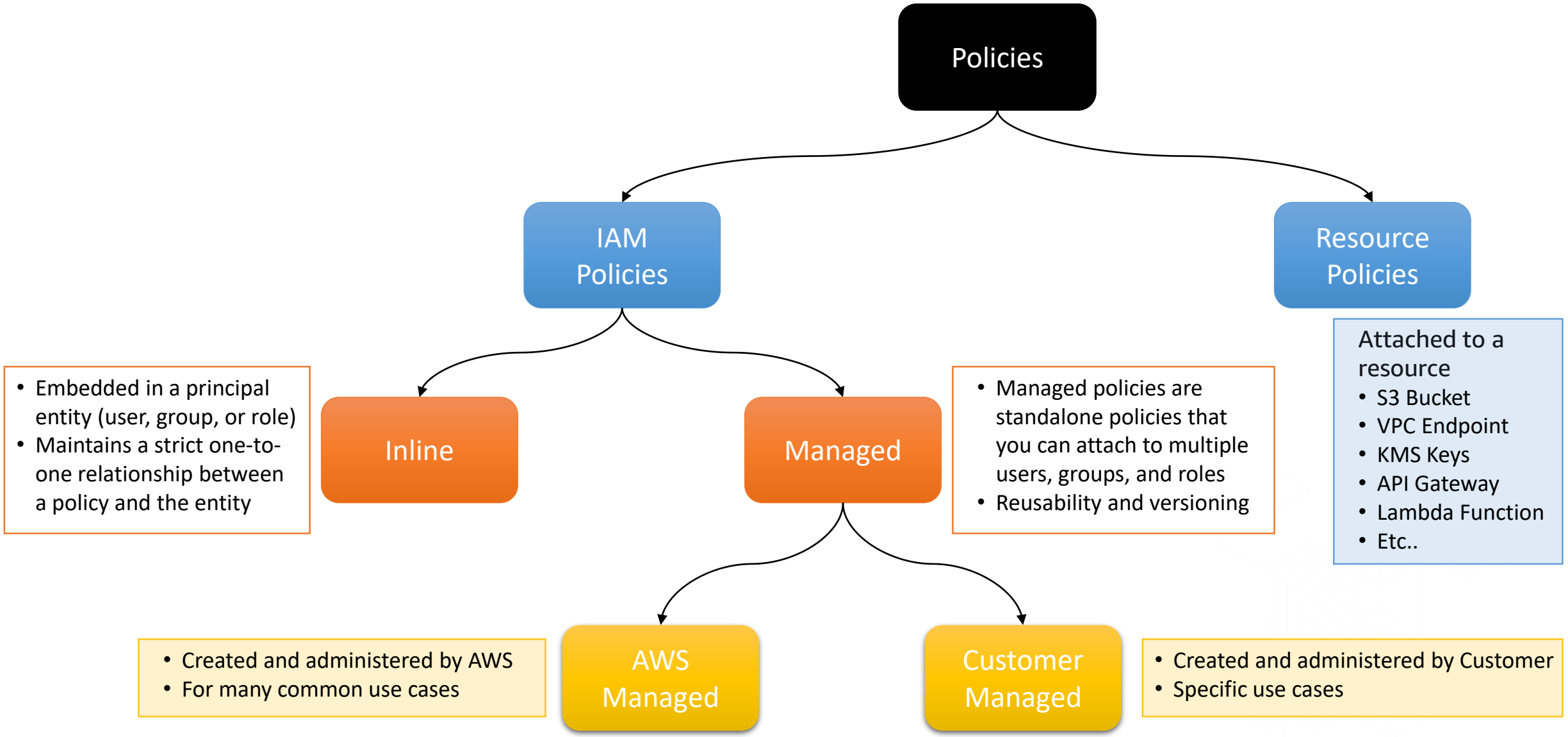
API
Application Programming Interface

AWS

IAM Resources



IAM and Resource Policies



AWS IAM

- Supports Identity Federation
- Use IAM Policy Simulator for troubleshooting
- Prefer Roles for temporary access
- Policy evaluation Logic

Step 1
- For every API call all applicable policies are combined.

Step 2
- If there is a matching Deny statement – decision is **Deny**.

Step 3
- If there is a matching Allow statement – decision is **Allow**.

Step 4
- If there is no matching statement – decision in **Deny**.

Reference:

FAQs

Category:

Security, Identity, and Compliance

AWS Identity and Access Management (IAM)

Created by:

Ashish Prajapati

What?

- AWS Identity and Access Management (IAM) provides fine-grained access control across all of AWS Services. With IAM, you can specify who can access which services and resources, and under which conditions.
- With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.

Why?

- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

When?

- You want to grant different fine-grained permissions to different people for different resources.
- You want to add two-factor authentication to your account and to individual users for extra security.
- You need to use existing corporate identities to grant secure access to AWS resources using identity federation.

Where?

- IAM is a global service.
- You use IAM to control access to tasks that are performed using the AWS Management Console, the AWS Command Line Tools, or service API operations using the AWS SDKs.

Who?

- You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources.
- You can create multiple IAM users under your AWS account or enable temporary access through identity federation.

How?

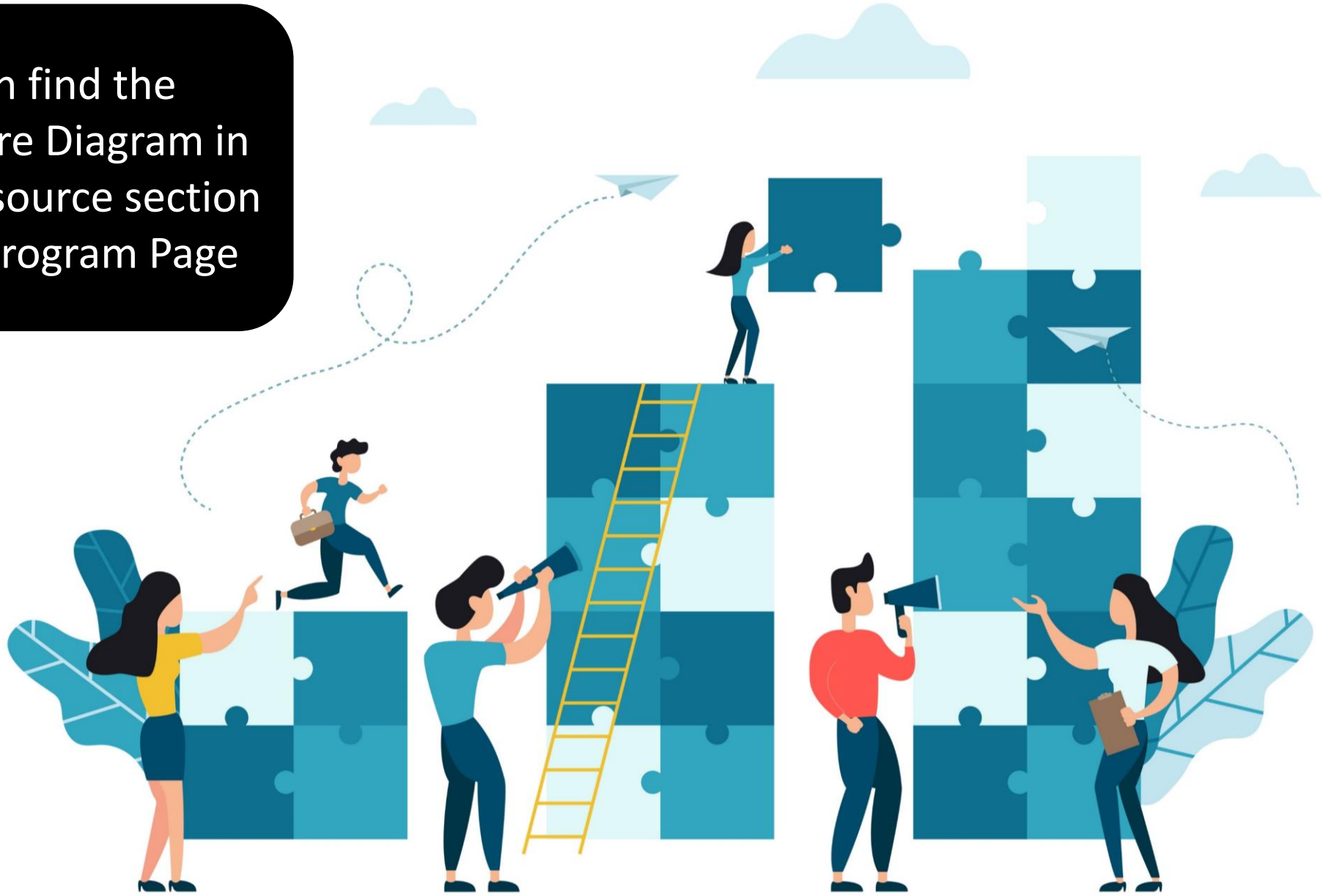
- With IAM, you define who can access what by specifying fine-grained permissions. IAM then enforces those permissions for every request. Access is denied by default and access is granted only when permissions specify an “Allow”.
- You can delegate access to users or AWS services to operate within your AWS account.

How much?

- There is no charge to use IAM.

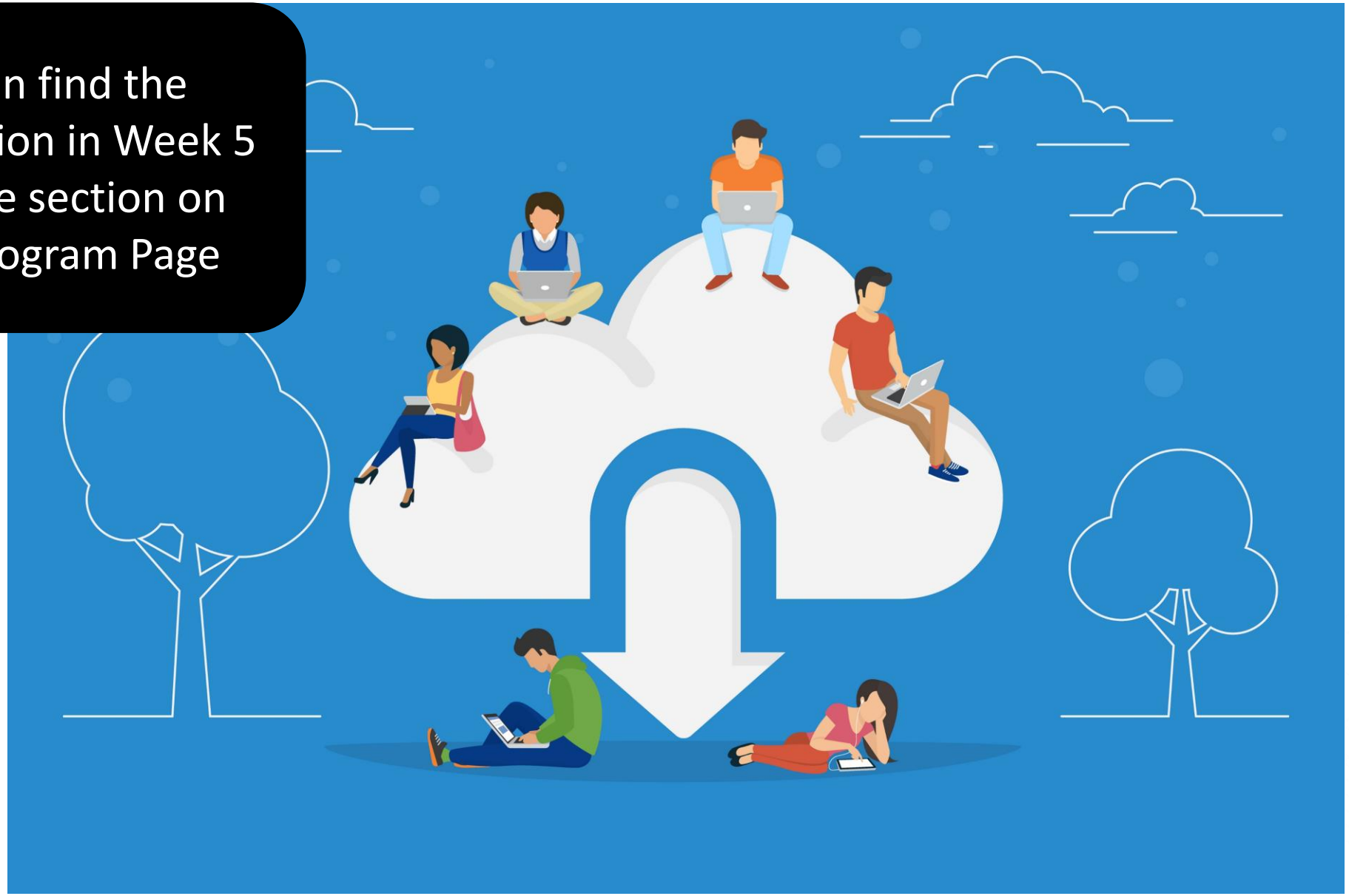
Architecting for Security - Alex

You can find the Architecture Diagram in Week 5 Resource section on BeSA Program Page



Create your own six-month cloud learning plan - Prasad

You can find the Presentation in Week 5 Resource section on BeSA Program Page



Thank you for attending. See you next Saturday (11-Jun-2022)

BeSA

Become a Solutions Architect

For content check **Resources Link** on BeSA Home Page