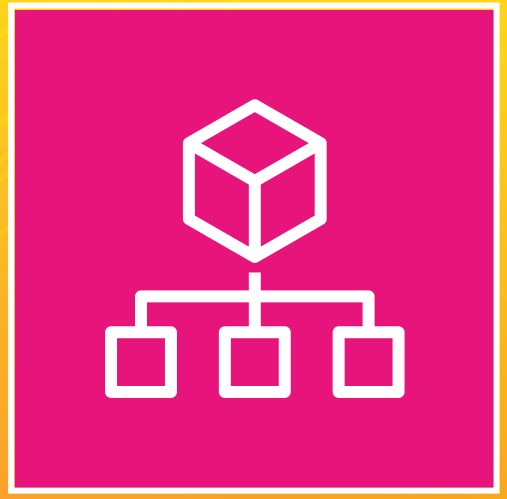
Identify

AWS Foundational and Layered Security Services



AWS Organizations

Why multiple accounts?

Governance

Security Policies

Blast Radius

Account limits

Operational Boundary

Cost Visibility

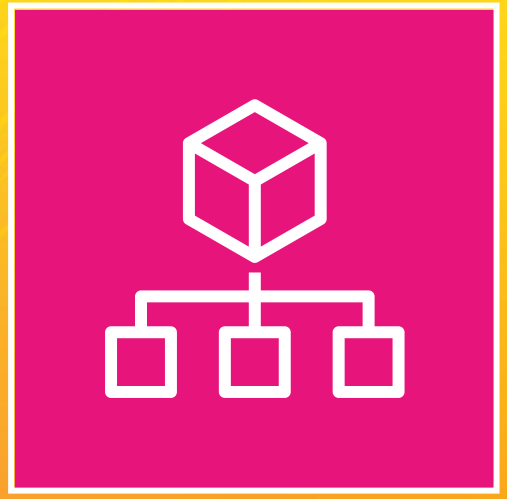
Support Plan

Challenges in Multi Account AWS Environment

Operational Overhead

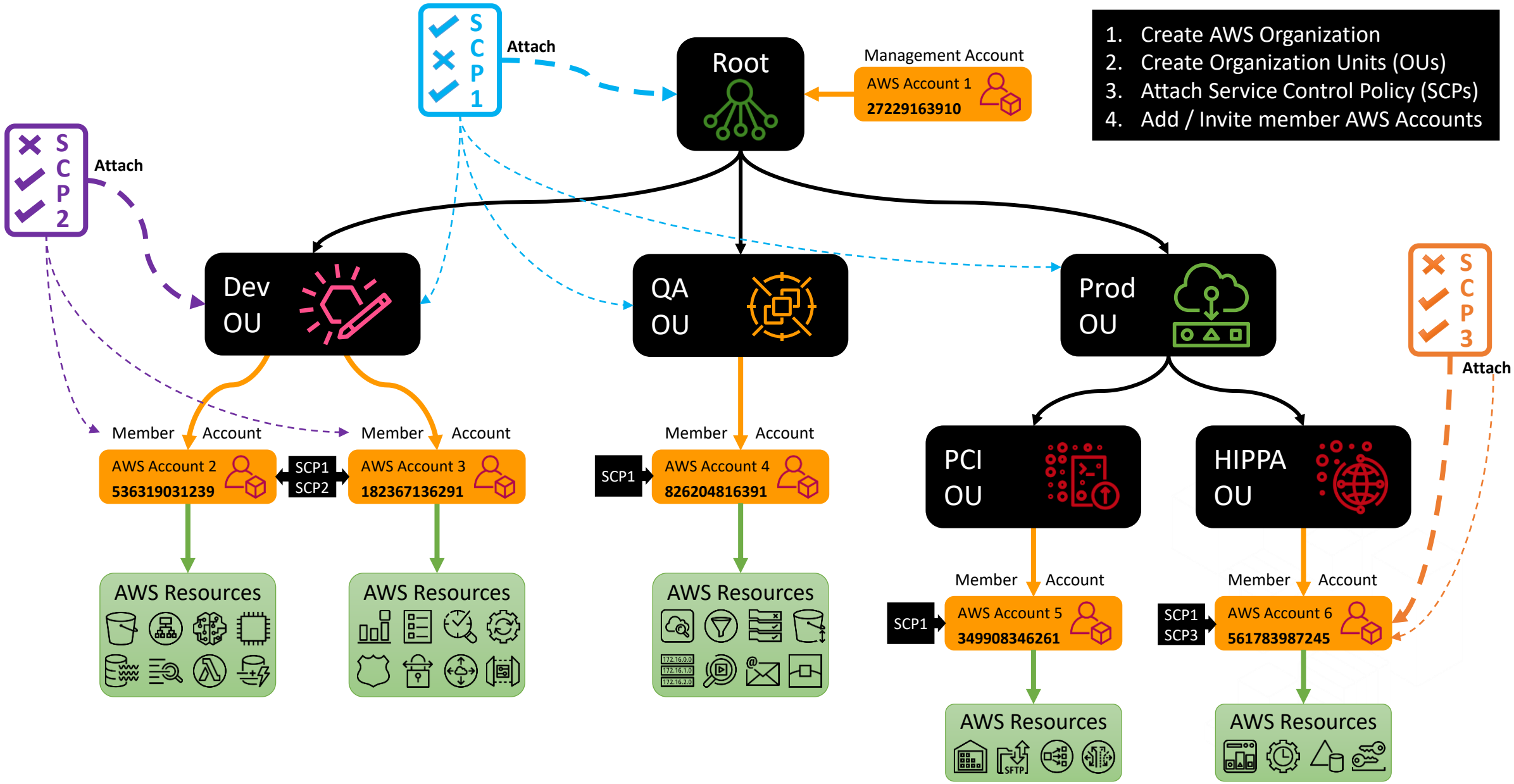
Individual Billing

Security Control



AWS Organizations

AWS Organization



SCP Examples

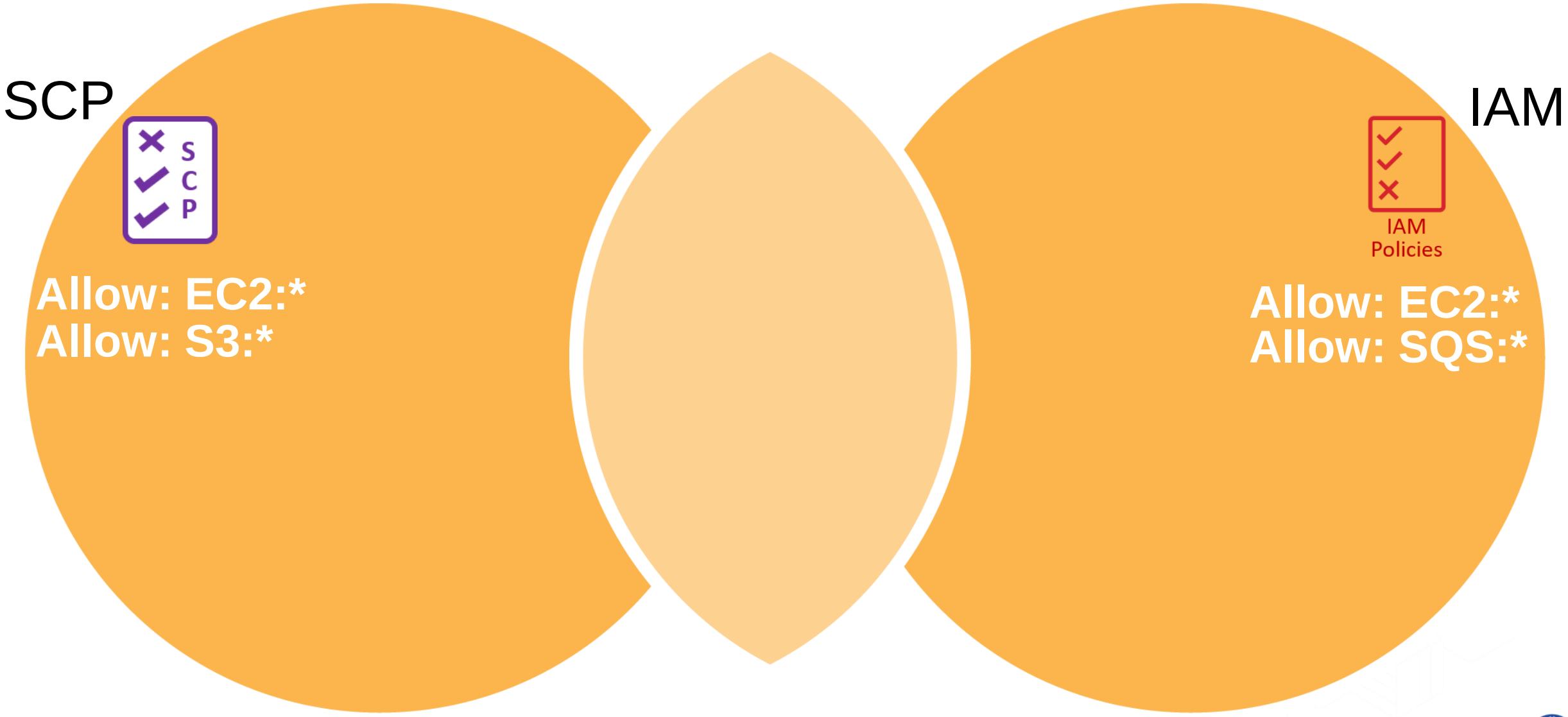
Allow example

```
{
 "Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":[
     "EC2:*","S3:*”
      ],
    "Resource":"*"
    }
  ]
}
```

Deny example

```
{
 "Version":"2012-10-17",
  "Statement":[
   {
    "Effect":”Deny",
    "Action":[
     ”SQS:*”
      ],
    "Resource":"*"
    }
  ]
}
```

Effective Permission



SCP Examples

- No Internet Gateway for VPC

```
"Statement": [
       {
      "Effect": "Deny",
      "Action": [
              "ec2:AttachInternetGateway”,
              “ec2:CreateInternetGateway”,
              “ec2:AttachEgressOnlyInternetGateway”,
              “ec2:CreateVpcPeeringConnection”,
              “ec2:AcceptVpcPeeringConnection"
                    ],
      "Resource": "*"
    }
  ]
```

- Stop CloudTrail from being disabled

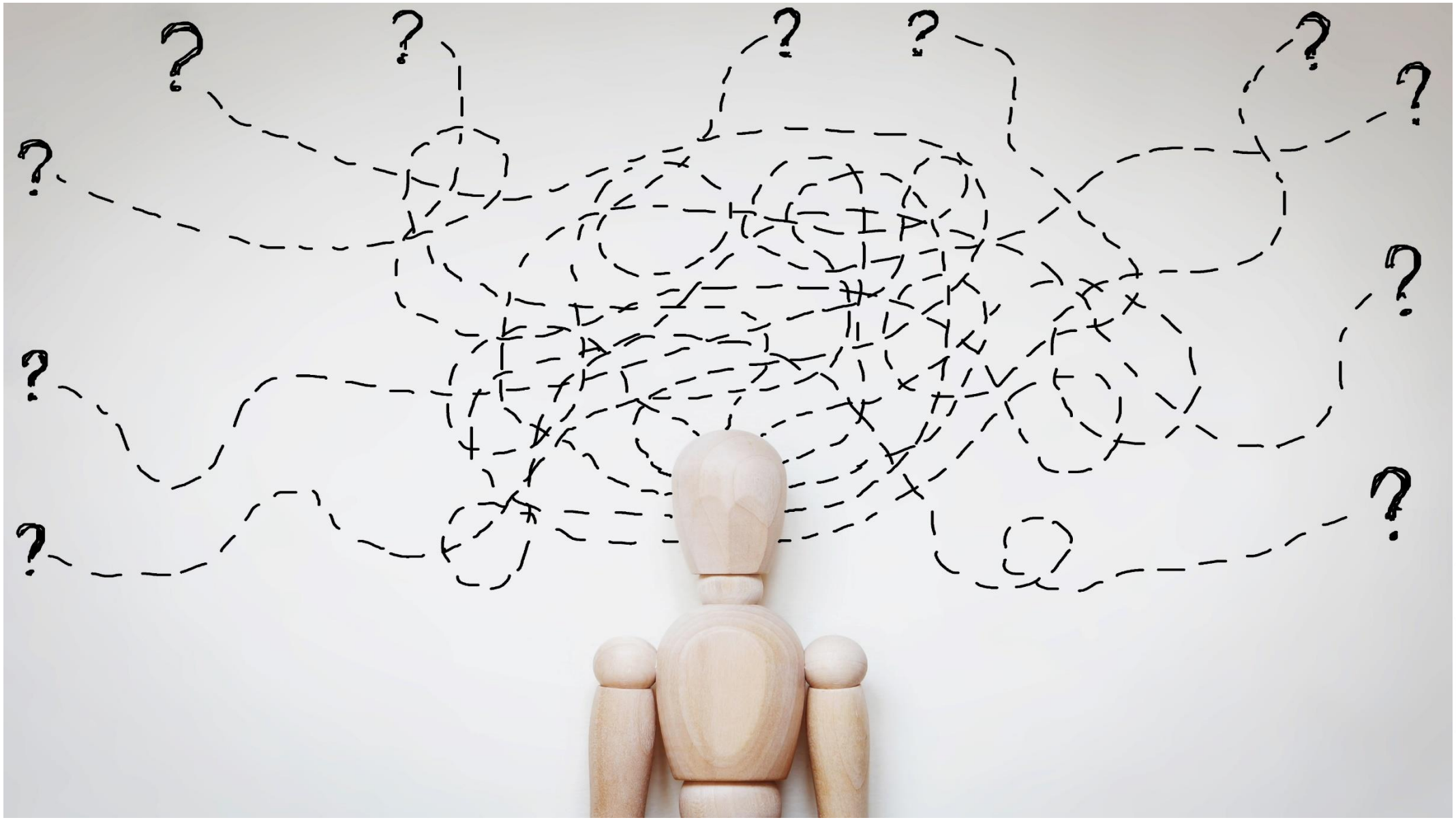
```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": ”cloudtrail:StopLogging",
      "Resource": "*"
    }
  ]
}
```

More Example service control policies

AWS Control Tower

Can you design an airport?

Where to start?



Lets use the best practices from other successful airport designs

Setting up a new AWS Multi-account architecture

Initial Setup

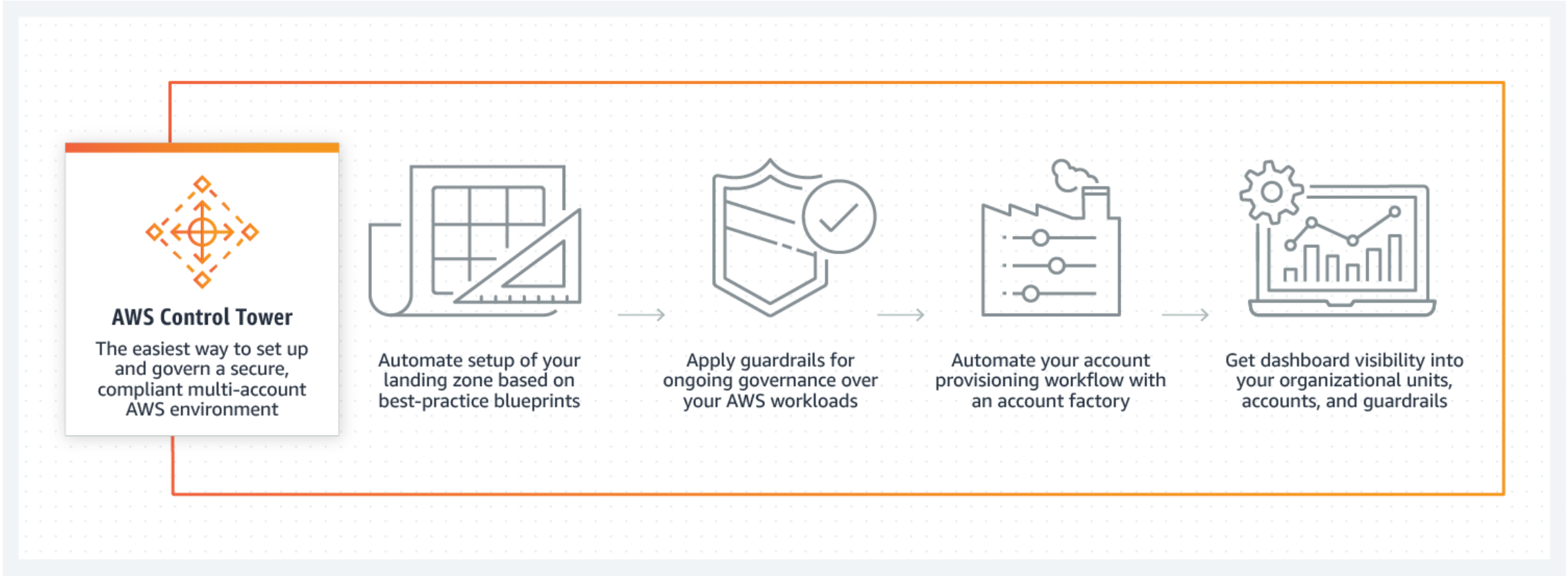
- Create Organization Management account
  - Create temporary Amazon S3 bucket of AWS CloudTrail logs
  - Enable CloudTrail locally
  - Enable AWS Organization full feature
- Create Log Archive account
  - Create bucket(s) for security logs
- Create Security account
  - Create Roles – Read Only | Power Users | Admin
- Create a Shared Services Account
  - Configure Single Sign-On (SSO)

Repeat setup for every account

- Secure Root credentials
- Complex password policy
- Link to Organization Master account
- Enable CloudTrail
- Send Log to Archive account
- Enable Amazon GuardDuty
- Enable AWS Config
- Enable appropriate Config rules
  - Amazon S3 bucket encryption
  - Amazon S3 block public access
  - EBS Volume encryption
  - Etc…
- Create common cross-account Security role
  - Read Only | Power User | Admin
- Create VPC (non-overlapping IP space)
- Enable federation into account (SSO)
- Etc..

AWS Control Tower

- AWS Control Tower provides the easiest way to set up and govern a secure, compliant, multi-account AWS environment based on best practices established by working with thousands of enterprises.



AWS Control Tower

Landing zone

Guardrails

Account Factory

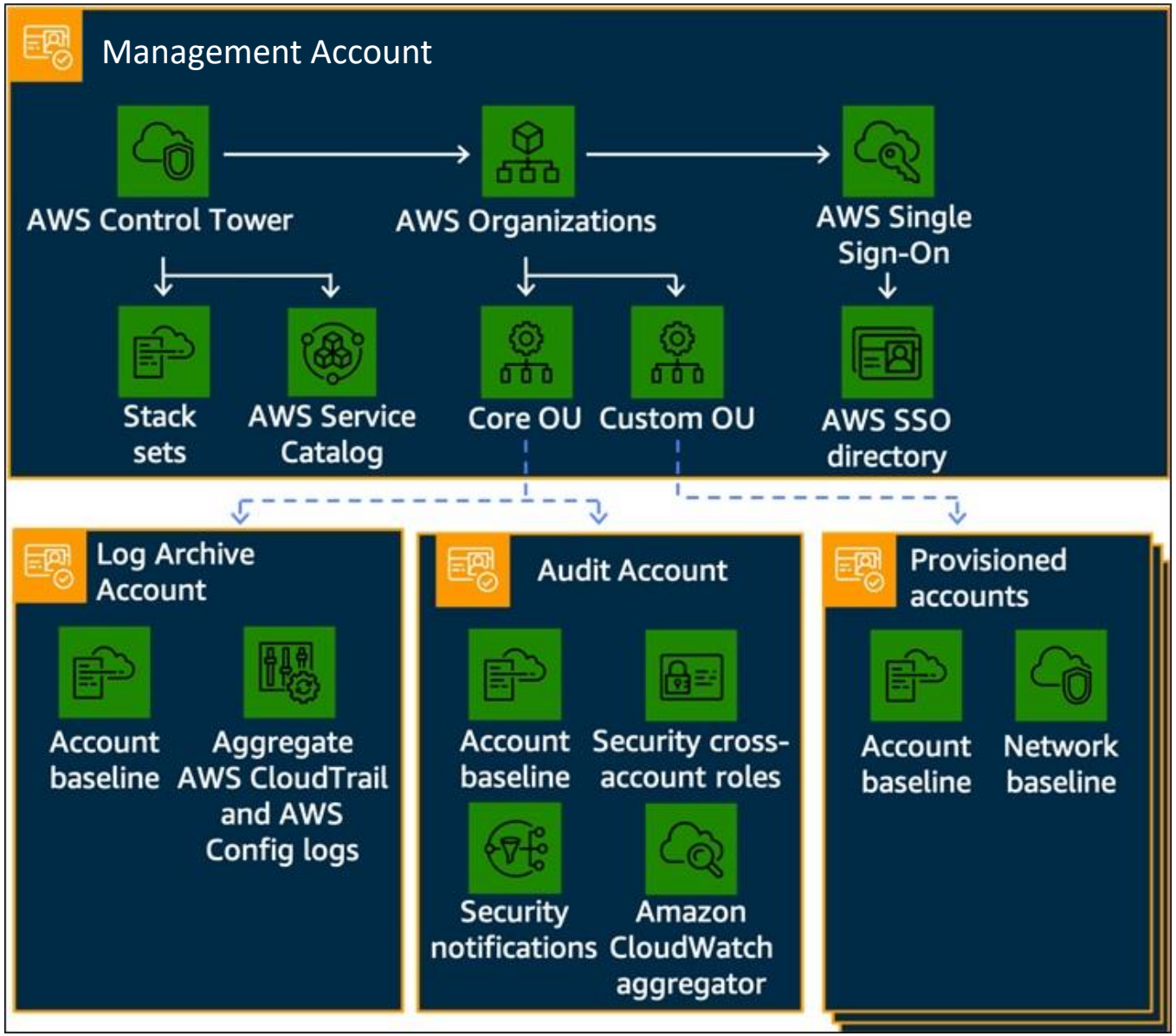
Dashboard

AWS Control Tower – Landing Zone

Landing zone

A well-architected, multi-account AWS environment based on security and compliance best practices.

Landing Zone Structure



Underlying services

- AWS Organizations
- AWS Service Catalog
- AWS Single Sign-on
- AWS Config
- AWS CloudFormation

▼ View all underlying services

- Amazon CloudWatch
- AWS CloudTrail
- AWS Identity and Access Management
- Amazon Simple Storage Service
- Amazon Simple Notification Service
- AWS Lambda
- AWS Step Functions

Related services

- AWS Security Hub
- AWS Systems Manager

No additional charge exists for using AWS Control Tower.

AWS Control Tower - Guardrails

Landing zone

A well-architected, multi-account AWS environment based on security and compliance best practices.

Guardrails

A high-level rule that provides ongoing governance for your overall AWS environment.

AWS Control Tower – Account Factory

Landing zone

A well-architected, multi-account AWS environment based on security and compliance best practices.

Guardrails

A high-level rule that provides ongoing governance for your overall AWS environment.

Account Factory

A configurable account template that helps provisioning of new AWS accounts with pre-approved account configurations.

AWS Control Tower

Landing zone

A well-architected, multi-account AWS environment based on security and compliance best practices.

Guardrails

A high-level rule that provides ongoing governance for your overall AWS environment.

Account Factory

A configurable account template that helps provisioning of new AWS accounts with pre-approved account configurations.

Dashboard

Offers continuous oversight of your landing zone to your team of central cloud administrators.