A unique opportunity for you to be mentored by Amazonians

BeSA

Become a Solutions Architect

Week 4
8-Oct-2022

Agenda

Technical Track

- Multi Account Structure
  - Ashish Prajapati

Serverless Track

- Step Functions
  - James Eastham

Behavioural Track

- Guest Speaker
  - Prasad Rao

Why multiple accounts?

Governance

Security Policies

Blast Radius

Account limits

Operational Boundary

Cost Visibility

Support Plan

Challenges in Multi Account AWS Environment

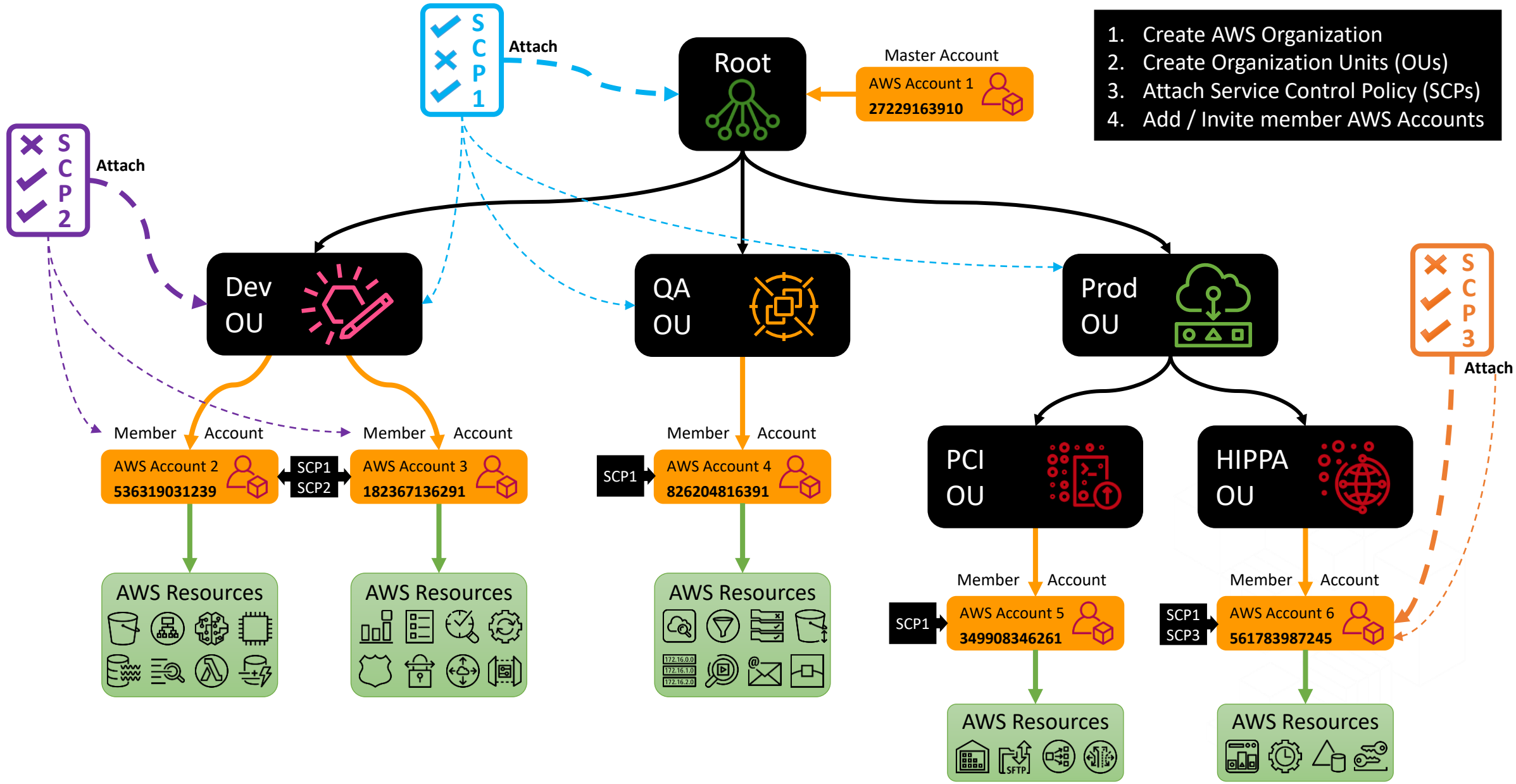
Operational Overhead

Individual Billing

Security Control

AWS Organizations

AWS Organization



SCP Examples

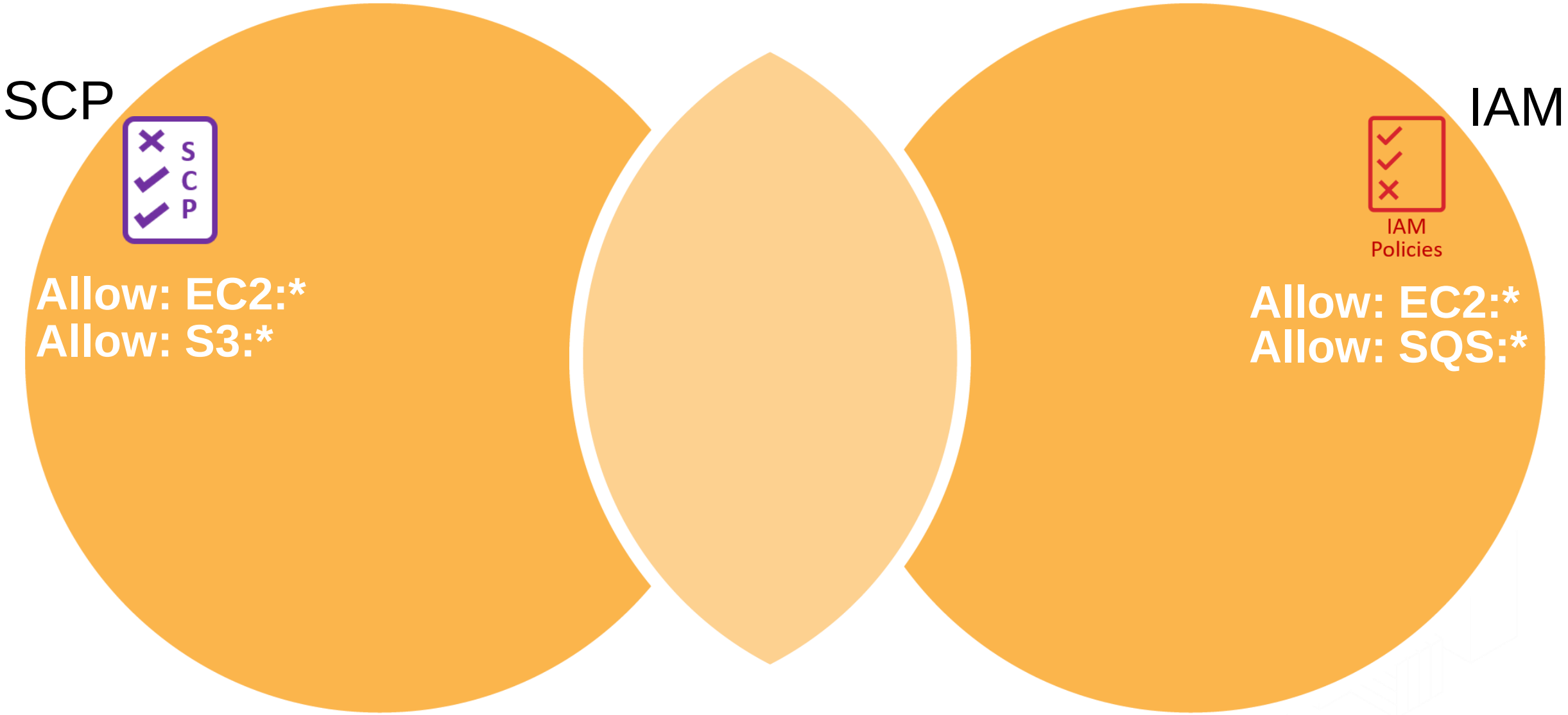
Allow example

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

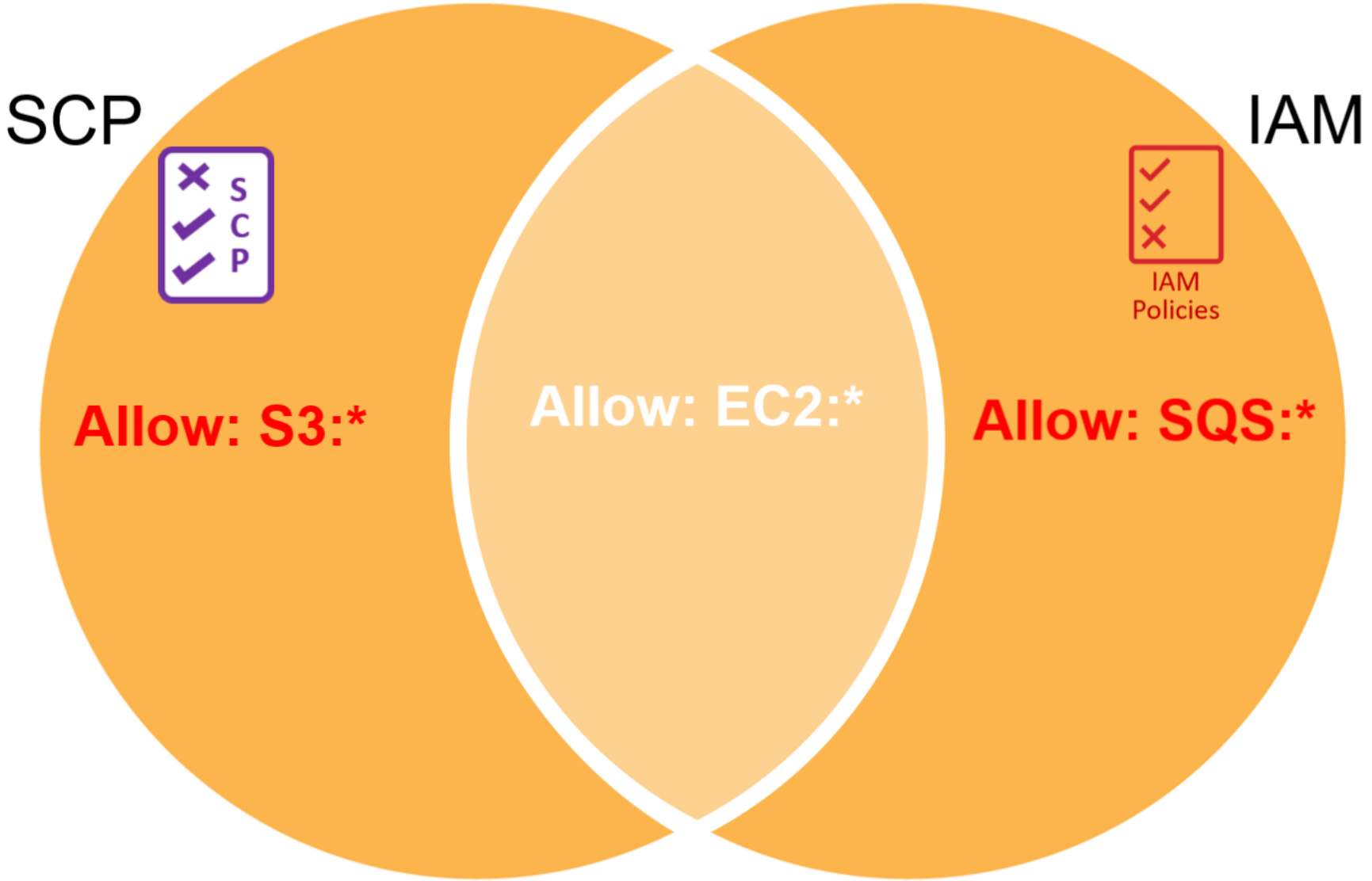
Deny example

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

Effective Permission



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

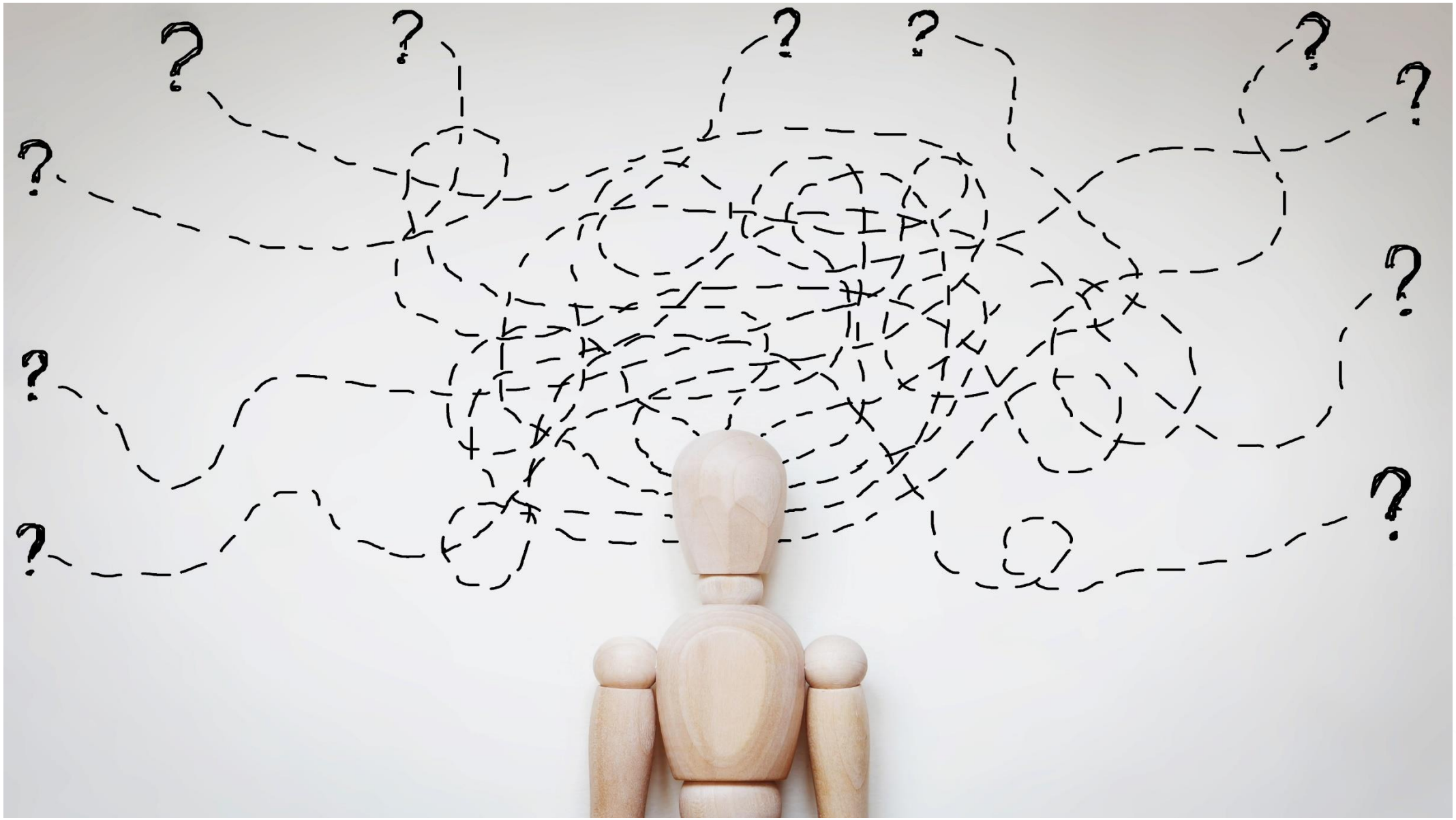
```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": ”cloudtrail:StopLogging",
      "Resource": "*"
    }
  ]
}
```

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

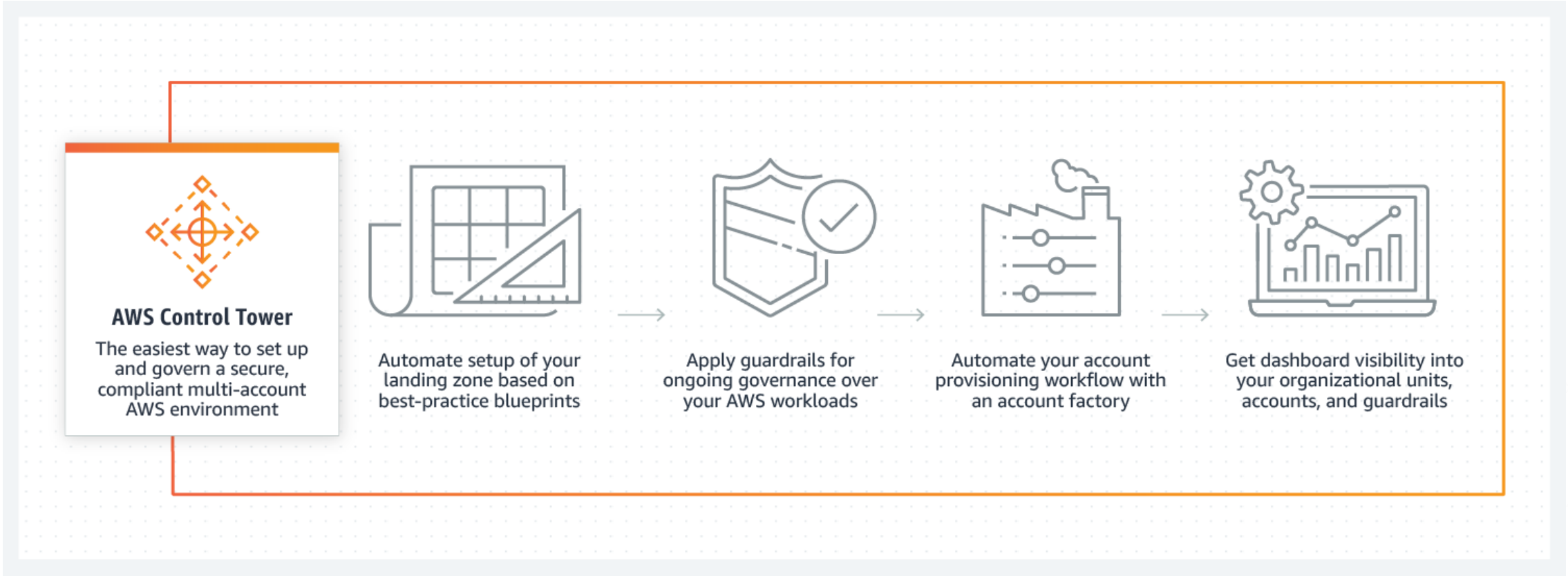
- Create Organization Master account
  - Create temporary Amazon S3 bucket of AWS CloudTrail logs
  - Enable CloudTrail locally
  - Enable AWS Organization full feature
- Create Log Archive account
  - Create bucket(s) for security logs
- Create Security account
  - Create Roles – Read Only | Power Users | 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

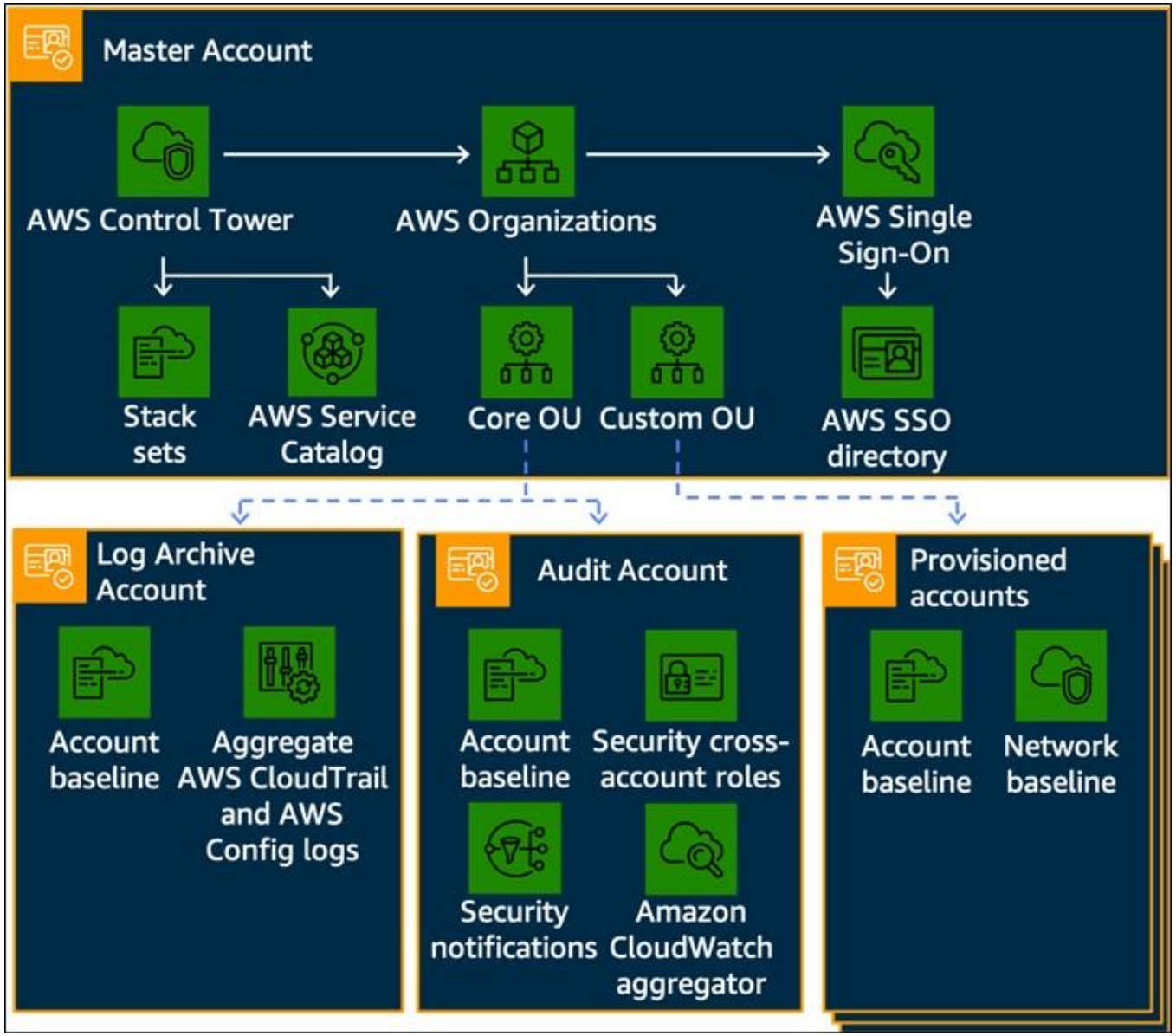
Dashboard

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

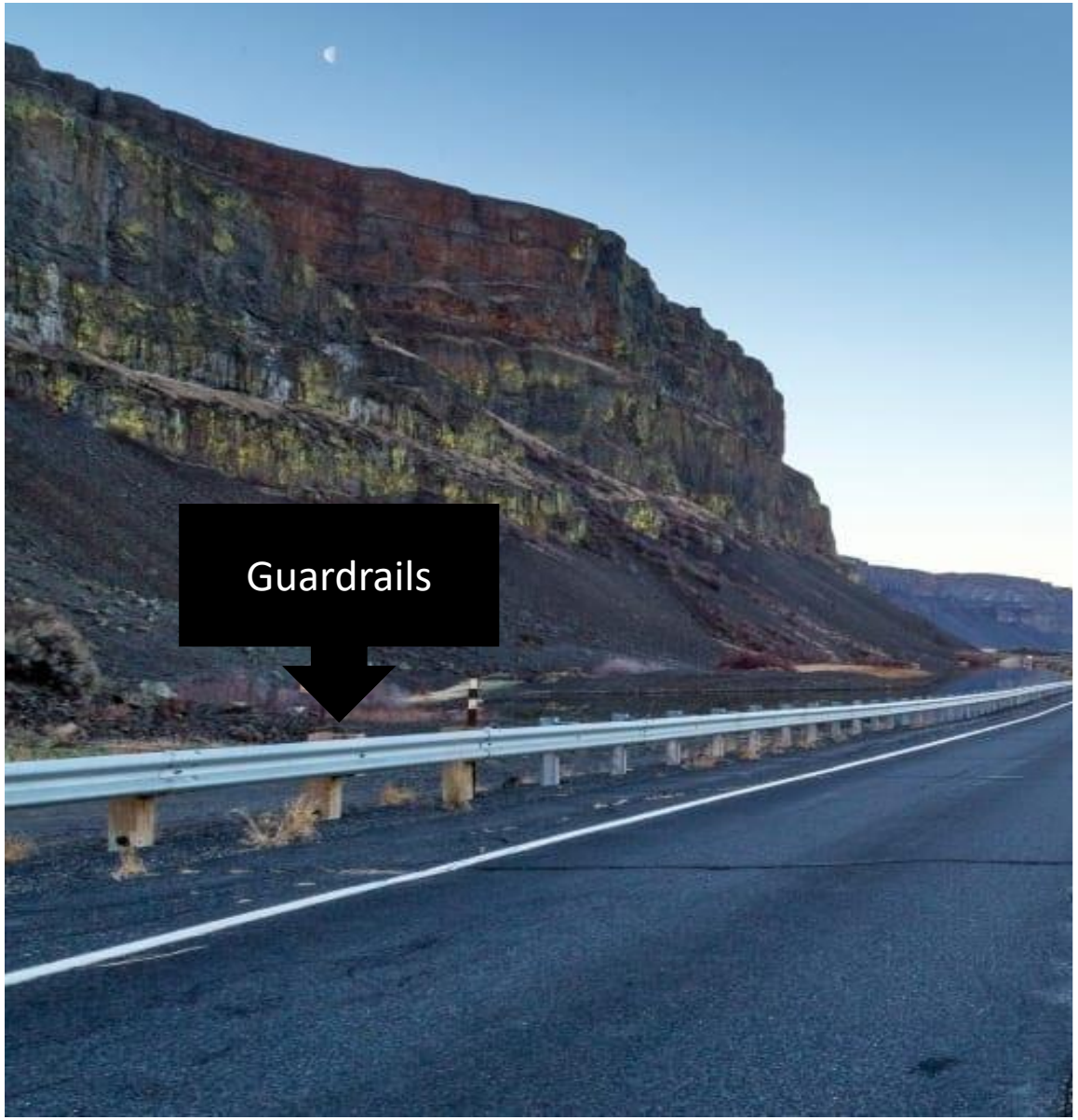
A well-architected, multi-account AWS environment based on security and compliance best practices.

Guardrails

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

Guardrails in real life

Guardrails in real life



Guardrails in AWS Control Tower

- A guardrail is a high-level rule that provides ongoing governance for your overall AWS environment. It's expressed in plain language.
- Through guardrails, AWS Control Tower implements **preventive** or **detective** controls that help you govern your resources and monitor compliance across groups of AWS accounts.

Goal/category	Example
IAM security	Require MFA for root user
Data security	Disallow public read access to Amazon S3 buckets
Network security	Disallow internet connection via Remote Desktop Protocol (RDP)
Audit logs	Enable AWS CloudTrail and AWS Config
Monitoring	Enable AWS CloudTrail integration with Amazon CloudWatch
Encryption	Ensure encryption of Amazon EBS volumes attached to Amazon EC2 instances
Drift	Disallow changes to AWS Config rules set up by AWS Control Tower

AWS Control Tower – Account Factory

Landing zone

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

Guardrails

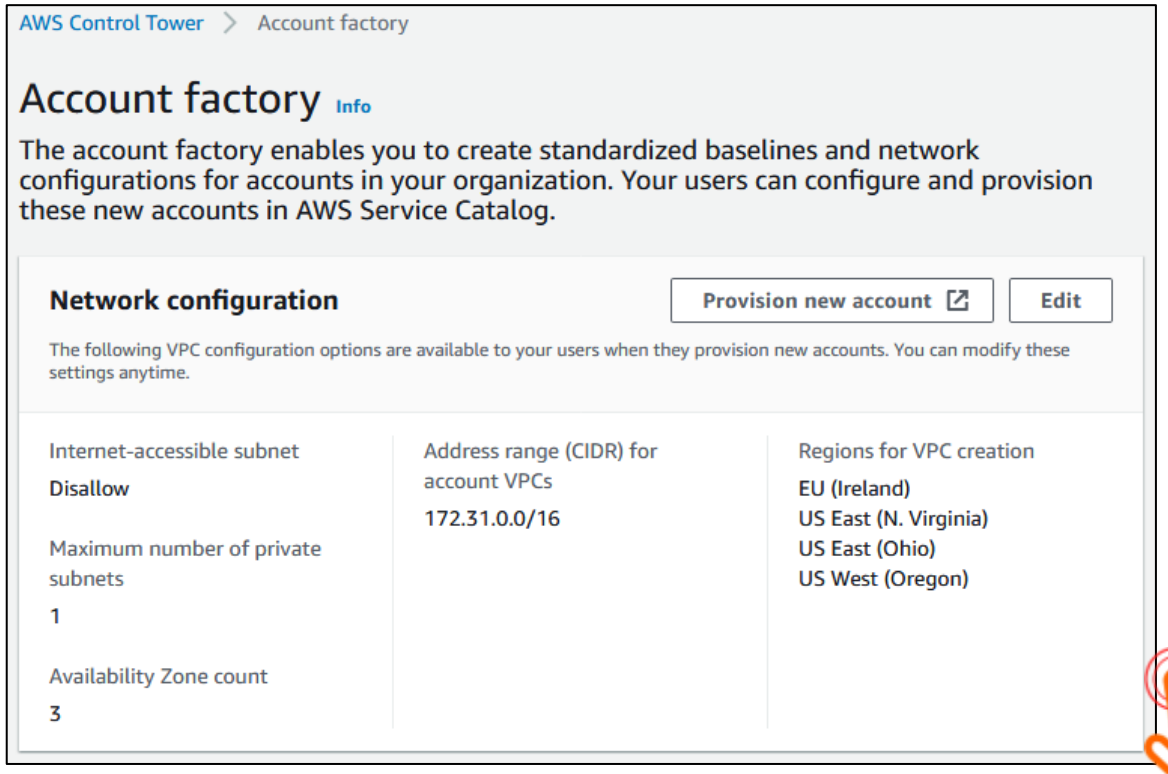
A high-level rule that provides ongoing governance for your overall AWS environment.

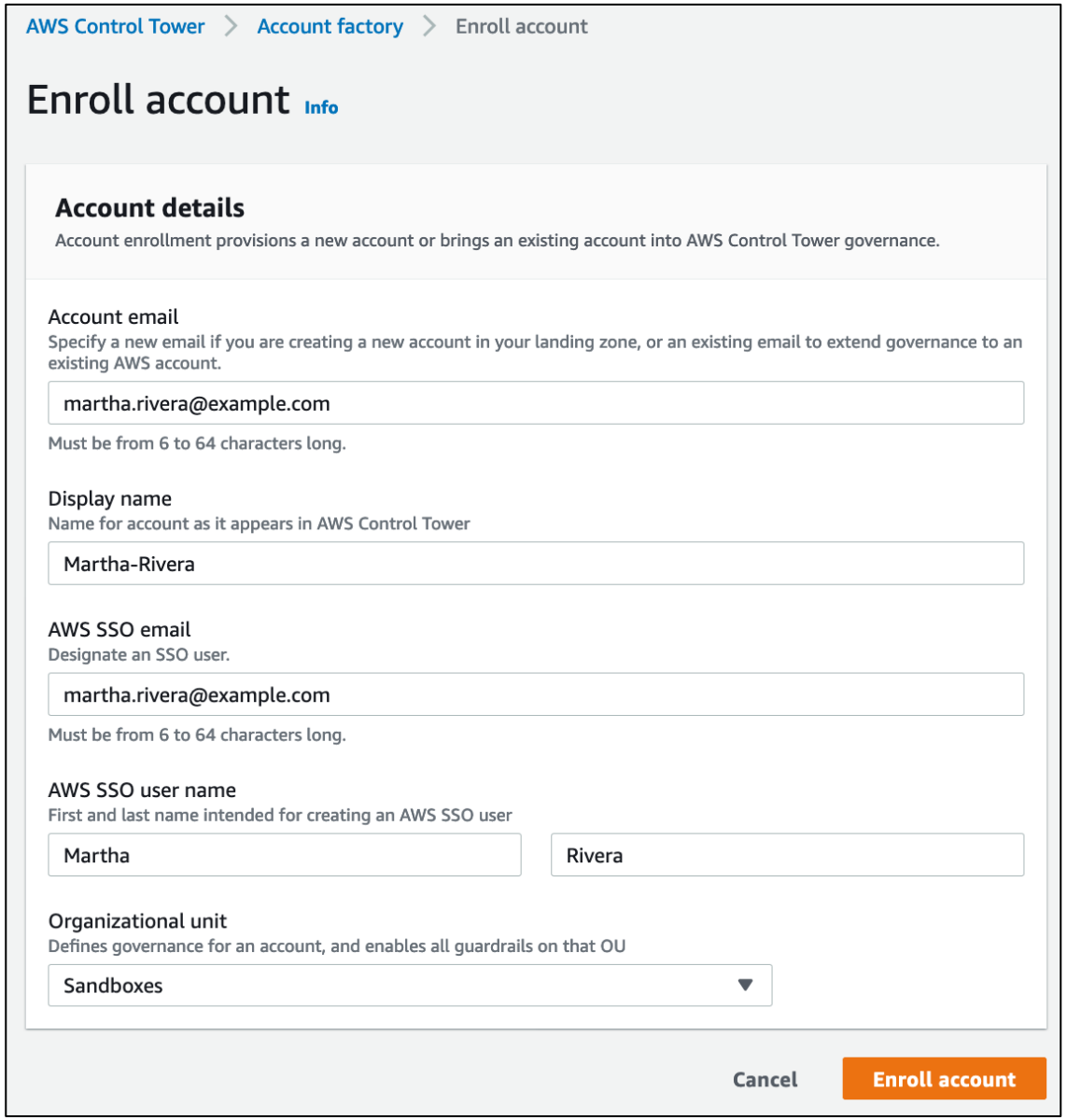
Account Factory

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

Account factory

- Account factory for controls on account provisioning
  - Pre approved account baselines with VPC options
  - Pre approved configuration options





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

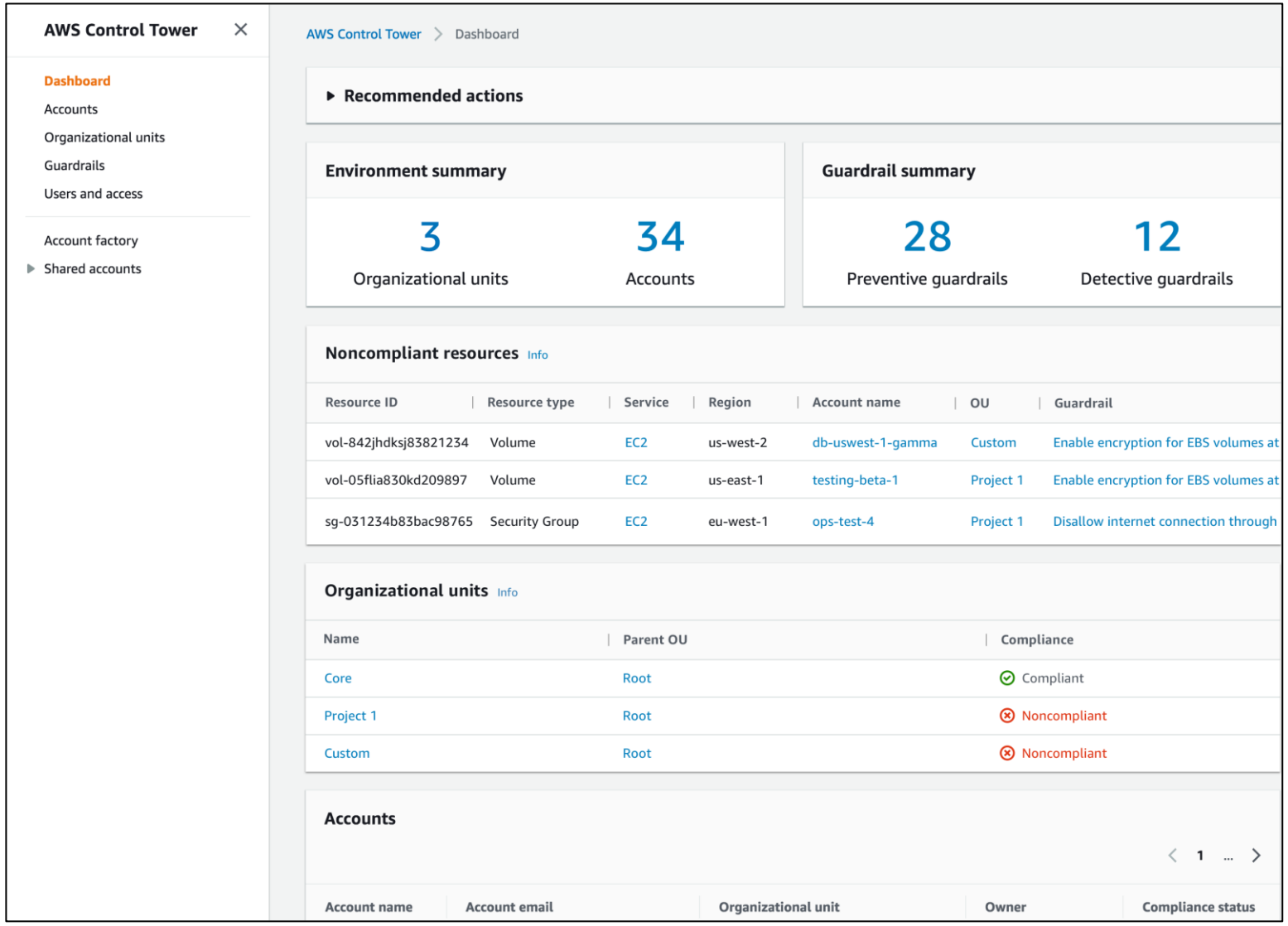
A configurable account template that helps provisioning of new AWS accounts with pre-approved account configurations.

Dashboard

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

Dashboard

- The Control Tower dashboard gives you continuous visibility into your AWS environment.
- You can view the number of OUs and accounts provisioned, the number of guardrails enabled, and the check the status of your OUs and accounts against those guardrails.
- You can also see a list of noncompliant resources with respect to enabled guardrails.

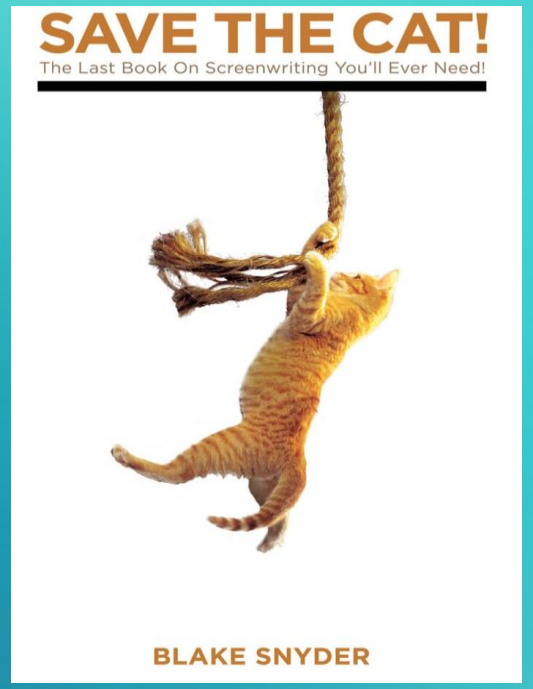


Let’s read some superb books

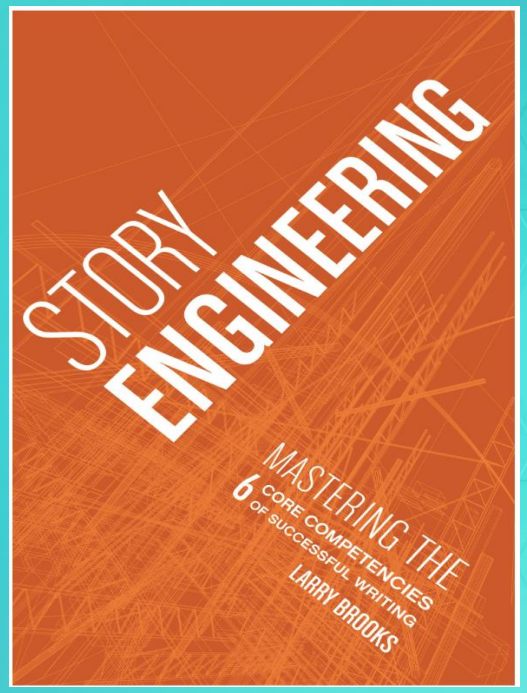
- Jamila Jamilova

BeSA
Become a Solutions Architect

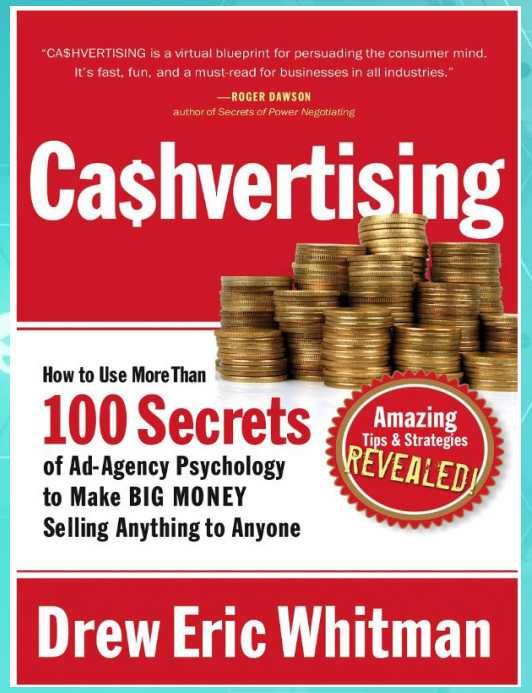
Essential books on structure and frame of mind



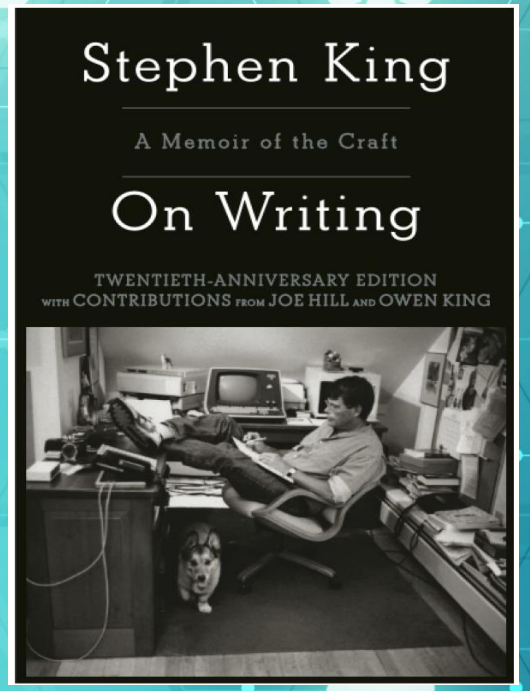
Categories: Primarily structure and formula



Categories: Heavy on structure



Categories: Structure and using the mechanics of language



Categories: Primarily writing life with a frame of mind and structure insight

Serverless Track

- James Eastham

Thank you.

See you next week.