

A unique opportunity for you to be mentored by Amazonians



Week 4
8-Oct-2022



Training



Motivation



Direction



Success



Advice



Goal



Coaching



Support



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



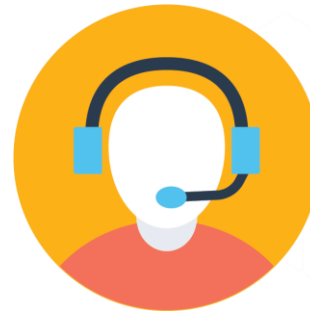
Account limits



Operational Boundary



Cost Visibility



Support Plan



Challenges in Multi Account AWS Environment



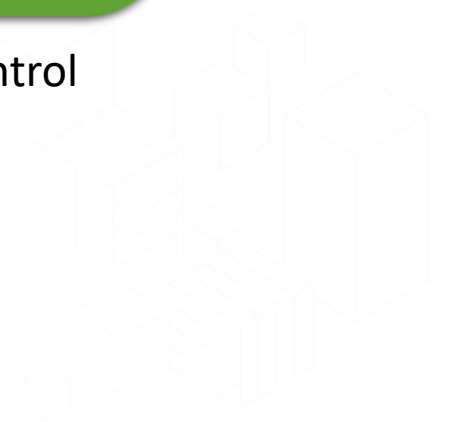
Operational Overhead

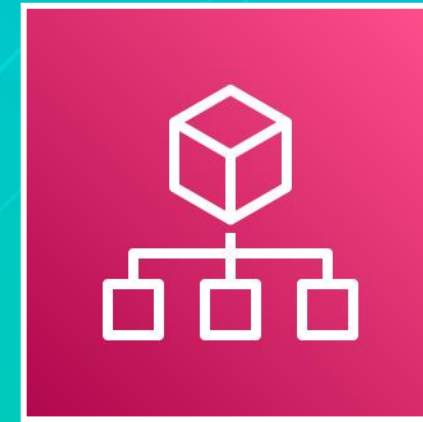


Individual Billing



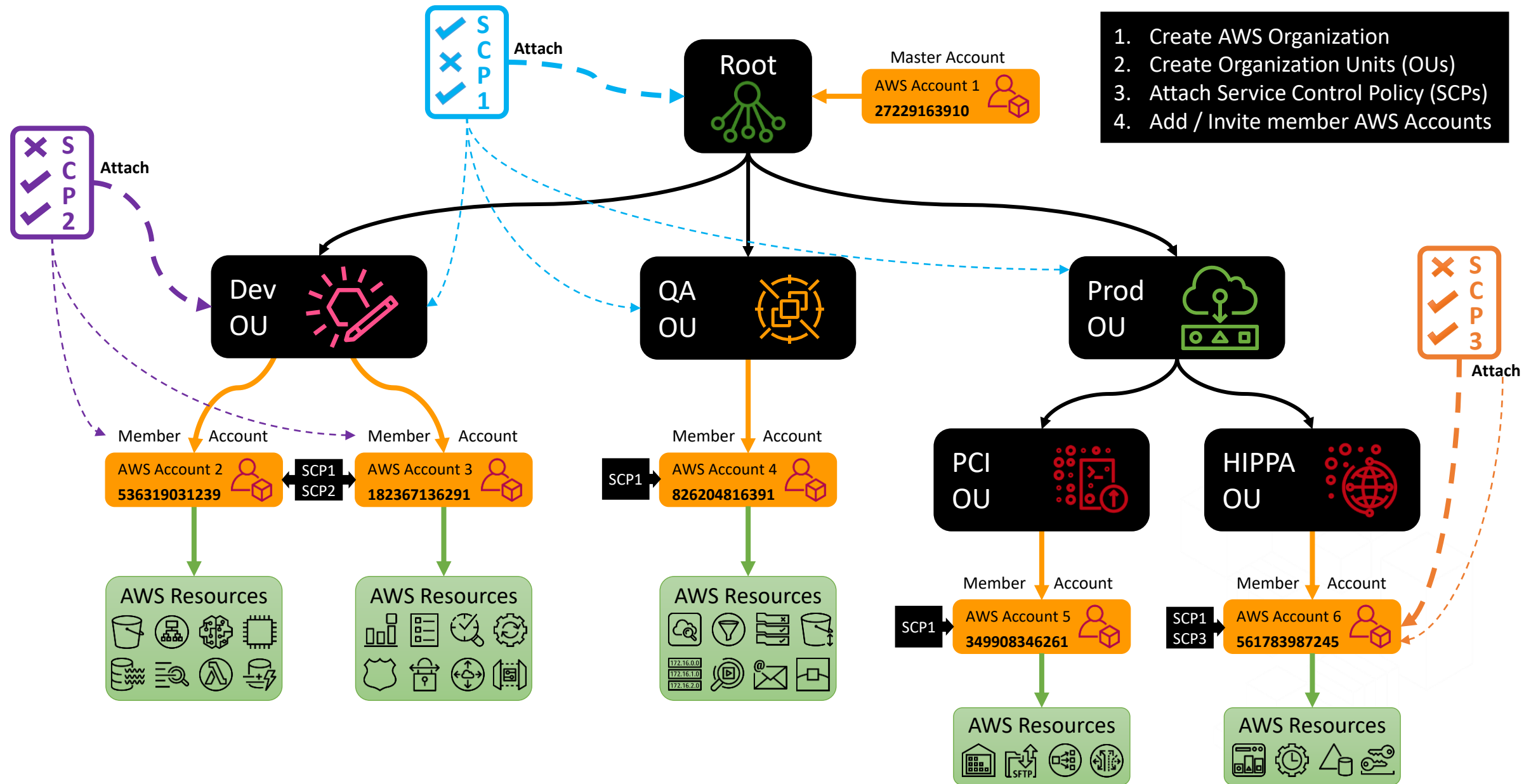
Security Control





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

SCP



Allow: EC2:*
Allow: S3:*

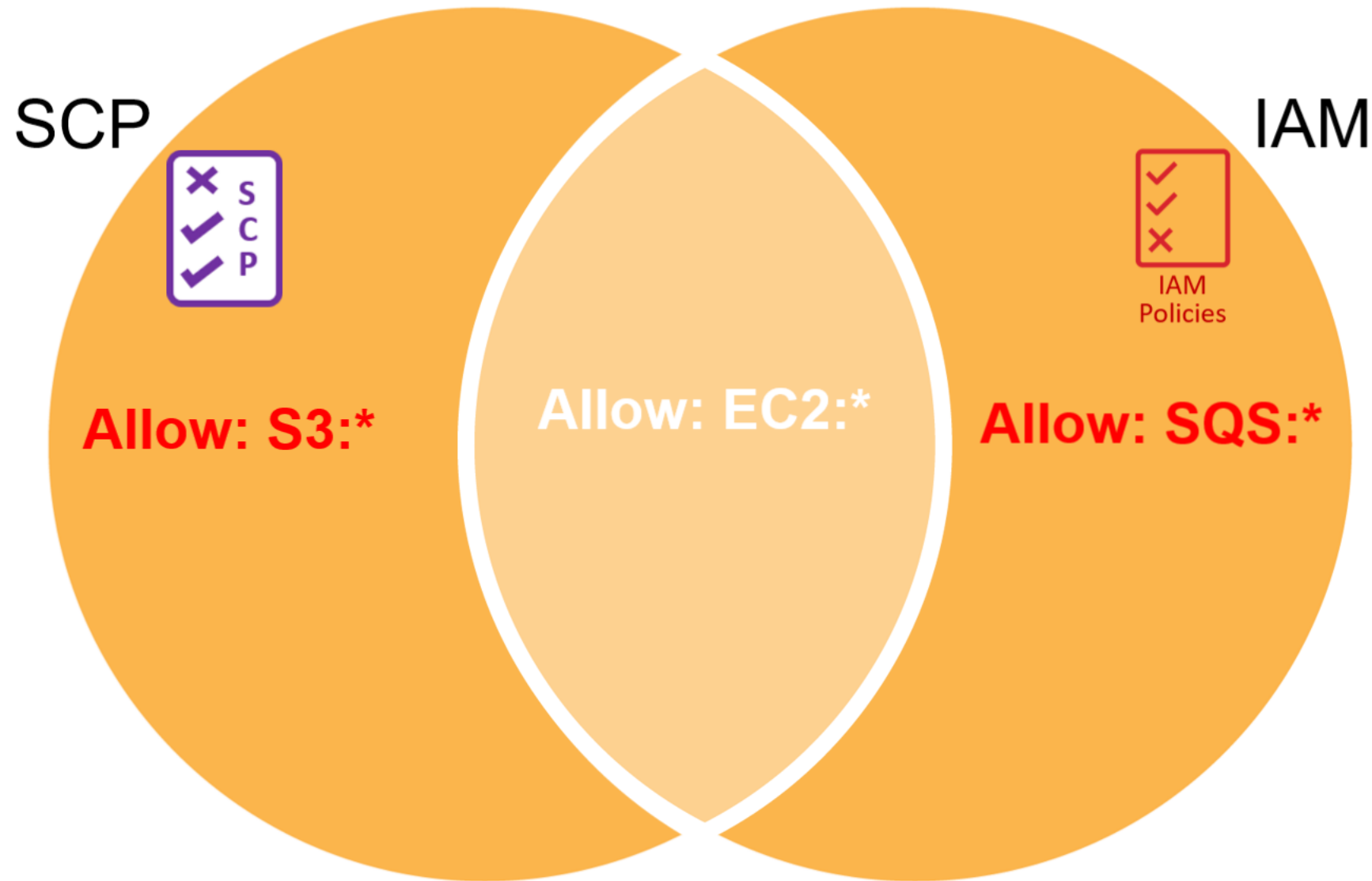
IAM



IAM
Policies

Allow: EC2:*
Allow: SQS:*

Effective Permission



SCP Examples

- No Internet Gateway for VPC

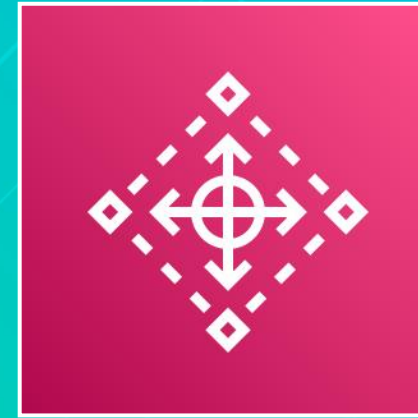
```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": [  
      "ec2:AttachInternetGateway",  
      "ec2:CreateInternetGateway",  
      "ec2:AttachEgressOnlyInternetGateway",  
      "ec2:CreateVpcPeeringConnection",  
      "ec2:AcceptVpcPeeringConnection"  
    ],  
    "Resource": "*"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

- 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?



PASSPORT CONTROL



Where to start?



Lets use the best practices from other successful airport designs



Setting up a new AWS Multi-account architecture

Initial Setup

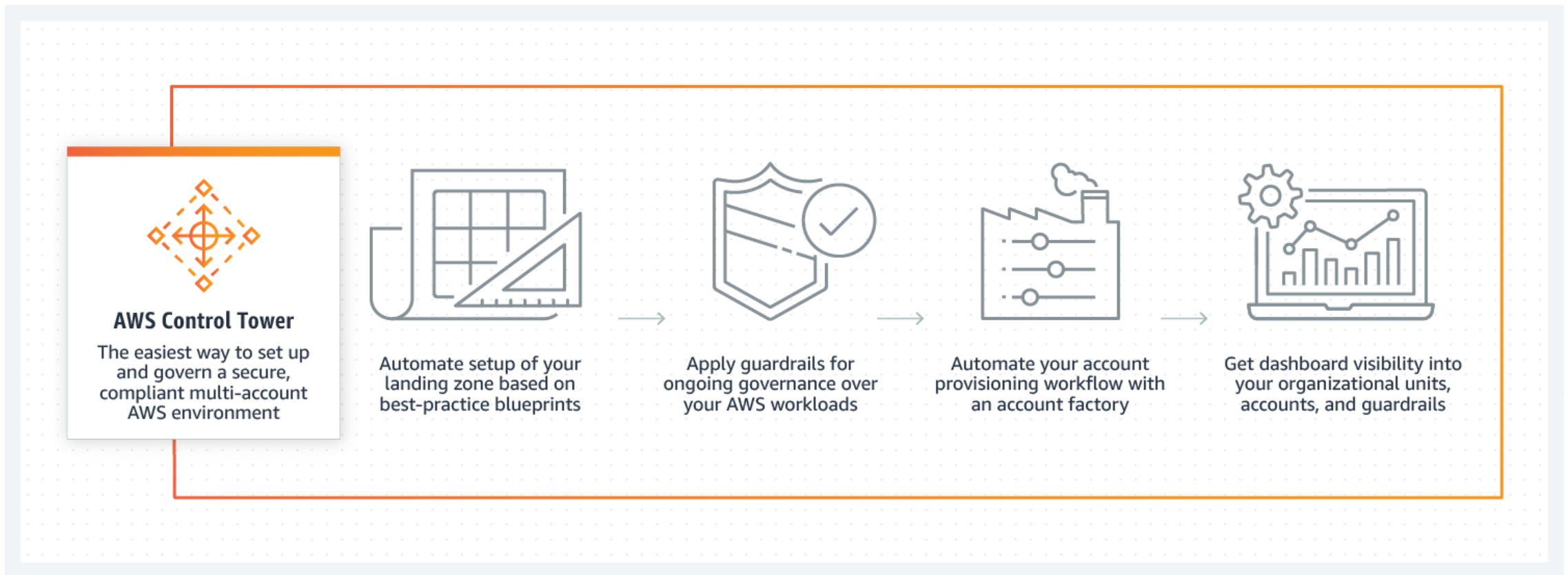
- Create Organization Master account
 - Create temporary Amazon S3 bucket of AWS CloudTrail logs
 - Enable CloudTrail locally
 - Enable AWS Organization full feature
- Create Log Archive account
 - Create bucket(s) for security logs
- Create Security account
 - Create Roles – Read Only | Power Users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



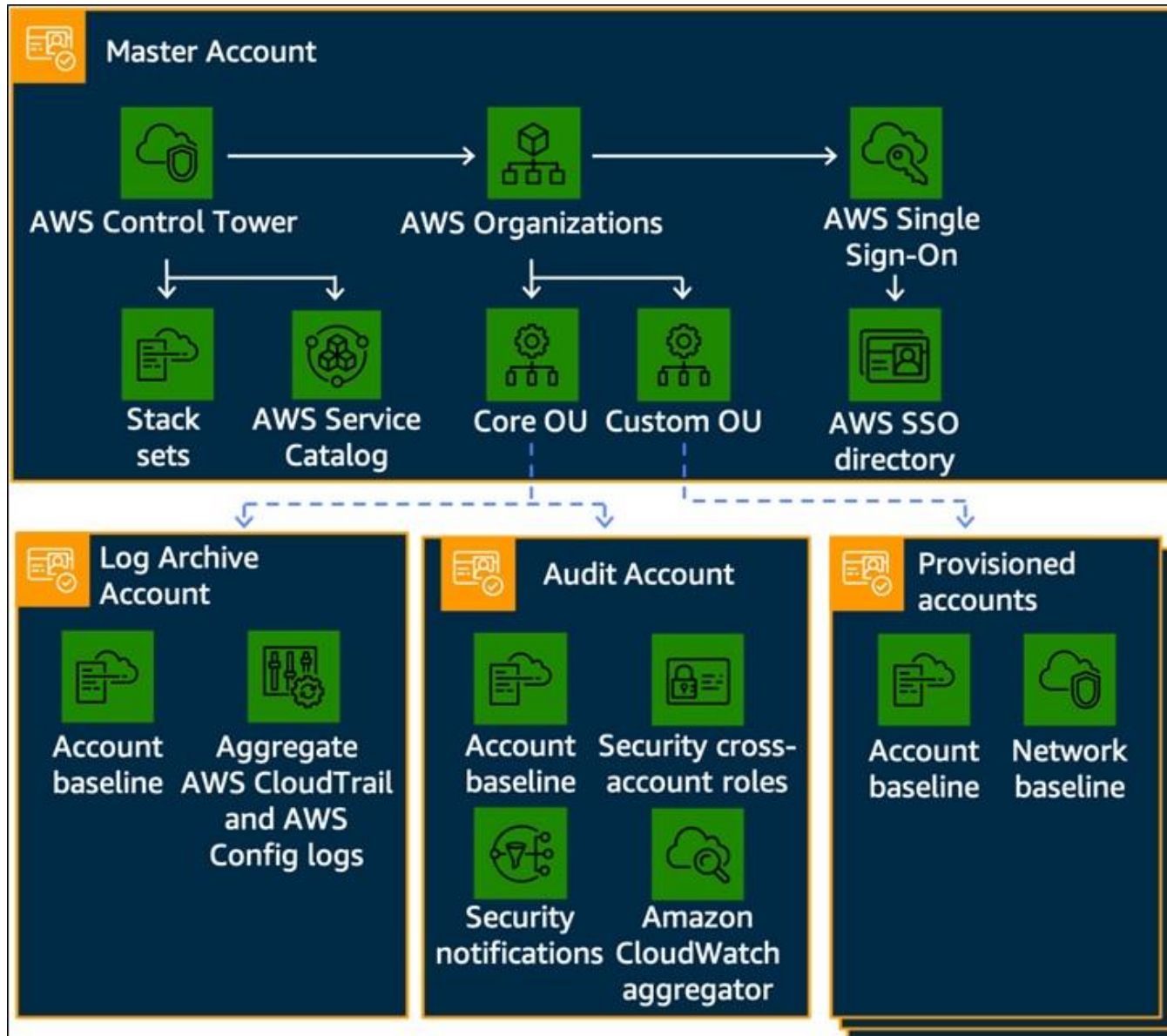
AWS Control Tower – Landing Zone

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

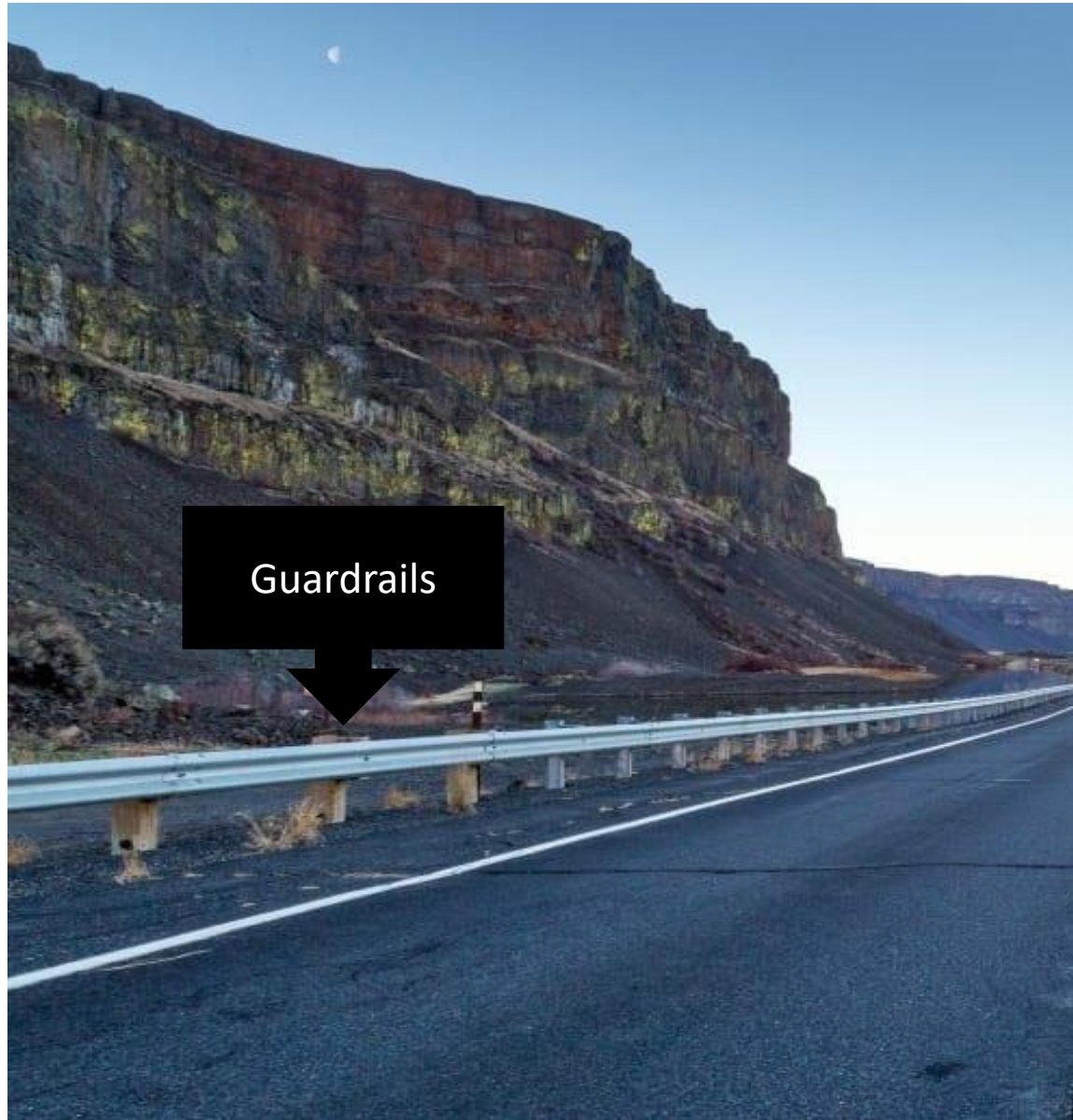
A high-level rule that provides ongoing governance for your overall AWS environment.



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 > Account factory

Account factory [Info](#)

The account factory enables you to create standardized baselines and network configurations for accounts in your organization. Your users can configure and provision these new accounts in AWS Service Catalog.

Network configuration

The following VPC configuration options are available to your users when they provision new accounts. You can modify these settings anytime.

Internet-accessible subnet	Address range (CIDR) for account VPCs	Regions for VPC creation
Disallow	172.31.0.0/16	EU (Ireland) US East (N. Virginia) US East (Ohio) US West (Oregon)
Maximum number of private subnets		
1		
Availability Zone count		
3		

[Provision new account](#) [Edit](#)

AWS Control Tower > Account factory > Enroll account

Enroll account [Info](#)

Account details

Account enrollment provisions a new account or brings an existing account into AWS Control Tower governance.

Account email
Specify a new email if you are creating a new account in your landing zone, or an existing email to extend governance to an existing AWS account.

Must be from 6 to 64 characters long.

Display name
Name for account as it appears in AWS Control Tower

AWS SSO email
Designate an SSO user.

Must be from 6 to 64 characters long.

AWS SSO user name
First and last name intended for creating an AWS SSO user

Organizational unit
Defines governance for an account, and enables all guardrails on that OU

[Cancel](#) [Enroll account](#)

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.

The screenshot displays the AWS Control Tower Dashboard. On the left is a navigation sidebar with links to Dashboard, Accounts, Organizational units, Guardrails, Users and access, Account factory, and Shared accounts. The main content area is titled 'AWS Control Tower > Dashboard' and includes a 'Recommended actions' section. Below this are two summary cards: 'Environment summary' showing 3 Organizational units and 34 Accounts, and 'Guardrail summary' showing 28 Preventive guardrails and 12 Detective guardrails. A 'Noncompliant resources' table lists three items with details on Resource ID, type, service, region, account name, OU, and the specific guardrail that is violated. Below this is an 'Organizational units' table showing the compliance status of Core, Project 1, and Custom OUs. At the bottom is an 'Accounts' table with columns for Account name, email, OU, owner, and compliance status, including a pagination control showing page 1 of 1.

Resource ID	Resource type	Service	Region	Account name	OU	Guardrail
vol-842jhdksj83821234	Volume	EC2	us-west-2	db-uswest-1-gamma	Custom	Enable encryption for EBS volumes at
vol-05flia830kd209897	Volume	EC2	us-east-1	testing-beta-1	Project 1	Enable encryption for EBS volumes at
sg-031234b83bac98765	Security Group	EC2	eu-west-1	ops-test-4	Project 1	Disallow internet connection through

Name	Parent OU	Compliance
Core	Root	Compliant
Project 1	Root	Noncompliant
Custom	Root	Noncompliant

Account name	Account email	Organizational unit	Owner	Compliance status
--------------	---------------	---------------------	-------	-------------------



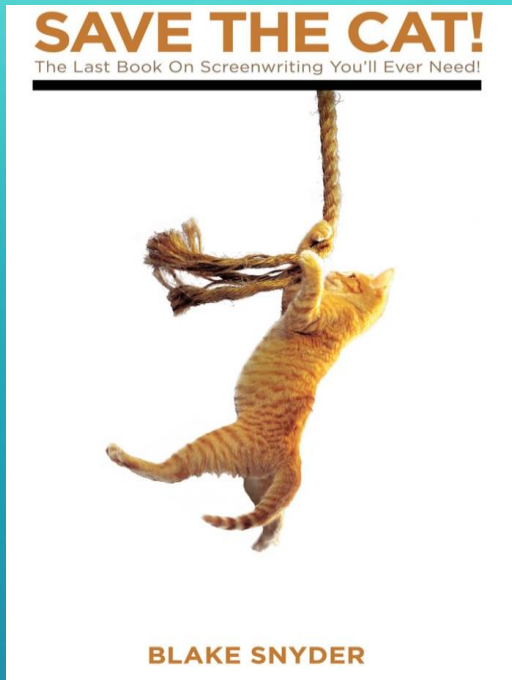
Let's read some superb
books

- Jamila Jamilova

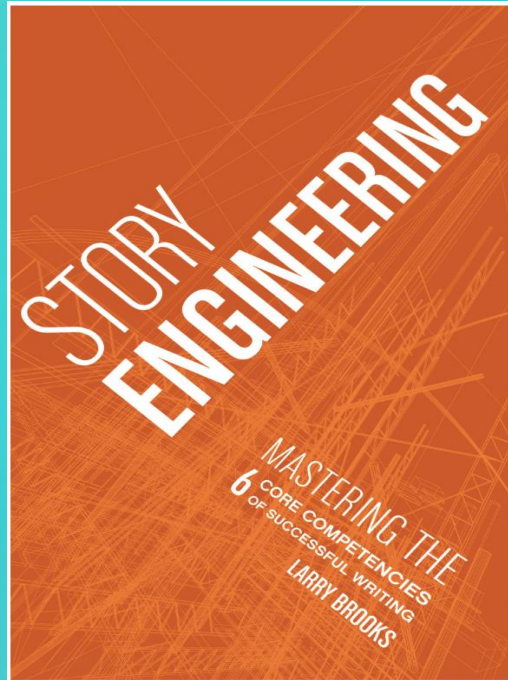


Become a Solutions Architect

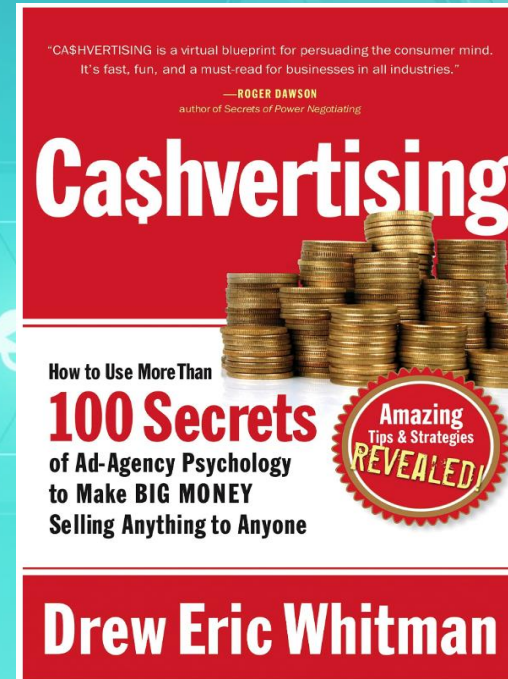
Essential books on structure and frame of mind



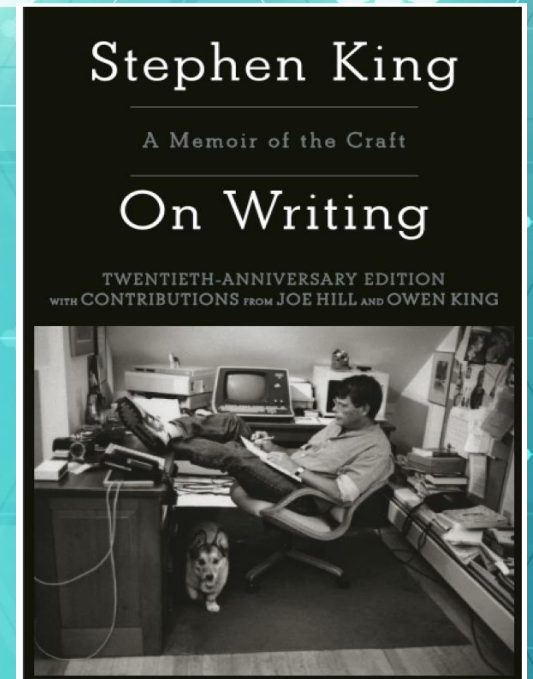
Categories: Primarily structure and formula



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.