# aws SUMMIT ONLINE

OPE06

# Establish and govern a multi-account AWS environment with AWS Control Tower

Emily Arnautovic

Enterprise Solutions Architect
Amazon Web Services

AWS SUMMIT ONLINE

# Agenda

Your AWS journey – scaling from one account to many accounts

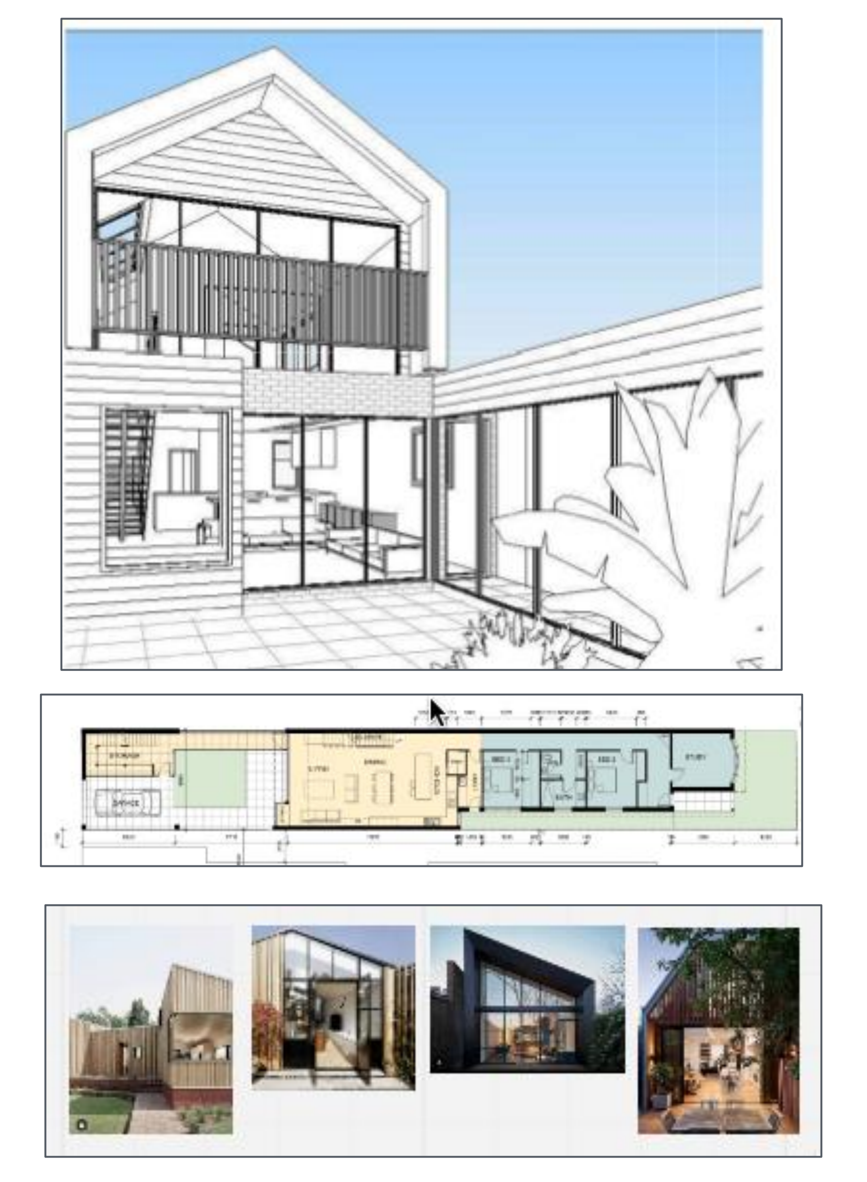
AWS Control Tower overview

AWS Control Tower integrations

AWS Control Tower deep dive

AWS Control Tower vs. AWS Landing Zones solution

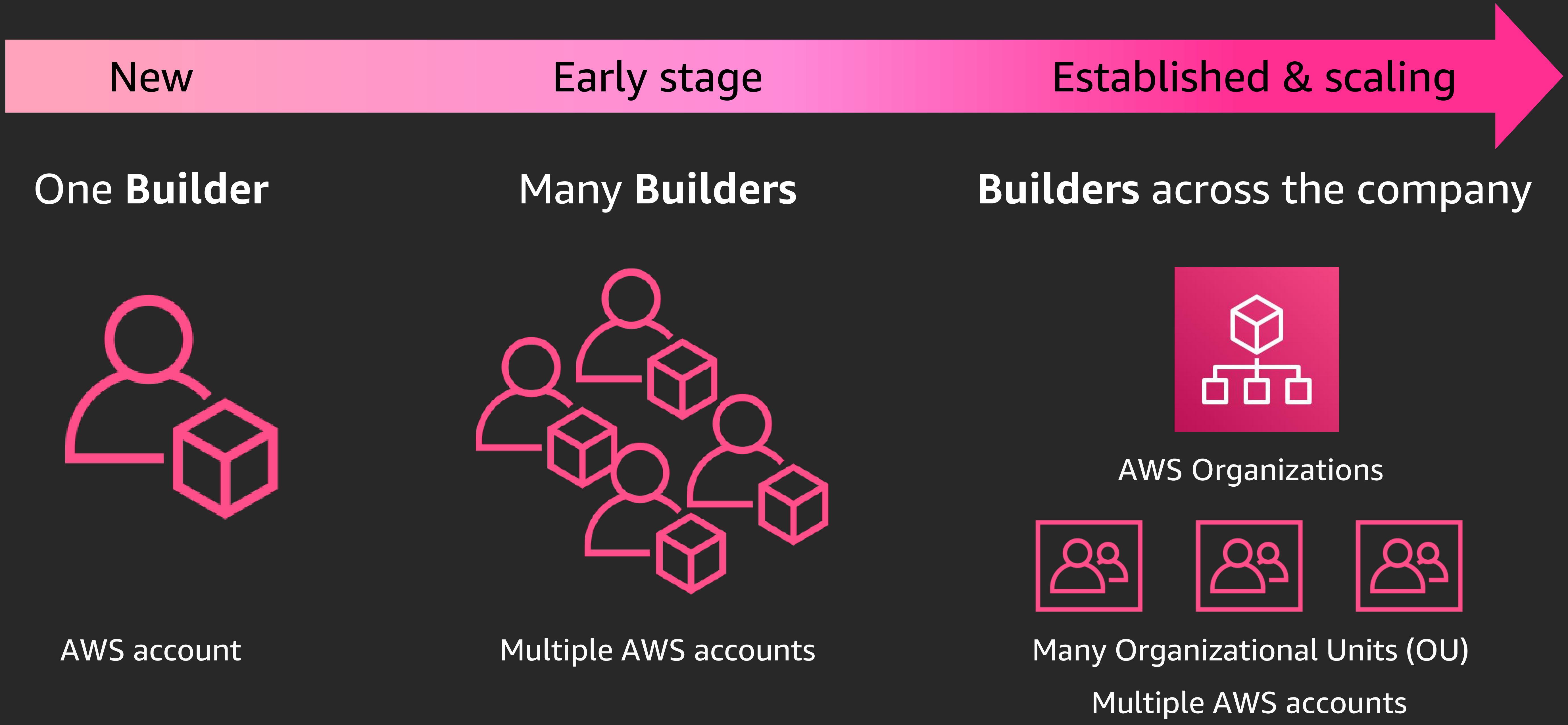
# Scaling out



One build

…to many builds

# From one Builder to many Builders



New

Early stage

Established & scaling

One **Builder**

AWS account

Many **Builders**

Multiple AWS accounts

**Builders** across the company

AWS Organizations

Many Organizational Units (OU)

Multiple AWS accounts

# Why use a multi-account AWS environment?

Many teams of **builders**

Isolation

Security/compliance controls

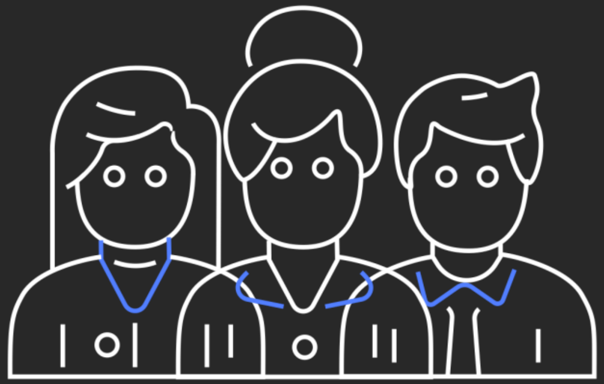
Business process

Billing

# Common personas working with AWS accounts

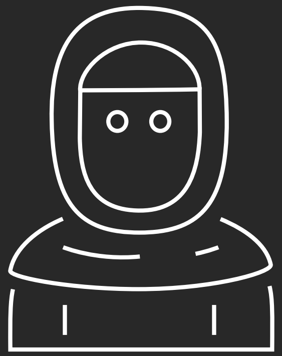
## Builders

Developers
Engineers
Data scientists
Marketers
Business unit teams



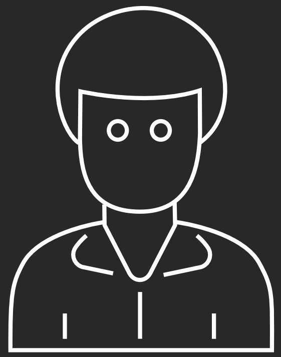
## Cloud IT

IT ops manager
Cloud services lead
IT admins



## Cloud IT

CISO
Security engineers
Compliance team



# Common goals for any AWS environment

Automated

Scalable

Self-service

Guardrails

Auditable

Flexible

# Not this!

We want to avoid:

- ⚠ Long delays to get builders building on AWS
- ⚠ Failing security and risk controls
- ⚠ Unknown state of our AWS accounts
- ⚠ Unmanaged activity in our AWS accounts

# More of this!

We seek:

- ☑ Builders building and innovating quickly on AWS
- ☑ Staying within our security and risk posture
- ☑ A known state of our AWS accounts
- ☑ Managed activity in our AWS accounts

# The challenge: balancing the needs

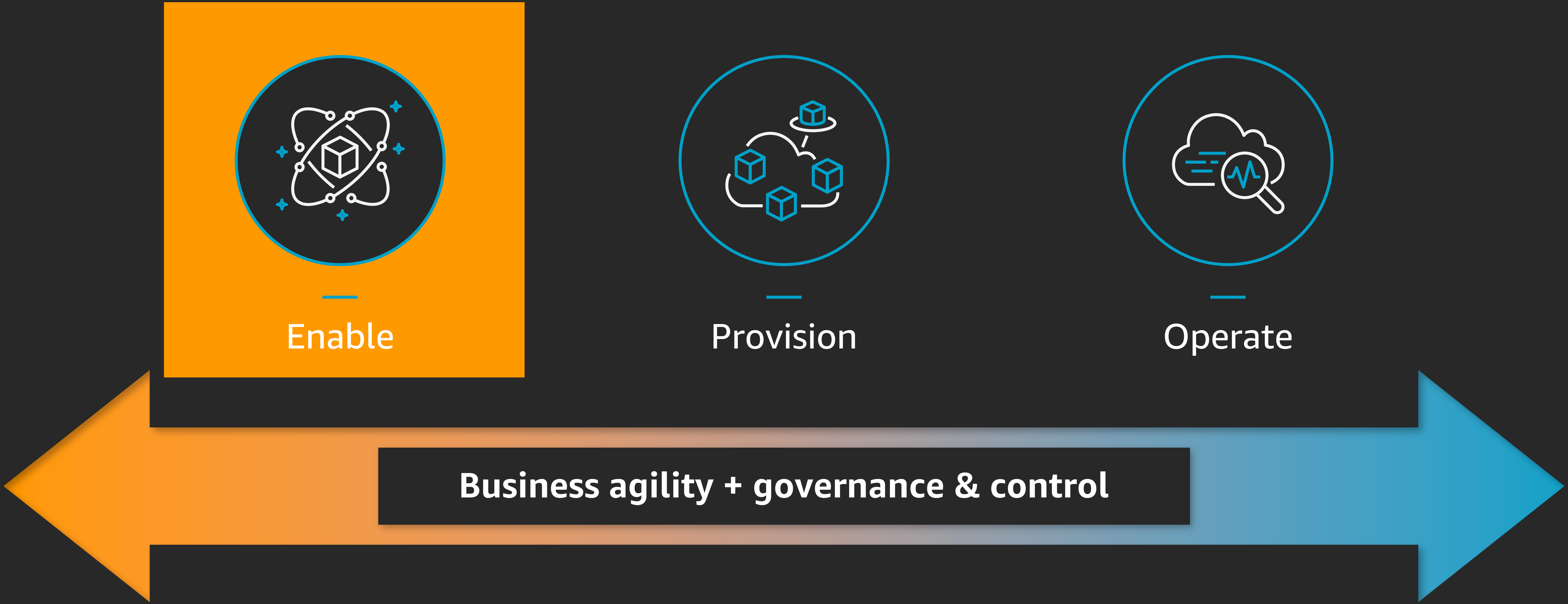
**Builders**:
Stay agile

Innovate with the speed and agility of AWS

**Cloud IT**:
Establish governance

Govern at scale with central controls

introducing …AWS Control Tower



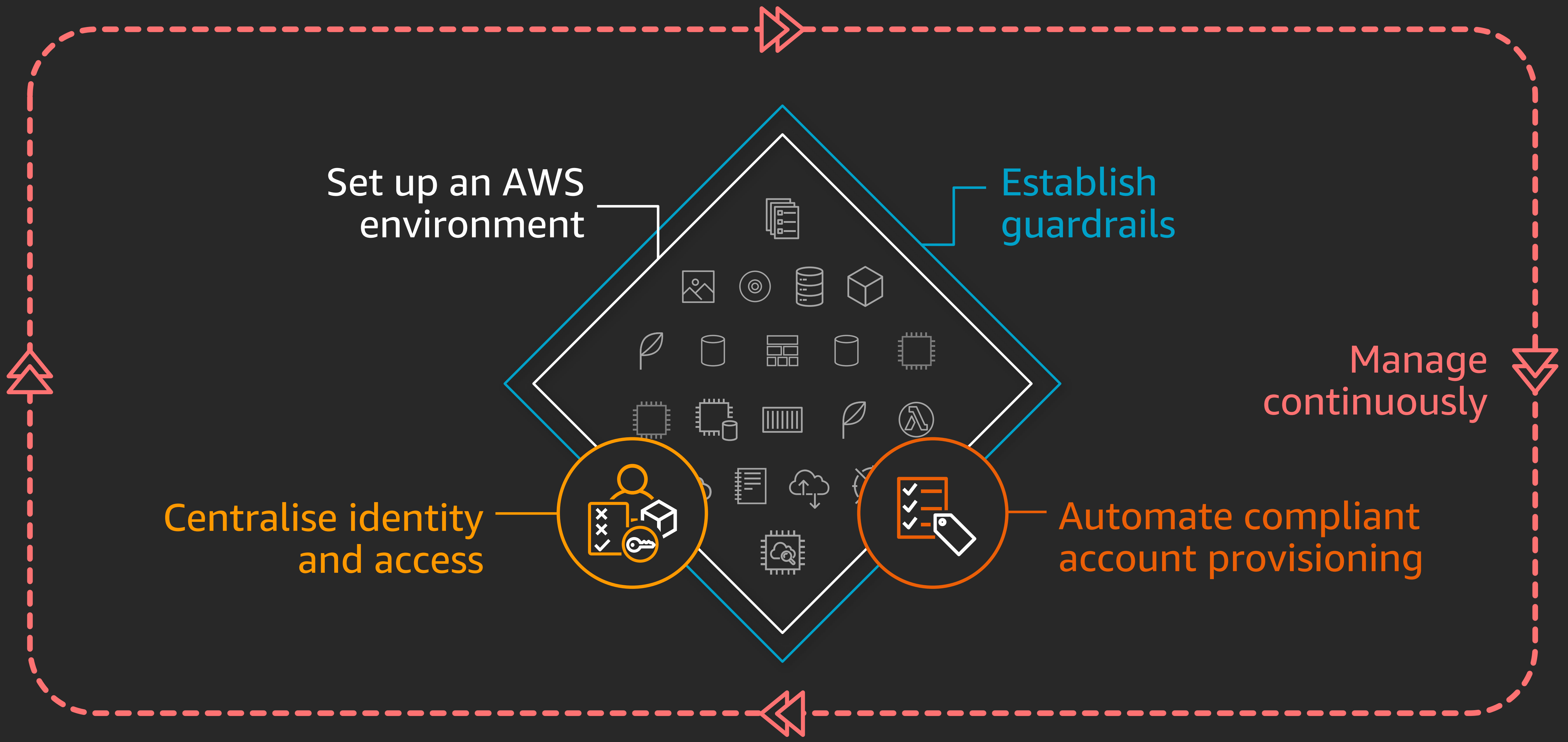
Enable

Provision

Operate

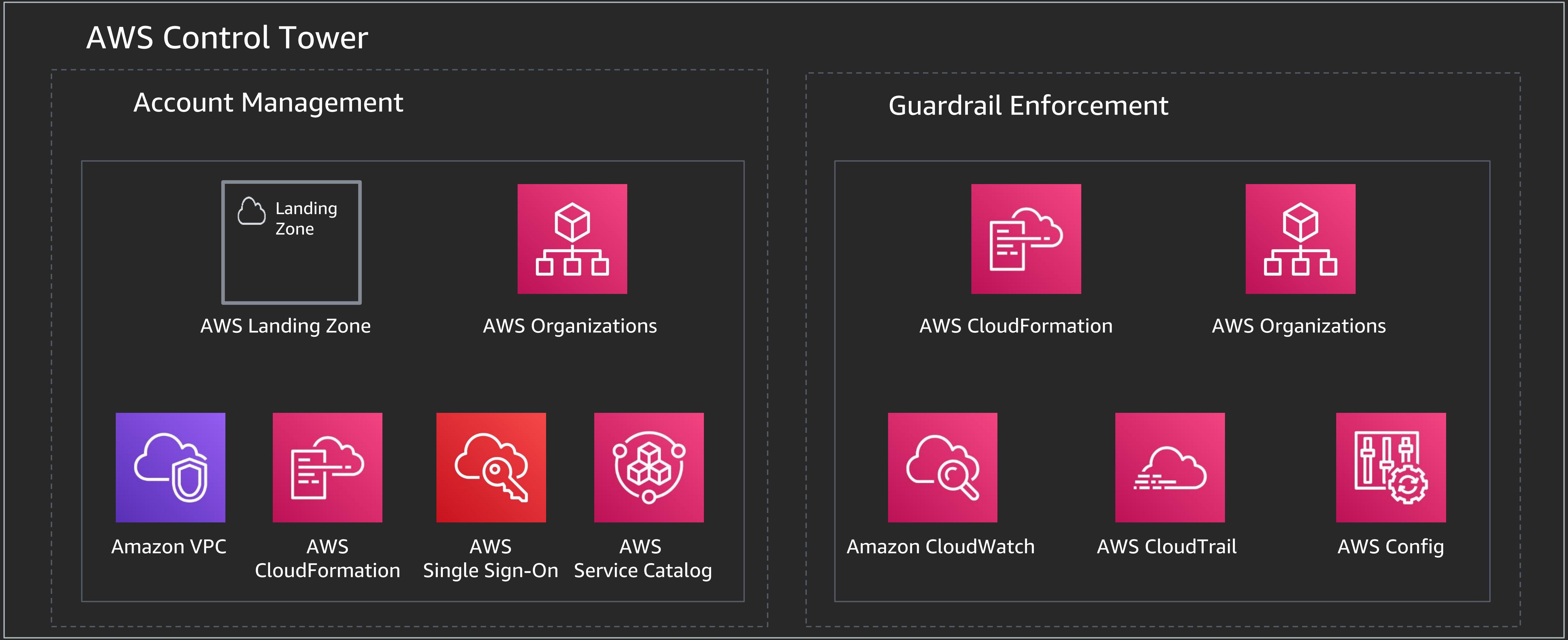
**Business agility + governance & control**

# Enable governance


Set up an AWS environment
Establish guardrails
Manage continuously
Centralise identity and access
Automate compliant account provisioning

# AWS Control Tower: Service orchestration

AWS Control Tower



AWS Control Tower

Account Management

Landing Zone

AWS Landing Zone

AWS Organizations

Amazon VPC

AWS CloudFormation

AWS Single Sign-On

AWS Service Catalog

Guardrail Enforcement

AWS CloudFormation

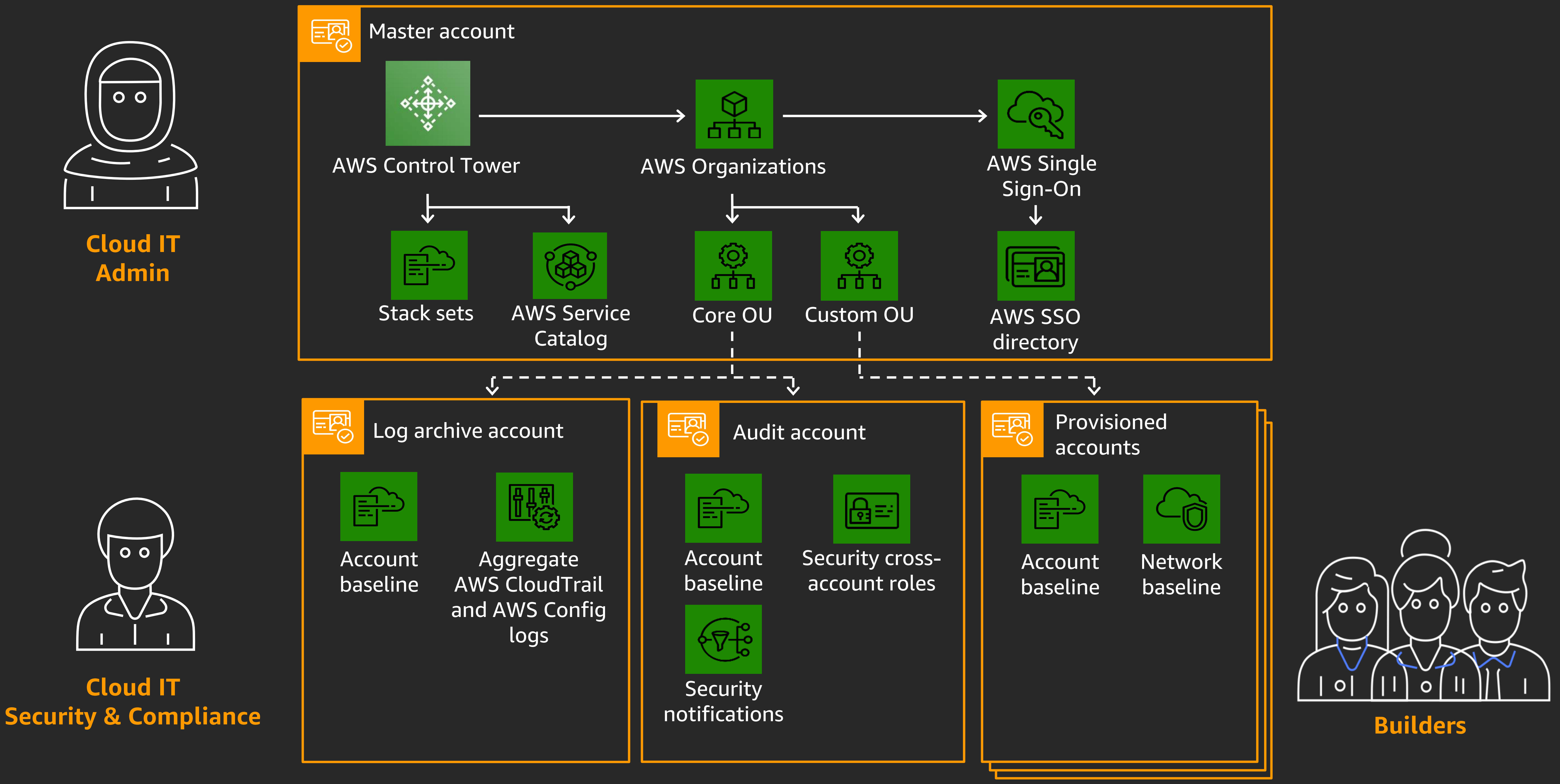
AWS Organizations

Amazon CloudWatch

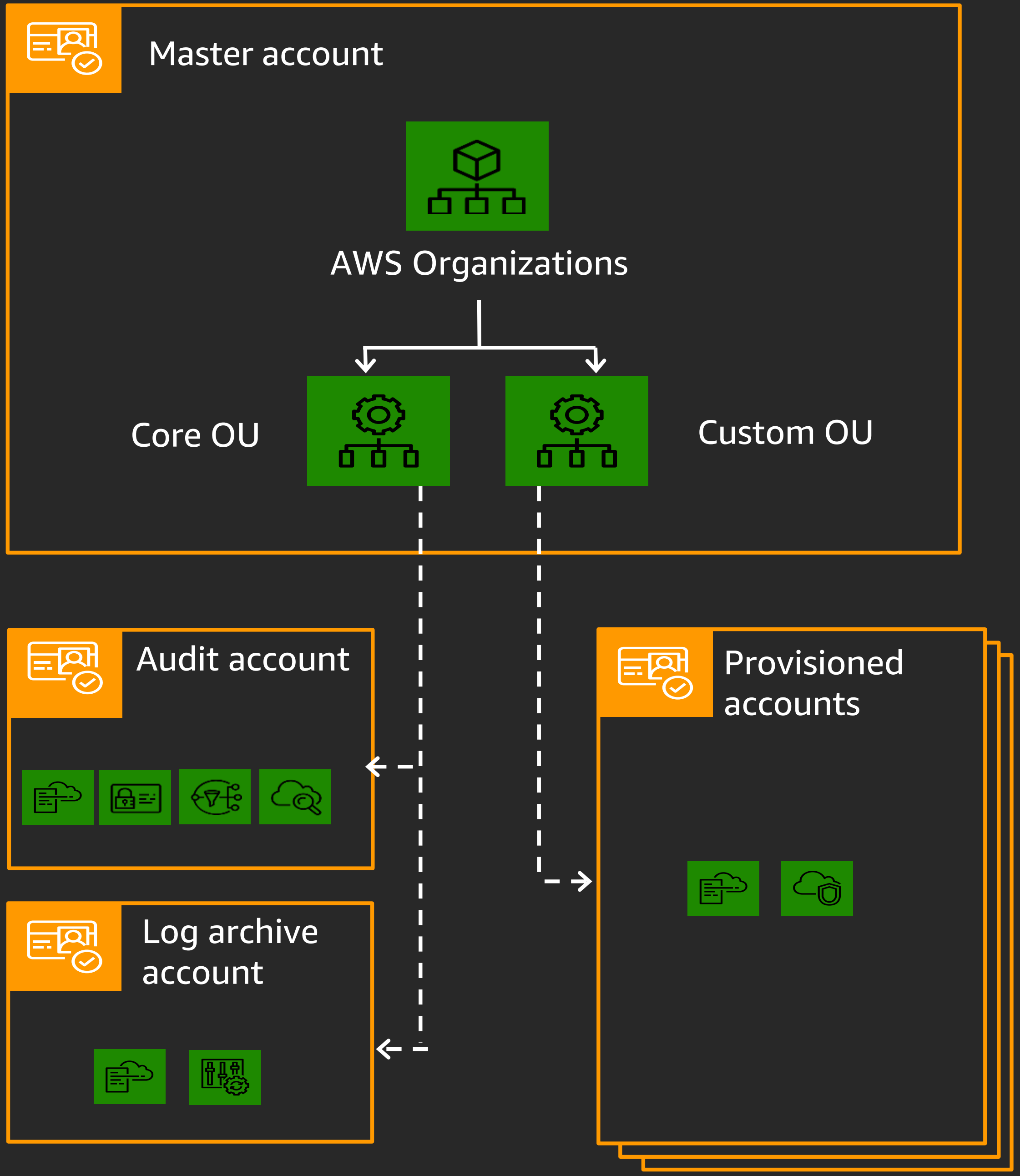
AWS CloudTrail

AWS Config

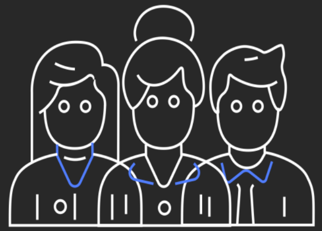
# AWS Control Tower - set up an AWS landing zone



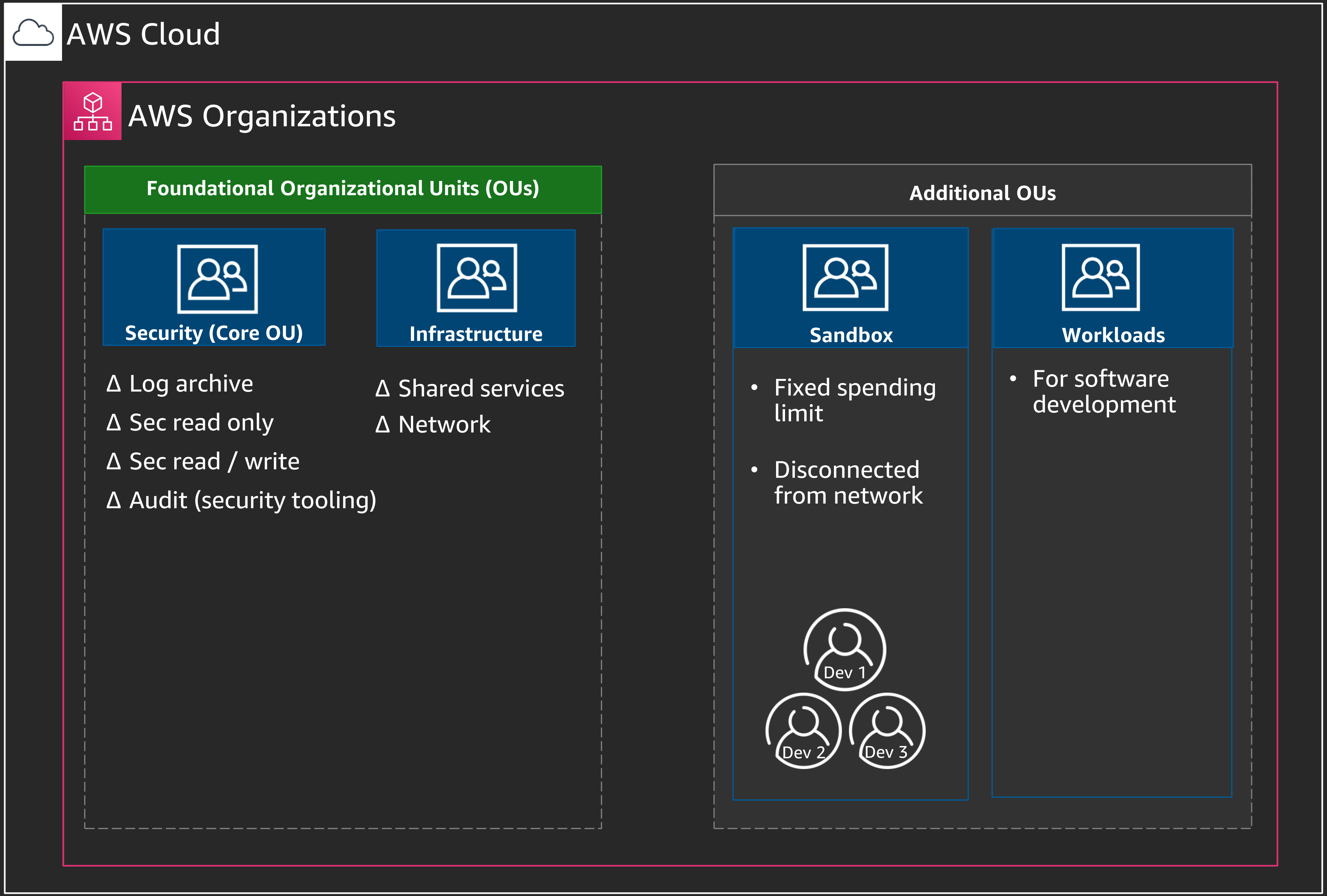
# Multi-account architecture



- Baseline AWS Organizations setup:
  - Core OU: AWS Control Tower baseline accounts (cannot change)
  - Custom OU: Your provisioned accounts to enable and organise your teams of **Builders**



# Starter AWS multi-account framework



AWS Cloud

AWS Organizations

**Foundational Organizational Units (OUs)**

**Security (Core OU)**

- Δ Log archive
- Δ Sec read only
- Δ Sec read / write
- Δ Audit (security tooling)

**Infrastructure**

- Δ Shared services
- Δ Network

**Additional OUs**

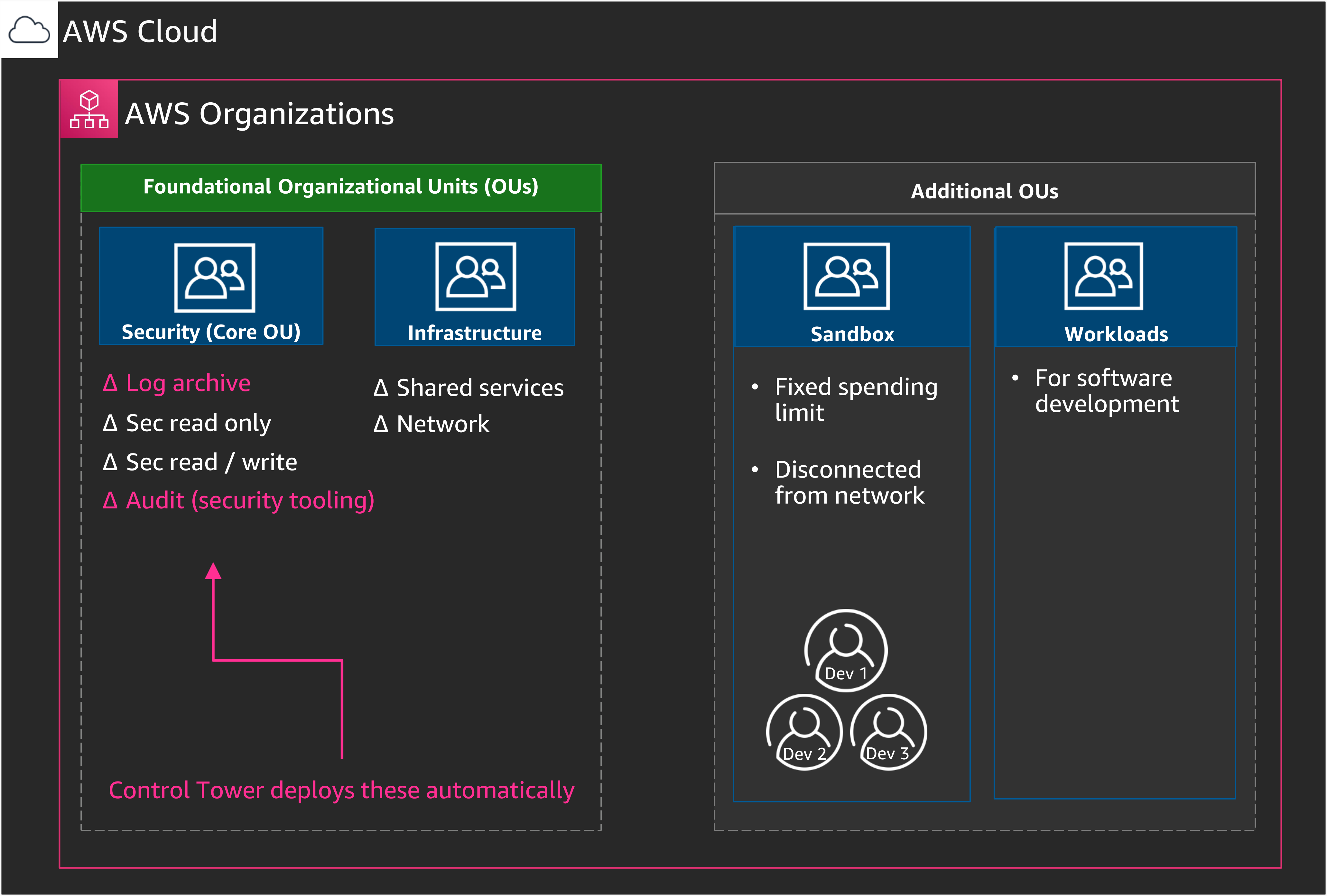
**Sandbox**

- Fixed spending limit
- Disconnected from network

**Workloads**

- For software development

# Starter AWS multi-account framework



AWS Cloud

AWS Organizations

**Foundational Organizational Units (OUs)**

**Security (Core OU)**

Δ Log archive

Δ Sec read only

Δ Sec read / write

Δ Audit (security tooling)

**Infrastructure**

Δ Shared services

Δ Network

Control Tower deploys these automatically

**Additional OUs**

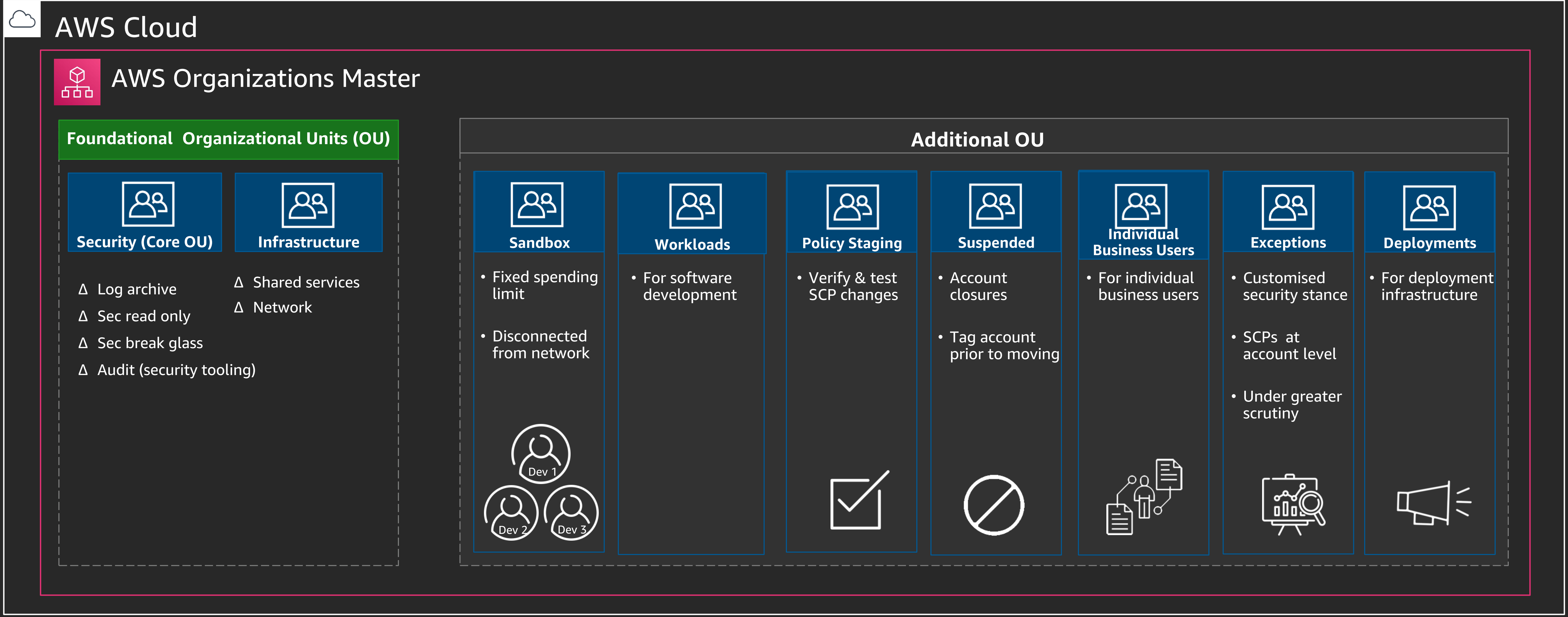
**Sandbox**

- Fixed spending limit
- Disconnected from network

**Workloads**

- For software development

# High-level OU structure



AWS Cloud

AWS Organizations Master

**Foundational Organizational Units (OU)**

**Security (Core OU)**

Δ Log archive
Δ Sec read only
Δ Sec break glass
Δ Audit (security tooling)

**Infrastructure**

Δ Shared services
Δ Network

**Additional OU**

**Sandbox**

- Fixed spending limit
- Disconnected from network

**Workloads**

- For software development

**Policy Staging**

- Verify & test SCP changes

**Suspended**

- Account closures
- Tag account prior to moving

**Individual Business Users**

- For individual business users

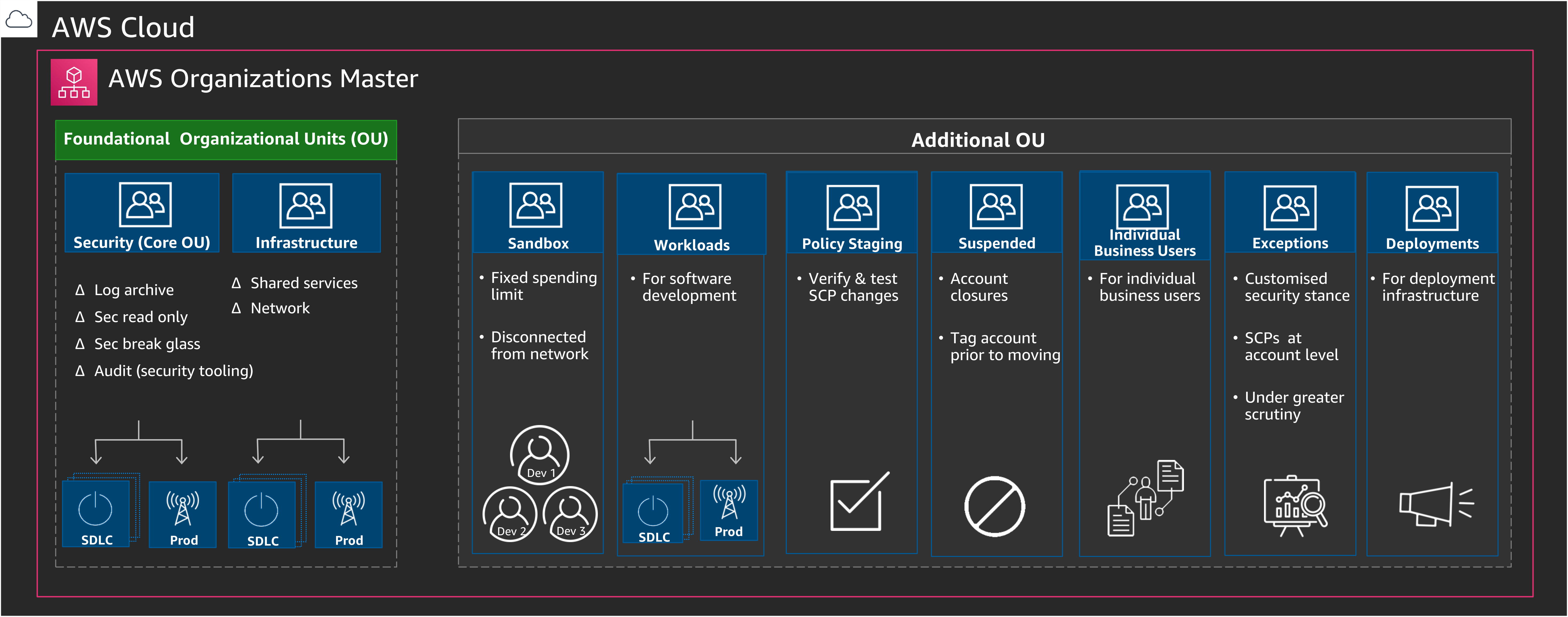
**Exceptions**

- Customised security stance
- SCPs at account level
- Under greater scrutiny

**Deployments**

- For deployment infrastructure

# Recommended AWS multi-account framework



AWS Cloud

AWS Organizations Master

**Foundational Organizational Units (OU)**

**Security (Core OU)**

- Δ Log archive
- Δ Sec read only
- Δ Sec break glass
- Δ Audit (security tooling)

**Infrastructure**

- Δ Shared services
- Δ Network

**Additional OU**

**Sandbox**

- Fixed spending limit
- Disconnected from network

**Workloads**

- For software development

**Policy Staging**

- Verify & test SCP changes

**Suspended**

- Account closures
- Tag account prior to moving

**Individual Business Users**

- For individual business users

**Exceptions**

- Customised security stance
- SCPs at account level
- Under greater scrutiny

**Deployments**

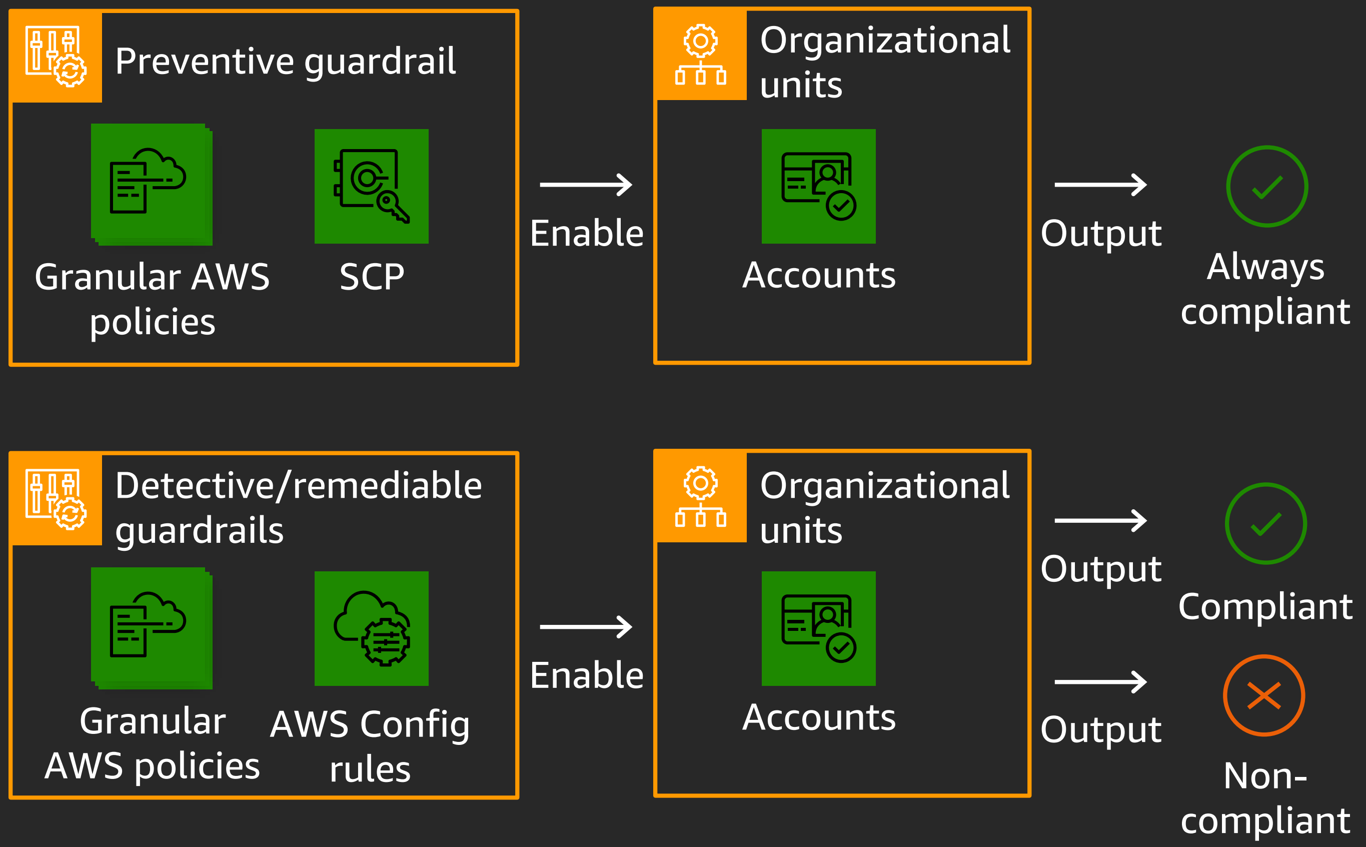
- For deployment infrastructure

# Centralise identity and access

- AWS SSO provides default directory for identity
- Preconfigured groups and permission sets
- Option to integrate with your managed or on-premises Active Directory (AD) using AWS Managed Microsoft AD
- Other integrations: Okta

# Establish guardrails

Cloud IT
security & compliance

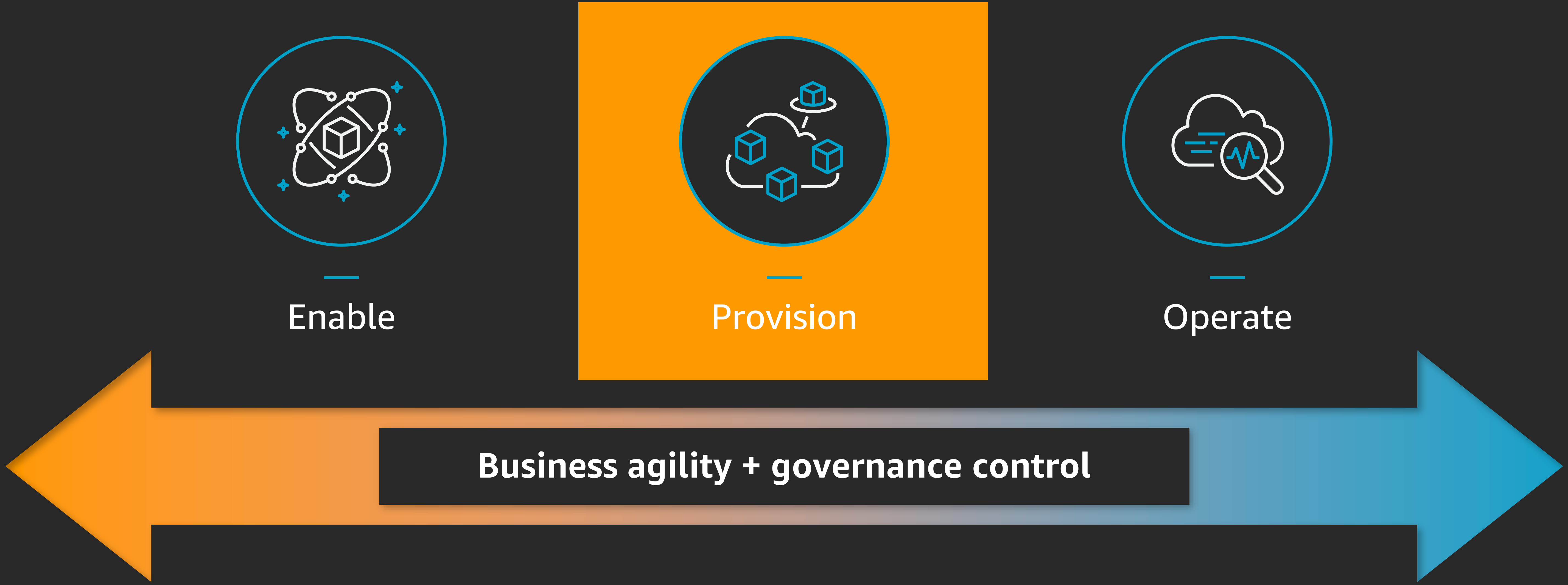


- Preventive: prevents policy violations using Service Control Polices (SCPs), part of AWS Organizations
- Detective: detect policy violations using AWS Config rules
- A guardrail can be: mandatory, strongly recommended, or elective
- Guardrails apply to organizational units (OUs) and all child accounts (new and existing)

# Guardrail examples

| Goal/category | Example |
|---|---|
| IAM | Require MFA for root user |
| Data security | Disallow public read access to Amazon S3 buckets<br>Disallow public access to Amazon RDS database instances |
| Network | Disallow internet connection via Remote Desktop Protocol (RDP)<br>Disallow internet connection through SSH |
| Audit logs | Enable AWS CloudTrail and AWS Config |
| Monitoring | Disallow policy changes to log archive |
| AWS Control Tower setup | Disallow changes to IAM roles set up by AWS Control Tower |
| Operations | Disallow EBS volumes that are unattached to an EC2 instance |

# AWS Service Catalog: Secure self-service provisioning



Enable

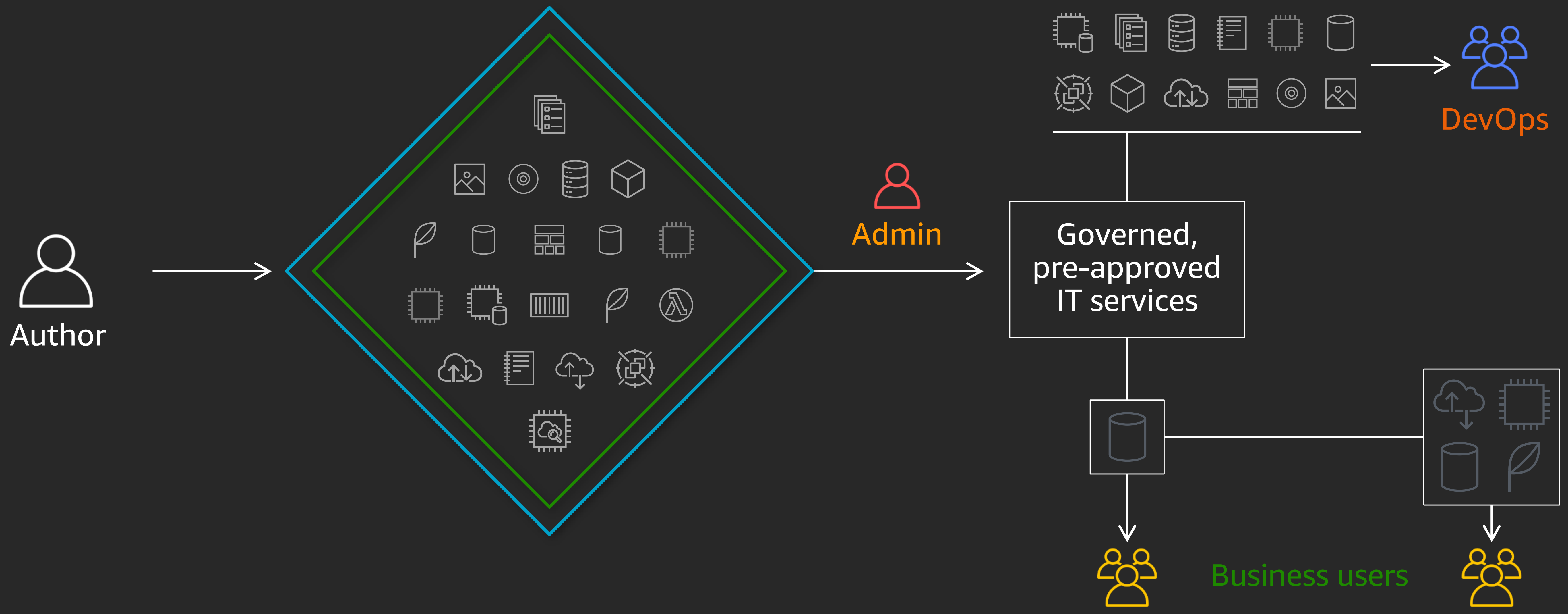
Provision

Operate

**Business agility + governance control**

# Automate provisioning

Provision



Author

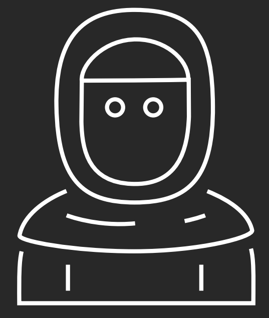
Admin

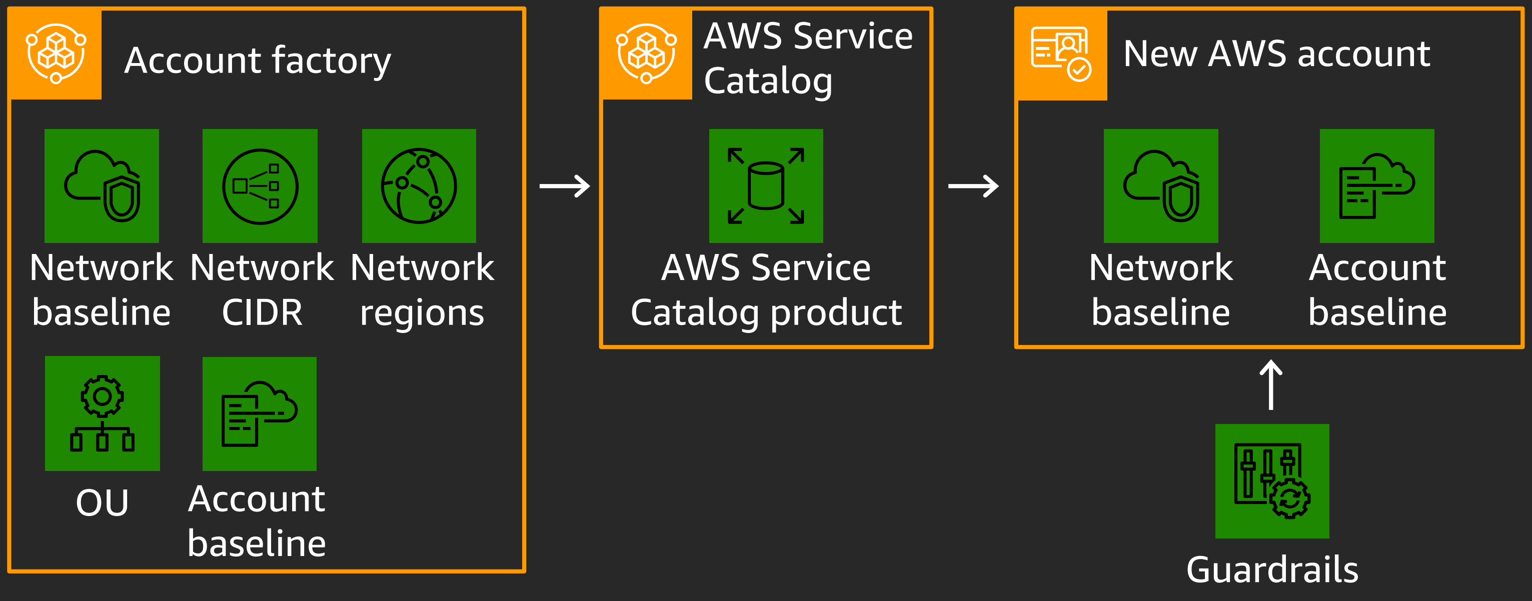
Governed, pre-approved IT services

DevOps

Business users

# Automate compliant account provisioning

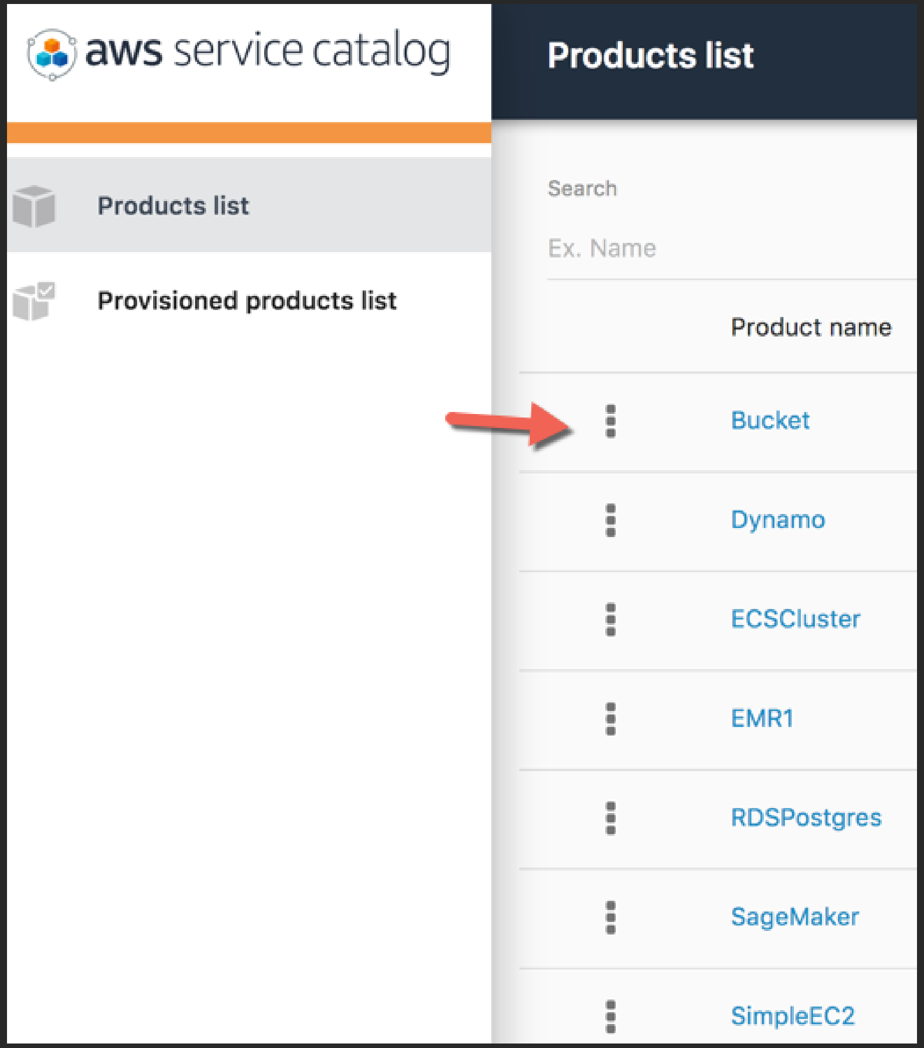




- Standardised account provisioning
- Automatic enforcement of guardrails
- Configurable network settings

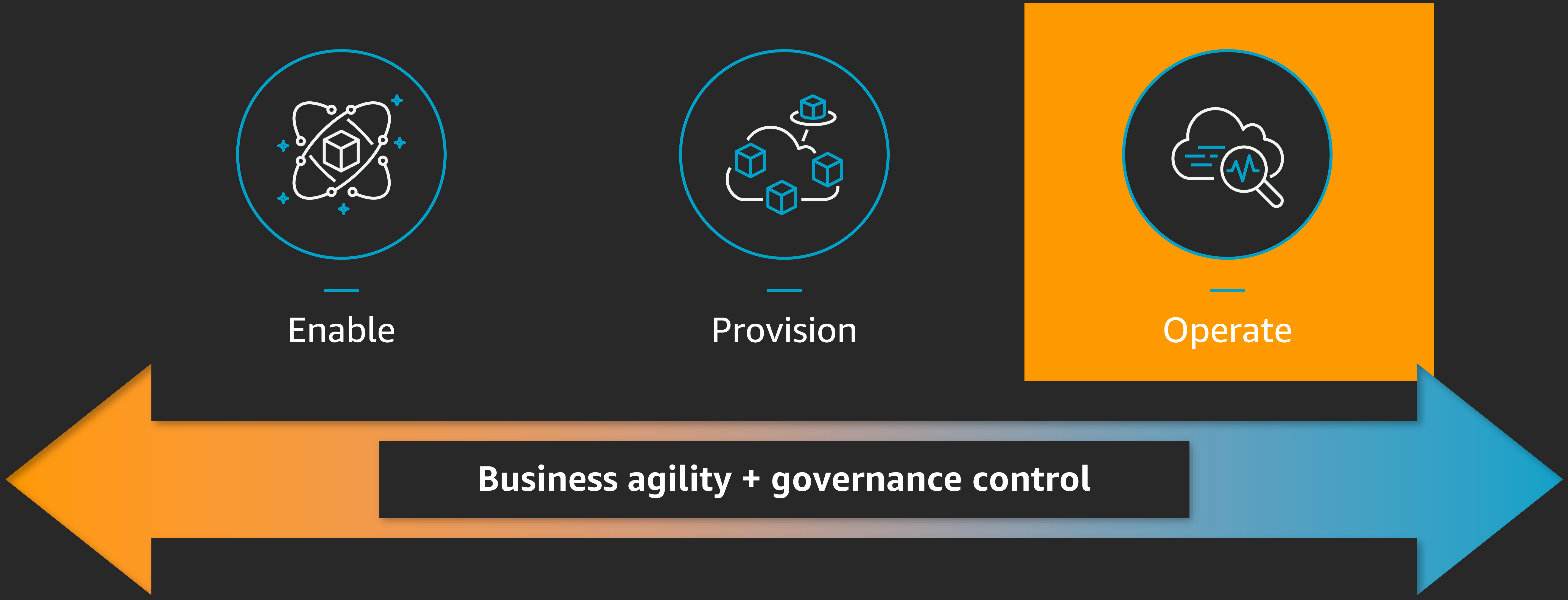
# Enable secure self-service provisioning

- Create best-practices templates with AWS CloudFormation or Terraform for commonly used products (Amazon EMR, Amazon EC2, etc.)
- Create AWS Service Catalog products in the master AWS Control Tower account
- Distribute products via AWS Organizations to all of your AWS Control Tower managed accounts



| Product name |
|---|
| Bucket |
| Dynamo |
| ECSCluster |
| EMR1 |
| RDSPostgres |
| SageMaker |
| SimpleEC2 |

# AWS Control Tower: Easiest way to set up and govern at scale



Enable

Provision

Operate

Business agility + governance control

# Operate with agility + control

**Monitor**

Monitor resources and workloads

**Audit**

Audit resource configurations, user access, and policy enforcement

**Act**

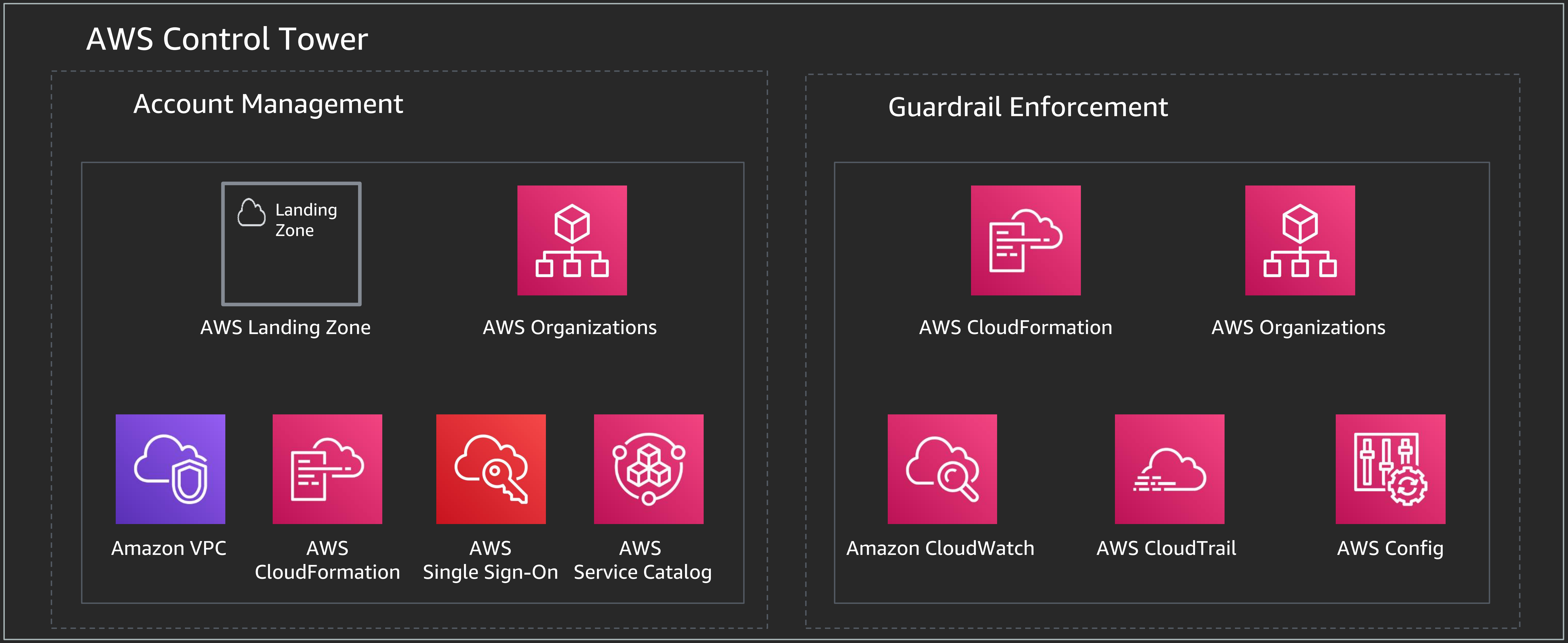
Take operational action on resources

**Dashboard**

Continuous visibility into your multi-account environment

# AWS Control Tower: Service orchestration

AWS Control Tower



AWS Control Tower

Account Management

Landing Zone

AWS Landing Zone

AWS Organizations

Amazon VPC

AWS CloudFormation

AWS Single Sign-On

AWS Service Catalog

Guardrail Enforcement

AWS CloudFormation

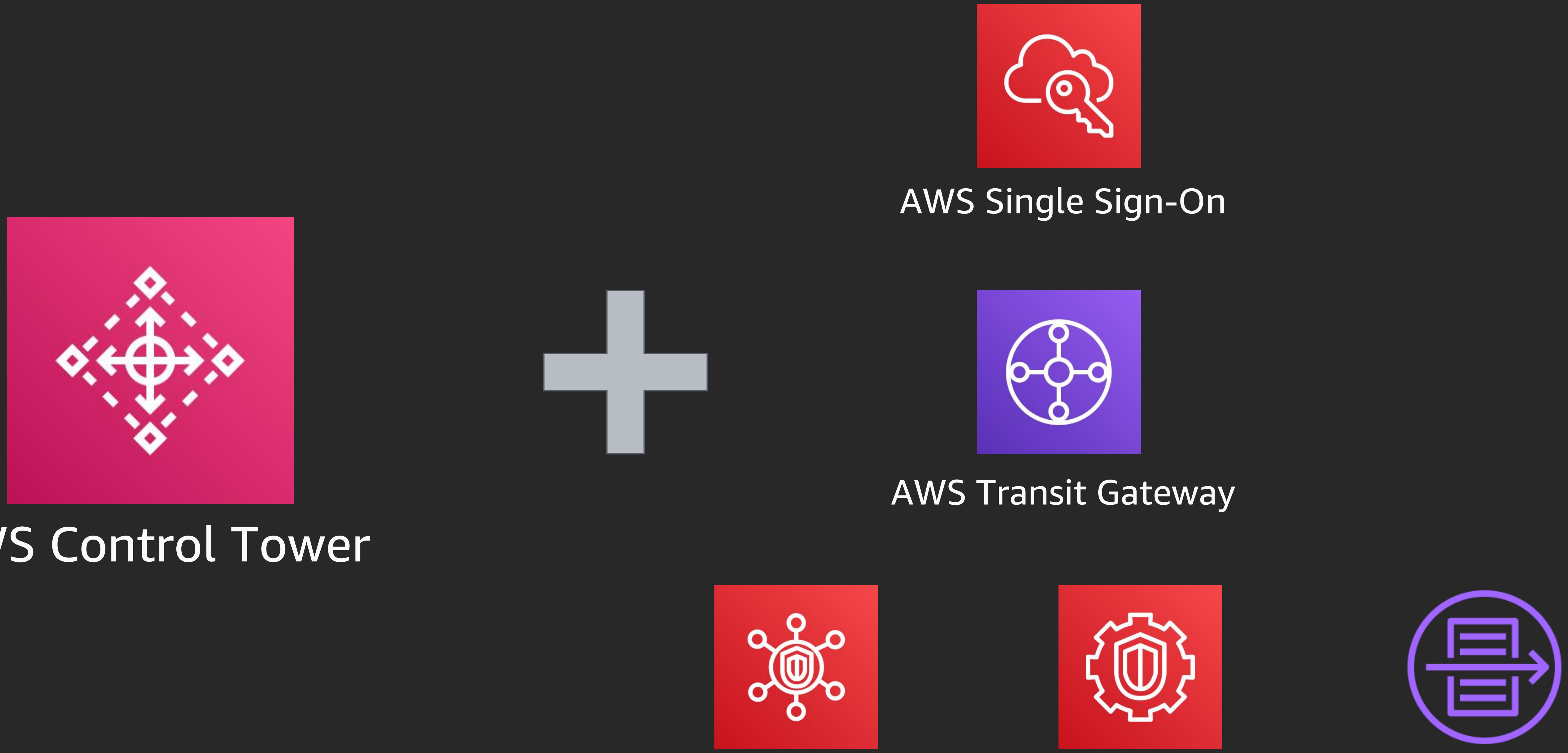
AWS Organizations

Amazon CloudWatch

AWS CloudTrail

AWS Config

# AWS Control Tower integrations



AWS Control Tower

AWS Single Sign-On

AWS Transit Gateway

AWS Security Hub

Amazon GuardDuty

Flow logs

# Deep dive

# Scenarios

## Builders

Developers
Engineers
Data scientist
Marketers
Business unit teams

## Cloud IT

IT Ops Manager
IT Admin
Cloud Services lead

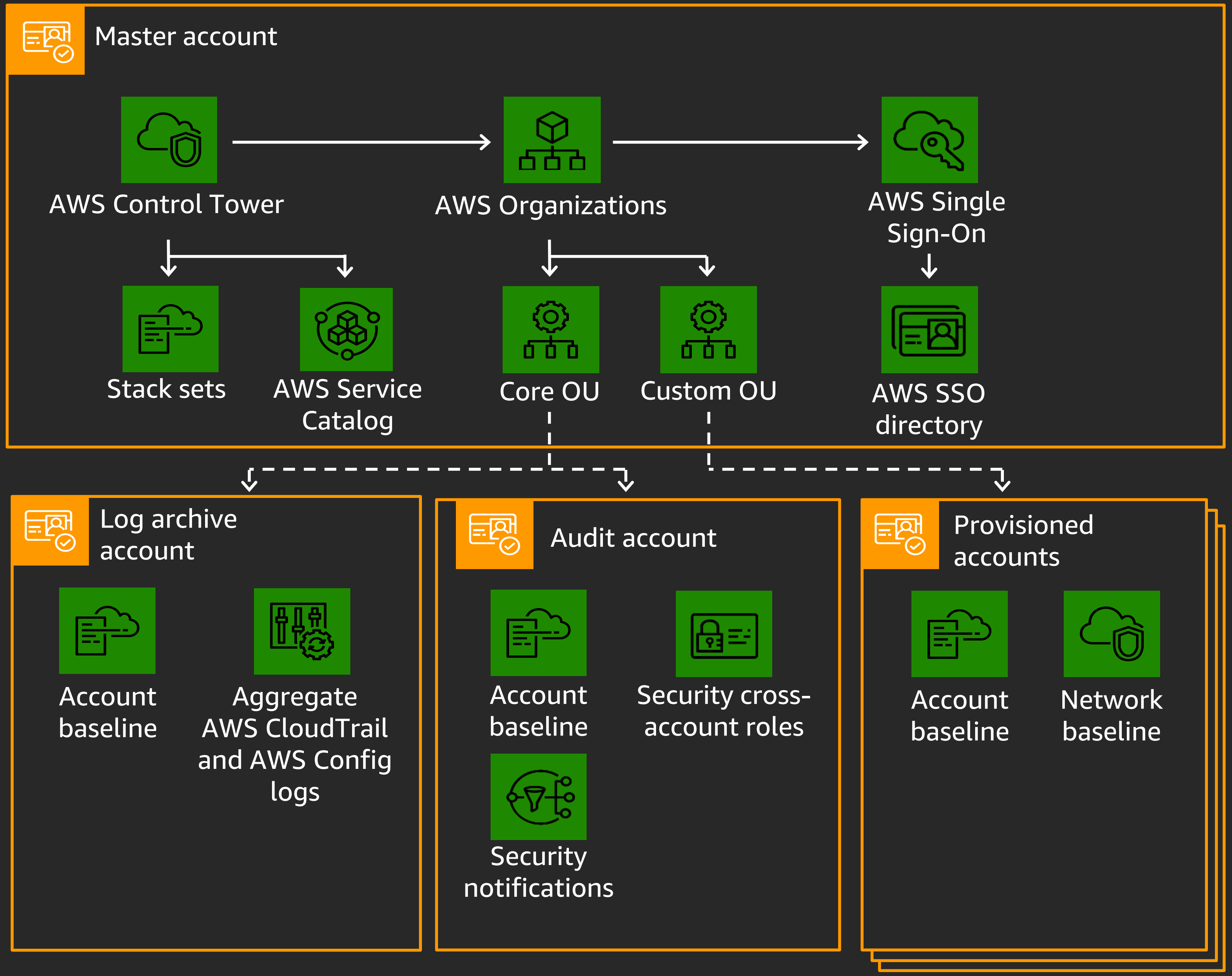
## Cloud IT

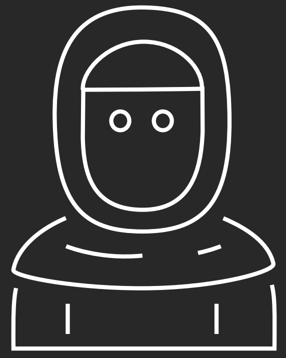
CISO
Security Engineers
Compliance team

"We are completely new to AWS.
Where do we start?!"

# Demo: Provision AWS Control Tower landing zone and dashboard tour

# Set up an AWS Landing Zone





**Cloud IT Admin**

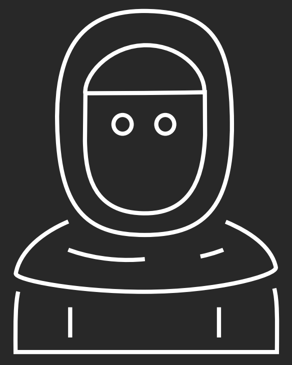
Role: IT Ops Manager

# “How do I provision new AWS accounts and provide access?

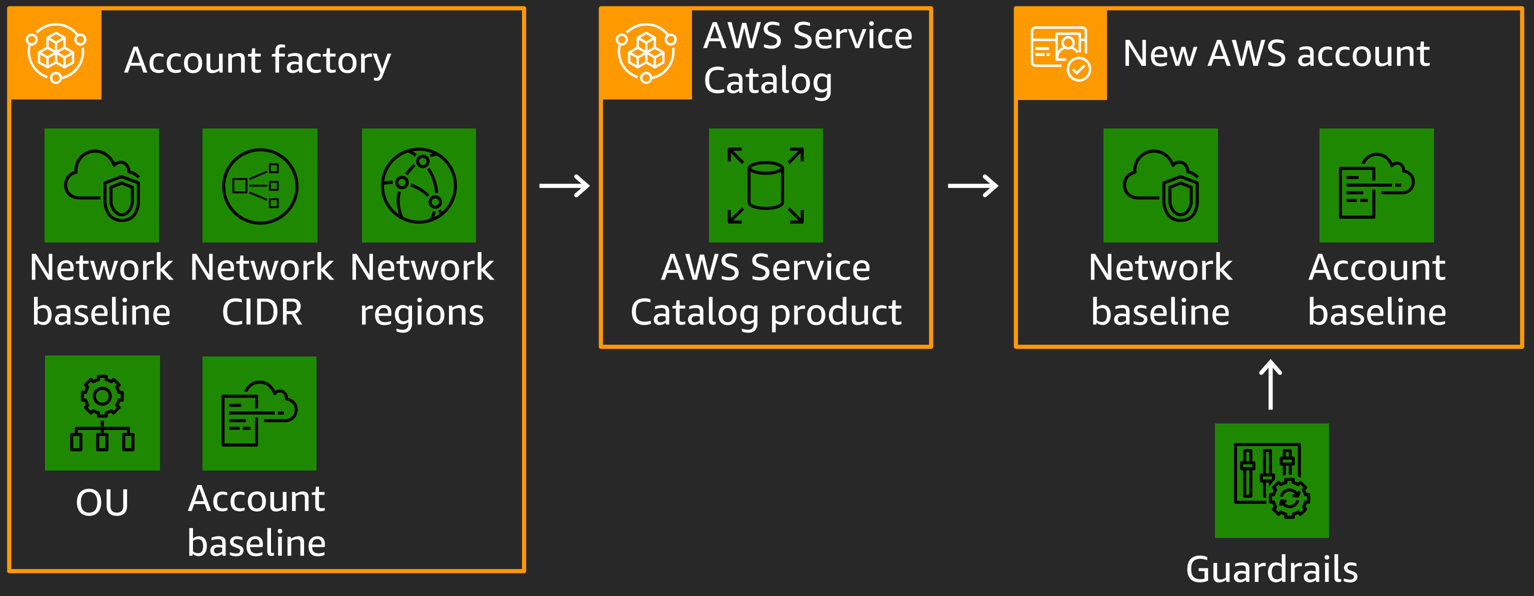
# Demo: Provision new user and AWS account

aws SUMMIT ONLINE

# Automate compliant account provisioning



**Cloud IT Admin**
Role: IT Ops Manager



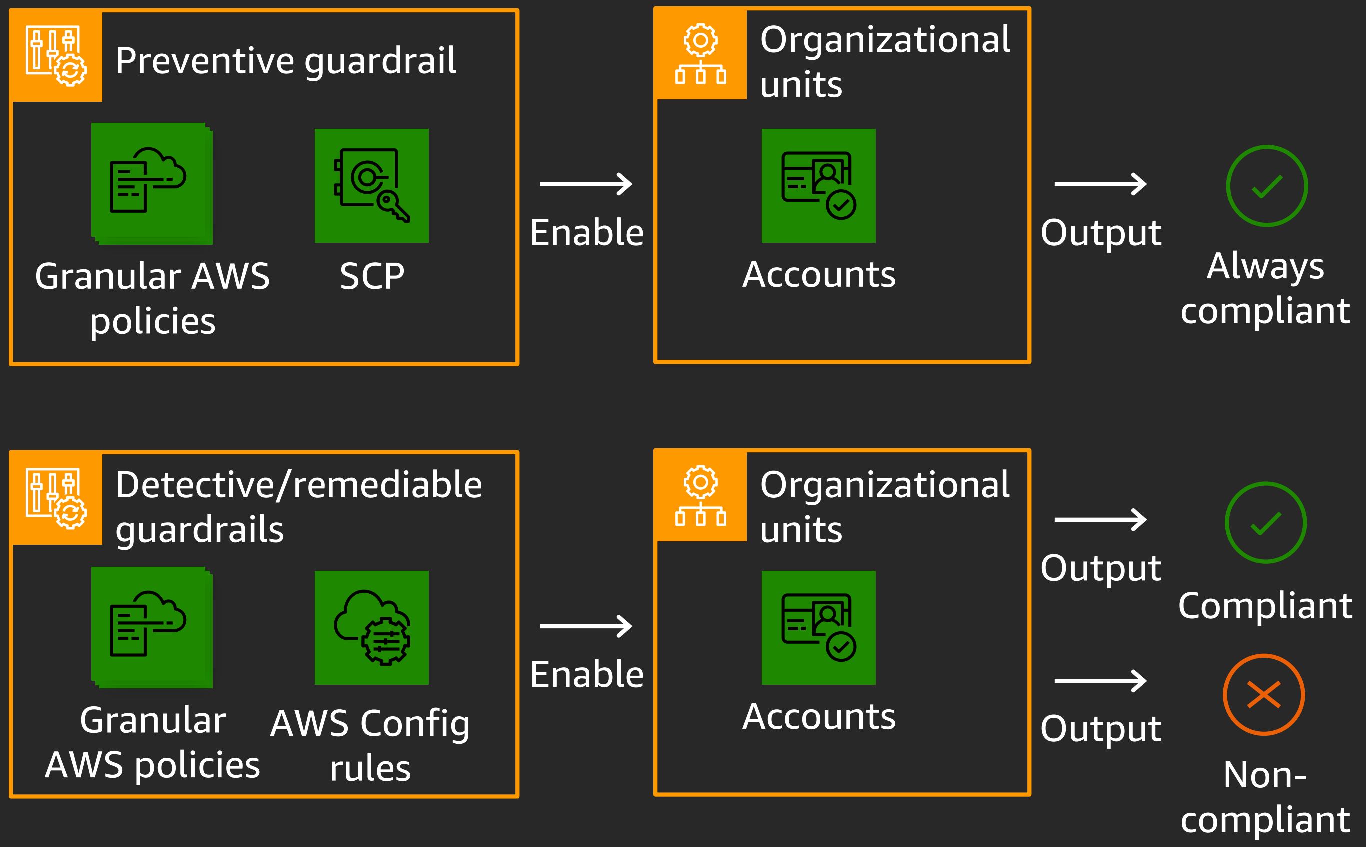
- Standardised account provisioning
- Automatic enforcement of guardrails
- Configurable network settings

“I want to ensure we are secure as we scale”

# Demo: Guardrails

# Establish guardrails

Cloud IT
security & compliance



- Preventive: prevents policy violations using Service Control Polices (SCPs), part of AWS Organizations
- Detective: detect policy violations using AWS Config rules
- A guardrail can be: mandatory, strongly recommended, or elective
- Guardrails apply to organizational units (OUs) and all child accounts (new and existing)

“Is there an easy way to deploy web servers so I can start testing quickly?”

# Demo: Enabling Builders

aws SUMMIT ONLINE

# landing zone

# vs AWS Landing Zone

# vs AWS Control Tower

# landing zone, AWS Landing Zone, AWS Control Tower

## landing zone:

- Secure pre-configured environment for your AWS presence
- Scalable and flexible
- Enables agility and innovation

## AWS Landing Zone solution:

- Implementation of a landing zone based on multi-account strategy guidance

# landing zone, AWS Landing Zone, AWS Control Tower

**landing zone:**

- Secure pre-configured environment for your AWS presence
- Scalable and flexible
- Enables agility and innovation

**AWS Landing Zone solution:**

- Implementation of a landing zone based on multi-account strategy guidance

**AWS Control Tower:**

- AWS service version of AWS Landing Zone

# Recommendations

**New customer:**

- Recommend AWS Control Tower
- Use out-of-box guardrails and blueprints
- Use AWS Control Tower Account Factory
- Enhance your landing zone with AWS Control Tower integrations and customizations

**Current AWS Landing Zone (ALZ) customers:**

- New version will allow future upgrade
- Replaces ALZ code with AWS Control Tower functionality
- Extensibility framework with AWS Control Tower

# Summary

AWS Control Tower

Enable

Provision

Operate

Business agility + governance & control

# Thank you!

aws SUMMIT ONLINE