Wifi / Password

Wifi name:
TDPK-WIFI

Username:
AWSWORKSHOP1
AWSWORKSHOP2
AWSWORKSHOP3
AWSWORKSHOP4
AWSWORKSHOP5
Password
Welcome@2022

https://github.com/TIDC-PS-Inter/AWS-Workshop

Part 1

AWS Workshop Series

Day 6: Control Tower

Taking Enterprise Beyond the Cloud by TrueIDC

Mr. Niran Sohinkong

Professional Service Manager

Presented by

- Niran Sohinkong (Nueng)
- Professional Service Manager, TrueIDC
- AWS DevOps
- AWS SysOps / Architect
- niran.soh@ascendcorp.com

Agenda

- Why Multiple Accounts
- Landing Zone
- AWS Control Tower

Isolation with IAM and VPC in one account?

AWS Account

Everything

“Gray” boundaries

Complicated and messy over time

Difficult to track resources

People stepping on each other

Single account vs. multiple accounts

AWS Organizations Concepts

Concepts and terms

Master account (★)

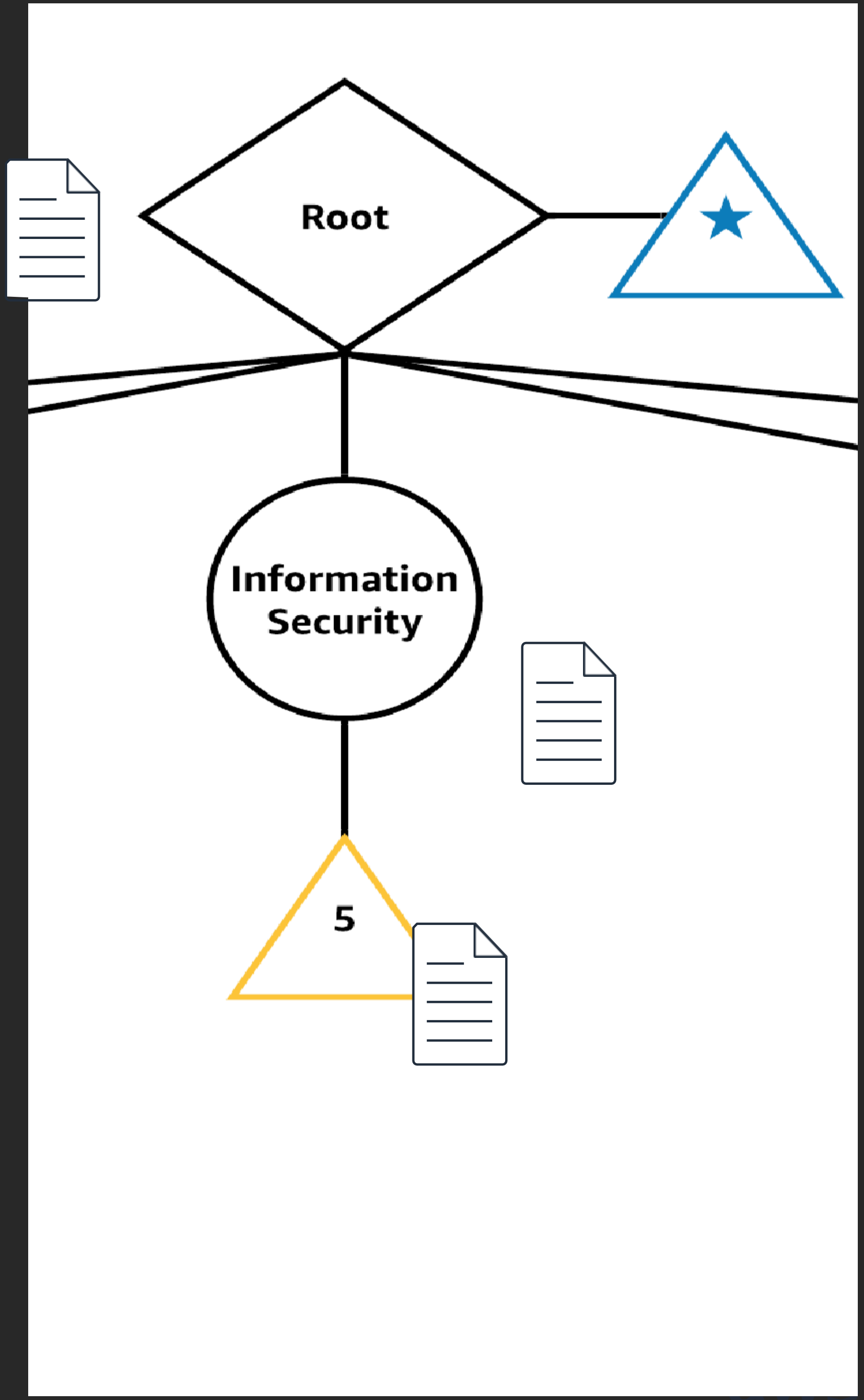
- Account used to create the organization (payer account)
- Central management and governance hub
- Minimal Resources

Organizational unit (OU)

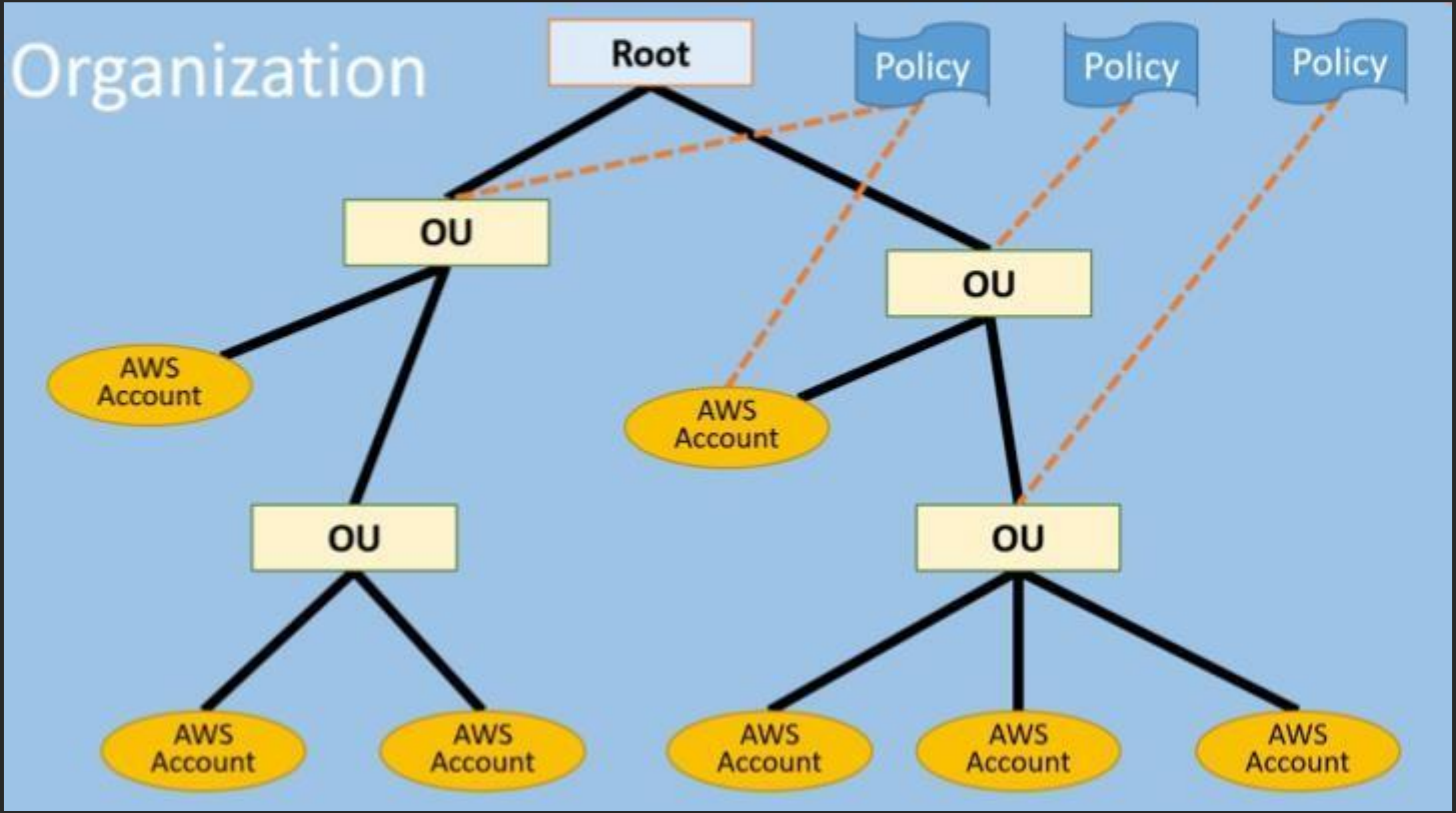
- Set of AWS accounts logically grouped within an organization

Policy

- Document describing controls to be applied to a selected set of accounts



AWS Oraganization structure



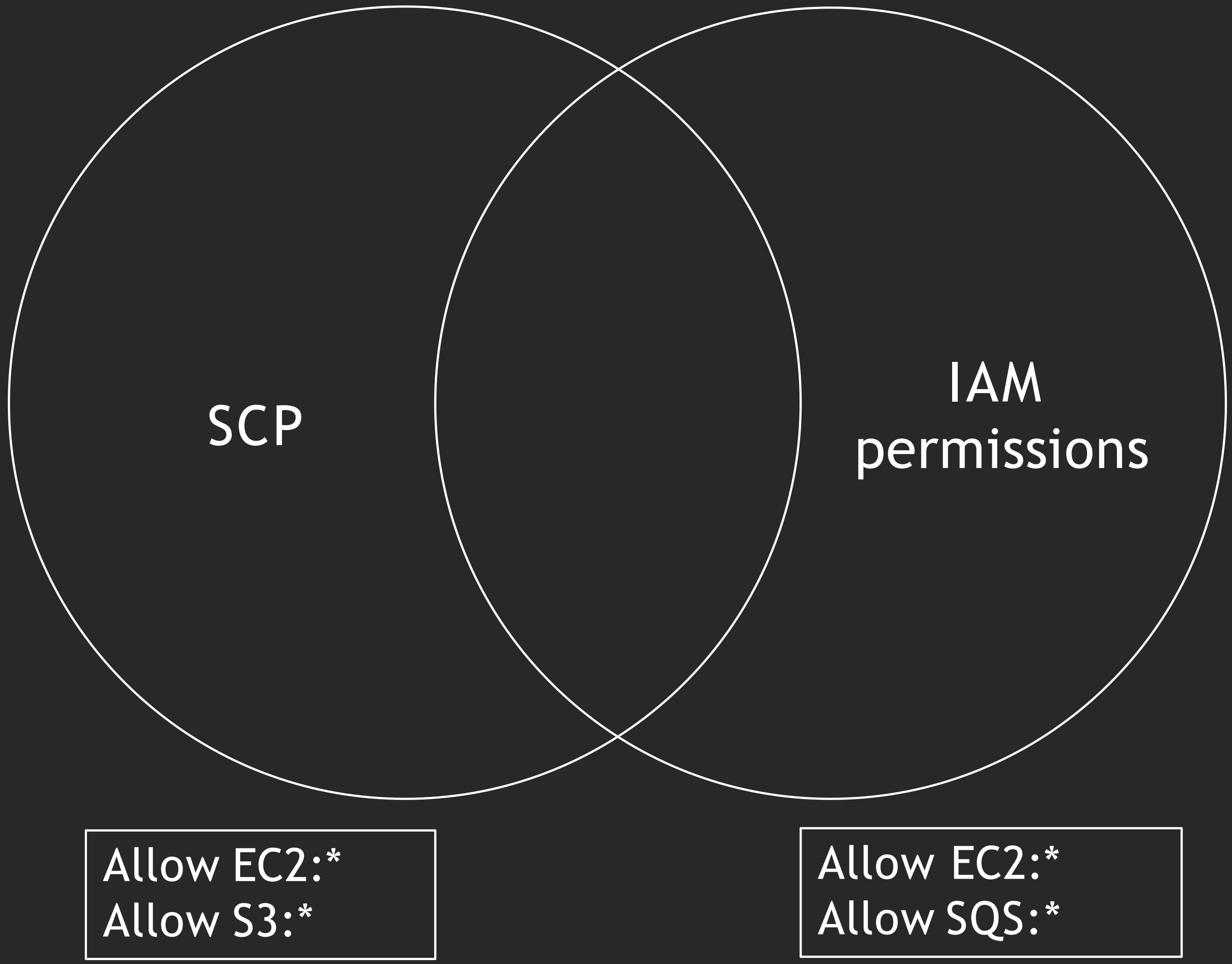
Service Control Policies (SCPs)

Define the maximum available permissions for IAM entities in an account

SCPs do not grant permission

Attach SCPs to the organization root, OUs, and individual accounts

SCPs attached to the root and OUs apply to all OUs and accounts inside of them



Allow EC2:*
Allow S3:*

Allow EC2:*
Allow SQS:*

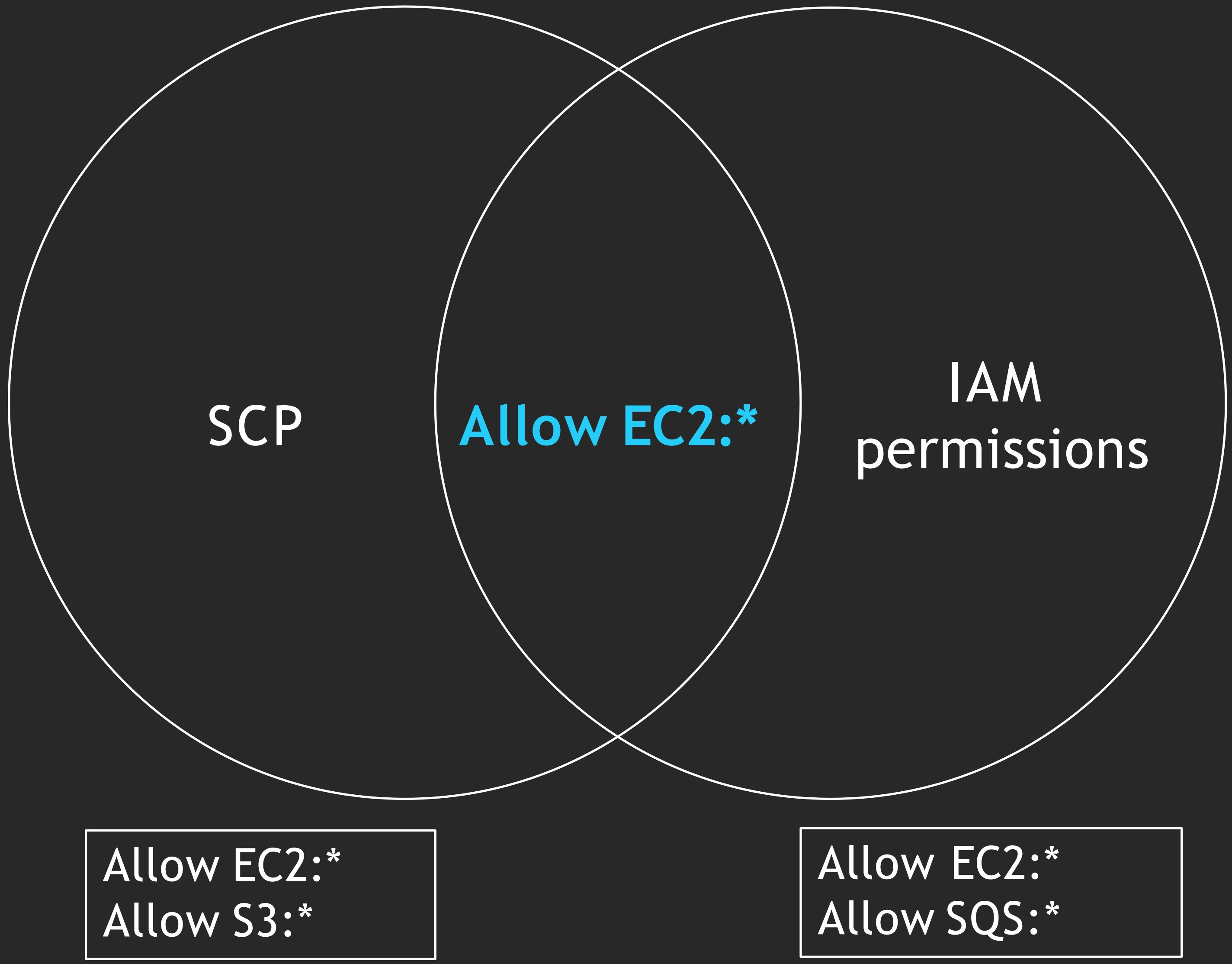
Service Control Policies (SCPs)

Define the maximum available permissions for IAM entities in an account

SCPs do not grant permission

Attach SCPs to the organization root, OUs, and individual accounts

SCPs attached to the root and OUs apply to all OUs and accounts inside of them



What is a “landing zone”

What is a “landing zone”

- A configured, secure, scalable, multi-account (multiple resource containers) AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for migrating applications
- An environment that allows for iteration and extension over time

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

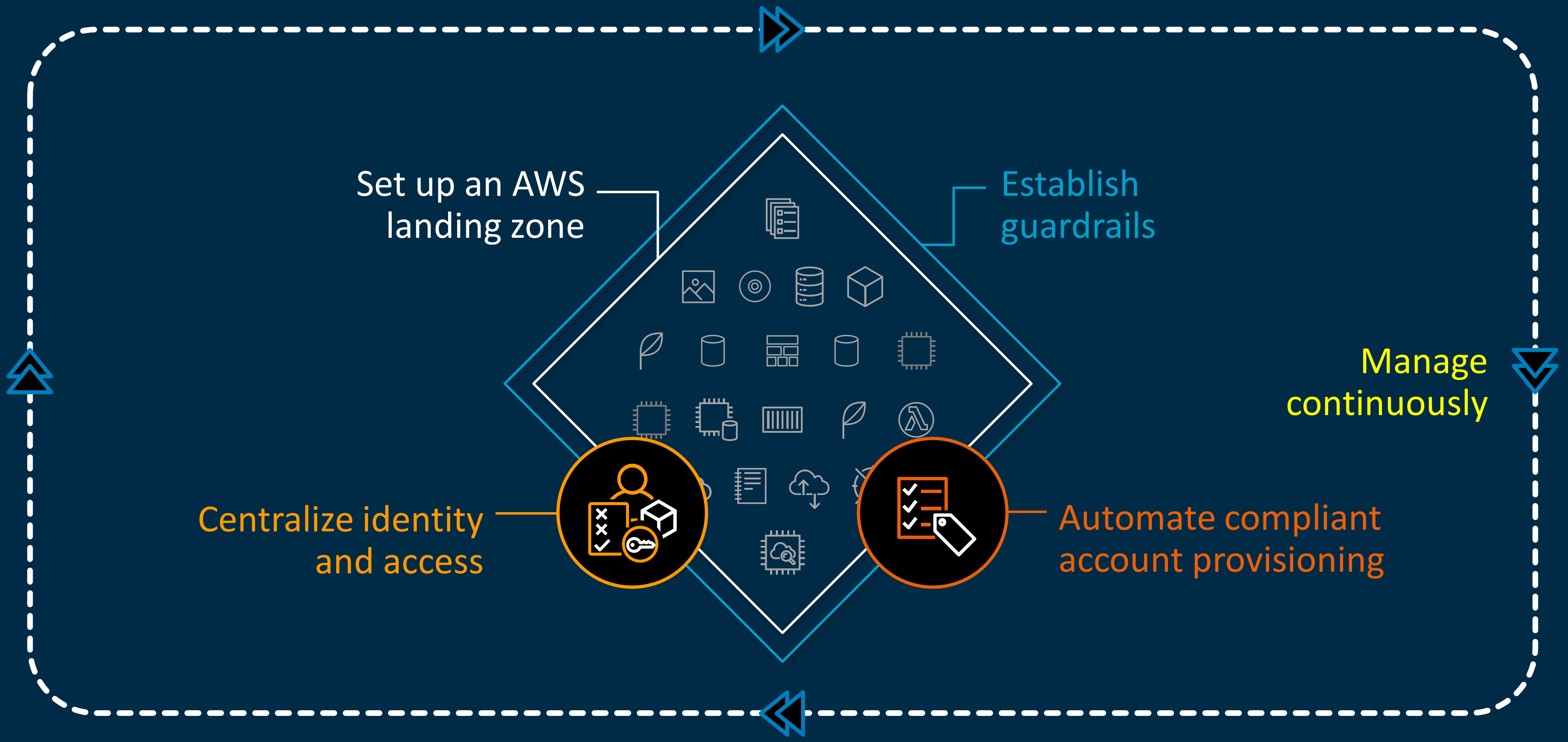
AWS Landing Zone Solution:

- Implementation of a landing zone based on multi-account strategy guidance
- Customers get code that they will need to manage & maintain

AWS Control Tower:

- AWS Managed Service version of AWS Landing Zone

Enable governance



Set up an AWS landing zone

Establish guardrails

Manage continuously

Centralize identity and access

Automate compliant account provisioning

Using AWS Control Tower to govern multi-account AWS environments at scale

Why use “AWS Control Tower”

Why use AWS Control Tower?

Set up a best-practices AWS environment in a few clicks

Standardize account provisioning

Centralize policy management

Enforce governance and compliance proactively

Enable end user self-service

Get continuous visibility into your AWS environment

Gain peace of mind

Balancing the needs of builders and central cloud IT

Builders: Stay agile

Innovate with the speed and agility of AWS

Cloud IT: Establish governance

Govern at scale with central controls

More innovation, greater agility, with control

Agility

Experiment

Be productive
Empower distributed teams
Self-service access

Respond quickly
to change

Don’t choose between
Agility or Control

You need and want both

Governance

Enable

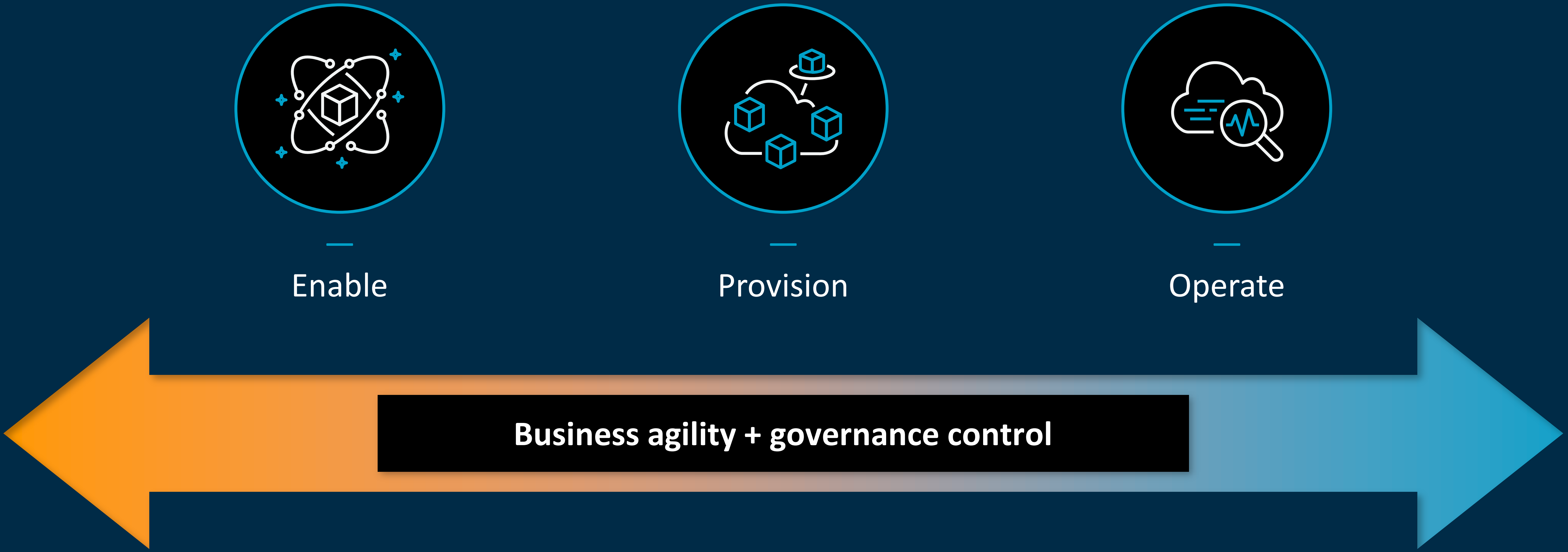
Provision

Operate

Secure & Compliant

Operations & Spend
Management

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



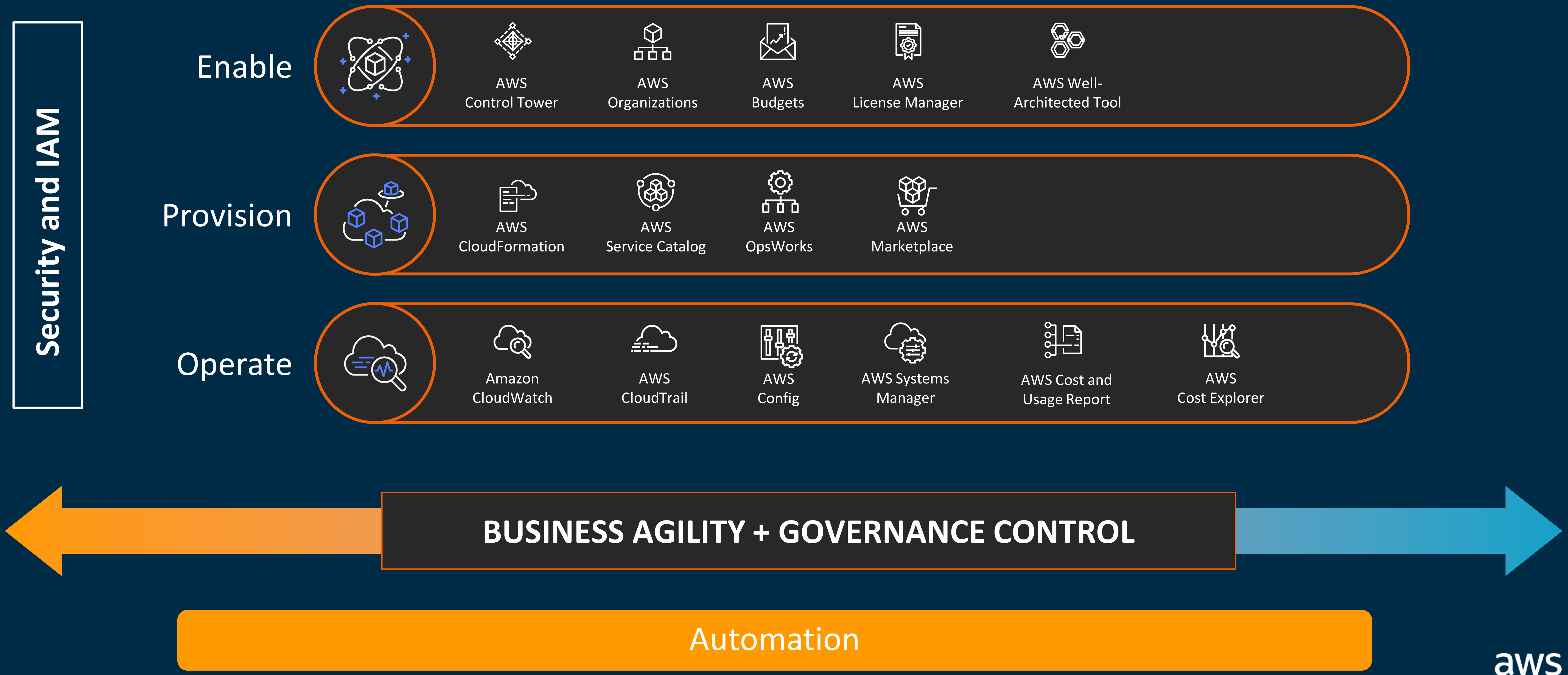
Enable

Provision

Operate

Business agility + governance control

AWS management and governance services



Security and IAM

Enable

AWS Control Tower

AWS Organizations

AWS Budgets

AWS License Manager

AWS Well-Architected Tool

Provision

AWS CloudFormation

AWS Service Catalog

AWS OpsWorks

AWS Marketplace

Operate

Amazon CloudWatch

AWS CloudTrail

AWS Config

AWS Systems Manager

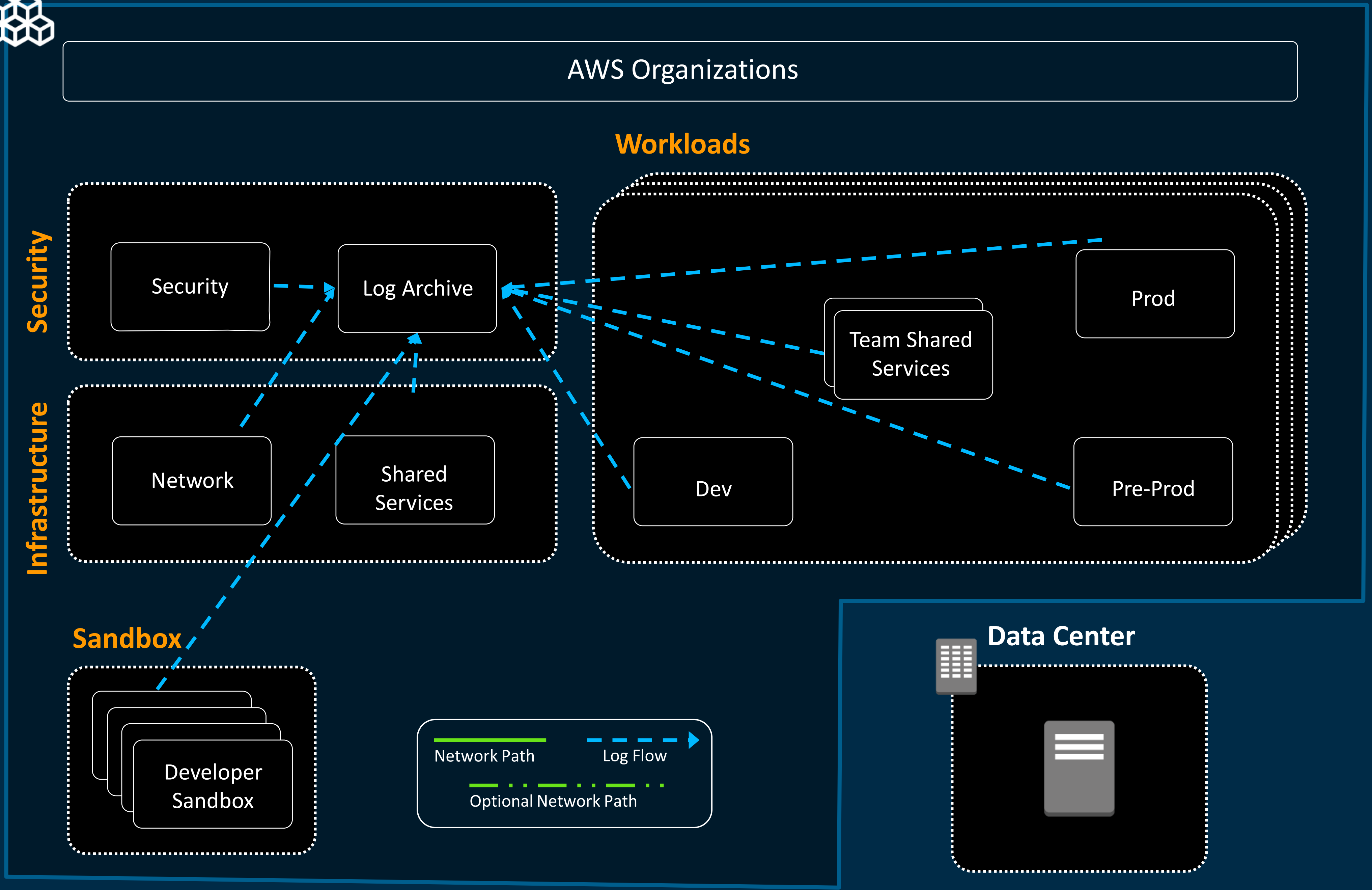
AWS Cost and Usage Report

AWS Cost Explorer

BUSINESS AGILITY + GOVERNANCE CONTROL

Automation

Multi-account approach // security log flow



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

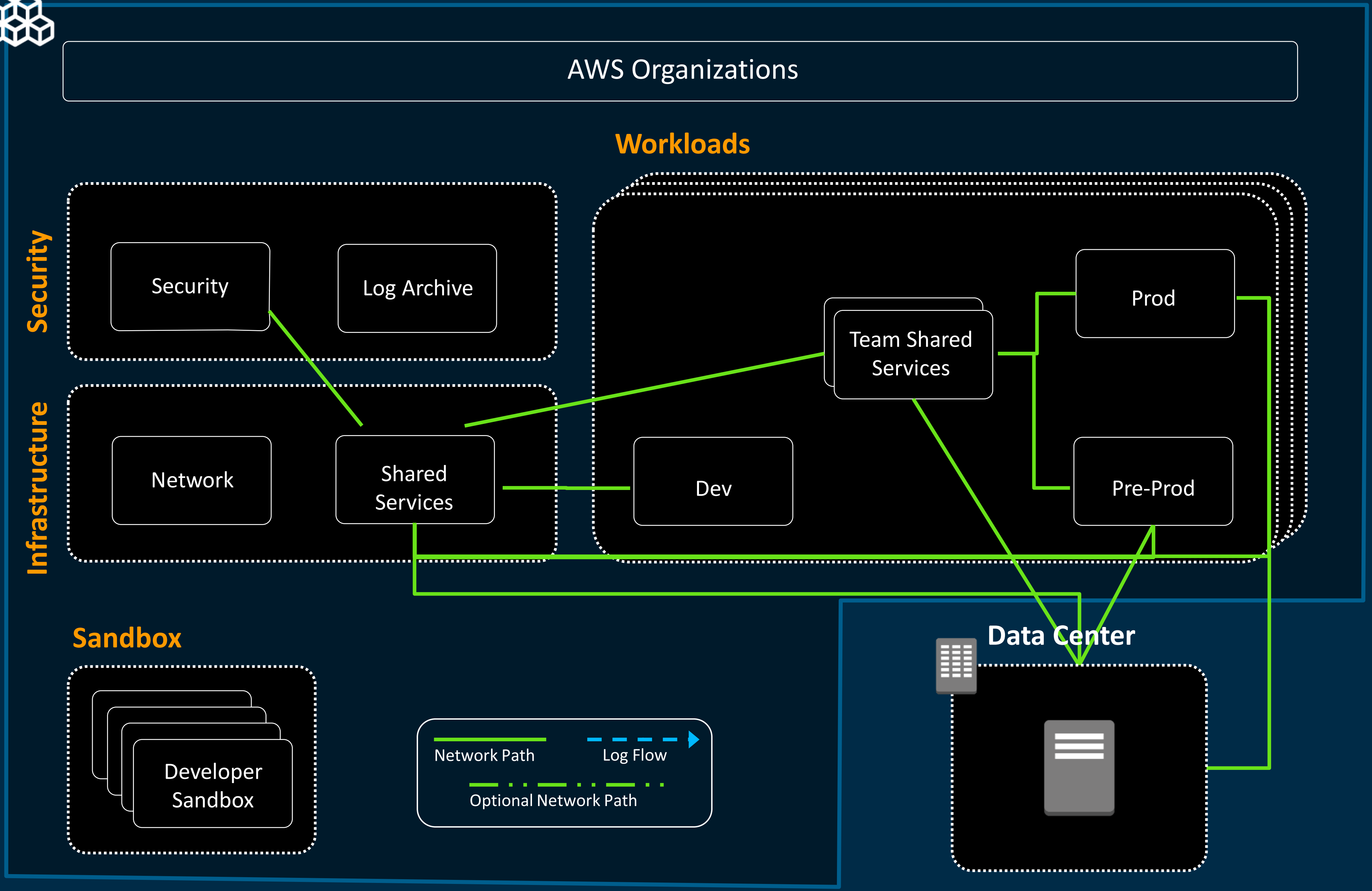
Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

Multi-account approach // network connectivity



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

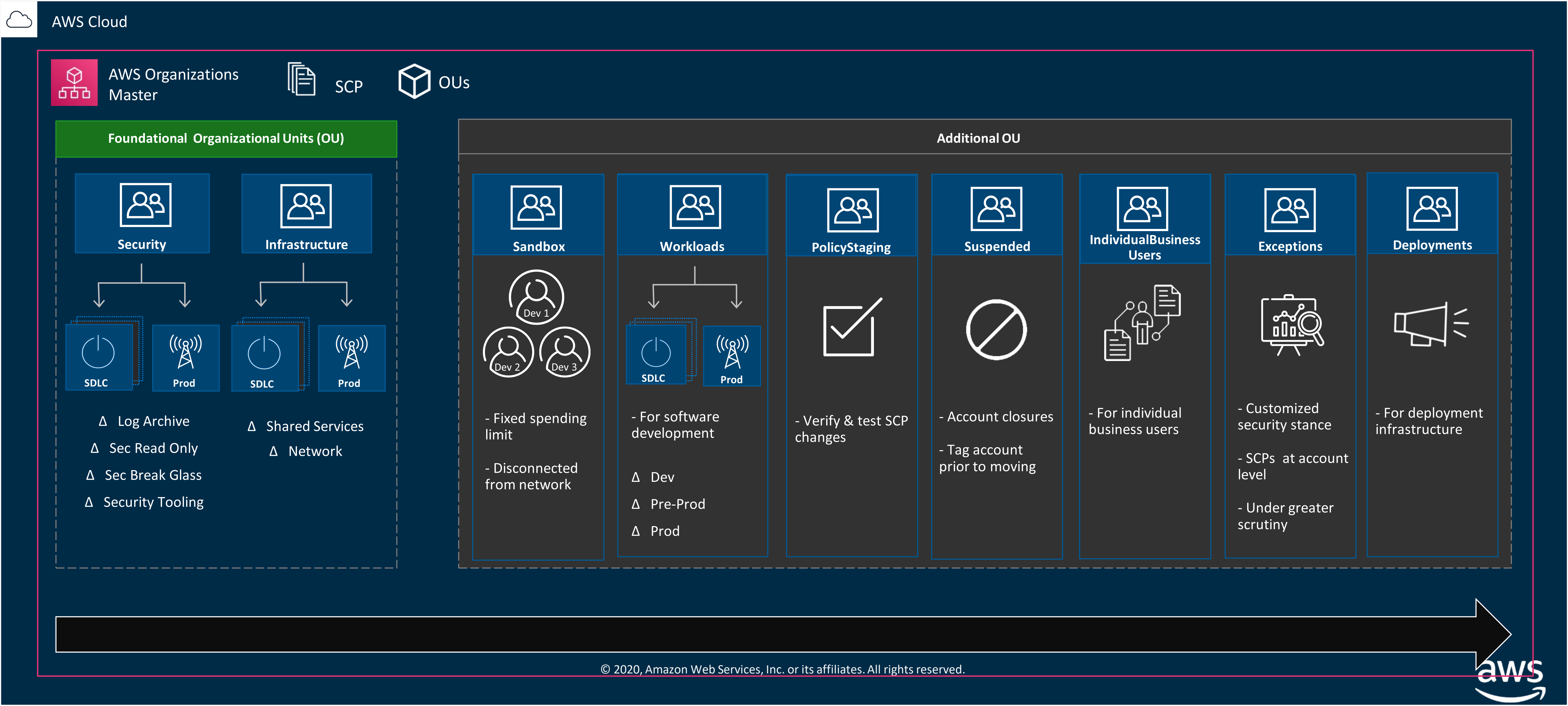
Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

Multi-account framework



AWS Cloud

AWS Organizations Master

SCP

OUs

Foundational Organizational Units (OU)

Security

SDLC

Prod

∆ Log Archive
∆ Sec Read Only
∆ Sec Break Glass
∆ Security Tooling

Infrastructure

SDLC

Prod

∆ Shared Services
∆ Network

Additional OU

Sandbox

Dev 1 Dev 2 Dev 3

- Fixed spending limit

- Disconnected from network

Workloads

SDLC

Prod

- For software development

∆ Dev
∆ Pre-Prod
∆ Prod

PolicyStaging

- Verify & test SCP changes

Suspended

- Account closures

- Tag account prior to moving

IndividualBusiness Users

- For individual business users

Exceptions

- Customized security stance

- SCPs at account level

- Under greater scrutiny

Deployments

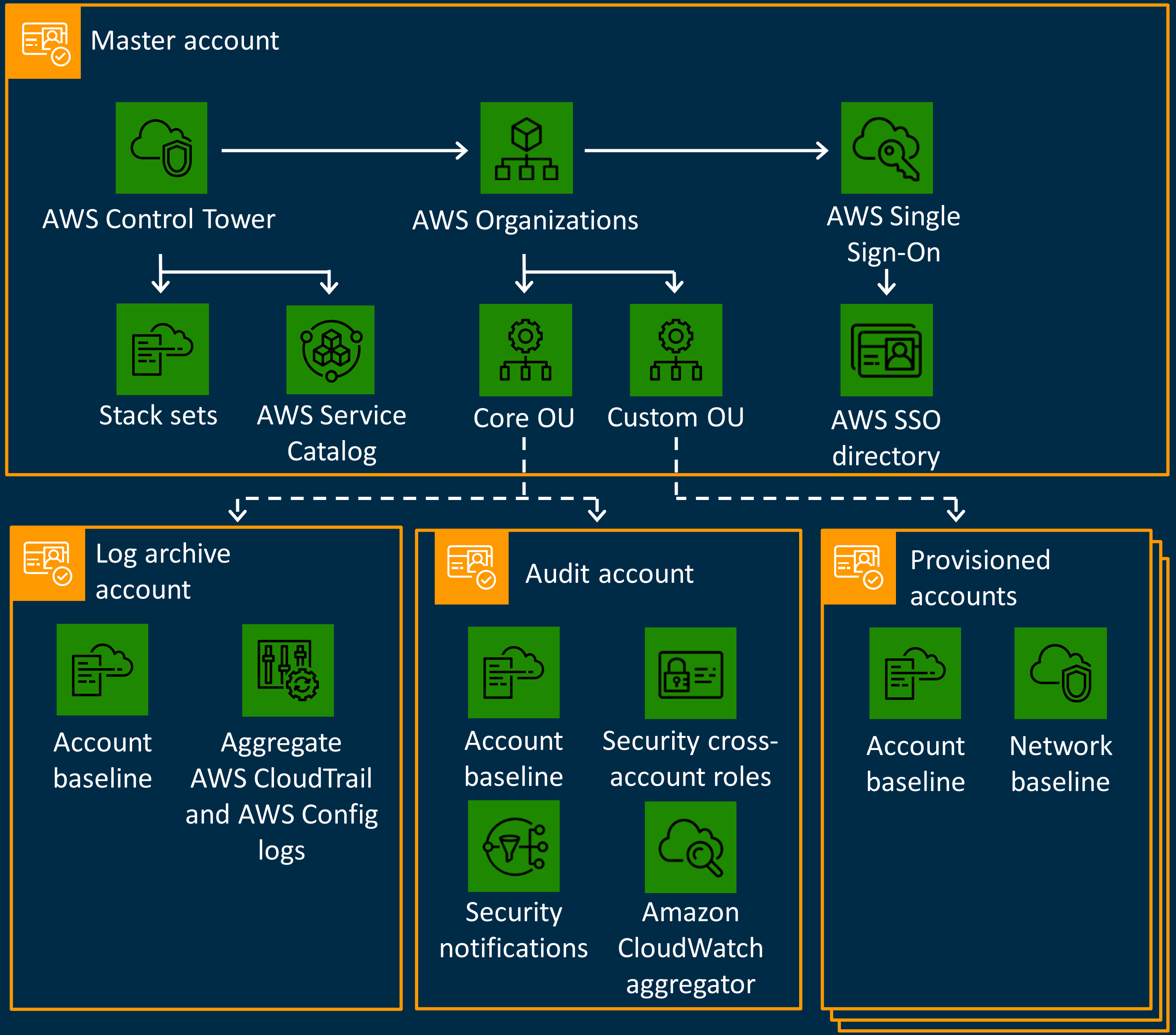
- For deployment infrastructure

AWS Control Tower

The easiest self-service solution to automate the setup of **new AWS multi-account environments**

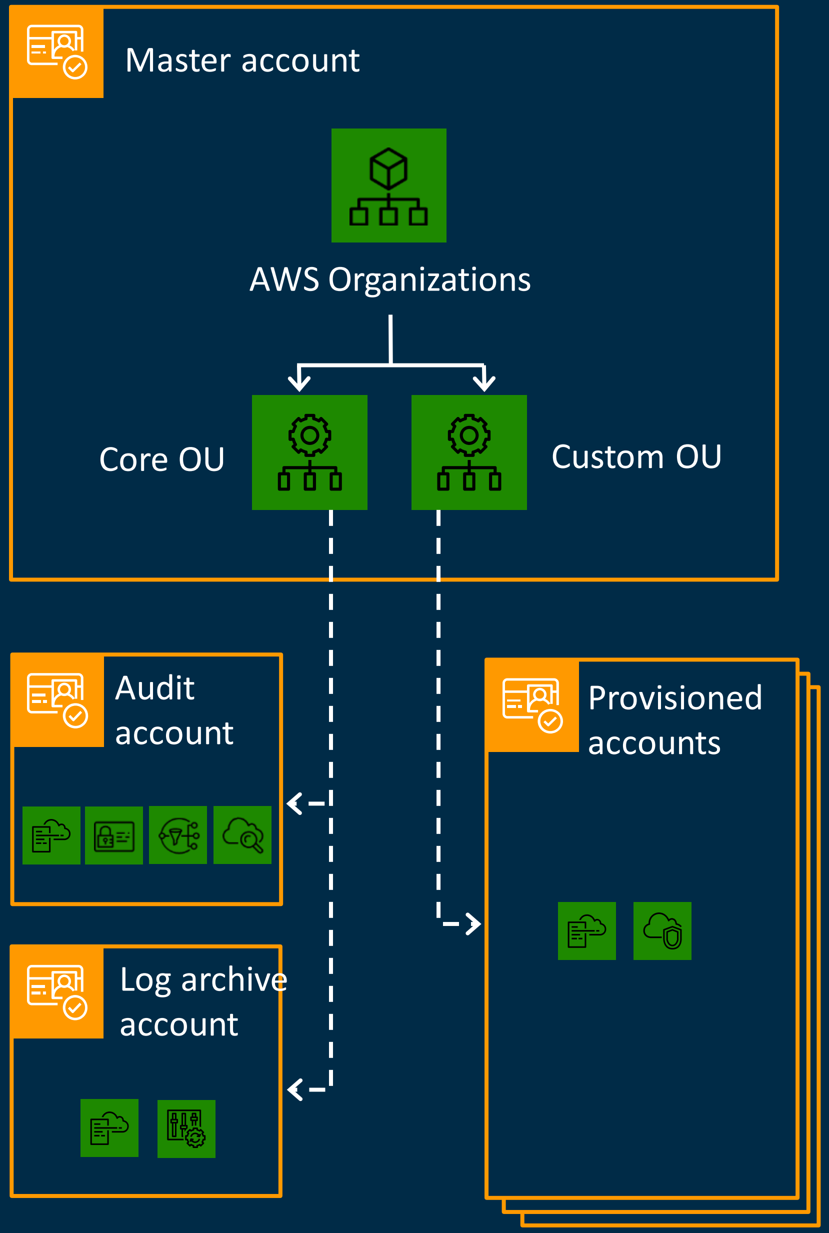
- An AWS service offering account creation based on AWS best practices
- Deployment of AWS best practice Blueprints and Guardrails
- Baseline fundamental accounts to provide standardization of best practices
- Single pane of glass for monitoring compliance to guardrails

Set up an AWS landing zone



- Landing zone - a preconfigured, secure, scalable, multi-account AWS environment based on best practice blueprints
- Multi-account management using AWS Organizations
- Identity and federated access management using AWS SSO
- Centralized log archive using AWS CloudTrail and AWS Config
- Cross-account audit access using AWS SSO and AWS IAM
- End user account provisioning through AWS Service Catalog
- Centralized monitoring and notifications using Amazon CloudWatch and Amazon SNS

Multi-account architecture

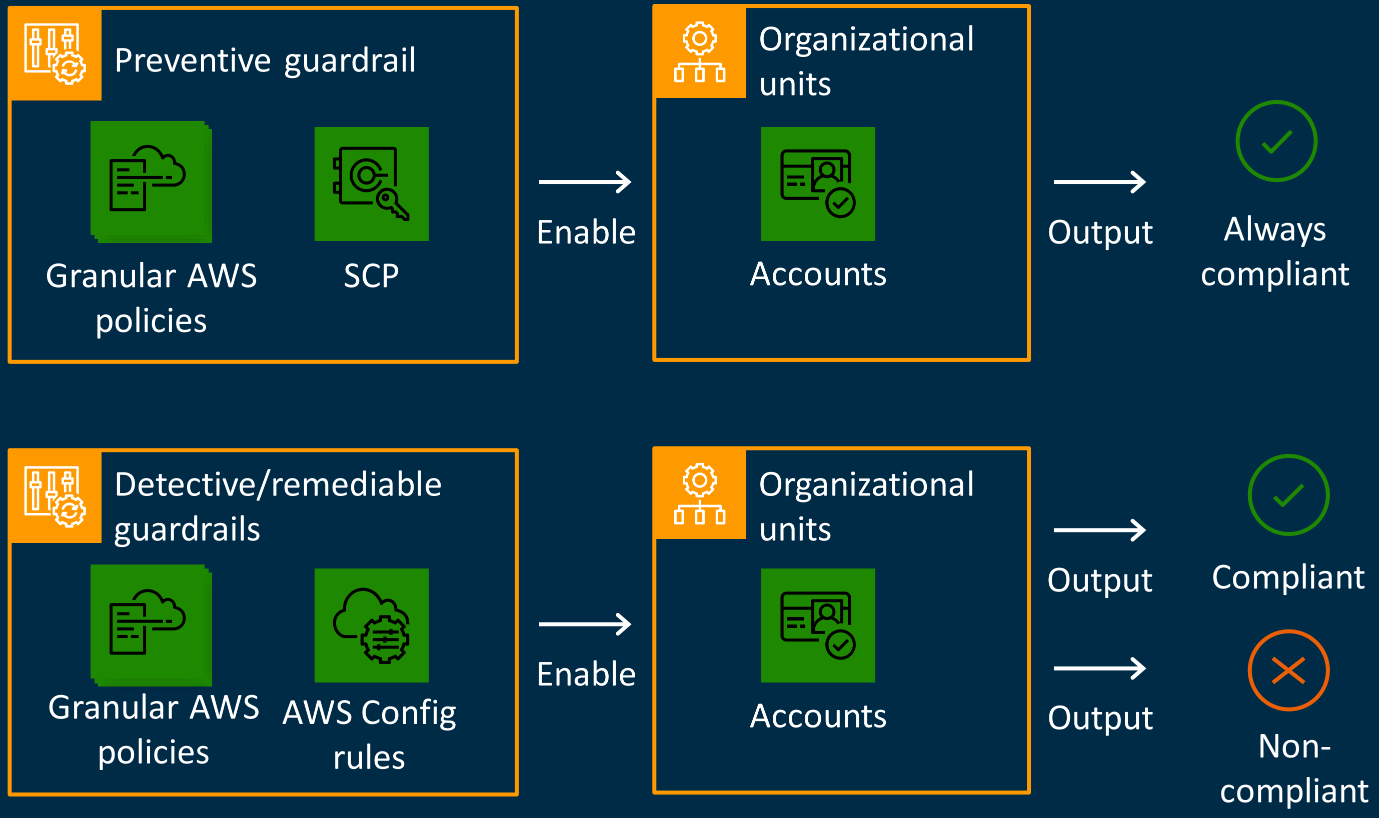


- Master account: designation of your existing account to create a new organization. Also your master payer account
- Organization consists of 2 OUs with pre-configured accounts -
  - Core OU: AWS Control Tower-created accounts, i.e., Audit account and Log archive account
  - Custom OU: Your provisioned accounts

Centralize identity and access

- AWS SSO provides default directory for identity
- AWS SSO also enables federated access management across all accounts in your organization
- Preconfigured groups (e.g., AWS Control Tower administrators, auditors, AWS Service Catalog end users)
- Preconfigured permission sets (e.g., admin, read-only, write)

Establish guardrails

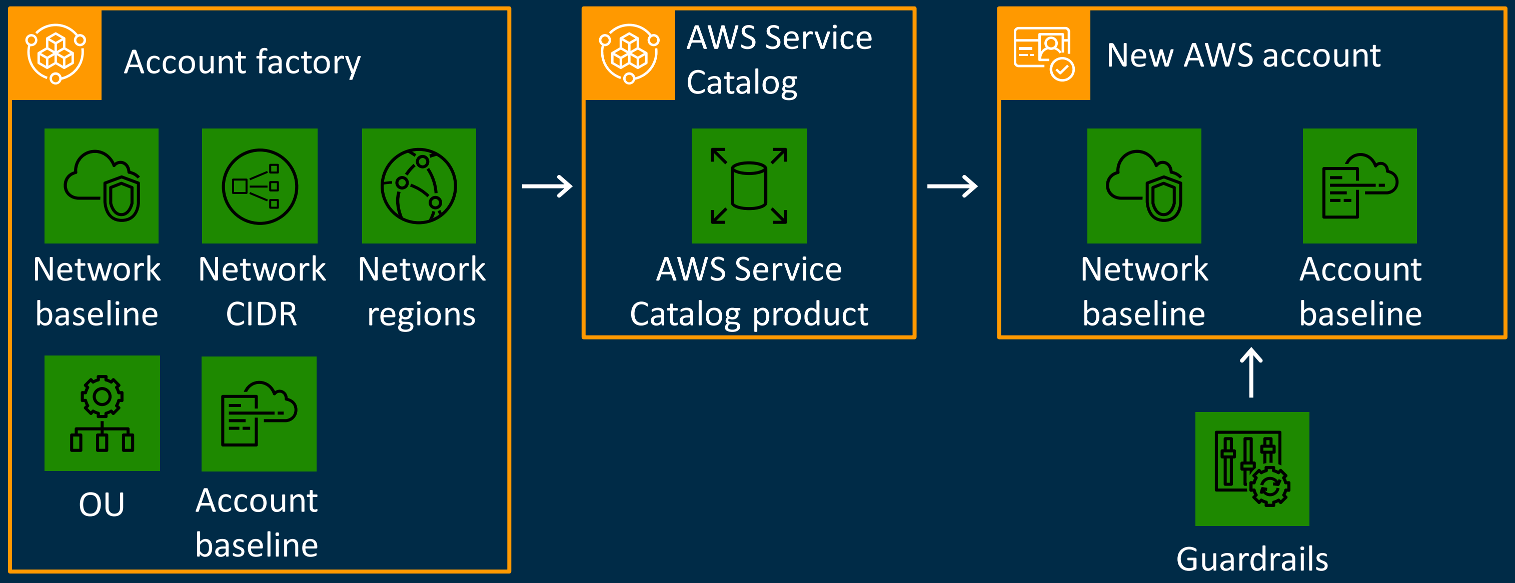


- Guardrails are preconfigured governance rules for security, compliance, and operations
- Expressed in plain English to provide abstraction over granular AWS policies
- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: detect policy violations and alert in the dashboard; implemented using AWS Config rules
- Mandatory and strongly recommended guardrails for prescriptive guidance
- Easy selection and enablement on organizational units

Guardrail examples

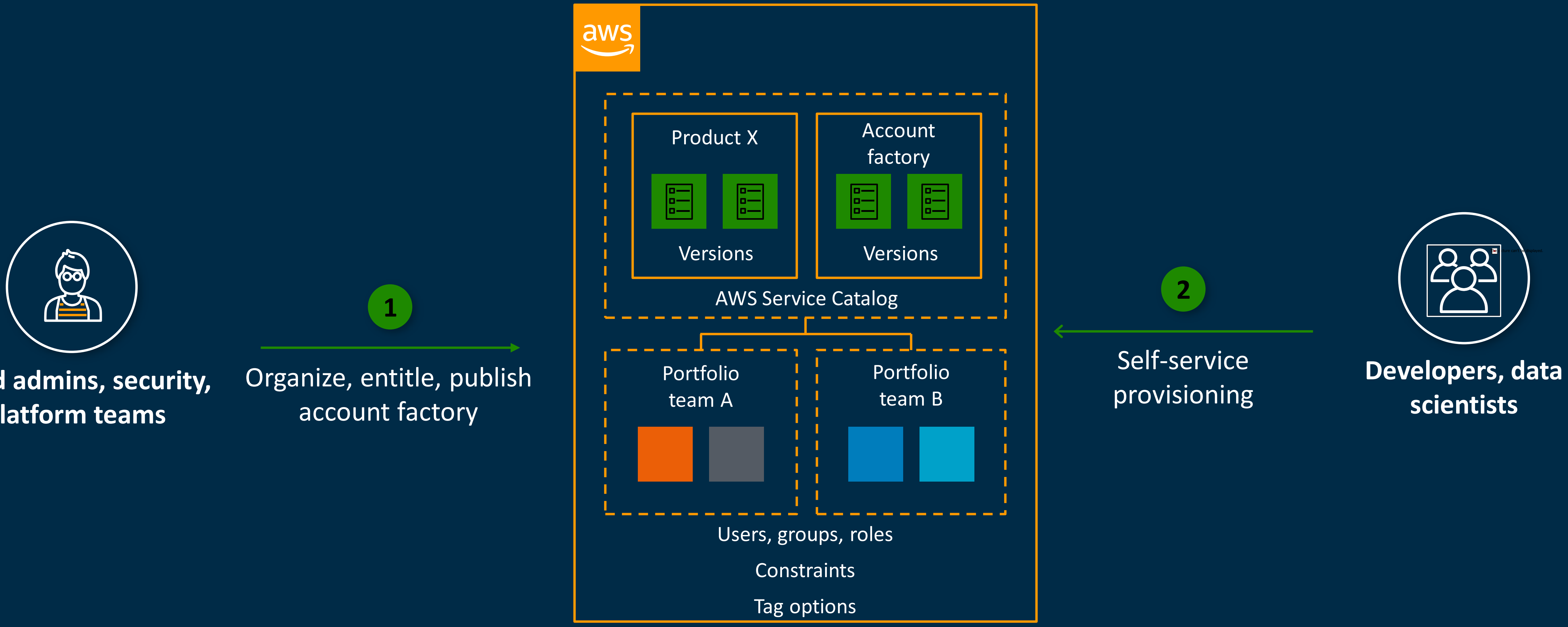
Goal/category	Example
IAM security	Require MFA for root user
Data security	Disallow public read access to Amazon S3 buckets
Network security	Disallow internet connection via Remote Desktop Protocol (RDP)
Audit logs	Enable AWS CloudTrail and AWS Config
Monitoring	Enable AWS CloudTrail integration with 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

Automate compliant account provisioning



- Built-in account factory provides a template to standardize account provisioning
- Configurable network settings (e.g., subnets, IP addresses)
- Automatic enforcement of account baselines and guardrails
- Published to AWS Service Catalog

Enable self-service with AWS Service Catalog



Cloud admins, security, platform teams

1

Organize, entitle, publish account factory

Product X

Versions

Account factory

Versions

AWS Service Catalog

Portfolio team A

Portfolio team B

Users, groups, roles

Constraints

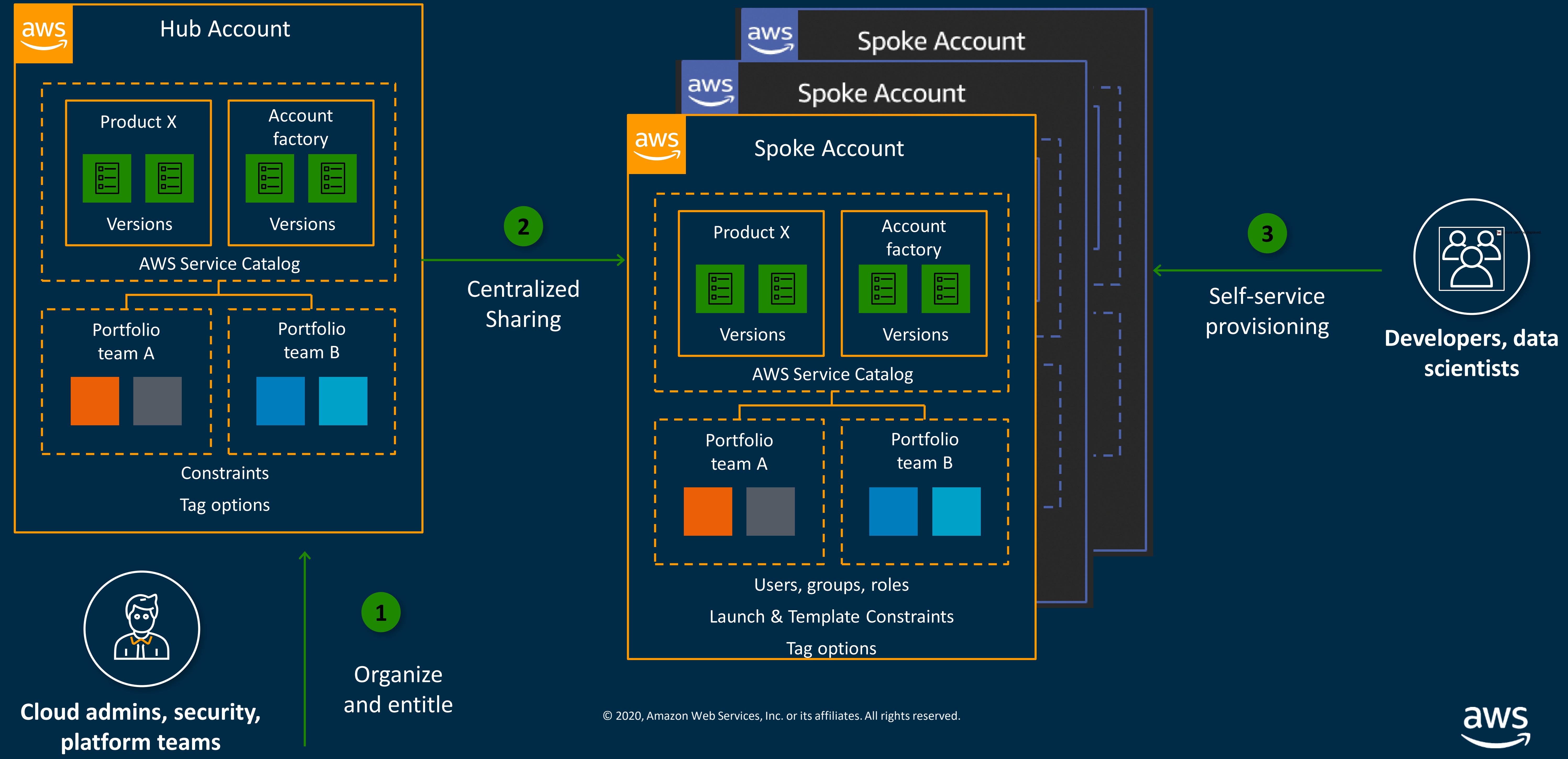
Tag options

2

Self-service provisioning

Developers, data scientists

Automate governance at scale



Benefits of governance at scale

Security

Curation
Compliance
Standardization

Speed

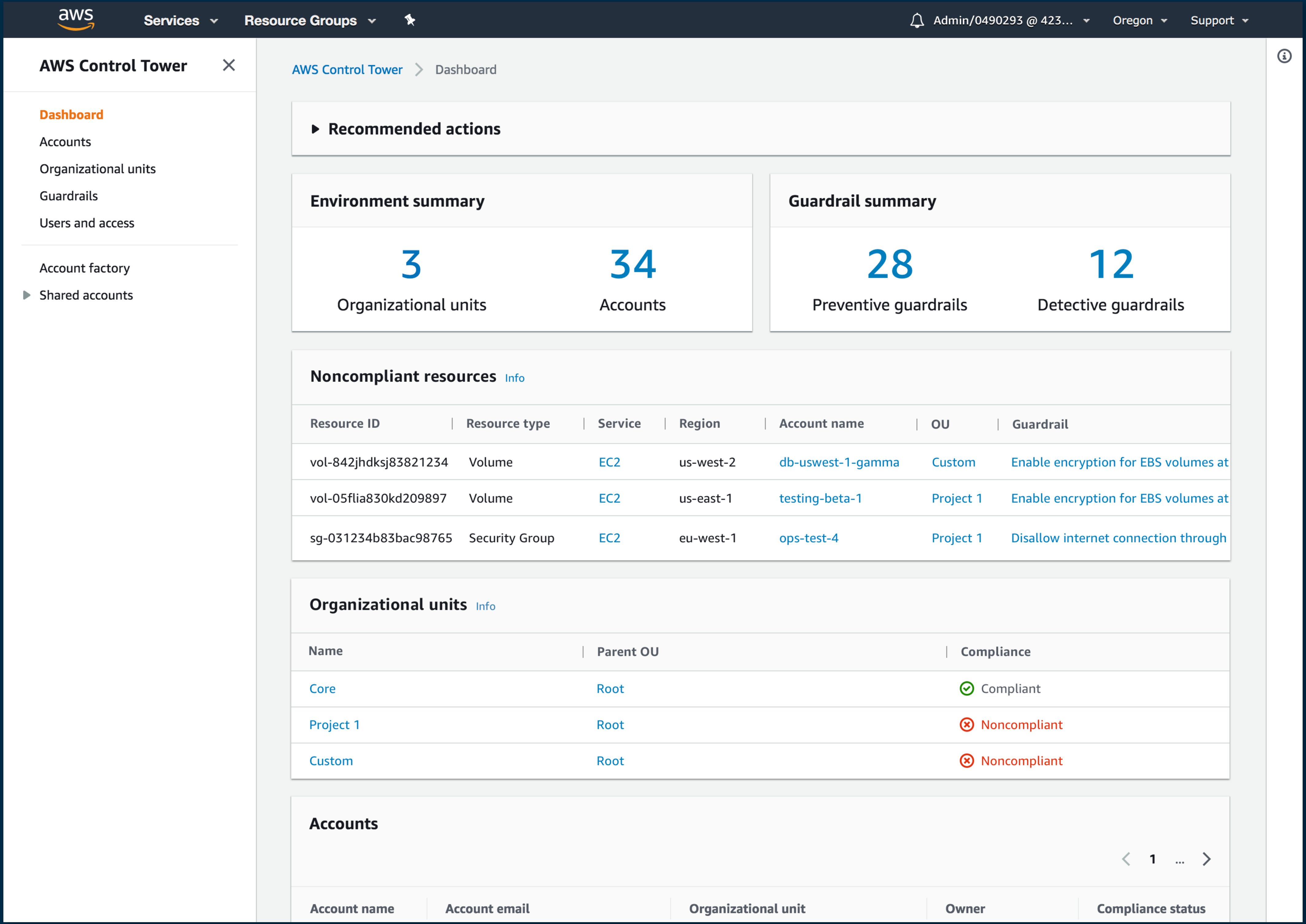
Agility
Self-service
Time to market

Organizations

Service catalogs enable organizations to deploy and manage infrastructure and applications that reflect the organization’s security and operational policies

End Users

Dashboard for oversight



AWS Control Tower > Dashboard

▶ Recommended actions

Environment summary

3 Organizational units

34 Accounts

Guardrail summary

28 Preventive guardrails

12 Detective guardrails

Noncompliant resources Info

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

Organizational units Info

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

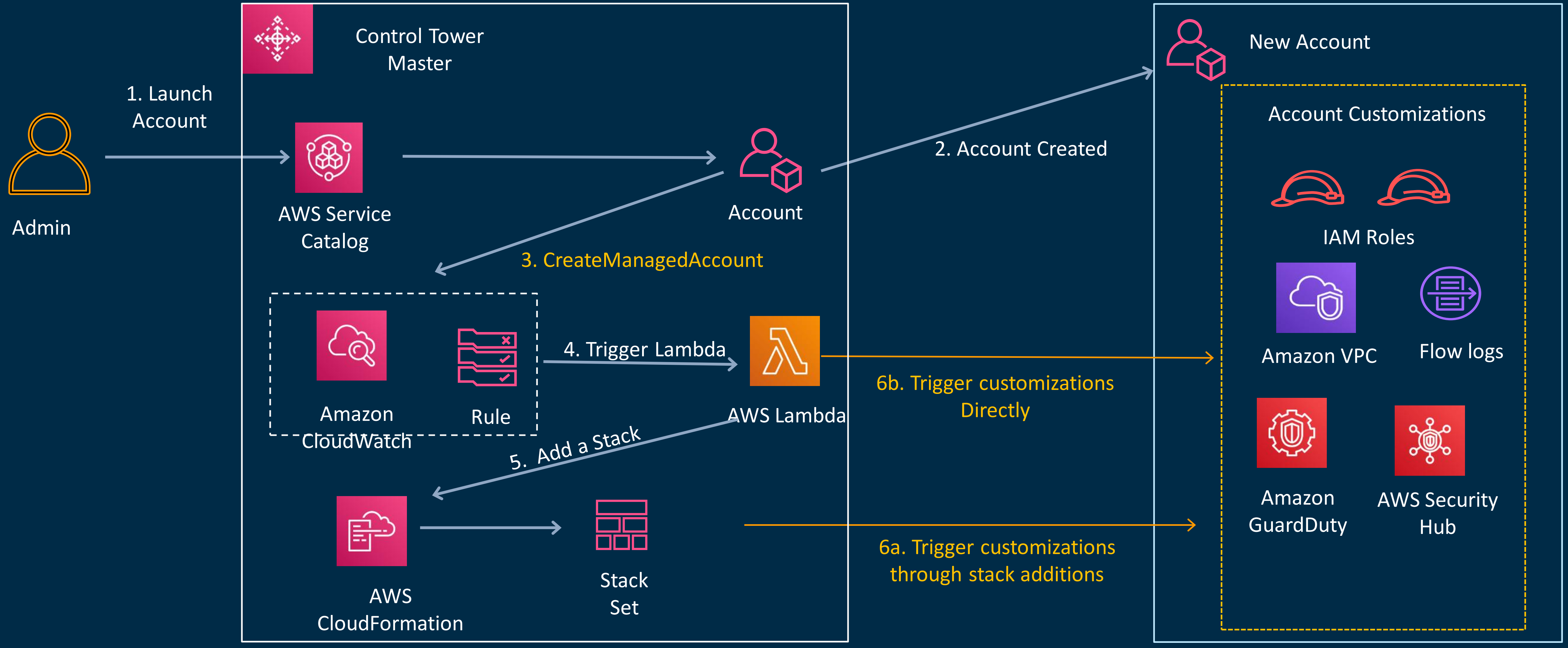
Accounts

< 1 ... >

Account name	Account email	Organizational unit	Owner	Compliance status

Configure with AWS Control Tower Lifecycle Events

- **CreateManagedAccount:** The log records whether AWS Control Tower successfully completed every action to create and provision a new account using account factory.



Considerations for a base foundation of services in each account

- Networking: VPC/TGW,
- Identity Management: Which provider, but also which IAM roles(SSO)
- Security tooling: Guard Duty, Security Hub, IAM Access Analyzer, 3rd party tools
- Logging Strategies: Which logs to locate where, and how to integrate to log aggregators
- Support level: Enterprise, business (may be different across each child account in the Master)
- Additional Guardrails (BYOG)
- Integration to Operational Processes: ITSM/ITIL tooling (ServiceNow, Jira Service Desk), asset management, CMDB, etc.)
- Base resources: Other AWS services required for the account - think lampstack, or 'approved' pipeline for architecture pattern

Summary of key features

- Automated landing zone with best practice blueprints
- Guardrails for policy management
- Account factory for account provisioning
- Dashboard for visibility and actions
- Built-in identity and access management
- Preconfigured log archive and audit access to accounts
- Built-in monitoring and notifications
- Automatic updates

Pricing and availability

Generally available
in US East (N. Virginia), US East (Ohio), US West (Oregon), and EU (Ireland), AP Southeast (Sydney)

No additional charge for using AWS Control Tower

Pay only for underlying AWS services (e.g., AWS Config rules, AWS Service Catalog) that are enabled