

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

NAME  
TITLE  
AWS  
DATE

# Balancing the needs of builders and central cloud IT

Builders:  
Stay agile



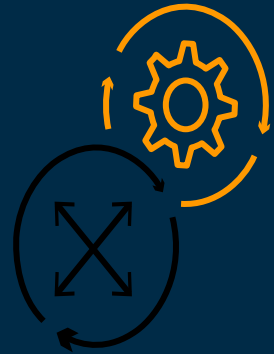
Innovate with the speed and  
agility of AWS

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

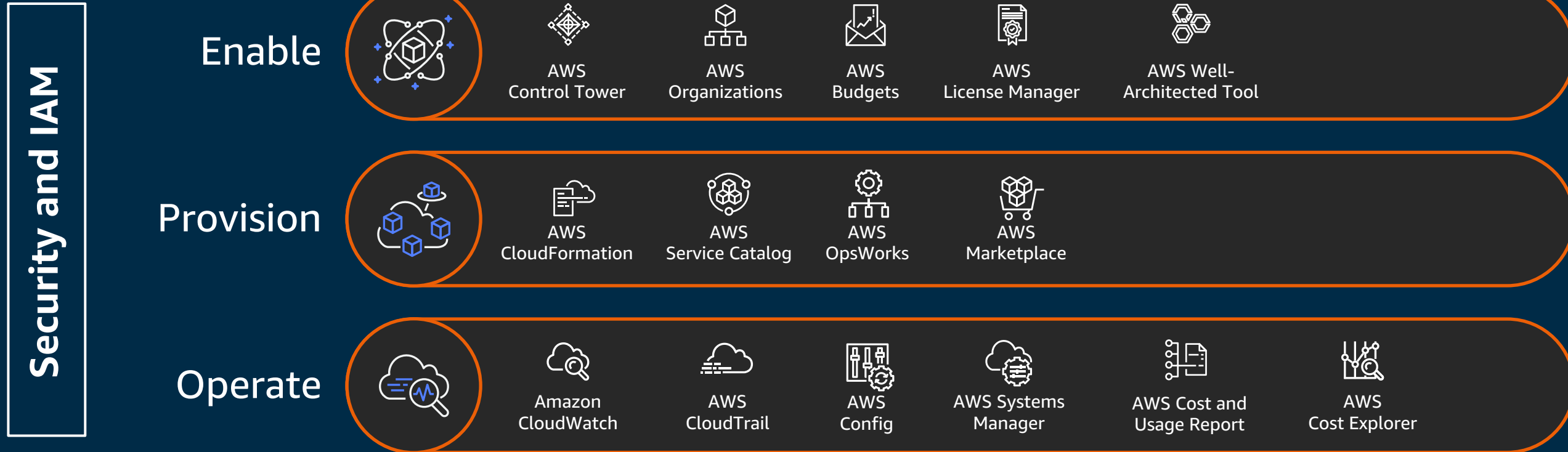
Provision

Operate

Secure & Compliant

Operations & Spend  
Management

# AWS management and governance services



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



Enable



Provision



Operate



**Business agility + governance control**

# 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

# 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
- Solution will no longer receive updates by EOY 2020

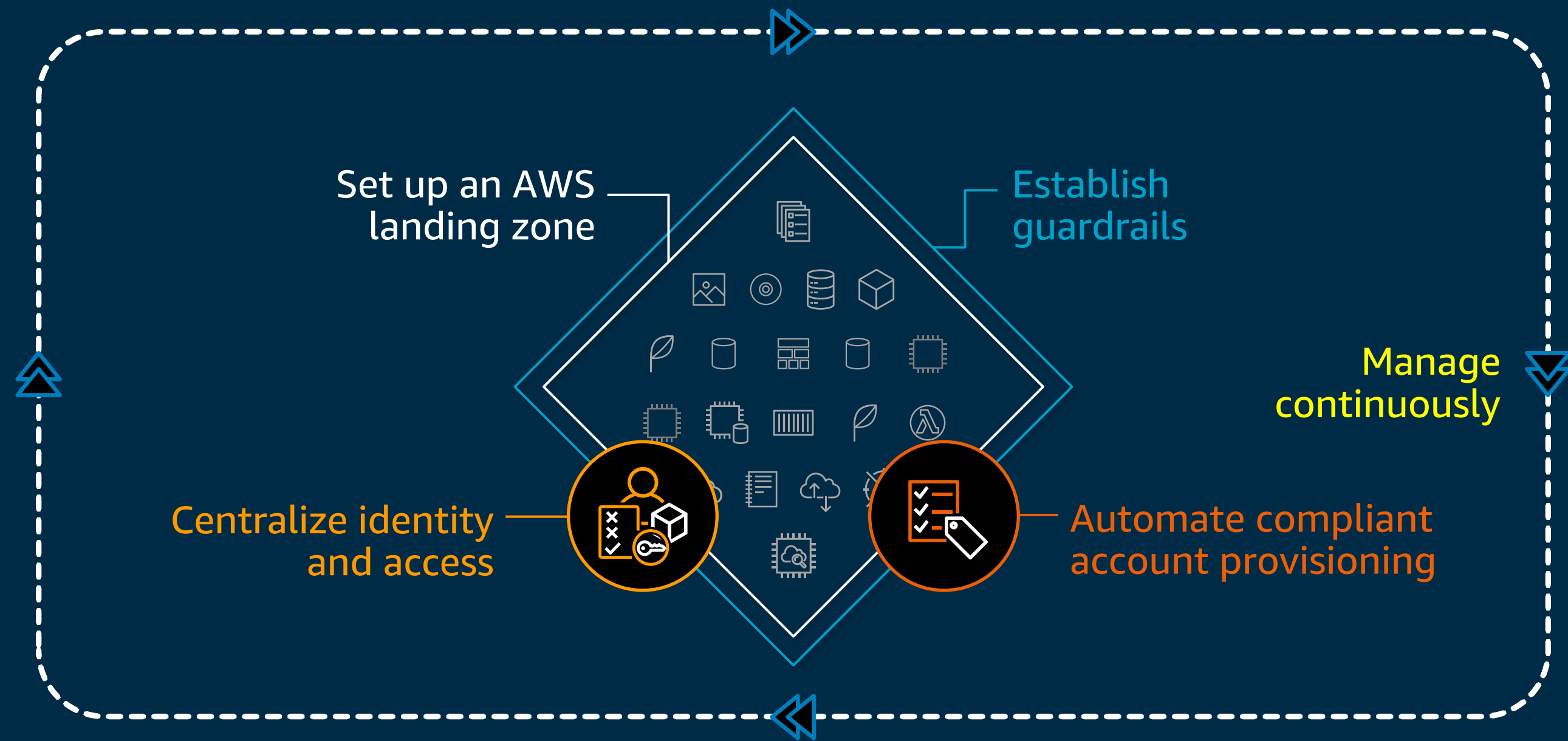
## AWS Control Tower:

- AWS Managed Service version of AWS Landing Zone



# Enable governance

 Enable



# 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



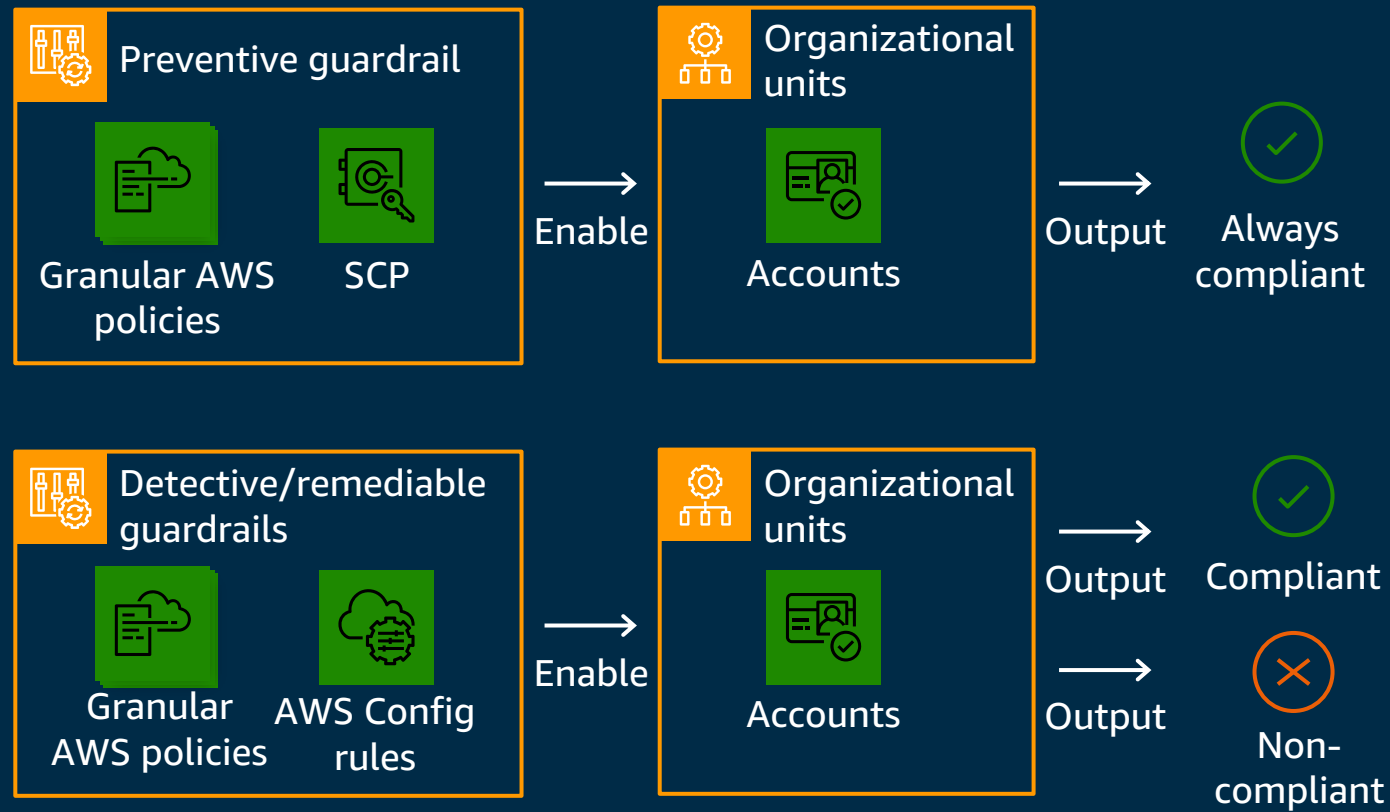
Single pane of glass for monitoring compliance to guardrails

# 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

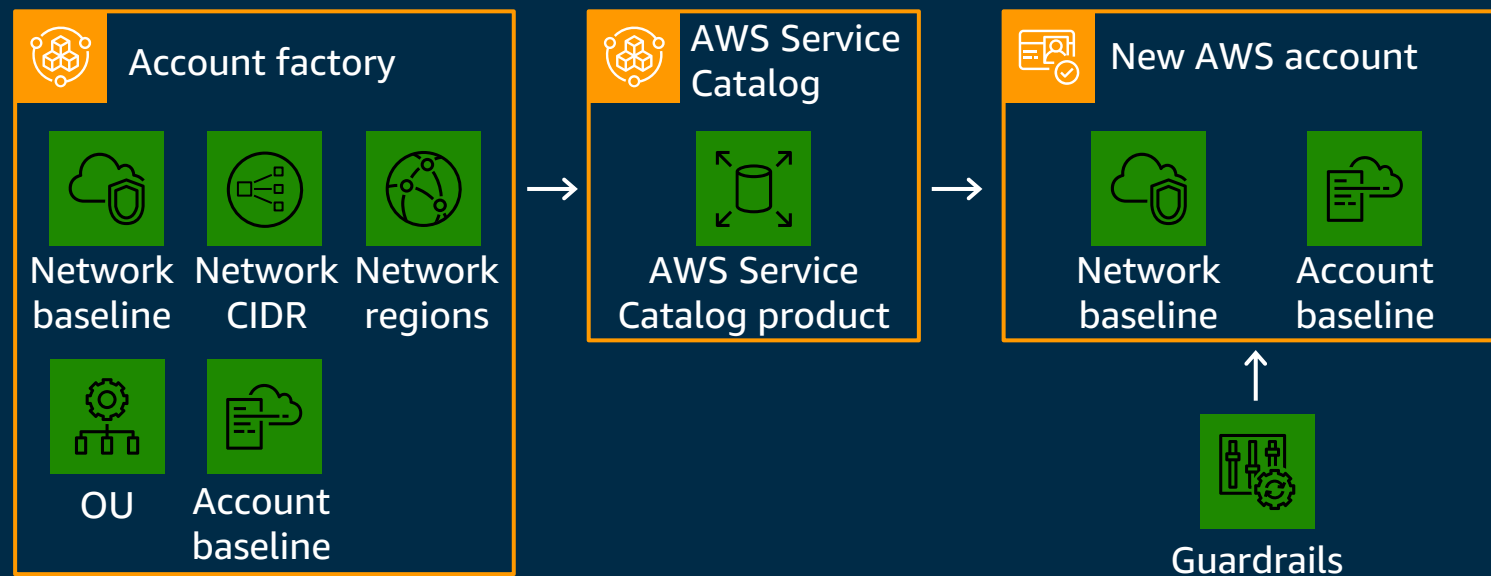


- Guardrails are preconfigured governance rules for security, compliance, and operations
- Expressed in plain English to provide abstraction over granular AWS policies
- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: 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

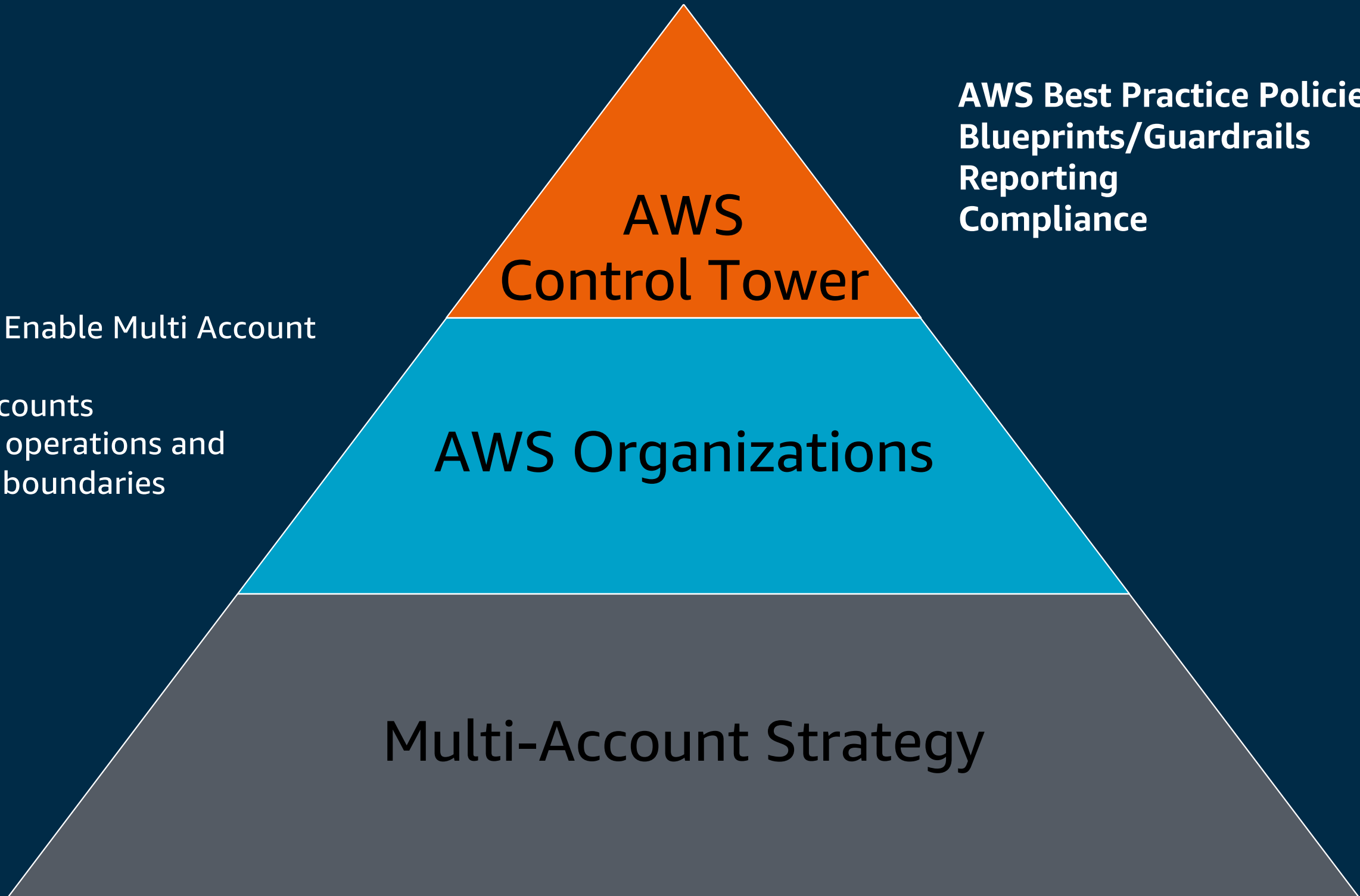
**AWS Best Practice Policies**  
**Blueprints/Guardrails**  
**Reporting**  
**Compliance**

**AWS**  
**Control Tower**

**AWS Organizations**

**Define and Enable Multi Account**  
**Strategy**  
**Manage Accounts**  
**Implement operations and**  
**functional boundaries**

**Multi-Account Strategy**



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



—  
Enable



—  
Provision



—  
Operate



**Business agility + governance control**



# Operate with agility + control

 Operate



# AWS Control Tower capabilities

## Account Management

- Framework for creating and baselining a multi-account environment using AWS Organizations
- Initial multi-account structure including security, audit, & shared service requirements
- An account vending machine that enables automated deployment of additional accounts with a set of managed and monitored security baselines
- A management console that shows compliance status of accounts
- The ability to apply AWS best practice guardrails and Blueprints to accounts at account creation
- The ability to detect and report on any drift/changes that have occurred that deviate from initial configuration options

## Identity & Access Management

- User account access managed through AWS SSO federation
- Integration options with other 3<sup>rd</sup> party SSO providers (PING/OKTA, Azure AD – native support)
- Cross-account roles enable centralized management

## Security & Governance

- Multiple accounts enable separation of duties
- Initial account security and AWS Config rules baseline
- Network baseline

# 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