AWS RESEARCH ROADSHOW – 4 APRIL 2023

Introduction to AWS Account Management Services

AWS Education & Research Team

Nikiforos Botis - nbotis@amazon.com

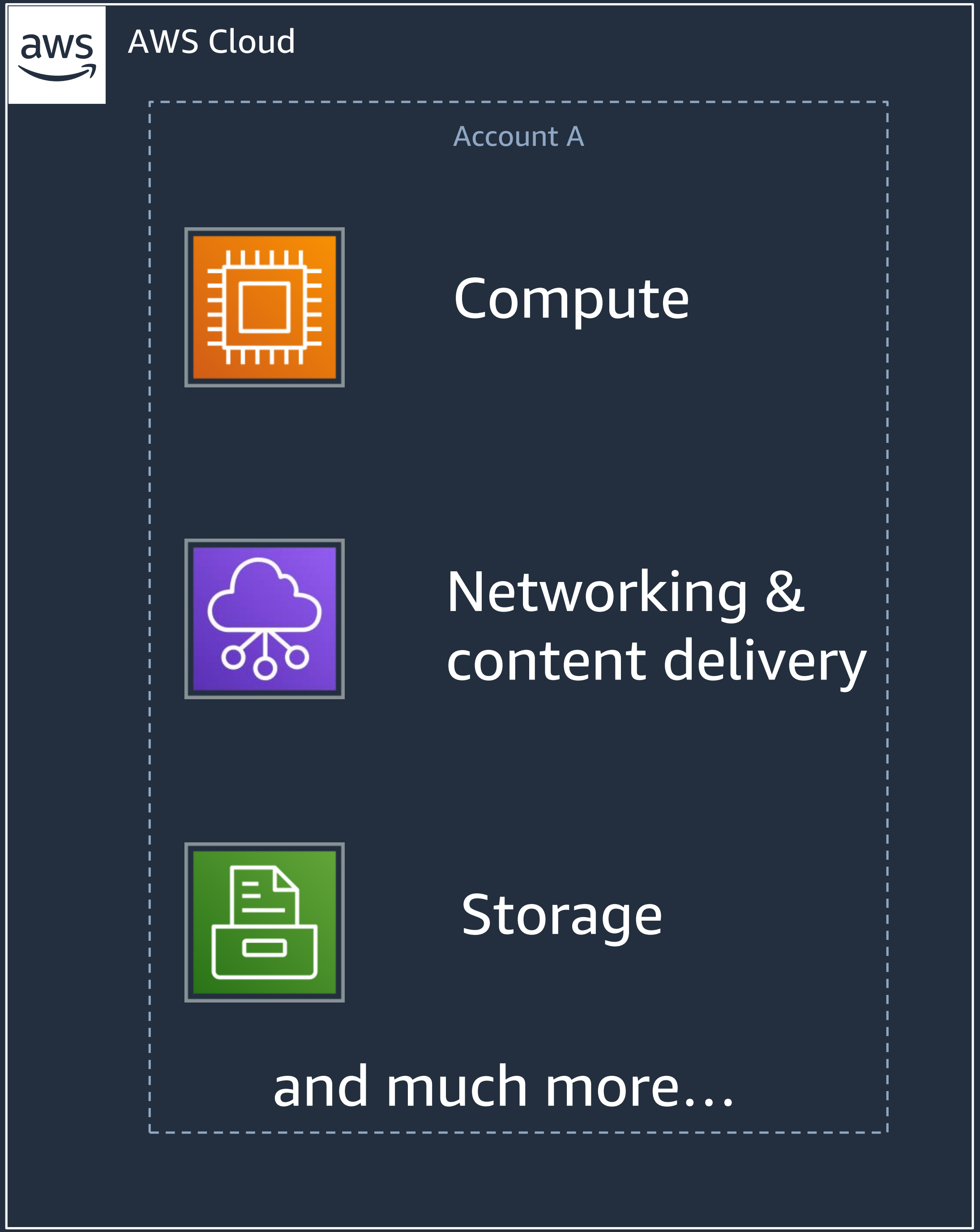
1. Why Multiple AWS Accounts?

What is an AWS Account?

Each AWS Account:

- Is a resource container for AWS services
- Is an explicit security boundary
- Is a container for cost tracking and billing
- Is a mechanism to enforce limits and thresholds
  - e.g. Service Quotas and API thresholds

- Over time, customers will add more accounts to support more applications and services


AWS Cloud

Account A

Compute

Networking & content delivery

Storage

and much more…

How about separating resources with IAM or VPC within a single account?

AWS Account

Everything

Gray boundaries

Hard to manage and track the resources

Ambiguous responsibilities between teams

Scaling to a multi-account model

Many teams

Rapid innovation with resources provisioned quickly and exclusively for each team

Billing

Simplify billing where resources used within an AWS account can be allocated to the business unit that is responsible for that account

Business process

Organize AWS accounts to reflect business processes with different operational, regulatory, and budgetary requirements

Isolation & security

Tight security boundaries enforced by built-in isolation between accounts, and consolidation for workloads with similar risk profiles

AWS Organizations
&
AWS Control Tower

2. AWS Organizations

AWS Organizations

AWS Organizations

Central governance and management across AWS accounts
for **a comprehensive multi-account AWS environment**

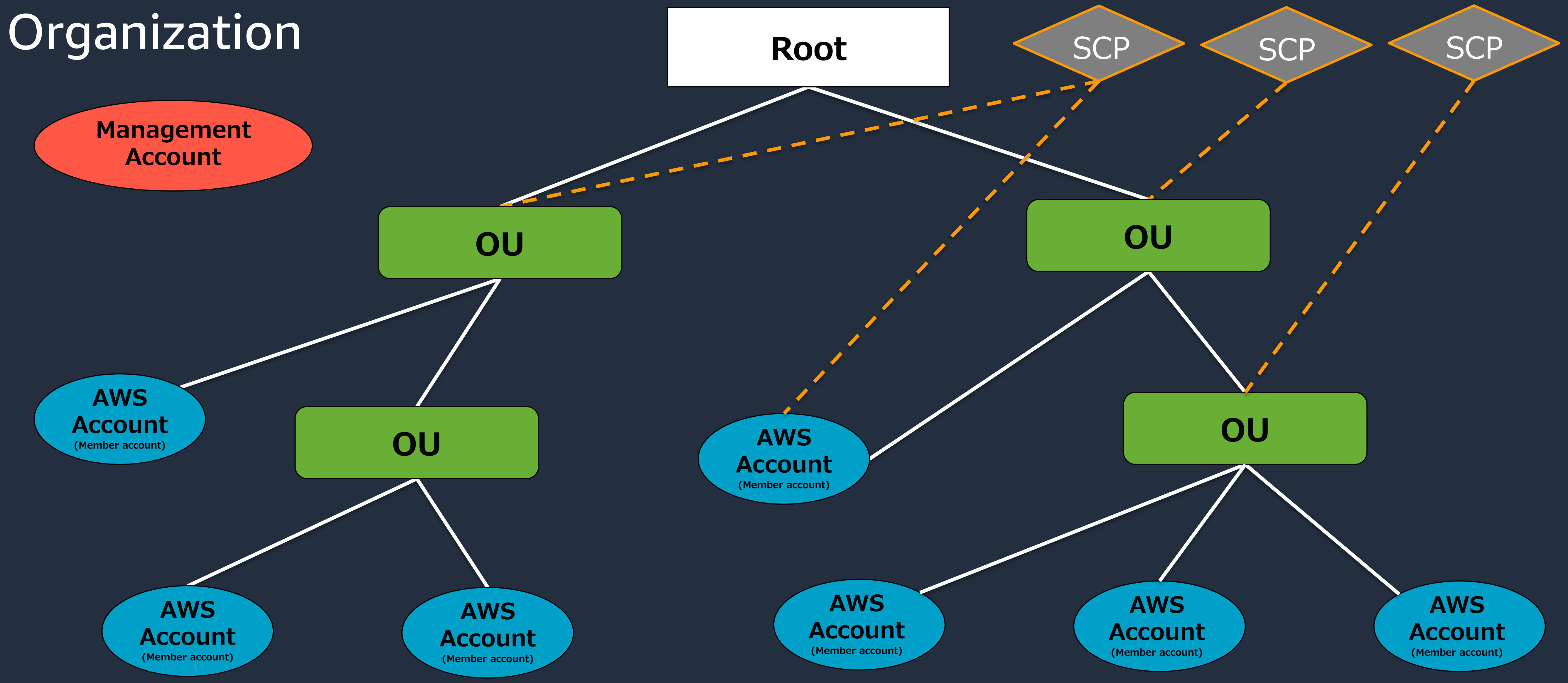
Overview

- Automates the creation and management of AWS accounts
  - ➢ The Organizations console can create accounts
  - ➢ Consolidated billing can be enabled
  - ➢ Combined with AWS SSO to centrally manage identities

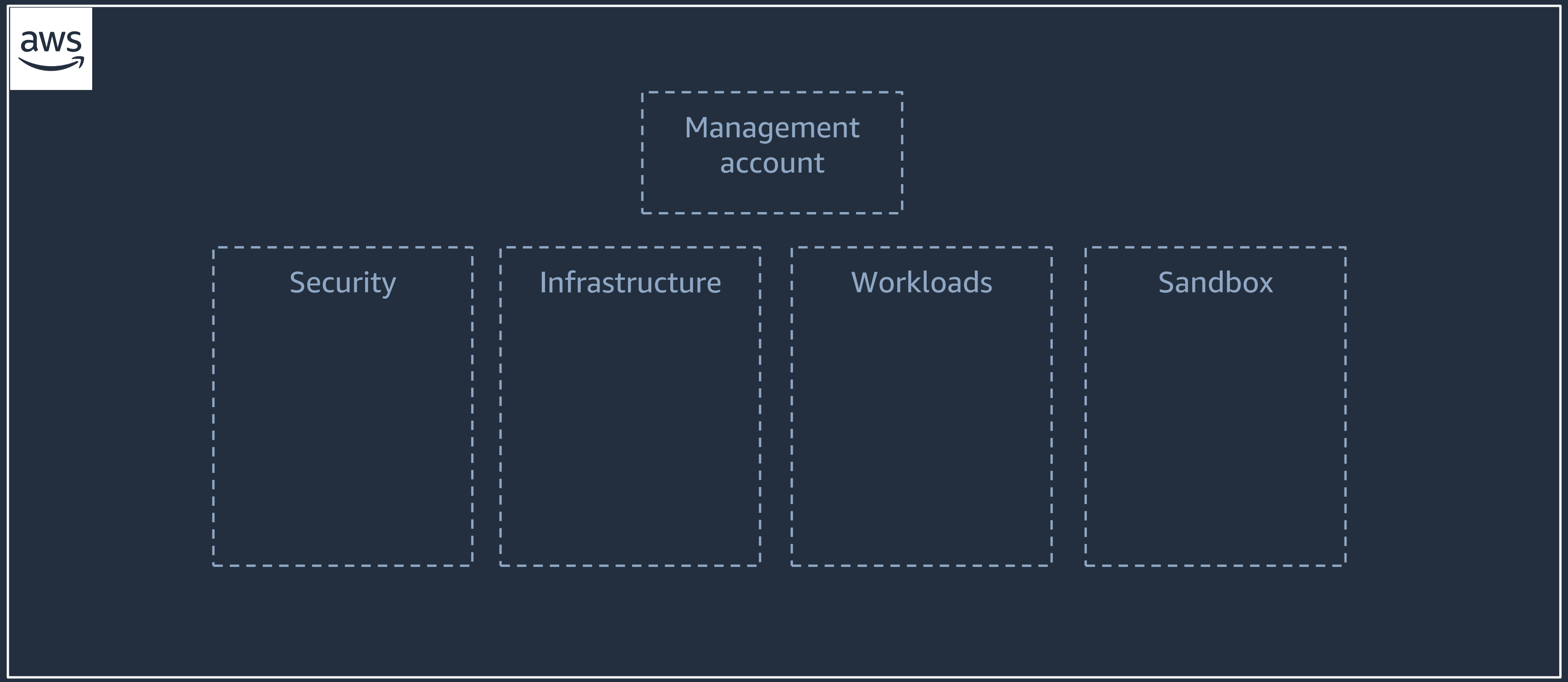
- Can enforce the policies across the AWS accounts for compliance (using Service Control Policies - SCPs)
  - ➢ Manages the access privileges for multiple accounts without custom scripts

- Free of charge

Components of AWS Organizations

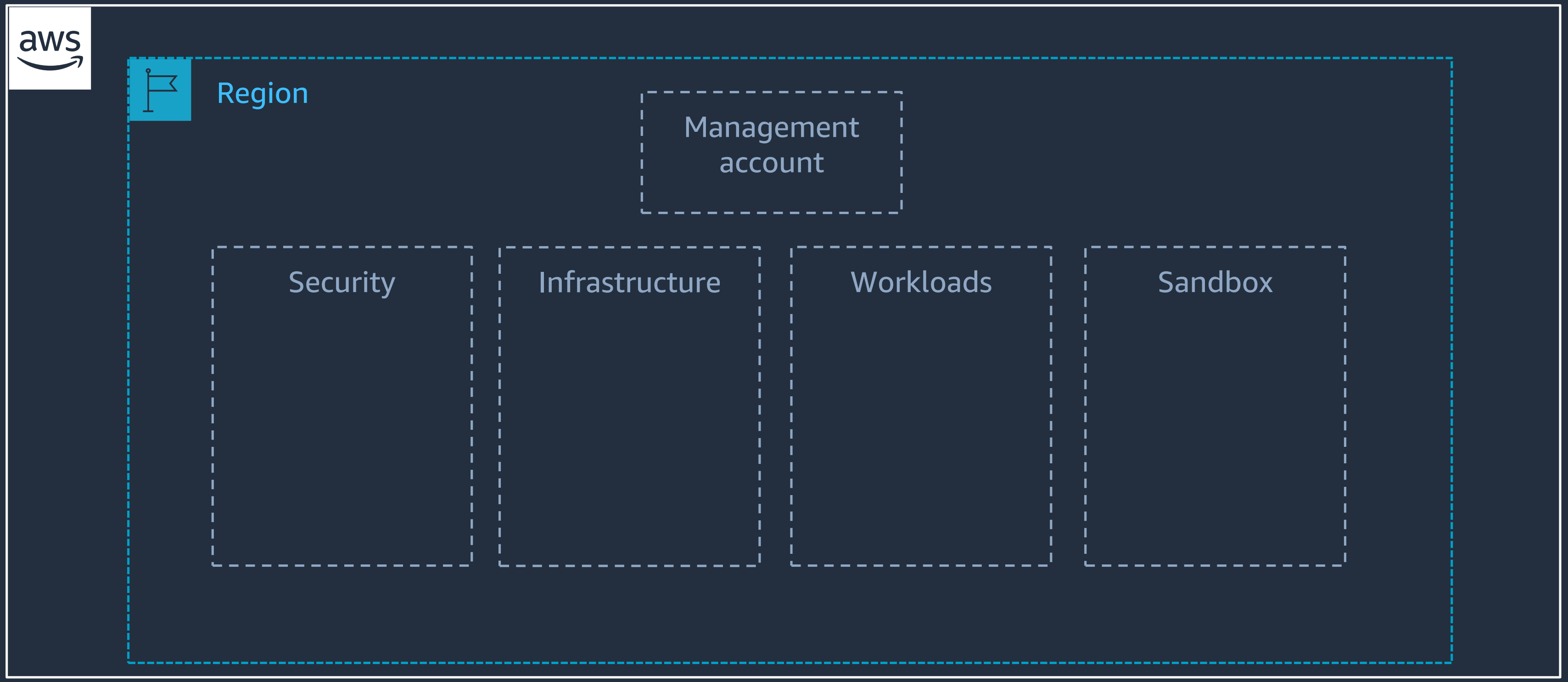

Organization
Root
SCP
SCP
SCP
Management Account
OU
OU
AWS Account (Member account)
OU
AWS Account (Member account)
OU
AWS Account (Member account)
AWS Account (Member account)
AWS Account (Member account)
AWS Account (Member account)
AWS Account (Member account)

Create a new organization



Created a new organization with four OUs

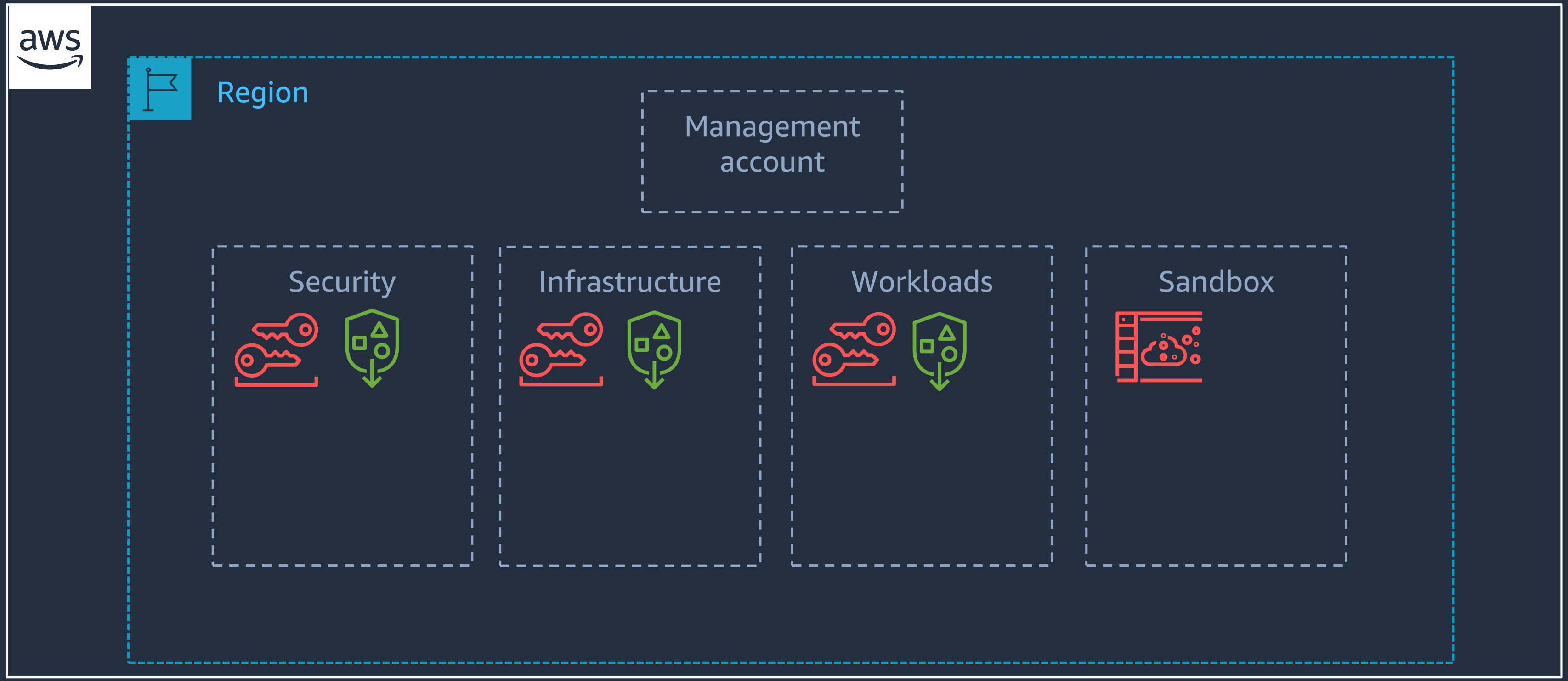
Operate workloads in specific regions



Applied a region-based SCP to the organization

Future instances/workloads can only be deployed in approved regions

Provide access and resources for developers

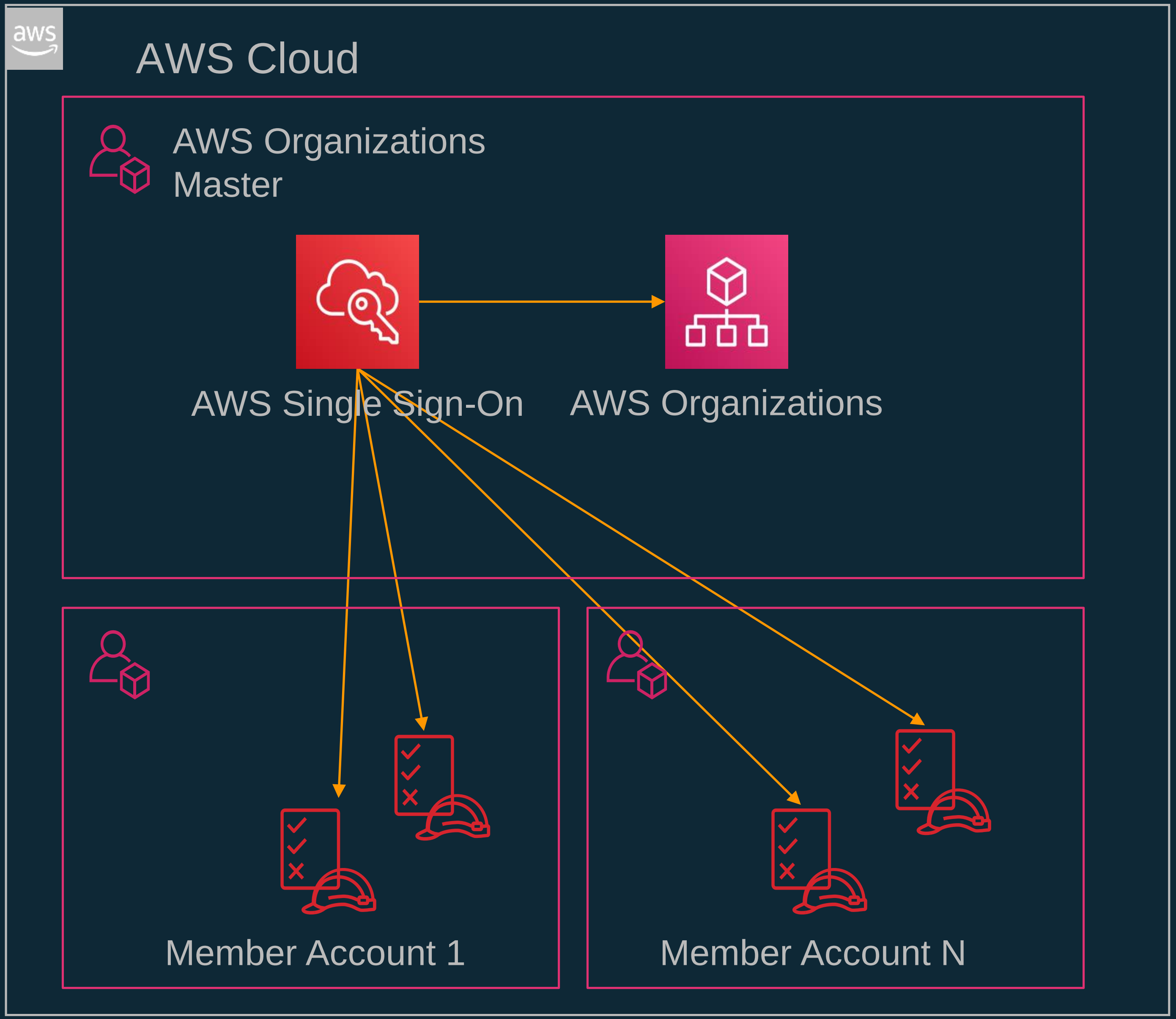


Enabled AWS Single Sign On (SSO) for access
Created a Sandbox OU for test accounts
Used Resource Access Management (RAM) to share subnets across accounts

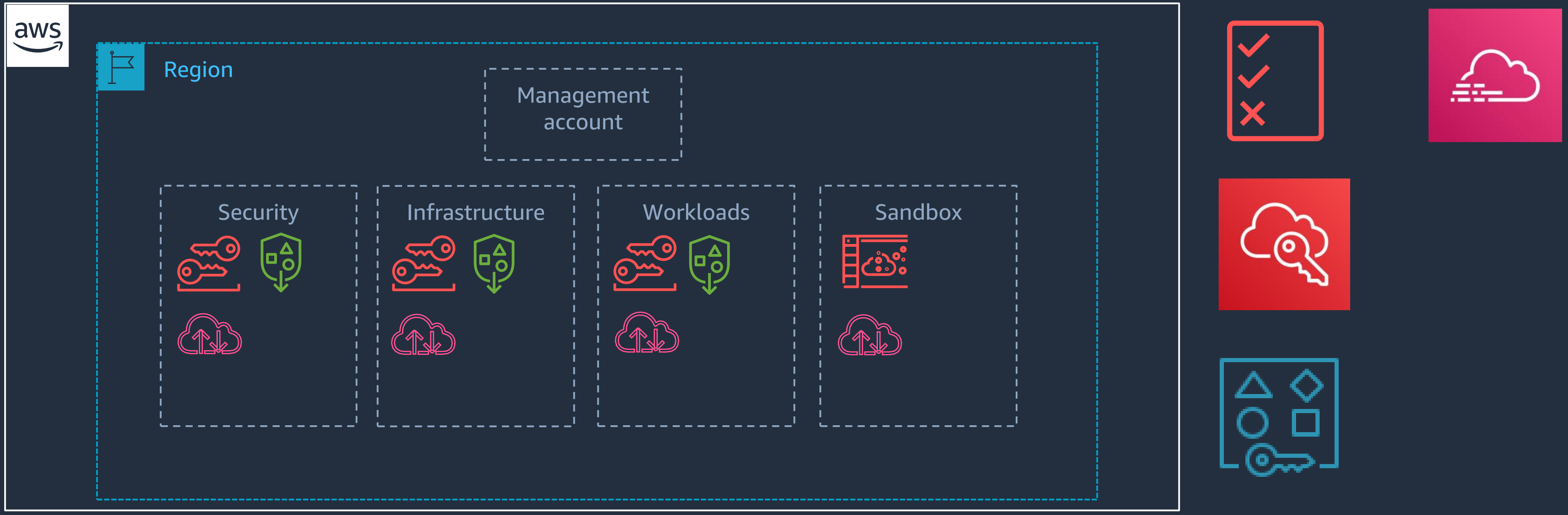
Developers have access to resources and a space to build

Manage account access with AWS Single-Sign-On

- Uses **AWS Organizations** to retrieve your list and **structure of accounts.**
- Define **permissions** using standard syntax and tools.
- Definitions and policies **automatically deployed and maintained** in member accounts.
- Use the AWS SSO internal directory, AWS Managed Microsoft Active Directory, or SAML compliant IdP.



Ensure all actions are logged for auditing



Enabled AWS CloudTrail to create a searchable log of all cloud activity from the organization

Logging (and log activity) cannot be turned off or modified by users

You need 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

3. AWS Control Tower

Overview of AWS Control Tower

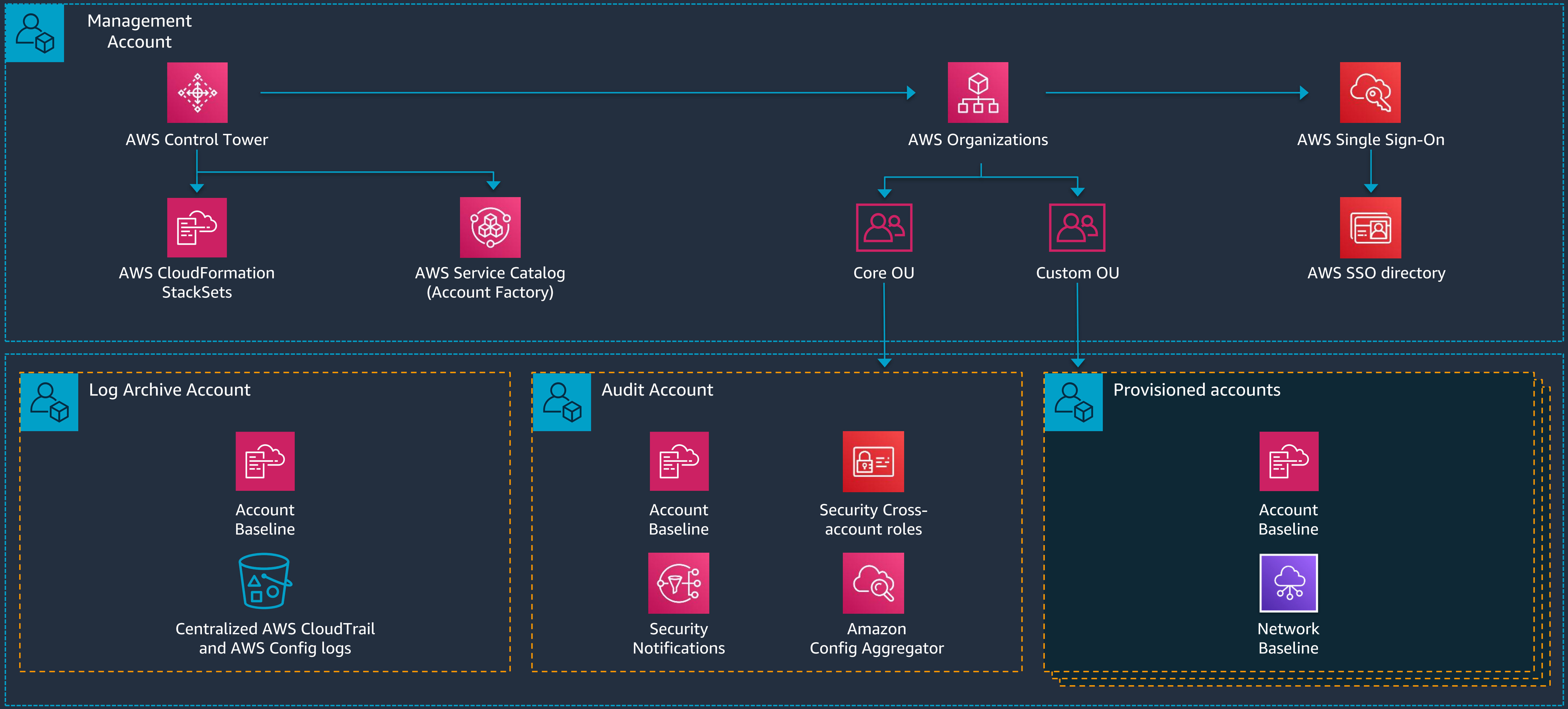
AWS Control Tower

Easily set up and manage a secure multi-account environment

Service overview

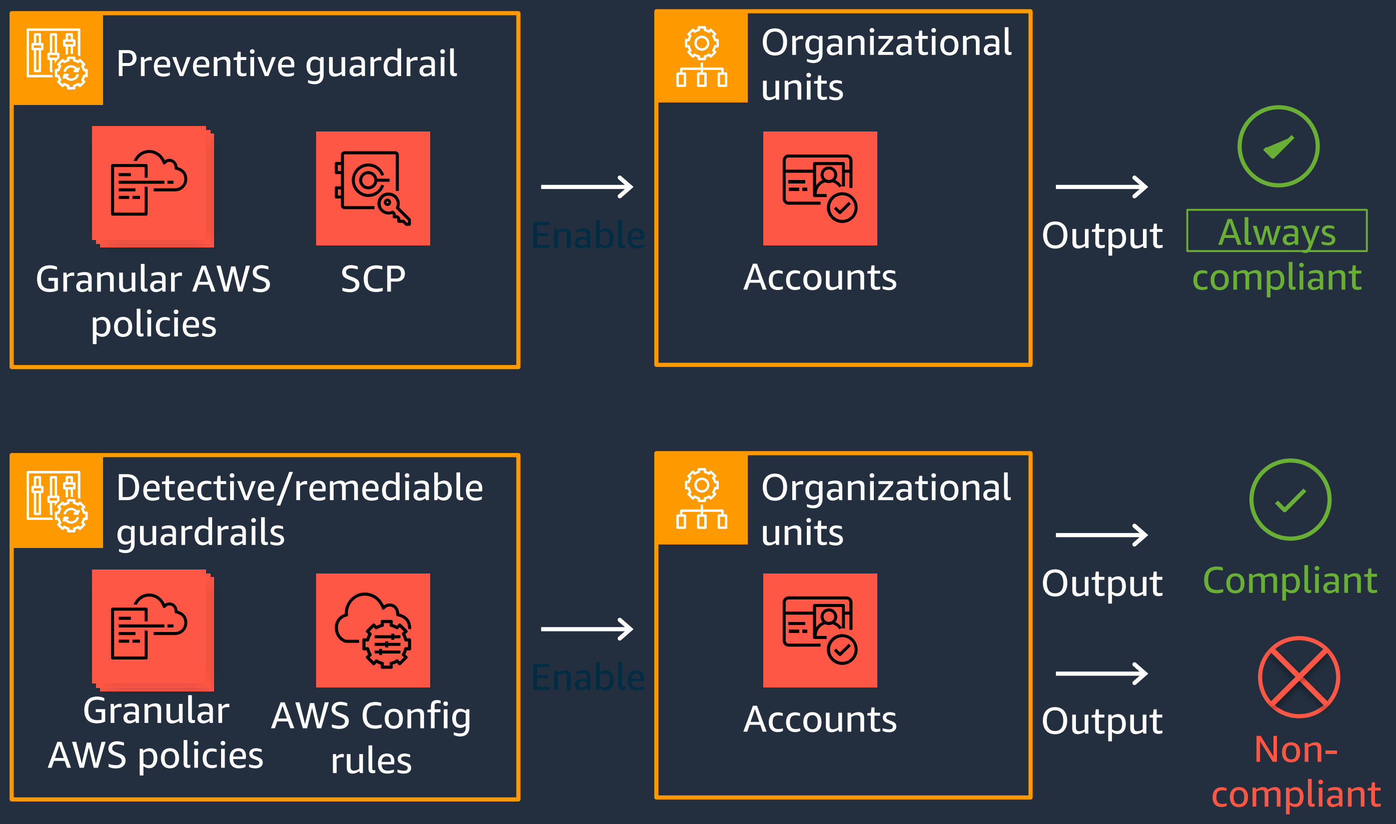
- Build an AWS management foundation based on best practices
  - ➢ Deploy Landing Zone using AWS Organizations, AWS CloudTrail, AWS IAM, etc.
- Install guardrails
  - ➢ Pre-packaged “guardrails” of security, operations, and compliance requests across the enterprise or only to specific accounts
- Free of charge
  (but incurs the cost of each AWS service required to configure the Landing Zone)

Landing Zone provisioned by AWS Control Tower



Establish Guardrails

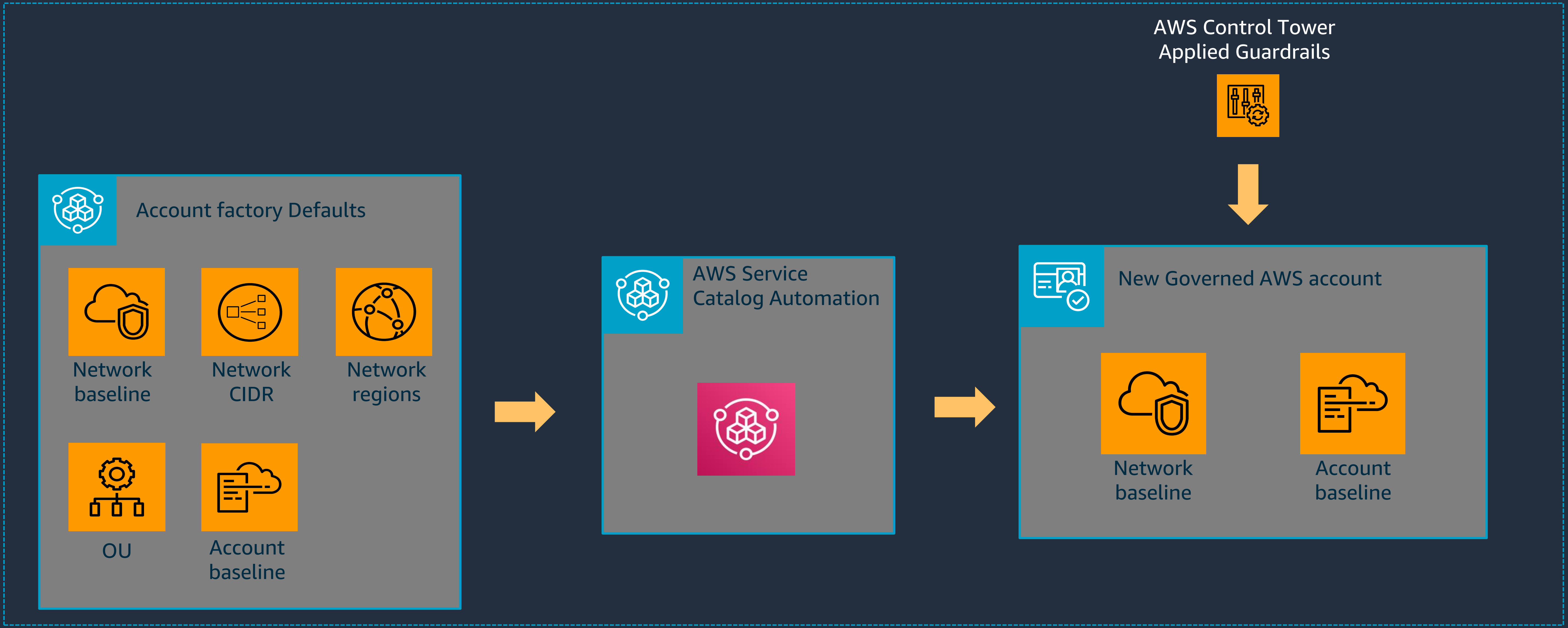
Guardrails are *preconfigured governance rules* for security, compliance, and operations, expressed in *plain English* to provide abstraction over granular AWS policies.



Guardrail Examples

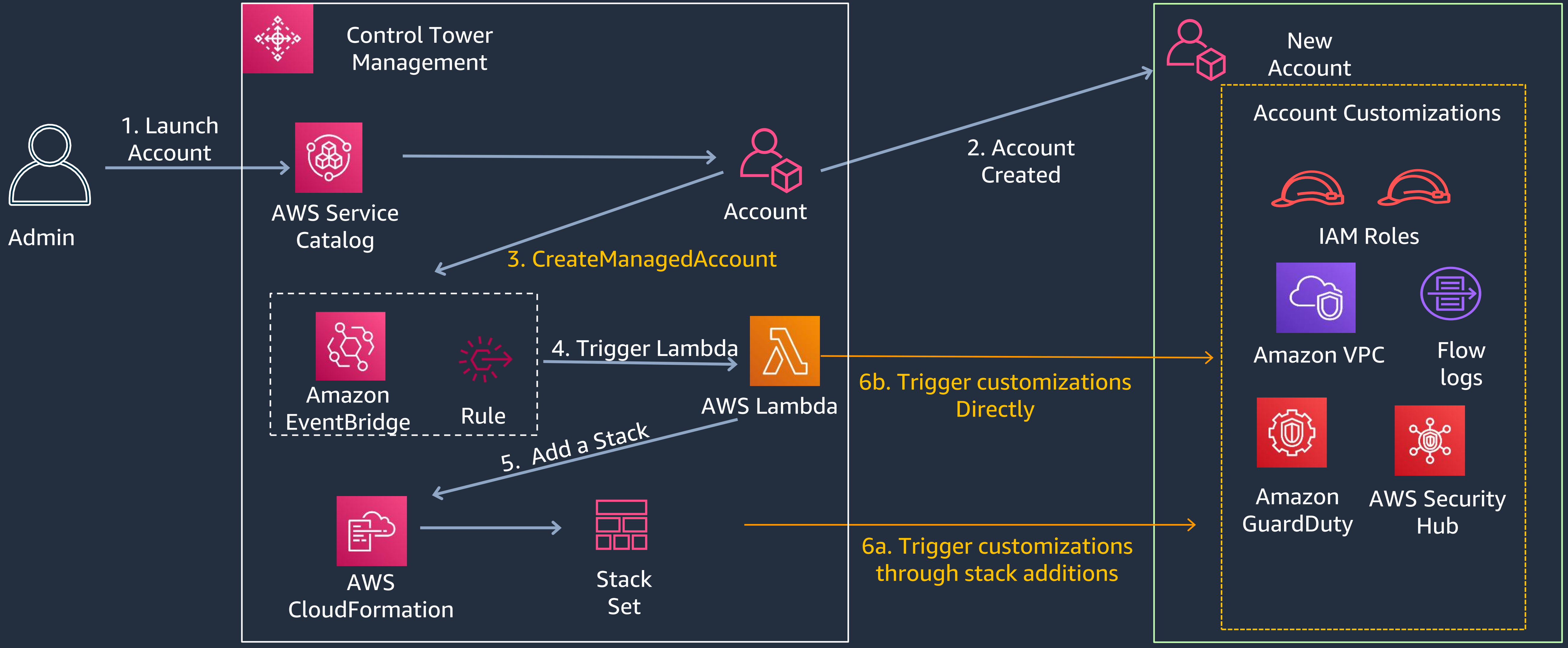
Guardrail	Type	Requirement
Enable MFA for the Root User	Detective	Strongly Recommended
Disallow public read access to S3	Detective	Strongly Recommended
Enable AWS Config in All Available Regions	Preventive	Mandatory
Disallow Policy Changes to Log Archive	Preventive	Mandatory
Integrate CloudTrail Events with CloudWatch Logs	Preventive	Mandatory
Disallow Amazon S3 Buckets That Are Not Versioning Enabled	Detective	Elective
Disallow Delete Actions on Amazon S3 Buckets Without MFA	Detective	Elective

Automate Compliant Account Provisioning



Configure/Trigger Customizations with LifeCycle Events

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



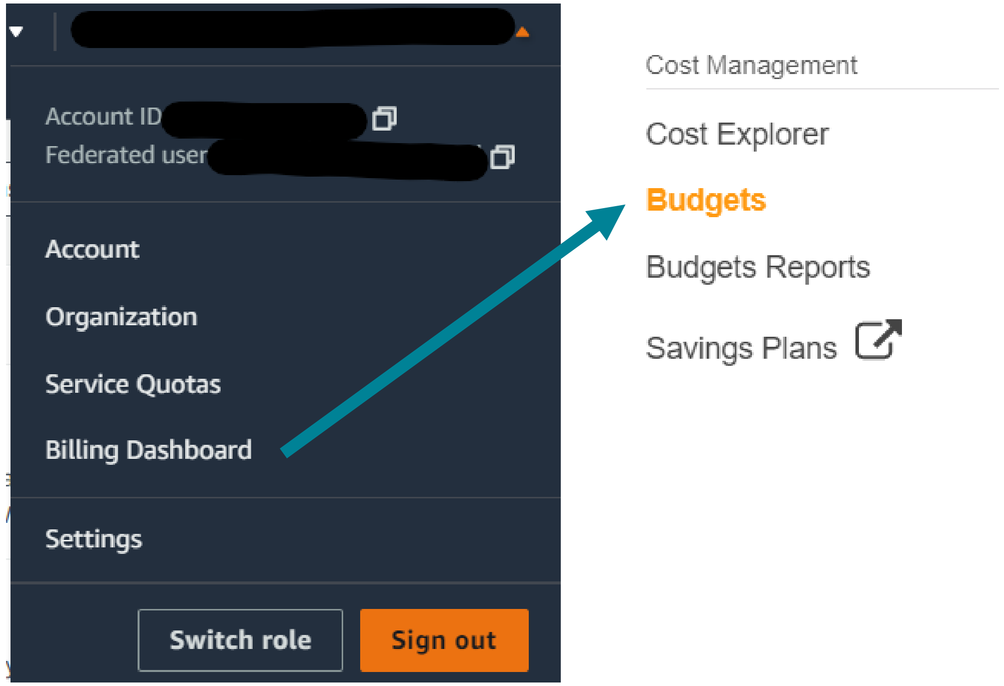
Summary of key features

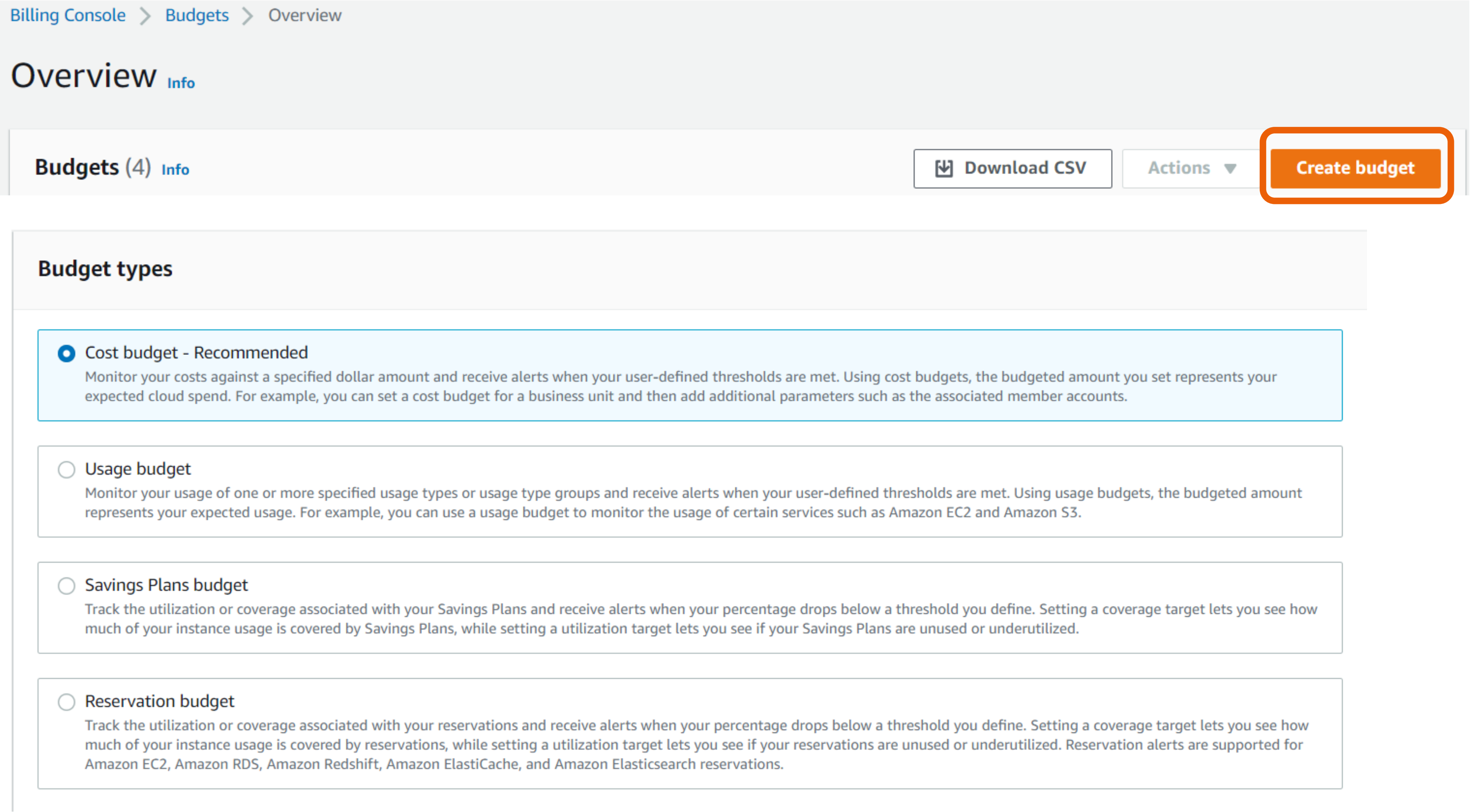
- Automated landing zone with best practice blueprints
- Guardrails for policy management
- Account factory for account provisioning
- Dashboard for visibility and actions
- Built-in identity and access management
- Preconfigured log archive and audit access to accounts
- Built-in monitoring and notifications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

AWS Budgets

AWS Budgets

AWS Budgets enable you to plan your service usage, service costs, your Reserved Instance utilization and coverage.





Overview Info

Budgets (4) Info

Budget types

● Cost budget - Recommended
Monitor your costs against a specified dollar amount and receive alerts when your user-defined thresholds are met. Using cost budgets, the budgeted amount you set represents your expected cloud spend. For example, you can set a cost budget for a business unit and then add additional parameters such as the associated member accounts.

○ Usage budget
Monitor your usage of one or more specified usage types or usage type groups and receive alerts when your user-defined thresholds are met. Using usage budgets, the budgeted amount represents your expected usage. For example, you can use a usage budget to monitor the usage of certain services such as Amazon EC2 and Amazon S3.

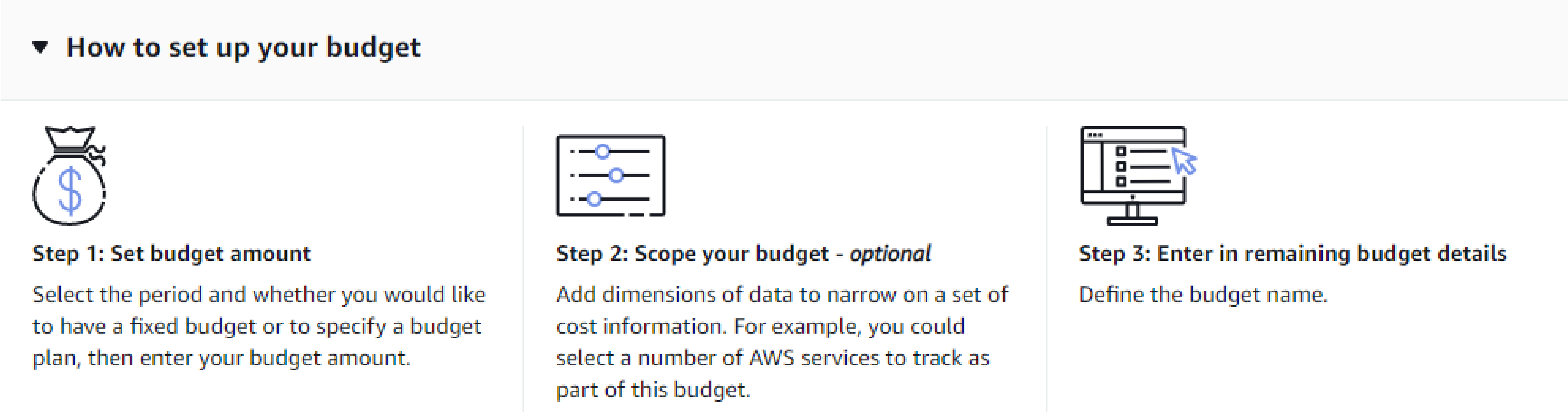
○ Savings Plans budget
Track the utilization or coverage associated with your Savings Plans and receive alerts when your percentage drops below a threshold you define. Setting a coverage target lets you see how much of your instance usage is covered by Savings Plans, while setting a utilization target lets you see if your Savings Plans are unused or underutilized.

○ Reservation budget
Track the utilization or coverage associated with your reservations and receive alerts when your percentage drops below a threshold you define. Setting a coverage target lets you see how much of your instance usage is covered by reservations, while setting a utilization target lets you see if your reservations are unused or underutilized. Reservation alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

Budgets can be created and tracked from the AWS Budgets dashboard or via the Budgets API.

AWS Budgets - Cost

Cost budgets allow you to say how much you want to spend on a service.



▼ **How to set up your budget**

Step 1: Set budget amount

Select the period and whether you would like to have a fixed budget or to specify a budget plan, then enter your budget amount.

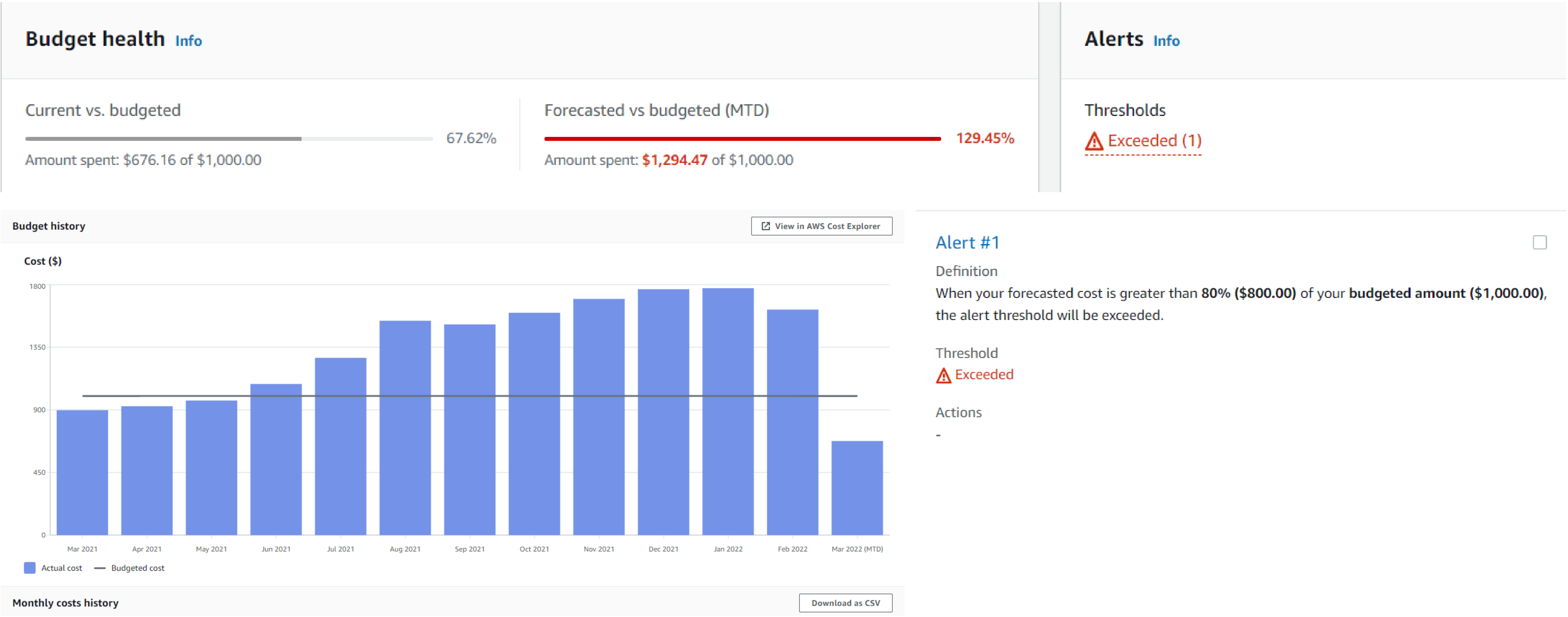
Step 2: Scope your budget - ***optional***

Add dimensions of data to narrow on a set of cost information. For example, you could select a number of AWS services to track as part of this budget.

Step 3: Enter in remaining budget details

Define the budget name.

AWS Budgets – Budget details



Budget health Info

Current vs. budgeted

67.62%

Amount spent: $676.16 of $1,000.00

Forecasted vs budgeted (MTD)

129.45%

Amount spent: **$1,294.47** of $1,000.00

Alerts Info

Thresholds

⚠ Exceeded (1)

Budget history

Alert #1 □

Definition

When your forecasted cost is greater than **80% ($800.00)** of your **budgeted amount ($1,000.00)**, the alert threshold will be exceeded.

Threshold

⚠ Exceeded

Actions

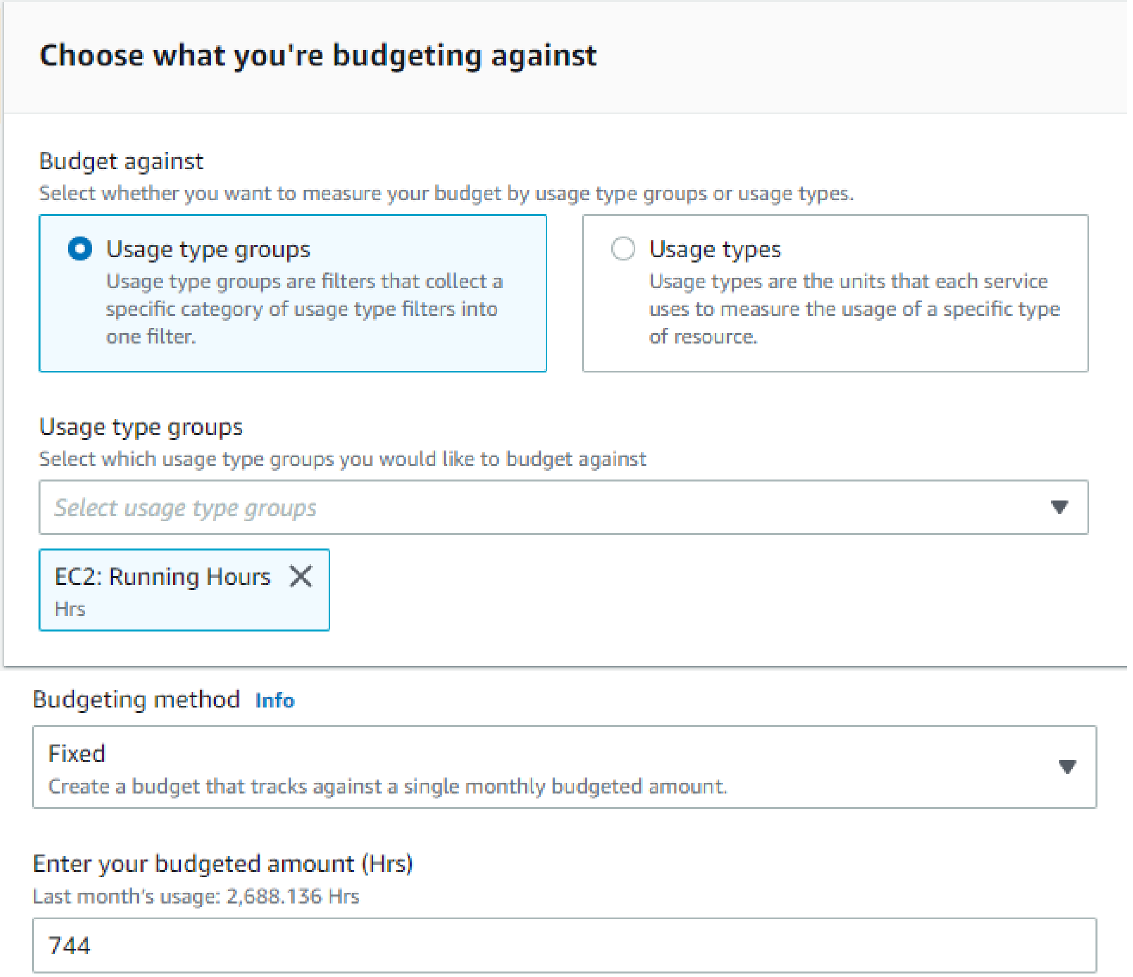
-

Monthly costs history

AWS Budgets - Usage

Usage budgets allow you to say how many hours, which amount of storage (or amount of other usage units) you want to use within one or more services.

1



Choose what you're budgeting against

Budget against

Select whether you want to measure your budget by usage type groups or usage types.

● Usage type groups
Usage type groups are filters that collect a specific category of usage type filters into one filter.

○ Usage types
Usage types are the units that each service uses to measure the usage of a specific type of resource.

Usage type groups

Select which usage type groups you would like to budget against

Select usage type groups ▼

EC2: Running Hours ✕
Hrs

Budgeting method Info

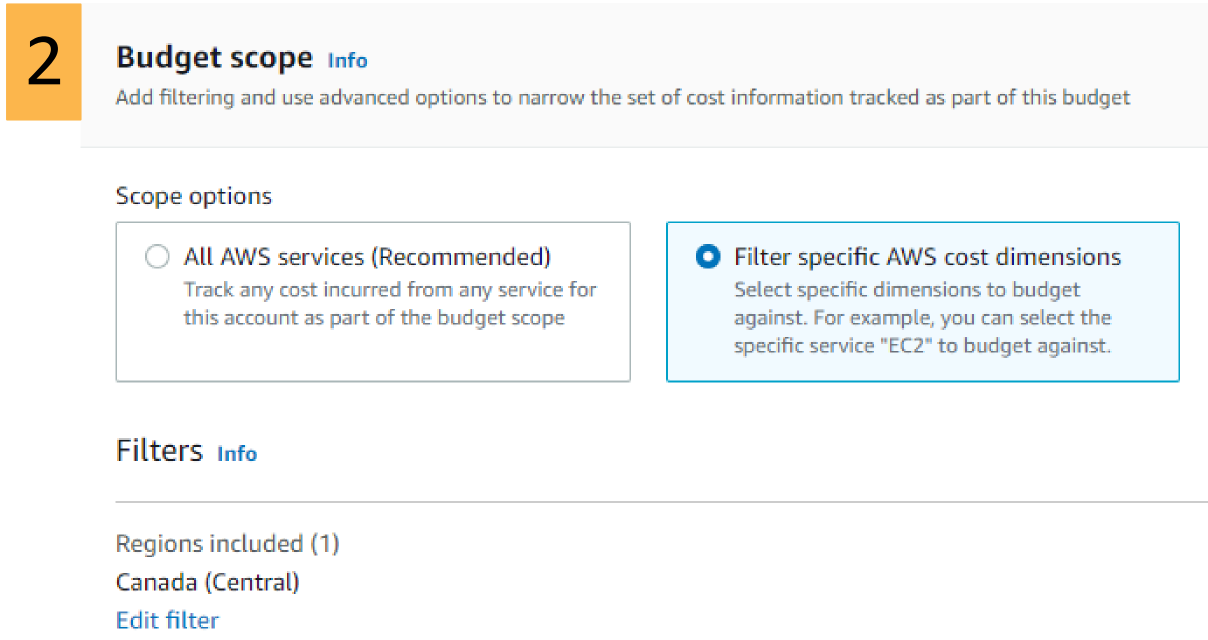
Fixed
Create a budget that tracks against a single monthly budgeted amount.

Enter your budgeted amount (Hrs)

Last month's usage: 2,688.136 Hrs

744

2



Budget scope Info

Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget

Scope options

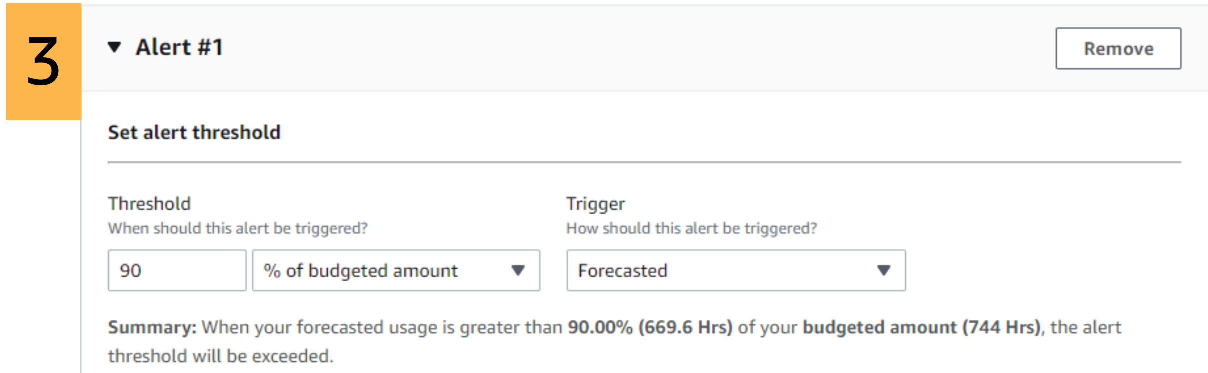
○ All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope

● Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.

Filters Info

Regions included (1)
Canada (Central)
Edit filter

3



▼ **Alert #1** Remove

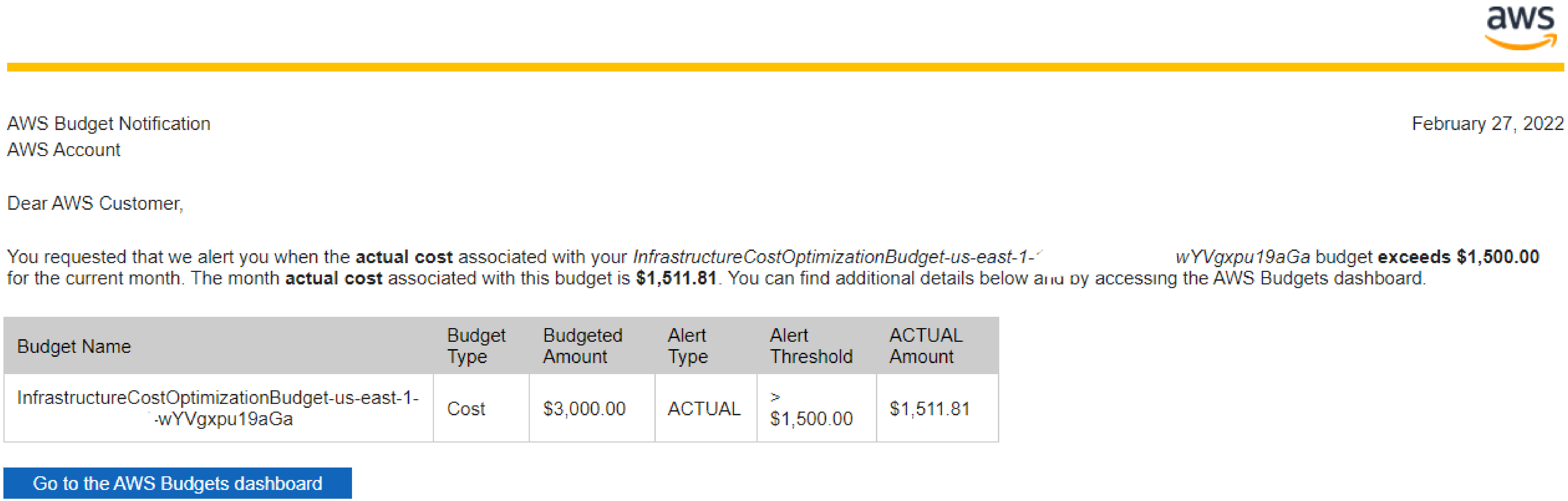
Set alert threshold

Threshold
When should this alert be triggered?
90 | % of budgeted amount ▼

Trigger
How should this alert be triggered?
Forecasted ▼

Summary: When your forecasted usage is greater than **90.00% (669.6 Hrs)** of your **budgeted amount (744 Hrs)**, the alert threshold will be exceeded.

AWS Budgets – notification email sample



AWS Budget Notification
AWS Account

February 27, 2022

Dear AWS Customer,

You requested that we alert you when the **actual cost** associated with your *InfrastructureCostOptimizationBudget-us-east-1-*[redacted]*wYVgxpu19aGa* budget **exceeds $1,500.00** for the current month. The month **actual cost** associated with this budget is **$1,511.81**. You can find additional details below and by accessing the AWS Budgets dashboard.

Budget Name	Budget Type	Budgeted Amount	Alert Type	Alert Threshold	ACTUAL Amount
InfrastructureCostOptimizationBudget-us-east-1-[redacted]-wYVgxpu19aGa	Cost	$3,000.00	ACTUAL	> $1,500.00	$1,511.81

Billing and Budgets Permissions

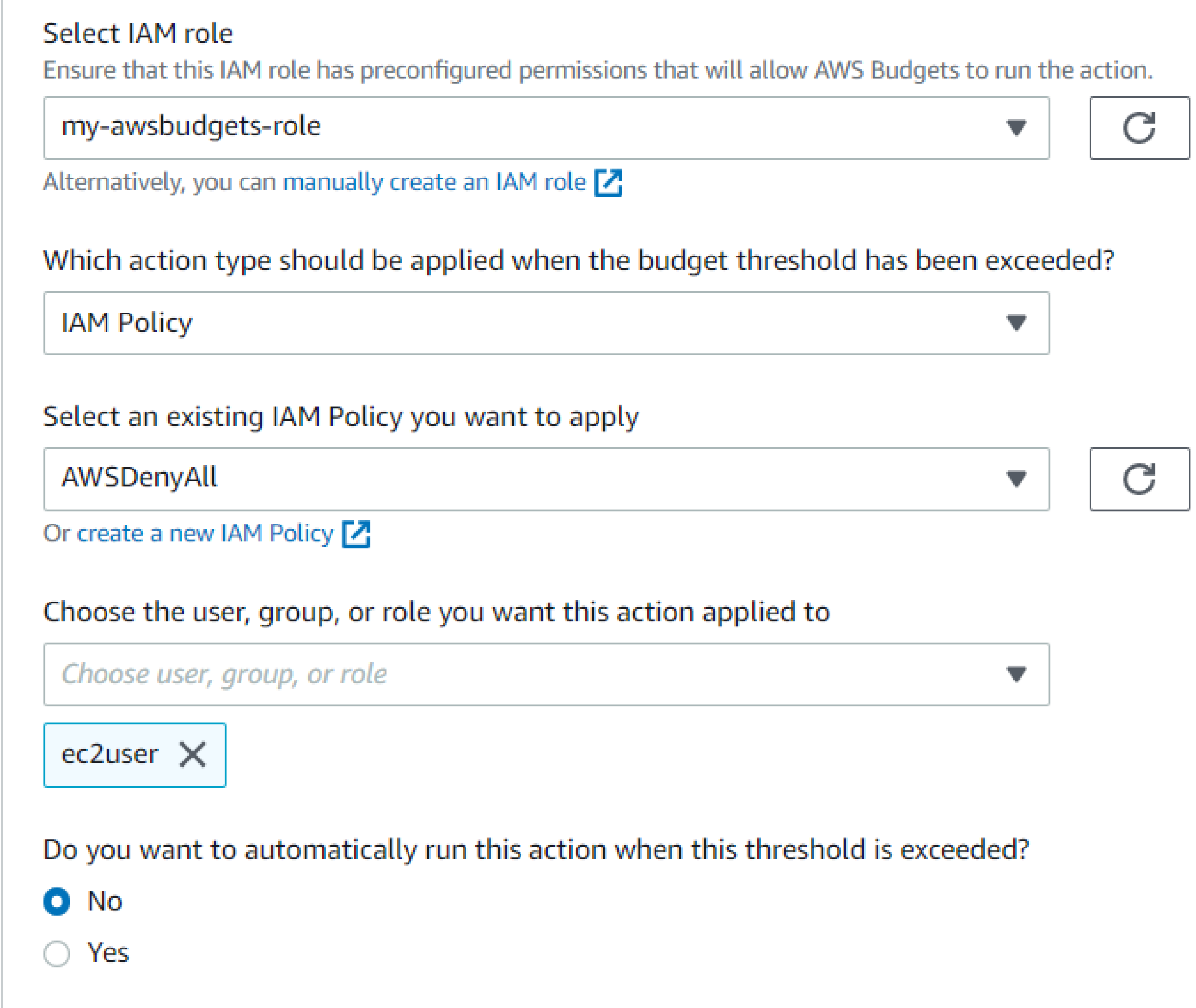
IAM users must be allowed to perform actions in Billing and Cost Management.

aws-portal:ViewBilling	Allow or deny IAM users permission to view the Billing and Cost Management console pages.
aws-portal:ModifyBilling	Allow or deny IAM users permission to modify the Billing and Cost Management console pages.
budgets:ViewBudget	Allow or deny IAM users permission to view Budgets. To allow IAM users to view budgets, you must also allow ViewBilling.
Budgets:ModifyBudget	Allow or deny IAM users permission to modify Budgets. To allow IAM users to view and modify budgets, you must also allow ViewBilling and ModifyBilling.

For more information regarding relevant IAM permissions, see our documentation: IAM permissions

AWS Budgets – Budget actions

The AWS Budgets dashboard is your hub for creating, tracking, and inspecting your budgets.



Select IAM role

Ensure that this IAM role has preconfigured permissions that will allow AWS Budgets to run the action.

my-awsbudgets-role ▼

Alternatively, you can manually create an IAM role

Which action type should be applied when the budget threshold has been exceeded?

IAM Policy ▼

Select an existing IAM Policy you want to apply

AWSDenyAll ▼

Or create a new IAM Policy

Choose the user, group, or role you want this action applied to

Choose user, group, or role ▼

ec2user ✕

Do you want to automatically run this action when this threshold is exceeded?

● No

○ Yes

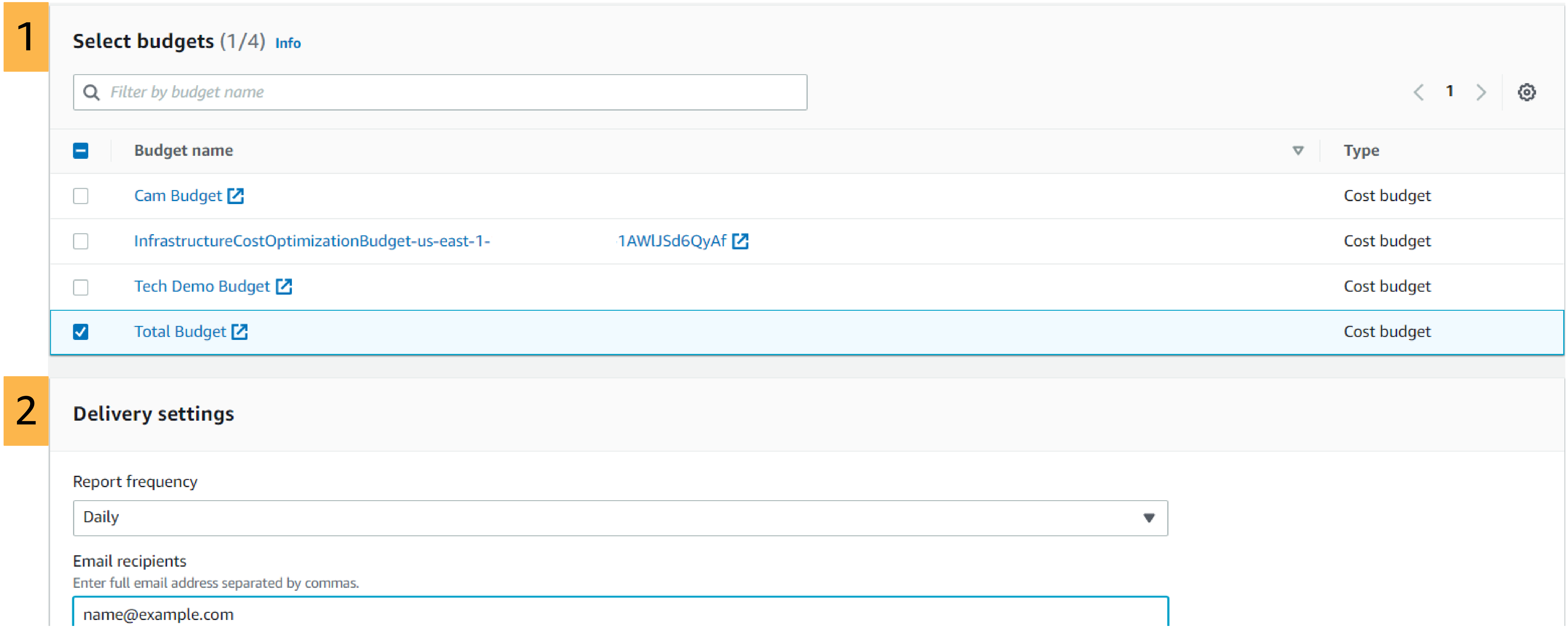
3 actions types:

- Identity and Access Management (IAM) policies
- Service Control Policies (SCPs)
- Target running instances (EC2 or RDS)

Note: Budget actions that are focused on applying policies (IAM or SCP) will be reset at the beginning of each budget period (e.g., October to November) while actions that are focused on targeting specific resources will not reset at the next budget period.

AWS Budgets – Budget Reports

Budget Reports group relevant budgets together and deliver updates regularly via email.



1

Select budgets (1/4) Info

Filter by budget name

☐	Budget name	Type
☐	Cam Budget	Cost budget
☐	InfrastructureCostOptimizationBudget-us-east-1- 1AWlJSd6QyAf	Cost budget
☐	Tech Demo Budget	Cost budget
☑	Total Budget	Cost budget

2

Delivery settings

Report frequency

Daily ▼

Email recipients

Enter full email address separated by commas.

name@example.com

AWS Budgets – Budget Reports

Up to 50 participants

Up to 50 reports

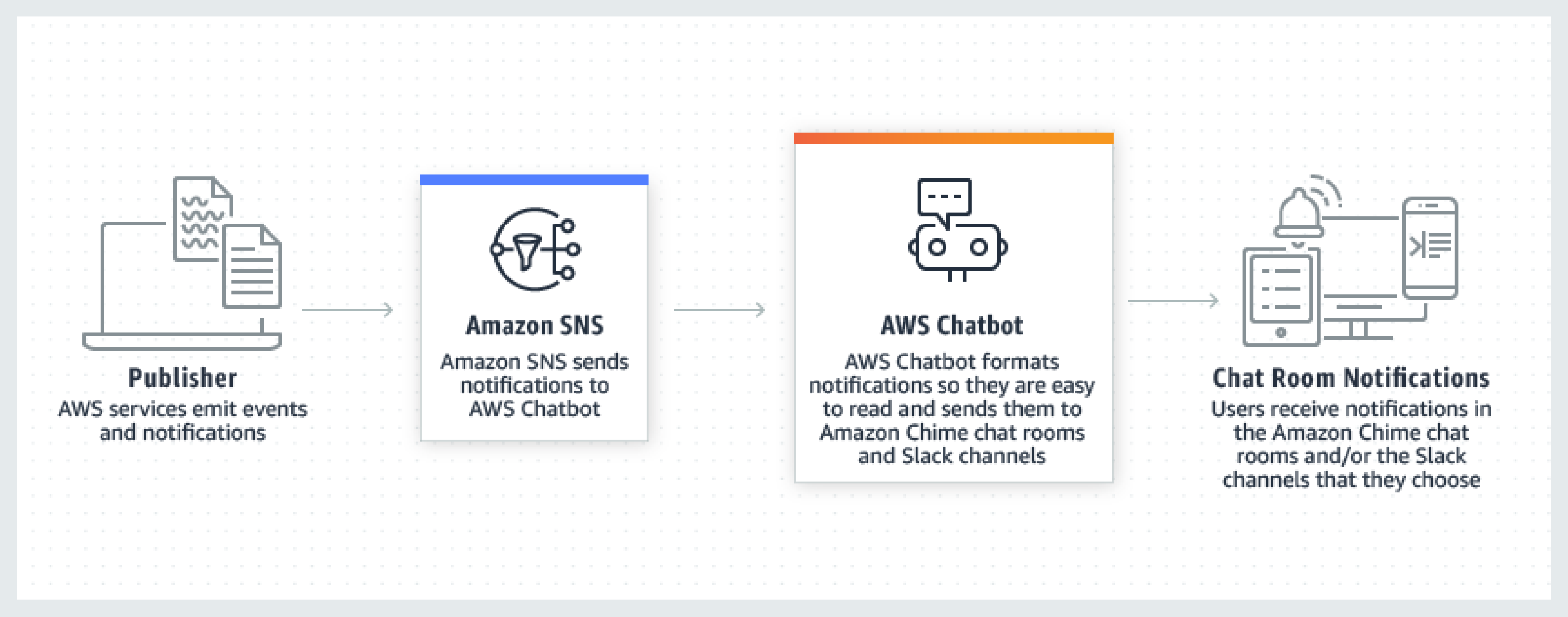
$0.01 USD per report delivered

Daily

Weekly

Monthly

AWS Chatbot ("ChatOps" on AWS)

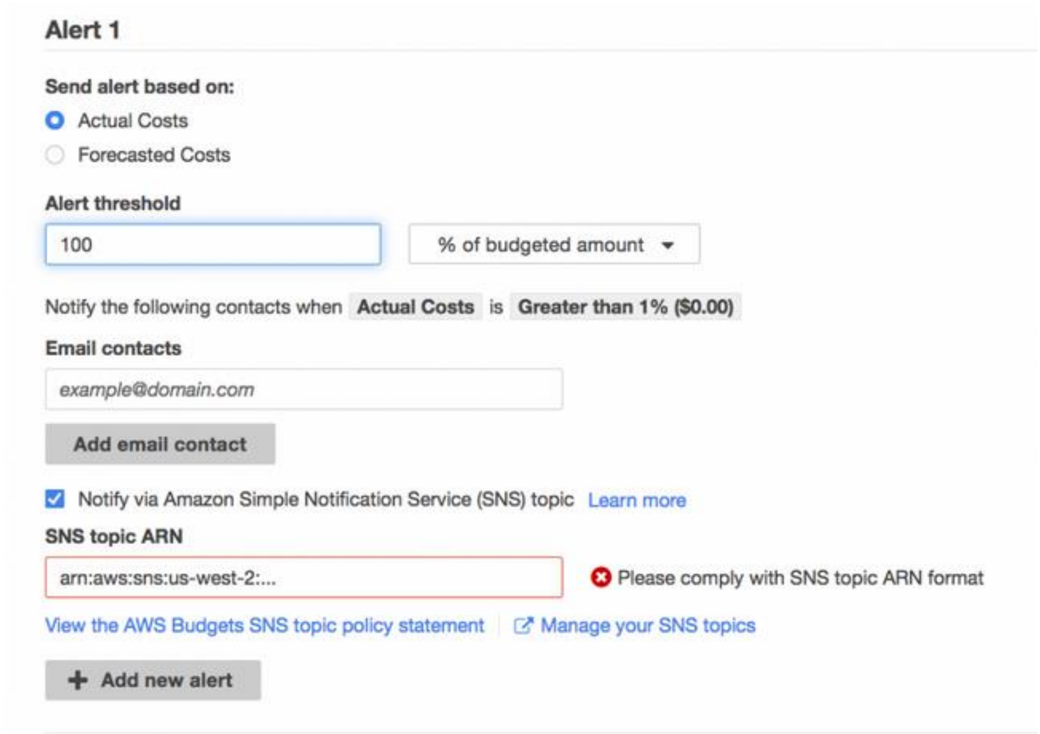

Publisher
AWS services emit events and notifications
Amazon SNS
Amazon SNS sends notifications to AWS Chatbot
AWS Chatbot
AWS Chatbot formats notifications so they are easy to read and sends them to Amazon Chime chat rooms and Slack channels
Chat Room Notifications
Users receive notifications in the Amazon Chime chat rooms and/or the Slack channels that they choose

Benefits:

- Quick setup
- Easily define permissions
- Faster response
- Entire team can see and discuss

AWS Chatbot – Slack

1



Alert 1

Send alert based on:

● Actual Costs

○ Forecasted Costs

Alert threshold

100 | % of budgeted amount ▾

Notify the following contacts when **Actual Costs** is **Greater than 1% ($0.00)**

Email contacts

example@domain.com

Add email contact

☑ Notify via Amazon Simple Notification Service (SNS) topic Learn more

SNS topic ARN

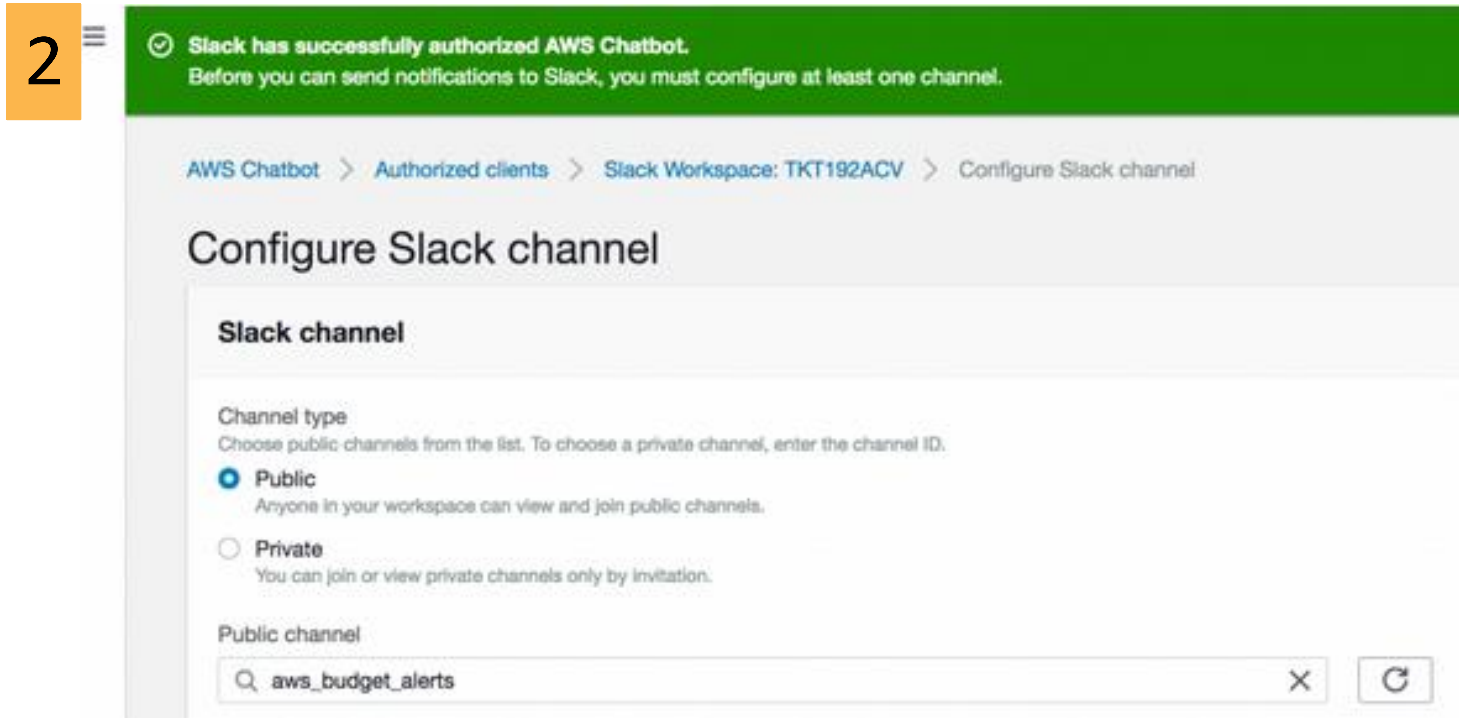
arn:aws:sns:us-west-2:...

Please comply with SNS topic ARN format

View the AWS Budgets SNS topic policy statement | Manage your SNS topics

+ Add new alert

2



Slack has successfully authorized AWS Chatbot.
Before you can send notifications to Slack, you must configure at least one channel.

AWS Chatbot > Authorized clients > Slack Workspace: TKT192ACV > Configure Slack channel

Configure Slack channel

Slack channel

Channel type
Choose public channels from the list. To choose a private channel, enter the channel ID.

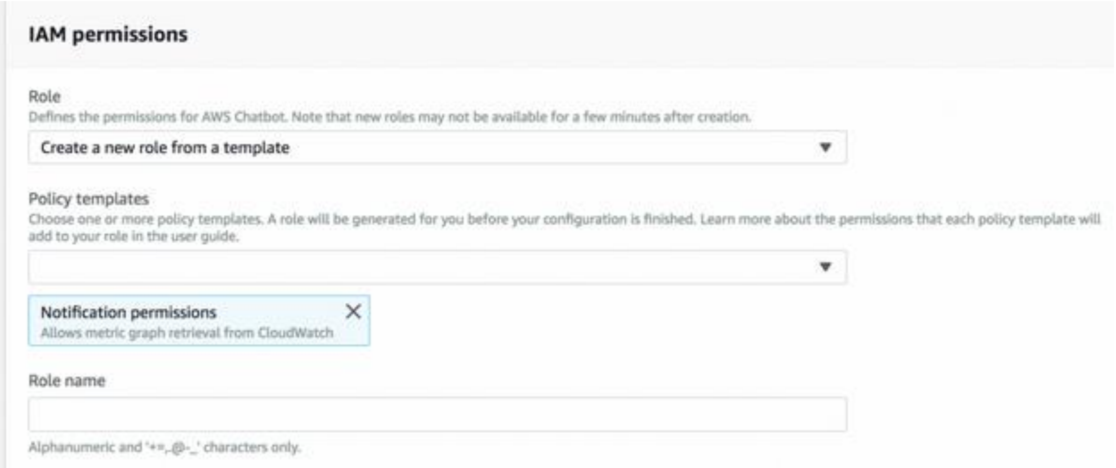
● Public
Anyone in your workspace can view and join public channels.

○ Private
You can join or view private channels only by invitation.

Public channel

aws_budget_alerts

3



IAM permissions

Role
Defines the permissions for AWS Chatbot. Note that new roles may not be available for a few minutes after creation.

Create a new role from a template ▾

Policy templates
Choose one or more policy templates. A role will be generated for you before your configuration is finished. Learn more about the permissions that each policy template will add to your role in the user guide.

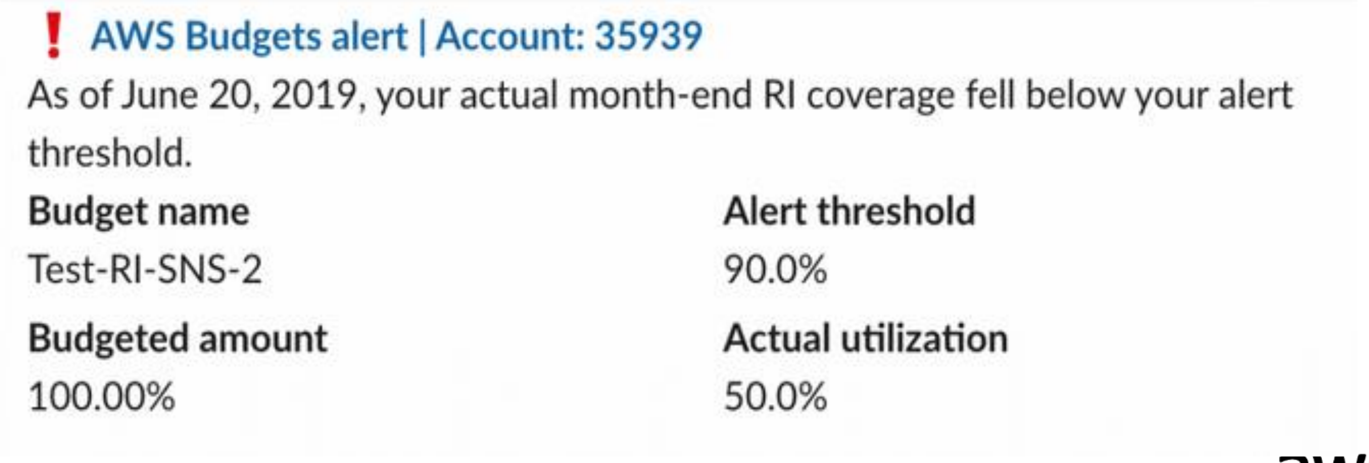
▾

Notification permissions
Allows metric graph retrieval from CloudWatch

Role name

Alphanumeric and '+=,.@-_' characters only.

4



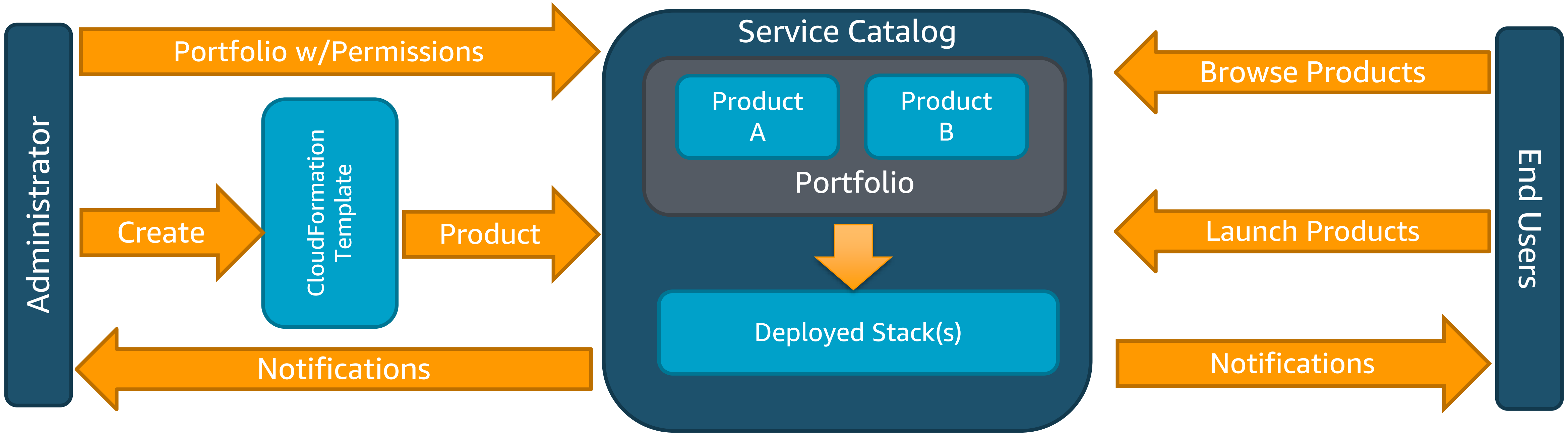
! AWS Budgets alert | Account: 35939

As of June 20, 2019, your actual month-end RI coverage fell below your alert threshold.

Budget name	**Alert threshold**
Test-RI-SNS-2	90.0%
Budgeted amount	**Actual utilization**
100.00%	50.0%

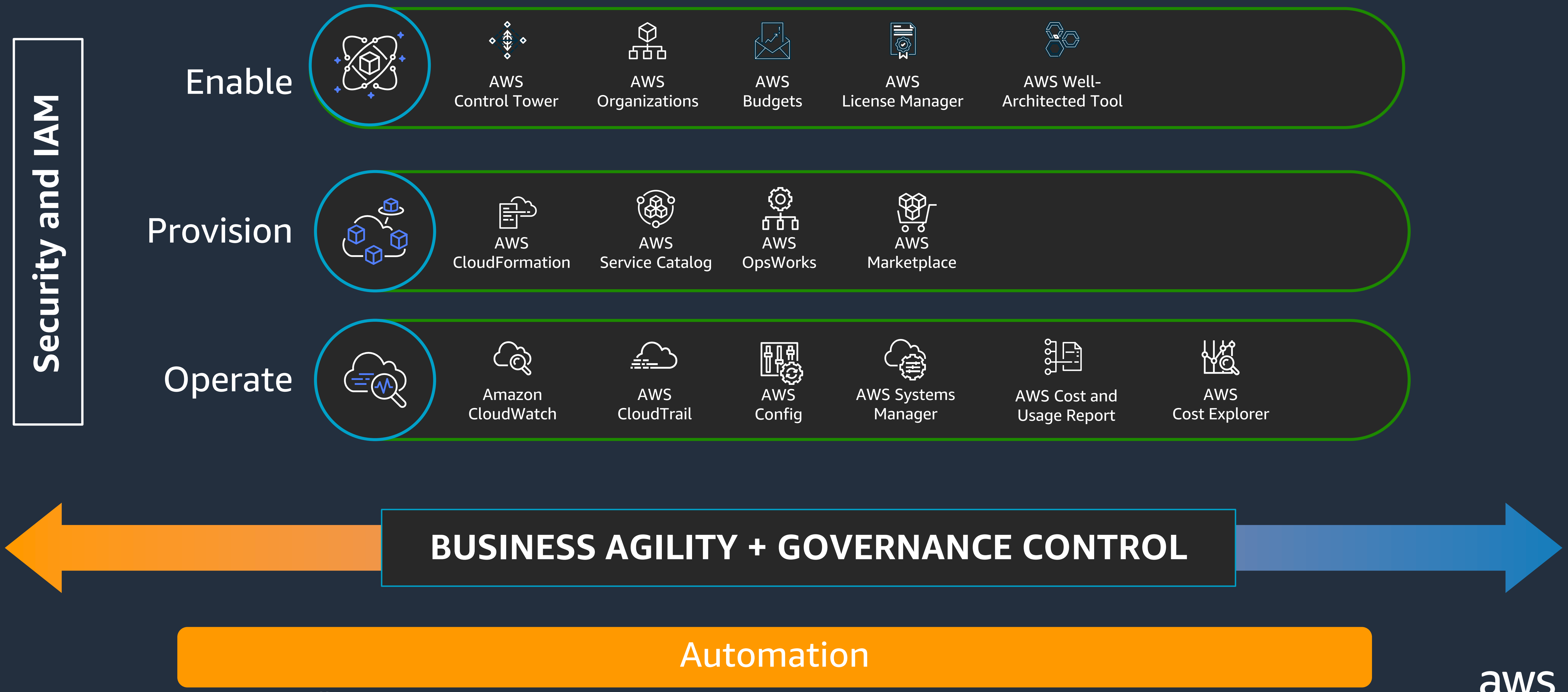
AWS Service Catalog

SELF-SERVICE PORTAL FOR CREATING AND MANAGING YOUR IT SERVICE CATALOG.



- Create and manage approved catalogs of resources.
- End users browse and launch products via self-service portal.
- Control user access to applications or AWS resources per compliance needs.
- Extensible via API to existing self-service frameworks.

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

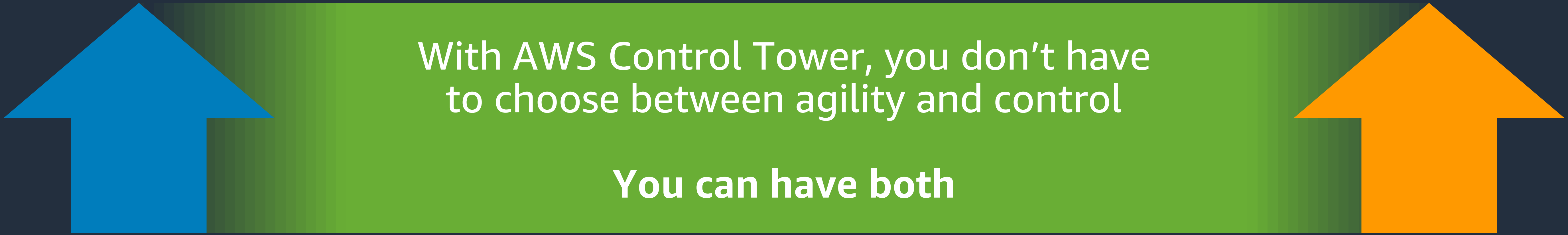
AWS Cost and Usage Report

AWS Cost Explorer

BUSINESS AGILITY + GOVERNANCE CONTROL

Automation

Business agility *and* governance control



With AWS Control Tower, you don’t have to choose between agility and control

You can have both

Governance

Security

Compliance

Operations

Spend Management

Agility

Self-service access

Experiment fast

Respond quickly to change

Thank you!

AWS Education & Research Team

Nikiforos Botis - nbotis@amazon.com