AWS State, Local, and Education Learning Days

Philadelphia

aws **Learning Days**
State, Local, and Education

Building and governing your cloud environment

Vinod Kisanagaram (he/him)

Solutions Architect
AWS
vinodaws@amazon.com

aws **Learning Days**
State, Local, and Education

Why do we need a
strong cloud governance?
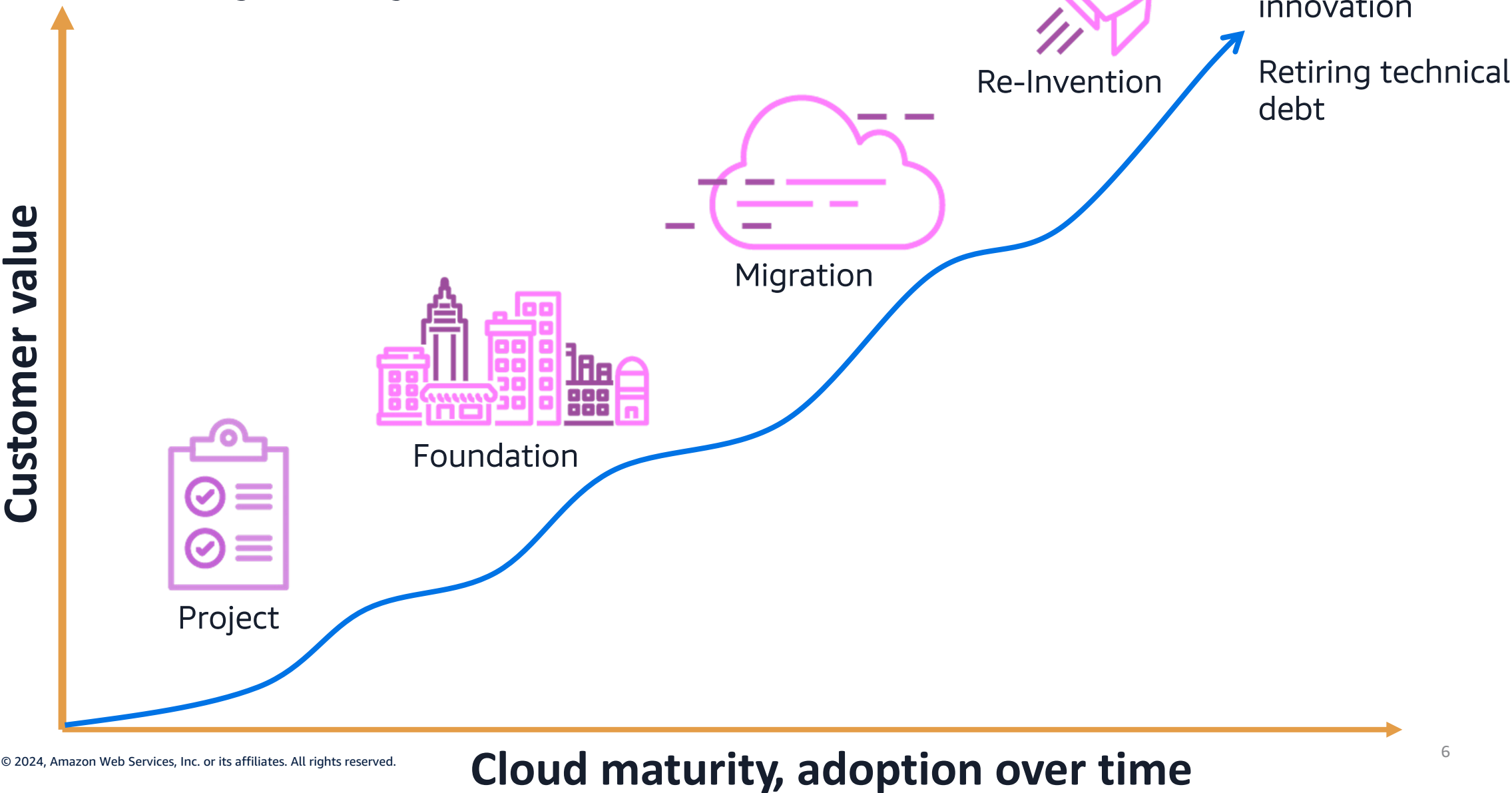
What we will cover today

- **Overview of cloud governance**

- **The customer journey**

- **Cloud governance best practices** Controls, identity, security, network, observability, cloud financial management

- **Q&A**

→

Cloud governance

is the set of rules, practices, and reports that help you align your cloud use to your business objectives

The customer journey

Customer value

Project

Foundation

Migration

Re-Invention

Cloud-native innovation

Retiring technical debt

Cloud maturity, adoption over time

How to prepare a cloud ready environment

Retire/retain   Re-purchase   Re-platform (lift, tinker, and shift)   Re-host (lift and shift)   Re-factor/re-architect (transform and modernize)
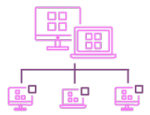
Cloud ready environments

Migration ready * Scale ready * Optimized and efficient

Interoperable management and governance functions

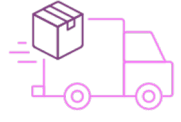| Controls and guardrails	Network connectivity	Identity management	Security operations	Service mgmt (ITSM)	Observability	Cloud financial management	Sourcing and distribution

AWS Well-Architected Pillars

Operational excellence   Security   Reliability   Performance efficiency   Cost optimization   Sustainability

Cloud governance best practices

Best practice
01
Controls and guardrails

Use accounts as
building blocks

Use accounts as building blocks

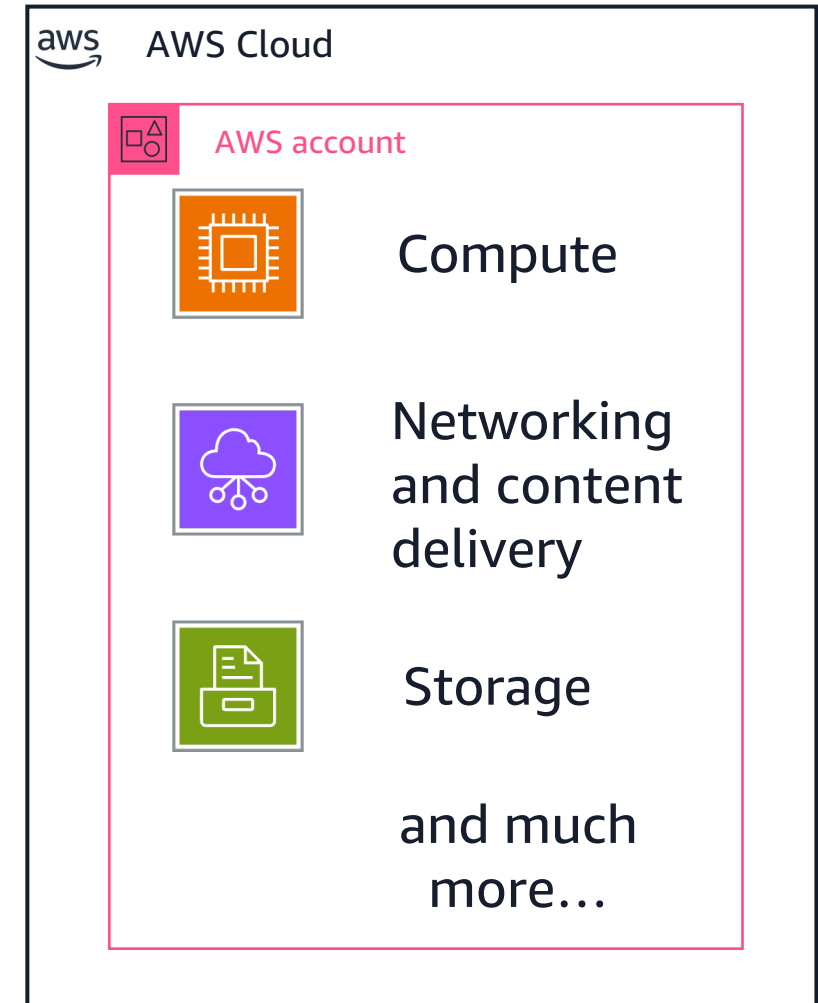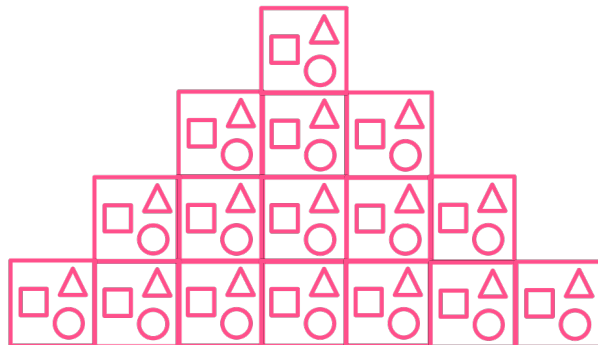• Controls and guardrails best practice | 01

Account limits
Quotas

Security
Natural boundaries, isolation

Compliance/ business processes
Billing, custom requirements

AWS Cloud

AWS account

Compute

Networking and content delivery
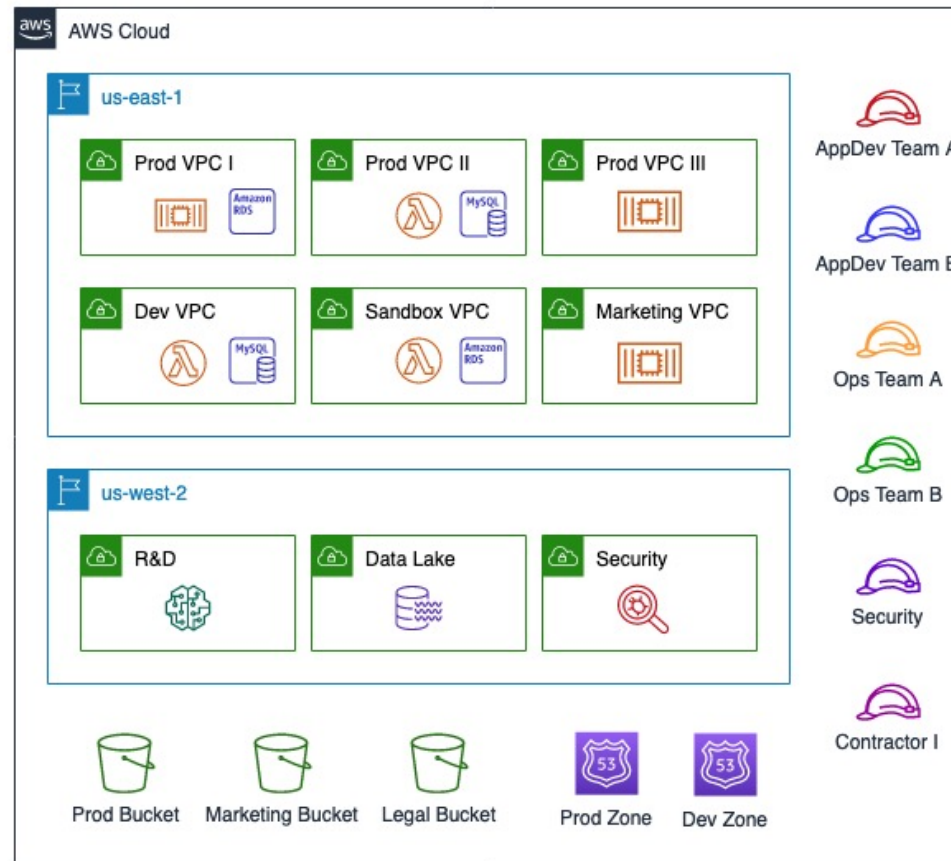
Storage

and much more…

Why use multiple AWS accounts?

when single account is no longer scalable for your business

Non prod may impact prod workload

Complex policy due to variety of services in use

Risk of elevated permissions and cross workload access

Complex billing structure and operational support

Multi-Account

AWS Control Tower: A self-service solution to automate the setup of new AWS multi-account environments

Managed-service version of multi-account environment
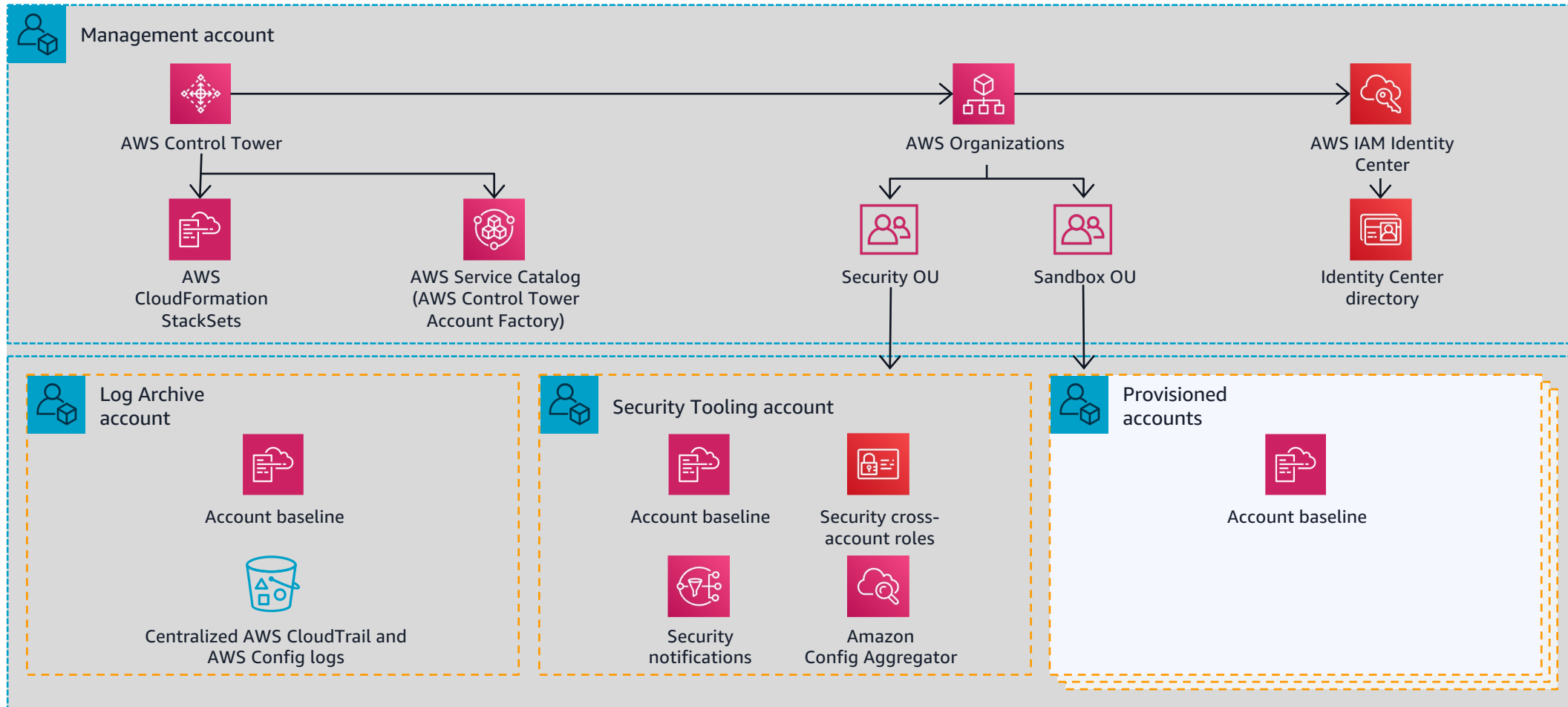
Deployment of AWS best practice blueprints and controls

Automated account creation based on AWS best practices

Dashboard for monitoring compliance status

Landing zone foundation of AWS Control Tower

Management account

- AWS Control Tower → AWS Organizations → AWS IAM Identity Center

  - AWS Control Tower
    - AWS CloudFormation StackSets
    - AWS Service Catalog (AWS Control Tower Account Factory)
  - AWS Organizations
    - Security OU
    - Sandbox OU
  - AWS IAM Identity Center
    - Identity Center directory

Log Archive account
- Account baseline
- Centralized AWS CloudTrail and AWS Config logs

Security Tooling account
- Account baseline
- Security cross-account roles
- Security notifications
- Amazon Config Aggregator

Provisioned accounts
- Account baseline

Best practice
02
Identity

Apply the principle
of **least privilege**

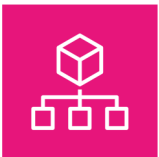# Managing access permissions to AWS accounts

- Identity best practices

IAM Identity Center

AWS Identity and Access Management (IAM)

AWS Organizations

01 Restrict access to the management account

02 Require MFA for users with elevated access

03 Require human users to use federation with an identity provider to access AWS using temporary credentials

Security Best Practices in IAM

Establish a centralized identity provider for human identities

Federation via
Third-party identity providers

Native identity
(AWS IAM Identity Center)

AWS Account

AWS IAM Identity Center can be used if you have no plans to use a third-party identity provider and need to setup identity federation.

Best practice 03

Network connectivity

Define a **network strategy**

17

Design your network strategy

- Network connectivity best practice | 03

Plan your IP address space
Non-overlap, IPv6, environment

Network Resiliency
Multi-AZ design
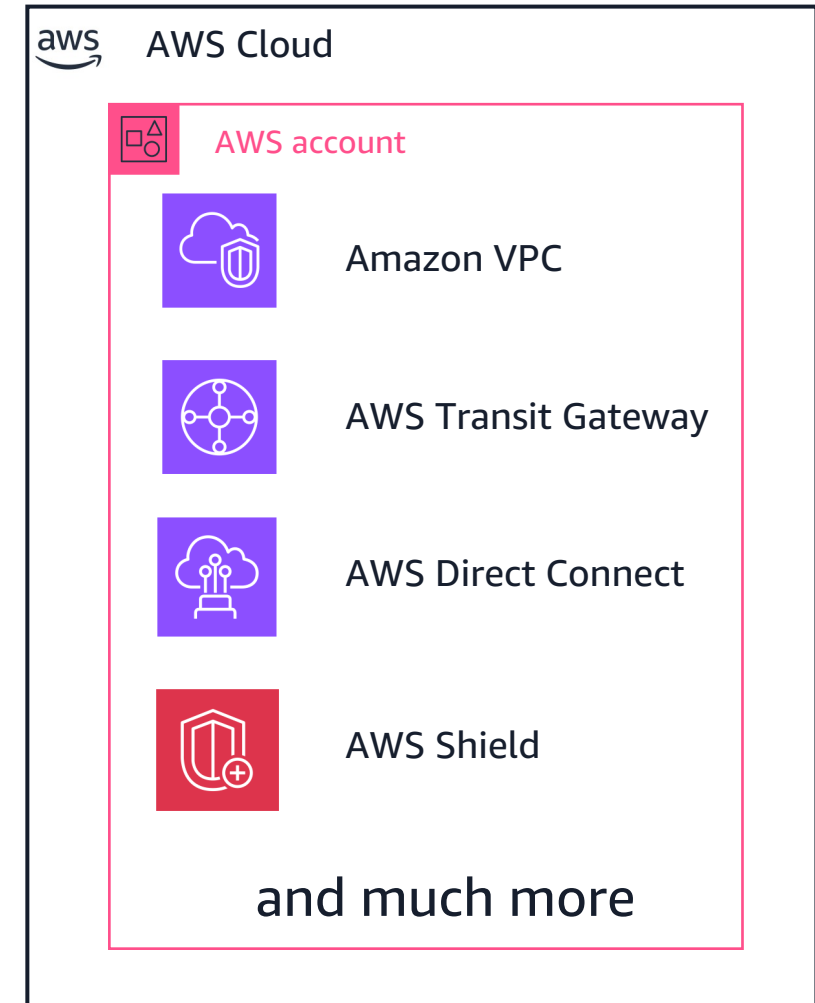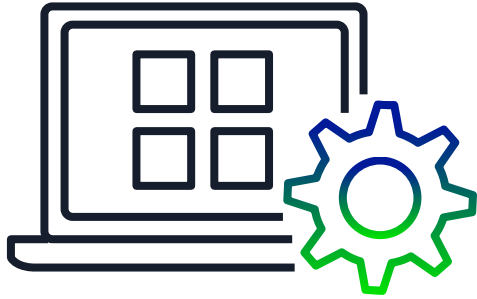
Network Monitoring
Network traffic, access

Network Security
Firewall, DDoS, WAF, third party integrations
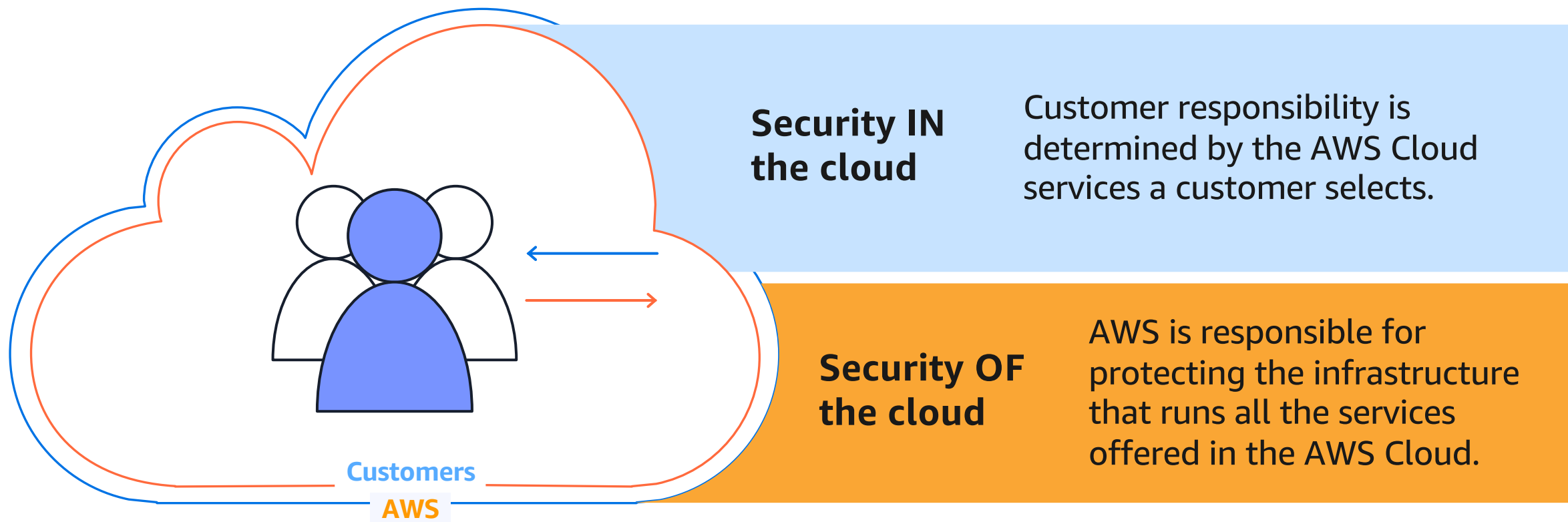
Network connectivity
On-prem, internet, internal, DNS

AWS Cloud
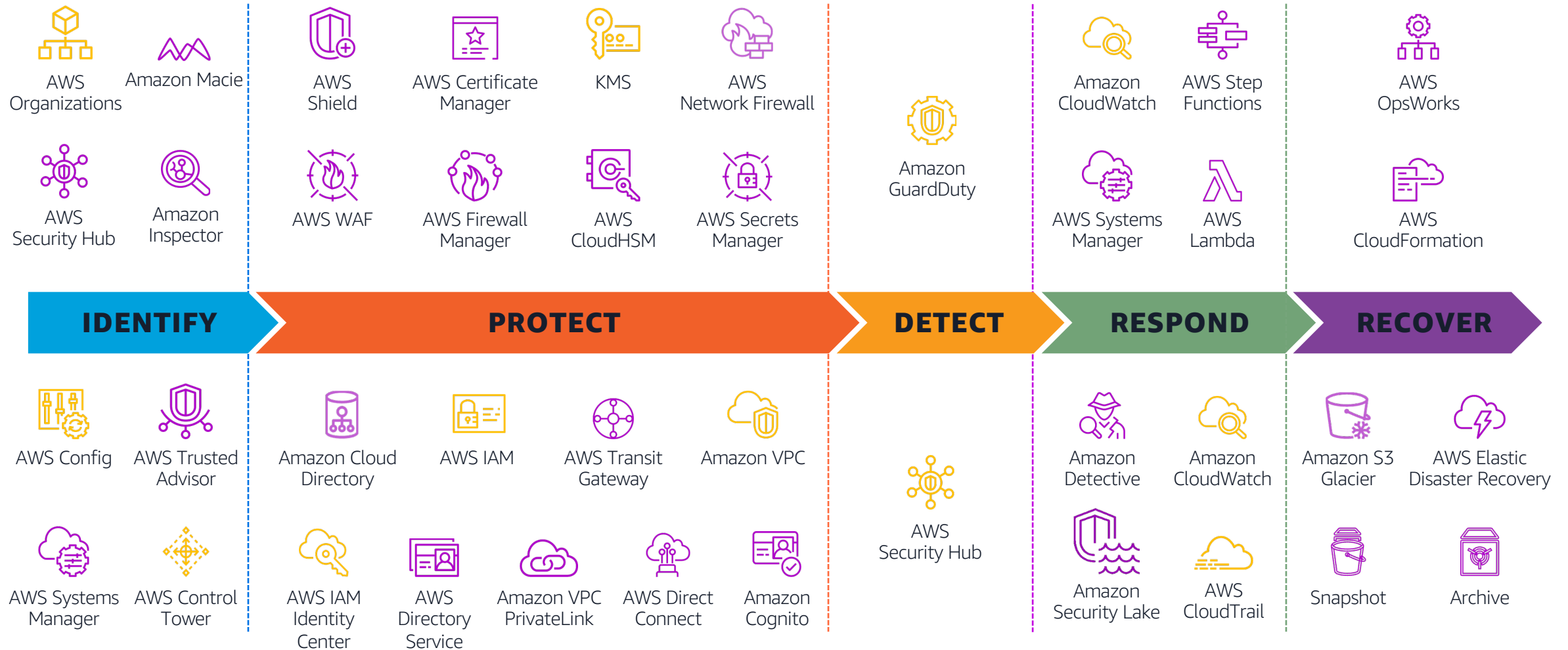
AWS account

Amazon VPC

AWS Transit Gateway

AWS Direct Connect

AWS Shield

and much more

Best practice
04
Security

Align control objectives to a **security framework**

Shared responsibility model

Security IN the cloud

Customer responsibility is determined by the AWS Cloud services a customer selects.

Security OF the cloud

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

Customers

AWS

Use AWS services to mitigate threats

IDENTIFY

AWS Organizations · Amazon Macie · AWS Security Hub · Amazon Inspector · AWS Config · AWS Trusted Advisor · AWS Systems Manager · AWS Control Tower

PROTECT

AWS Shield · AWS Certificate Manager · KMS · AWS Network Firewall · AWS WAF · AWS Firewall Manager · AWS CloudHSM · AWS Secrets Manager · Amazon Cloud Directory · AWS IAM · AWS Transit Gateway · Amazon VPC · AWS IAM Identity Center · AWS Directory Service · Amazon VPC PrivateLink · AWS Direct Connect · Amazon Cognito

DETECT

Amazon GuardDuty · AWS Security Hub

RESPOND

Amazon CloudWatch · AWS Step Functions · AWS Systems Manager · AWS Lambda · Amazon Detective · Amazon CloudWatch · Amazon Security Lake · AWS CloudTrail

RECOVER

AWS OpsWorks · AWS CloudFormation · Amazon S3 Glacier · AWS Elastic Disaster Recovery · Snapshot · Archive

What is Amazon GuardDuty?

Amazon GuardDuty is a threat detection service that uses **machine learning**, anomaly detection, and **integrated threat intelligence** to identify and prioritize potential threats.

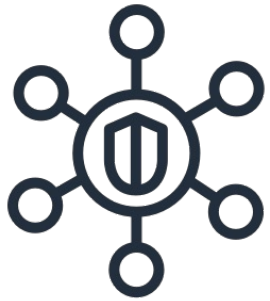| One-step activation | Continuous monitoring of AWS accounts and resources | Global coverage with regional results | Detect known and unknown threats | Enterprise-wide consolidation & management |

What is AWS Security Hub?

AWS Security Hub is a cloud security posture management service that **continuously** performs security best practice checks and **seamlessly** aggregates security findings from AWS and third-party services and enables automated response.
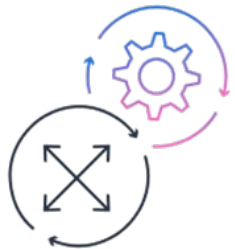
Automated, continuous best practice checks

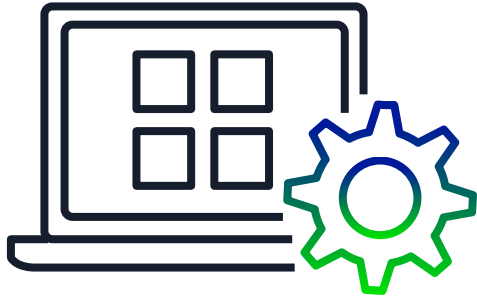Consolidated findings across AWS services and partner integrations

Standardized findings format and cross-Region aggregation

Standards aligned to regulatory and industry compliance frameworks

Automated response, remediation, and enrichment actions

Best practice 05
Security

Use controls to **protect security baselines** and identify **misconfigurations**

Control types

Detective
Detect resources that violate your defined security policies

> COMPLIANT

> NONCOMPLIANT

Preventive
Disallow actions that would lead to violations of your security policies
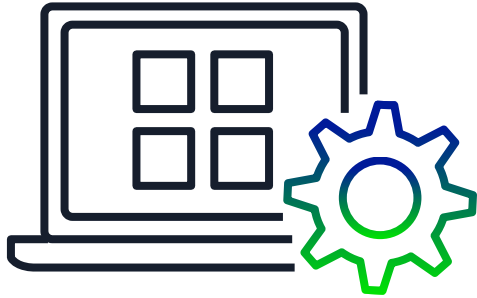
> ALWAYS COMPLIANT

Proactive
Scans resources before they are provisioned, blocking provisioning if resources aren't compliant

> APPROVED RESOURCES ONLY

> ALWAYS COMPLIANT

Best practice
06
Cloud Financial
Management

Enable mechanisms for
cost governance

Build your Cloud Financial Management portfolio

Plan

Plan and Evaluate

Migration Evaluator
AWS Pricing Calculator
AWS Budgets

Run

Manage and Control

Tagging Strategy
Billing Console
AWS Purchase Order Management
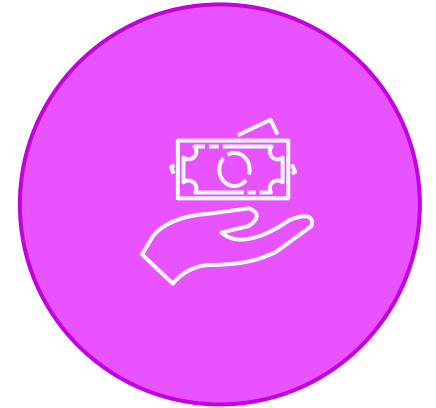AWS Budgets (Actions)
AWS Cost Anomaly Detection

See

Track and Allocate

AWS Cost Explorer
AWS Cost & Usage Reports
AWS Cost Categories
AWS Billing Conductor
AWS Application Cost Profiler

Save

Optimize and Save

Savings Plans
Reserved Instances
Recommendations

Define your tagging strategy

Identify tag requirements

Employ a Cross-Functional Team

Required and Conditionally Required Tags

Use Tags Consistently

Start Small; Less is More

Tagging use cases

AWS Console Organization and Resource Groups

Cost Allocation

Automation

Operations Support

Access Control

Security Risk Management

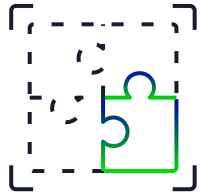### Tagging schema

Define mandatory tag keys

Define acceptable values and tag naming conventions

No personally identifiable information (PII)

Decide who can define and create new tag keys

Tag polices

Key takeaways
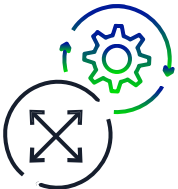
Use accounts as building blocks

Protect security baselines and stop cloud risks

Apply the principle of least privilege

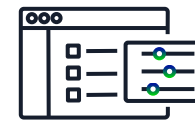Continuously monitor and test control effectiveness

Design your network strategy

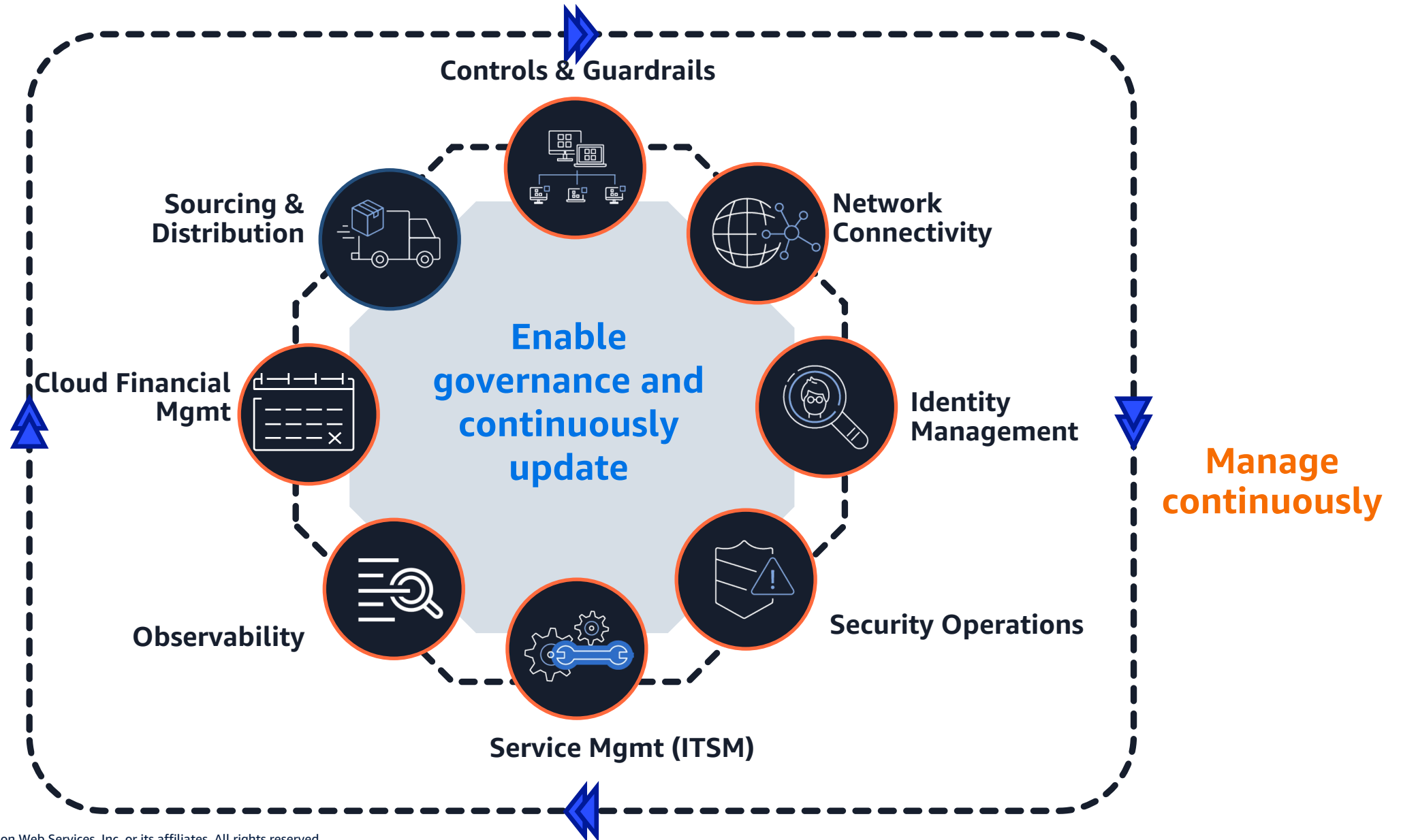Build your cloud financial management portfolio

Align control objectives to a security framework

Define a tagging strategy and enforce tagging

Remember - It is a continuous cycle

Controls & Guardrails

Network Connectivity

Identity Management

Security Operations

Service Mgmt (ITSM)

Observability

Cloud Financial Mgmt

Sourcing & Distribution

Enable governance and continuously update

Manage continuously

Using Innovative Documentation-as-Code Approach for the Georgia Department of Human Services System Security Plan

Georgia Department of Human Services

CHALLENGE

Manual, time-consuming process of creating and updating System Security Plan (SSP) Word/PDF documents to meet federal compliance requirements. They needed a better, more automated approach.

SOLUTION

Collaborated with AWS Professional Services to develop "documentation-as-code" approach for creating and maintaining the SSP's. Used logging and monitoring layer on Amazon CloudWatch, which collects and visualizes near-real-time logs, metrics, and event data in to streamline infrastructure and application maintenance. Used AWS CloudTrail to monitor account activity AWS and provide audit trails. Used AWS Config to monitor overall security and configurations of the organization's resources

OUTCOME

✓ Created SSP for the Document Imaging System application within 16 weeks

✓ Audit trails of changes to the SSP were improved, with visibility into who made each change, when, and why.

✓ The new approach streamlined the process of creating, updating, and tracking changes to the System Security Plans.
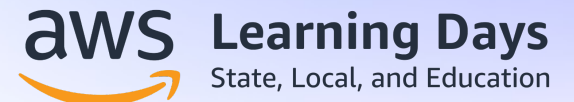
Additional resources

Organizing Your AWS Environment Using Multiple Accounts

AWS Services for Security, Identity and Compliance

aws

aws Learning Days
State, Local, and Education

aws

Thank you!

Vinod Kisanagaram

Solutions Architect
AWS

vinodaws@amazon.com

**Please complete the survey
for this session**

**Building and governing
your cloud environment**

aws **Learning Days**
State, Local, and Education