AWS State, Local, and Education Learning Days

Building and Governing your Cloud Environment

Varun Pole (he/him)

Manager - Solutions Architect
Amazon Web Services

Why do we need a
Strong cloud governance

How do we prepare our environment for a migration, a new project, or organization transitions?

How do we enable the right controls to adhere to our standards and/or regulatory requirements?

What can we do to drive efficiency and optimization for builders?

What we will cover today

01 **Overview of cloud governance**

02 **The Customer Journey**

03 **Cloud governance and Management best practices**

Controls. Identity. Security. Network. Observability. Cloud Financial Management

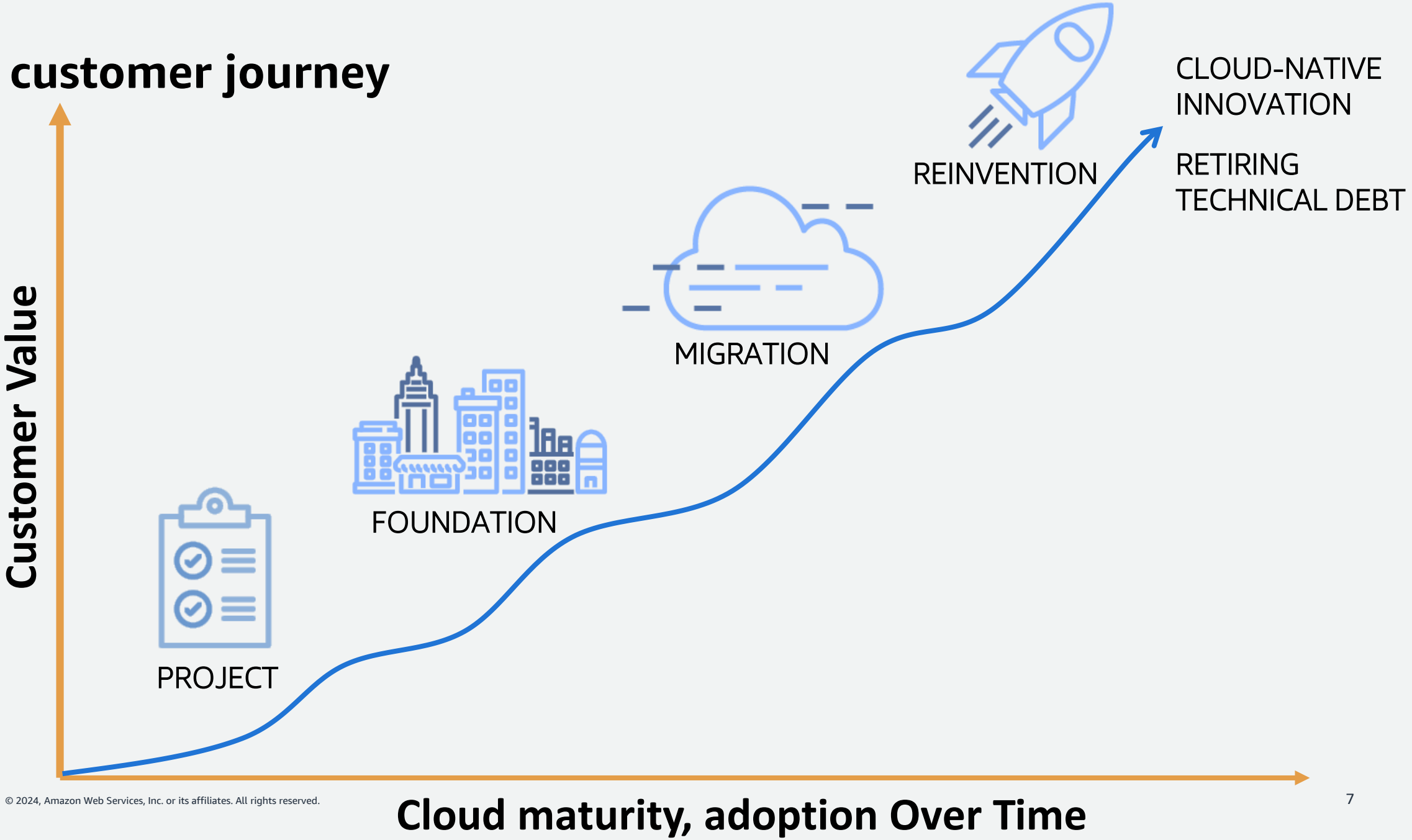
04 **Q&A**

Overview of cloud governance

Cloud governance

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

The customer journey



How to prepare a Cloud Ready Environment

Retire/Retain

Re-purchase

Re-platform
(Lift, Tinker & Shift)

Re-host
(Lift & Shift)

Re-factor/Re-architect
(Transform & Modernize)

Cloud Ready Environments

Migration Ready * Scale Ready * Optimized & Efficient

Interoperable Management & Governance Functions

- Controls & Guardrails
- Network Connectivity
- Identity Management
- Security Operations
- Service Mgmt (ITSM)
- Observability
- Cloud Financial Mgmt
- Sourcing & Distribution

AWS Well-Architected Pillars

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization

Cloud governance and management best practices

Best practice
01
Controls & Guardrails

Use accounts as **building blocks**

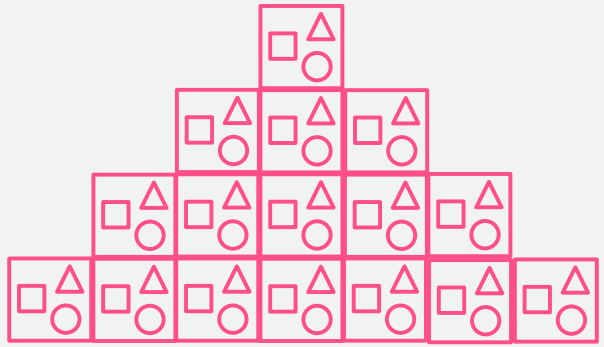
Use accounts as building blocks

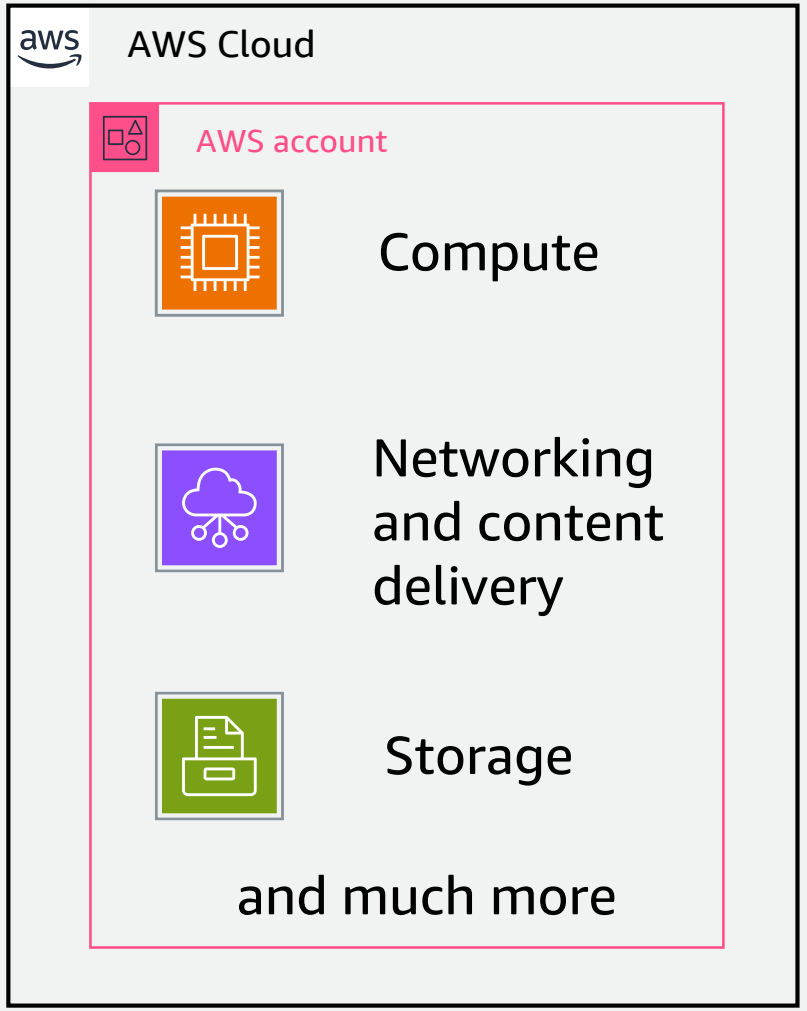
- Controls & Guardrails Best Practice | 01

Account limits
Quotas

Security
Natural boundaries, isolation

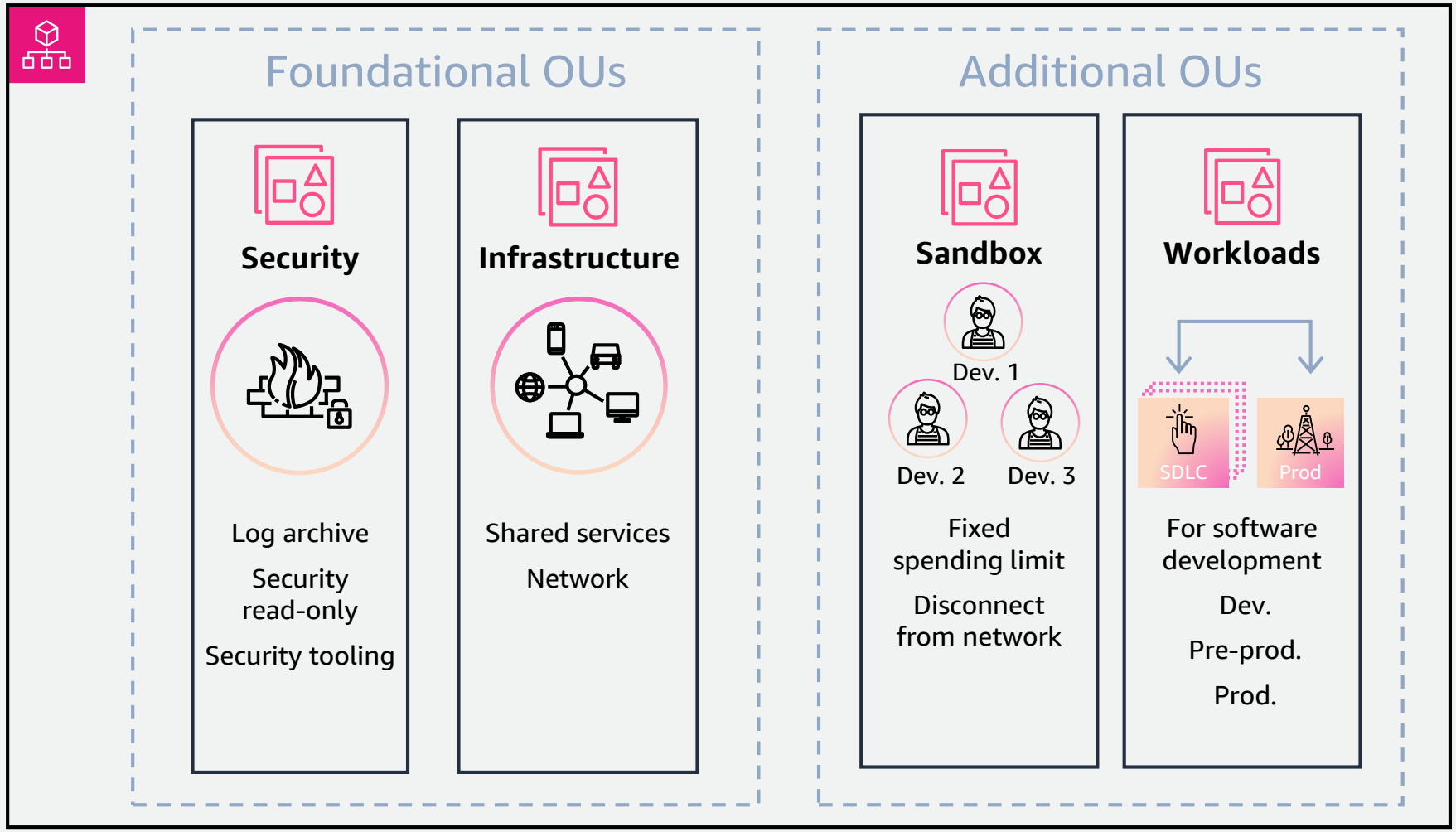
Compliance/ business processes
Billing, custom requirements





Recommended OU structure

- Controls & Guardrails Best Practice | 01



Organizing your AWS environment using multiple accounts

Identity

Best practice
02
Identity

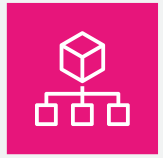
Apply the principle of least privilege

Managing access permissions to AWS accounts

- Identity Best Practice | 02

IAM Identity Center

AWS Identity and Access Management (IAM)



AWS Organizations

01 Restrict access to the management account

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

03 Require MFA for users with elevated access

04 Apply least-privilege permissions

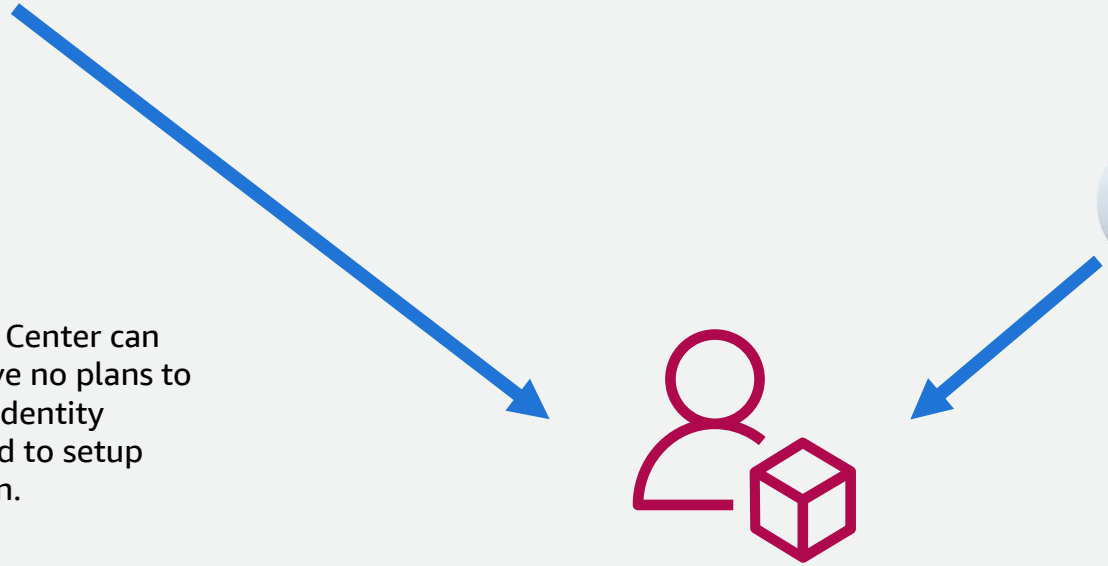
Security Best Practices in IAM

Establish a centralized identity provider for human identities

Native Identity
(AWS IAM Identity Center)

Federation via
3rd Party Identity Providers

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.



AWS Account

With AWS SSO you can continue to use your existing third-party identity provider as an identity source; allowing the external provider to retain management of your user credentials.

Network connectivity

Best practice
03
Network Connectivity

Design your **network strategy**

Design your network strategy

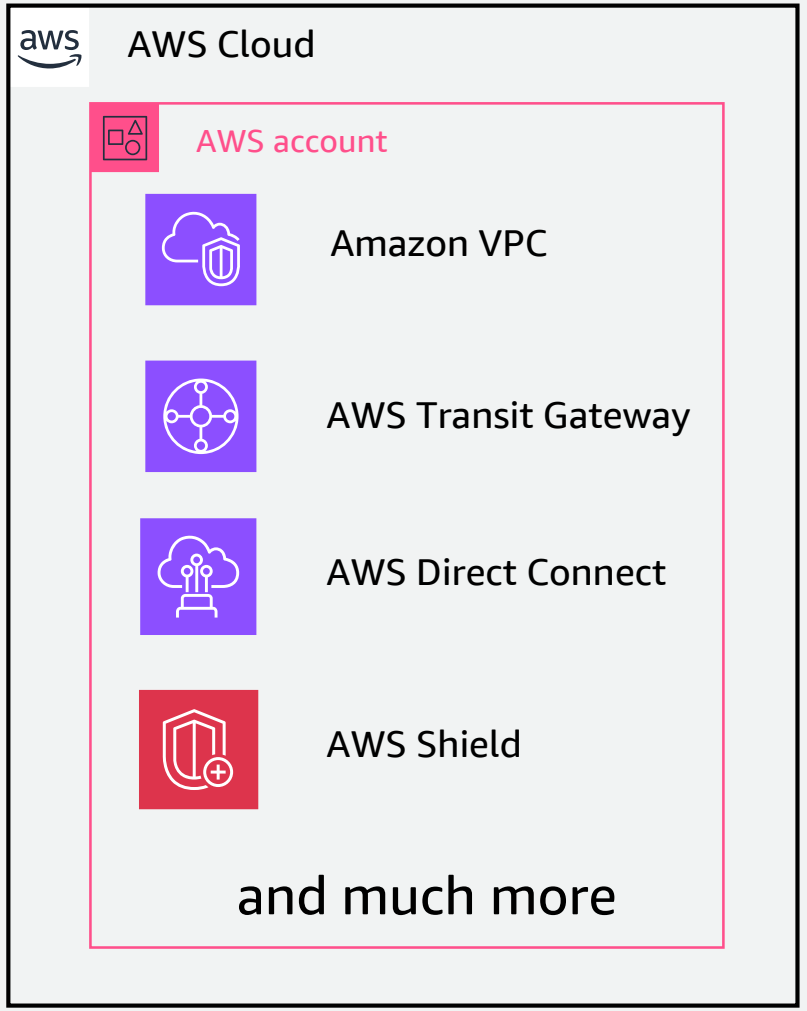
- Network connectivity Best Practice | 03

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

Network connectivity
On-prem, internet, internal, DNS

Network Security
Firewall, DDoS, WAF

Network Monitoring
Network traffic, access



Security

Security controls in the governance framework

Security controls

Establish safeguards that meet your standards

Standards

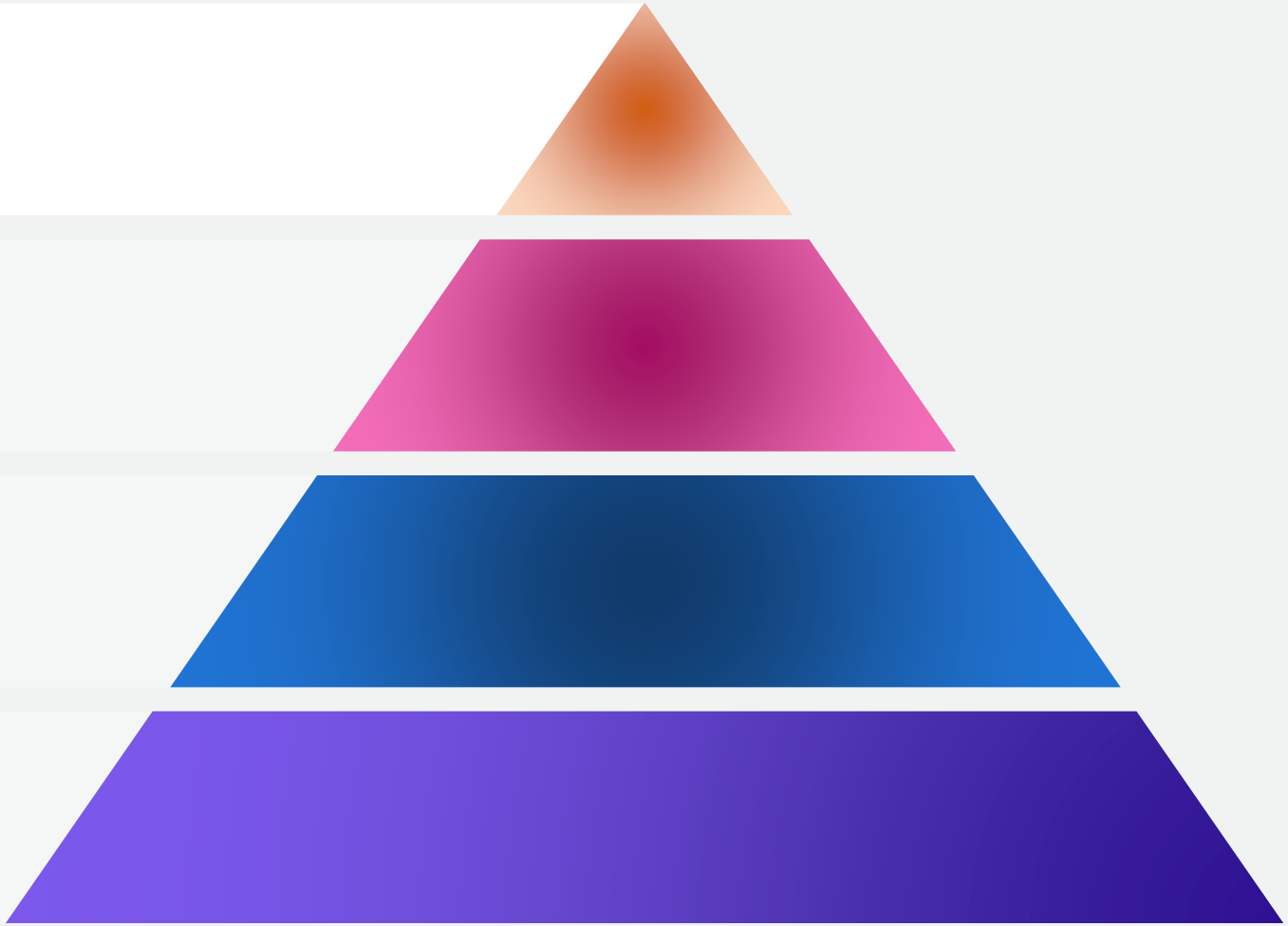
Define formal requirements

Control objectives

Identify the conditions to meet

Policies

Set high-level expectations



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

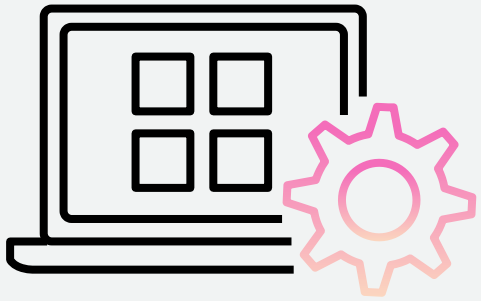
ALWAYS COMPLIANT

Proactive

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

APPROVED RESOURCES ONLY

ALWAYS COMPLIANT



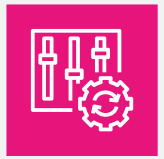
Best practice
04
Security

Align control objectives to a security framework

Align control objectives to a security framework

- Security Best Practice | 04

AWS Security Hub



AWS Config

AWS Control Tower

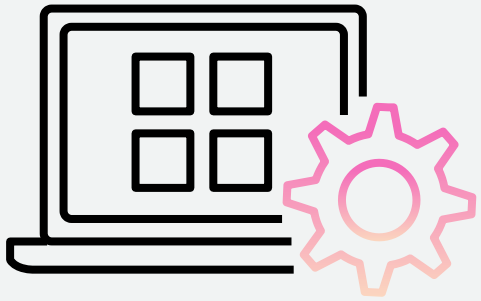
01 A security framework helps you establish a **consistent** and **repeatable foundation** for risk management

02 Well-defined control objectives and standards help establish a baseline for **measuring control effectiveness**

AWS Well-Architected Framework Security Pillar

Cloud Security Alliance Cloud Controls Matrix (CCM)

NIST SP 800-53 Rev. 5

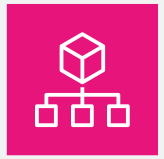


Best practice
05
Security

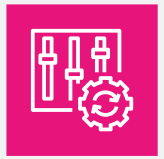
Use preventive controls to **protect security baselines** and proactive controls to **stop security misconfigurations from being deployed**

Protect security baselines and stop cloud risks

- Security Best Practice | 05



AWS Organizations



AWS Config

AWS Control Tower

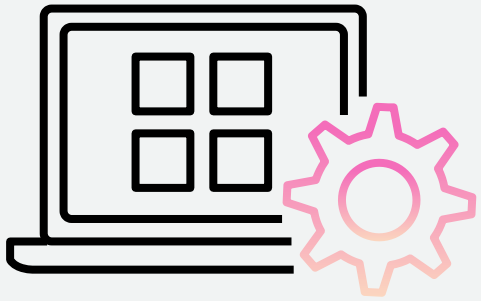
01 Preventive controls help you to **enforce** and **safeguard** critical security baselines and invariants

02 Stopping security misconfigurations before they're deployed helps **reduce attack surface** and helps builders **quickly remediate violations**

AWS Control Tower Proactive Controls

AWS Security Control Policy Examples Repository

Observability



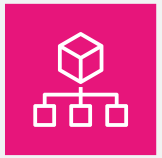
Best practice
06
Observability

Continuously monitor and test control effectiveness

Continuously monitor and test control effectiveness

- Observability Best Practice | 06


Amazon CloudWatch


AWS Organizations


AWS CloudTrail


AWS Systems Manager


AWS Systems Manager


Amazon GuardDuty

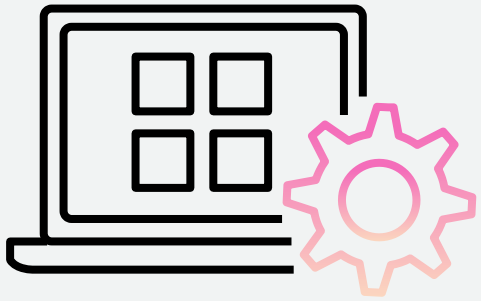
01 Collect, aggregate, and protect event and log data

02 Build capabilities to analyze and visualize log events and traces

03 Add detection and alerts for anomalous patterns across environments

04 Define, automate, and measure response and remediation

Cloud Financial Model



Best practice
07
Cloud Financial Management

Build your cloud financial management portfolio

Build your Cloud Financial Management Portfolio

- Cloud Financial Management Best Practice | 07

Plan

Plan and Evaluate

Migration Evaluator
AWS Pricing Calculator
AWS Budgets

Run

Manage and Control

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

See

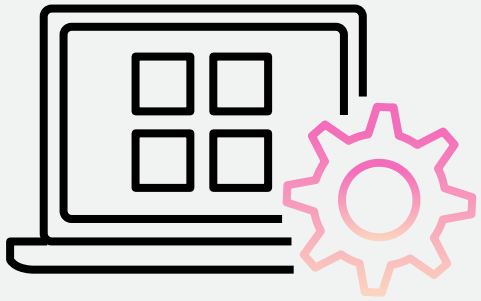
Track and Allocate

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



Best practice
08
Cloud Financial Management

Define a tagging strategy and enforce tagging

Define your tagging strategy

- Cloud Financial Management Best Practice | 08

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

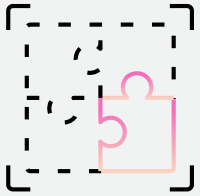
Define acceptable values and tag naming conventions

No personally identifiable information (PII)

Decide who can define and create new tag keys

Tag polices

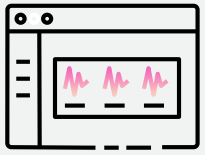
Key takeaways



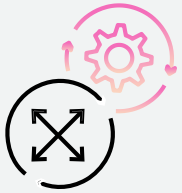
Use accounts as building blocks

Protect security baselines and stop cloud risks

Apply the principle of least privilege



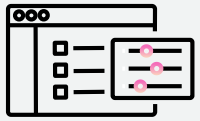
Continuously monitor and test control effectiveness



Design your network strategy

Build your cloud financial management portfolio

Align control objectives to a security framework



Define a tagging strategy and enforce tagging

Please complete the session survey by scanning the QR code

Thank you!

Varun Pole
varrampo@amazon.com

Security and Governance Track
Building and Governing Your Cloud Environment