AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

DOP302

Continuous compliance for your development workflow

Kanishk Mahajan
Sr. Solutions Architect
AWS

Jaswanthi Meganathan
Sr. Product Manager
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Cloud compliance at AWS

Understanding compliance as code

Compliance as code – preventive and detective controls

Demo – PCI compliance as code

Q&A

Additional demos – Amazon CodeGuru Reviewer and Profiler

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mapping AWS capabilities

THREE LINES MODEL



Manage risk



AWS Config



AWS CloudTrail



AWS Systems Manager



AWS Control Tower



AWS License Manager



Oversee risk



AWS Security Hub



AWS Systems Manager



AWS Config



Assurance of risk management



AWS Audit Manager

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

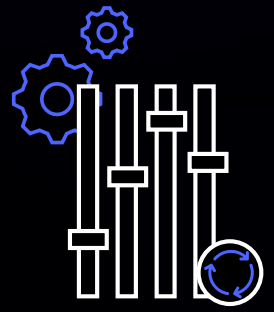
AWS Config

THREE LINES MODEL – MANAGE RISK



Identify

Identify control objectives across standards and regulations

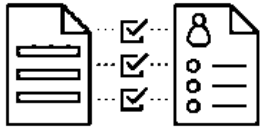


Configuration change occurs in your AWS resources



AWS Config

AWS Config records and normalizes the changes into a consistent format



AWS Config automatically evaluates the recorded configurations against the configurations you specify



AWS Config APIs & console



Amazon SNS



Amazon CloudWatch



Amazon S3

Access change history and compliance results using the console or APIs; Amazon CloudWatch Events or SNS alerts you when changes occur; deliver change history and snapshot files to your S3 bucket for analysis

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config: Conformance packs

THREE LINES MODEL – MANAGE RISK

Advanced queries



Configure attribute-based queries against current state metadata

>50 sample queries are available

Conformance packs



Simplified organization-wide deployment and reports of compliance

>50 sample templates are available to get started

Automatic remediation with AWS Config rules



Enables you to automatically remediate noncompliant resources

>170 managed rules (and growing), + create custom rules

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Systems Manager

THREE LINES MODEL – MANAGE RISK

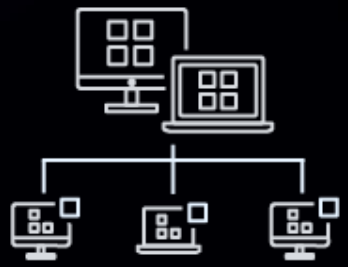


Design

Control design and control evaluation

AWS Systems Manager

Systems Manager helps you safely manage and operate your resources at scale



Group resources

Create groups of resources across different AWS services, such as applications or different layers of an application stack



Visualize data

View aggregated operational data by resource group



Take action

Respond to insights and automate operational actions across resource groups

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance as code

DEFINING COMPLIANCE AS CODE

Shift left – **with compliance**

Embed continuous and automated detection and remediation of compliance violations directly in your CI/CD pipelines

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance as code

PREVENTIVE AND DETECTIVE CONTROLS



- Detective controls = all controls in the Three Lines Model
- Both preventive and detective controls have a responsive component

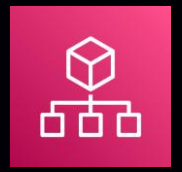
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance as code

PREVENTIVE CONTROLS

Manage



AWS Organizations service control policy



AWS Identity and Access Management (IAM)



AWS Control Tower

Provision



AWS CloudFormation



AWS Service Catalog



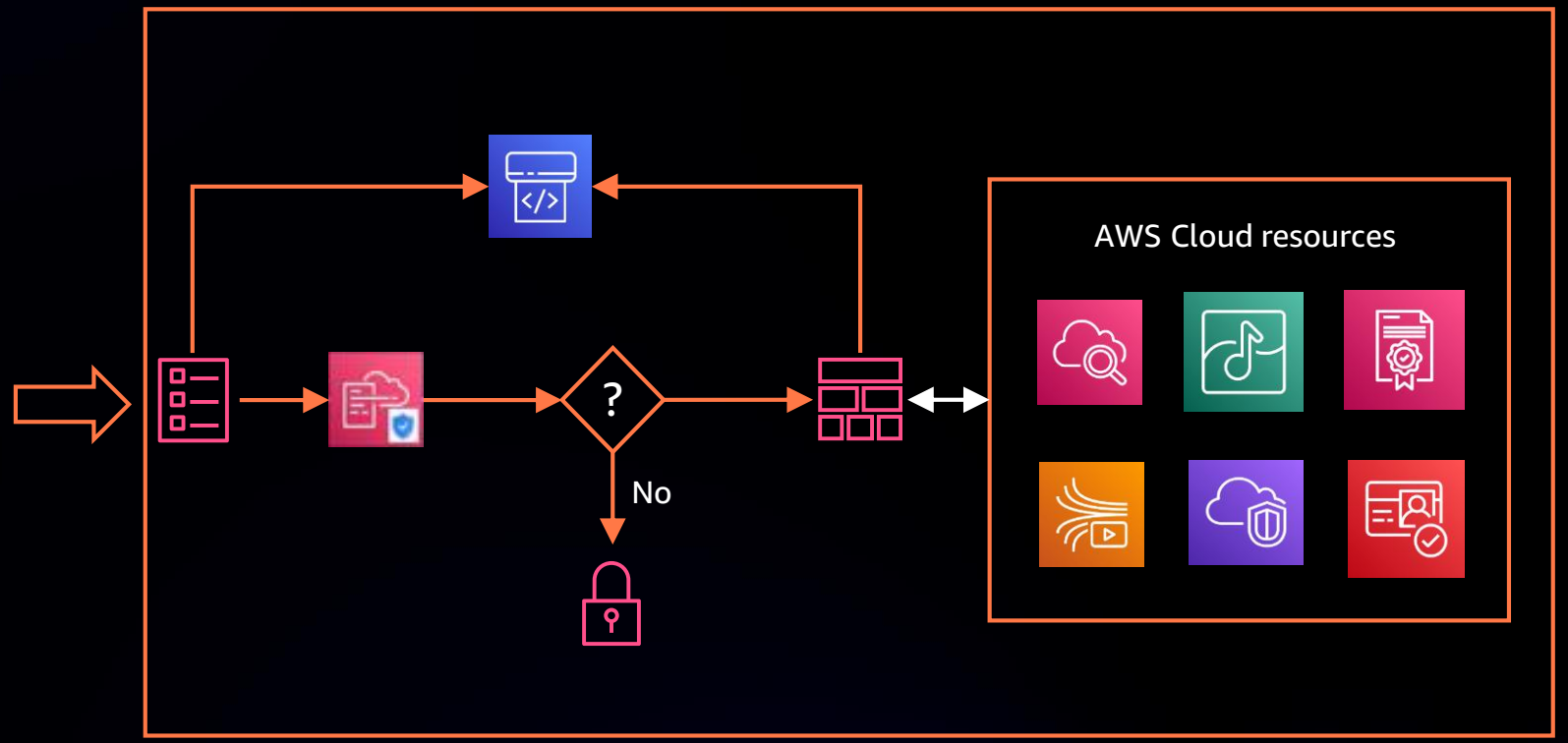
AWS Control Tower

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFormation Guard

COMPLIANCE AS CODE – PREVENTIVE CONTROLS WITH CLOUDFORMATION GUARD

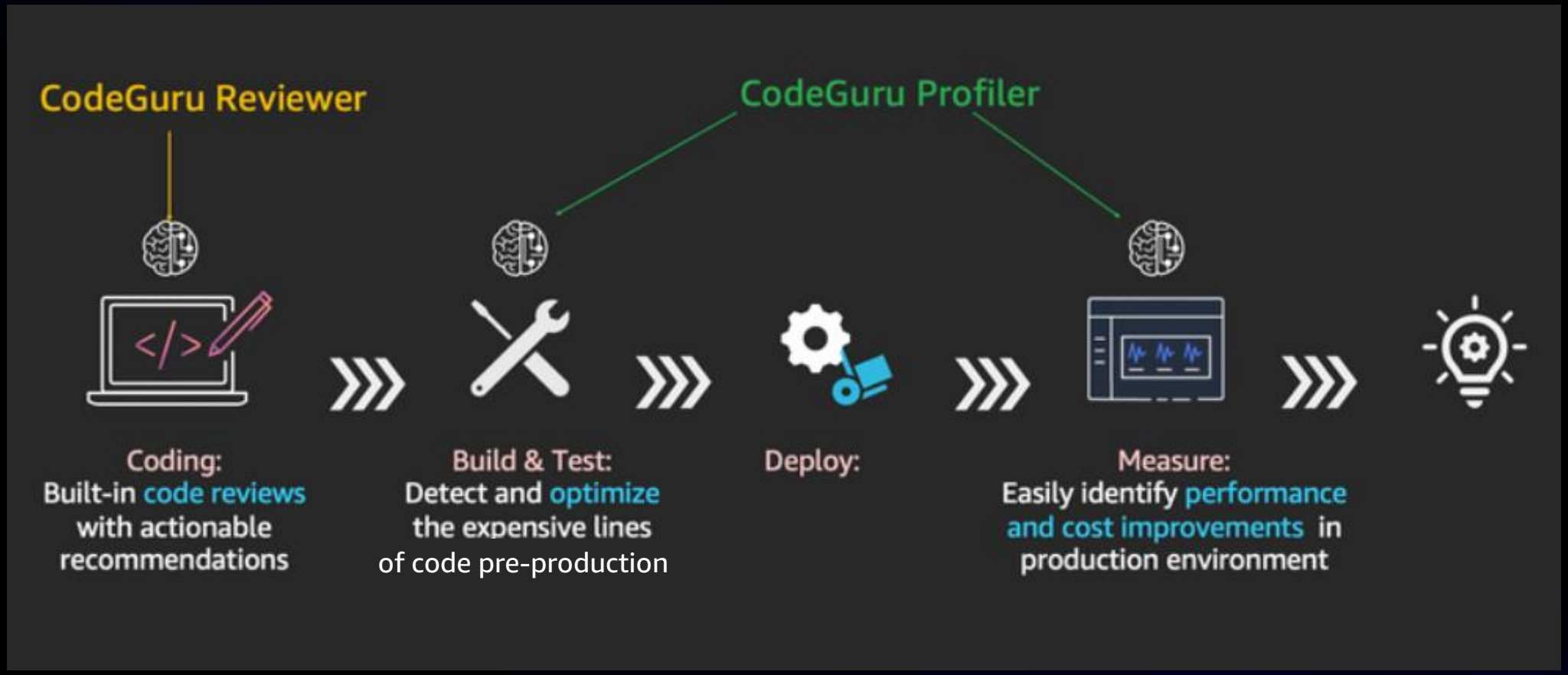
```
AWS::EC2::Volume {
     Properties {
        Size <=10
        VolumeType == ‘gp2’
        AvailabilityZone == ‘us-west-2’
     }
}
```



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Code review and profiling: CodeGuru

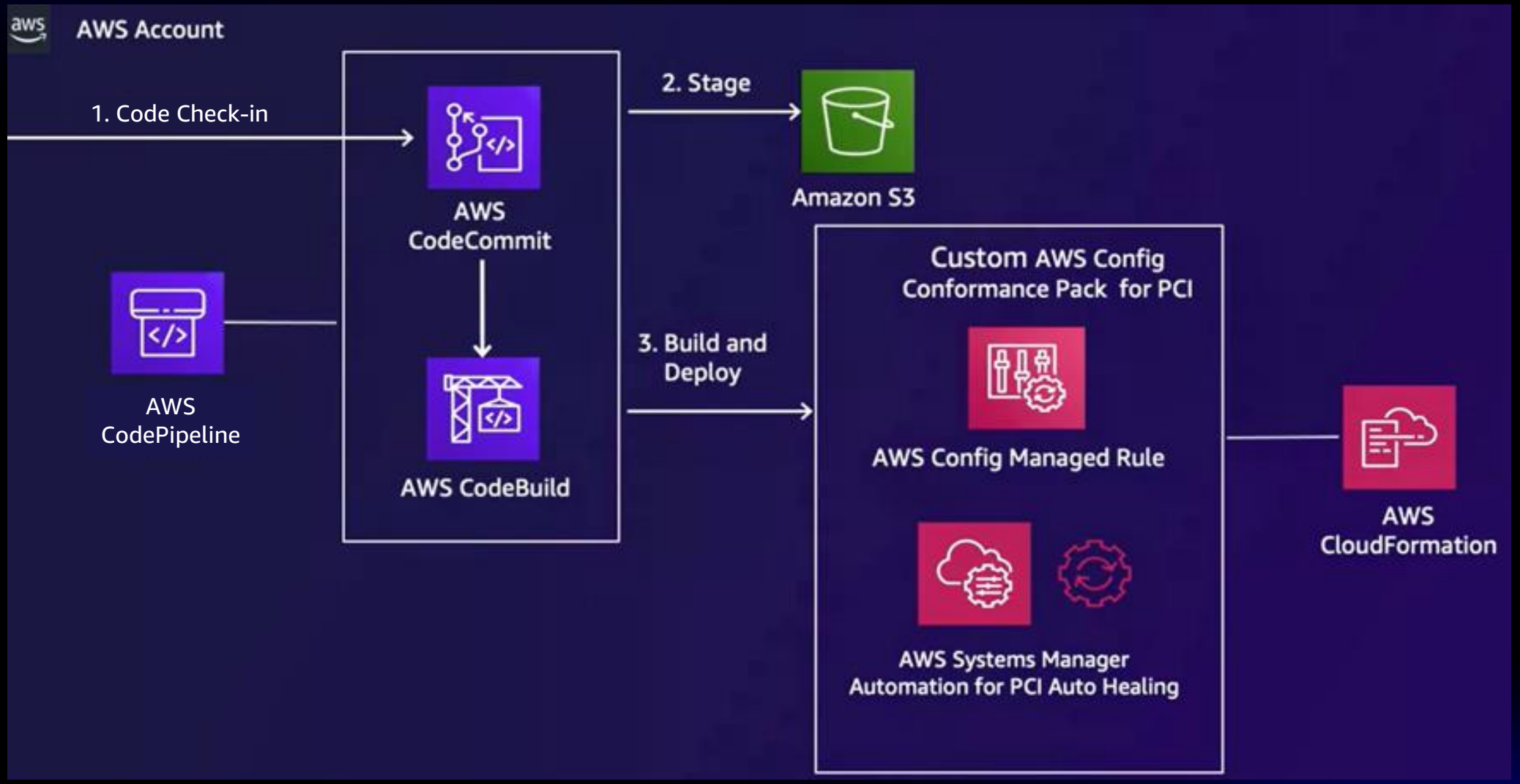
COMPLIANCE AS CODE BEST PRACTICE – CODE REVIEW AND PROFILING WITH CODEGURU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Demo – PCI compliance as code

PUTTING IT ALL TOGETHER – PCI COMPLIANCE AS CODE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

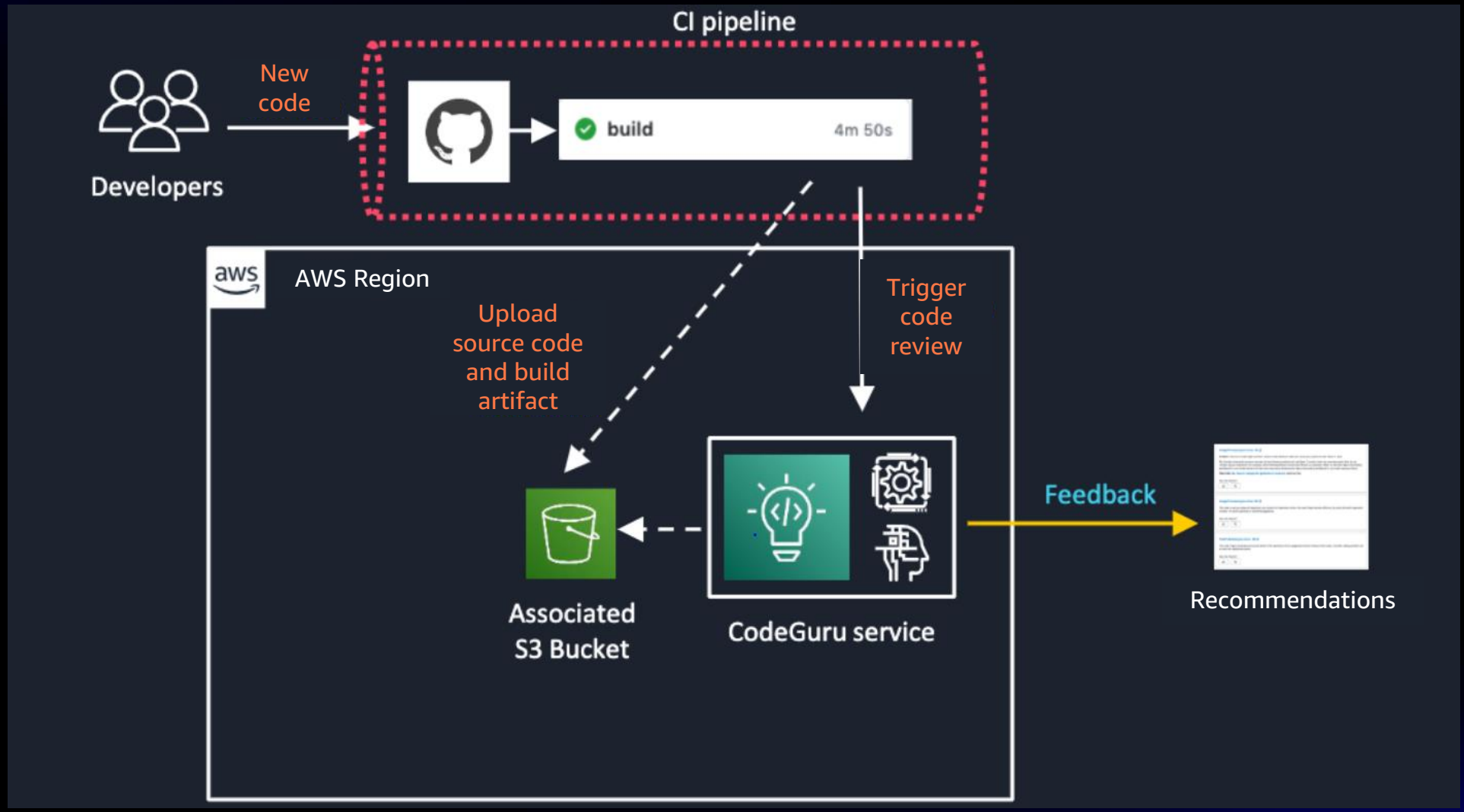
References

- DevSecOps for auto-healing PCI compliance on AWS
- Standardize compliance on AWS using DevOps and CCOE approach
- AWS reference solution – Cloud compliance and assurance
- Integrate across the Three Lines Model
- Automate code reviews and application profiling with Amazon CodeGuru

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Demo: CodeGuru Reviewer

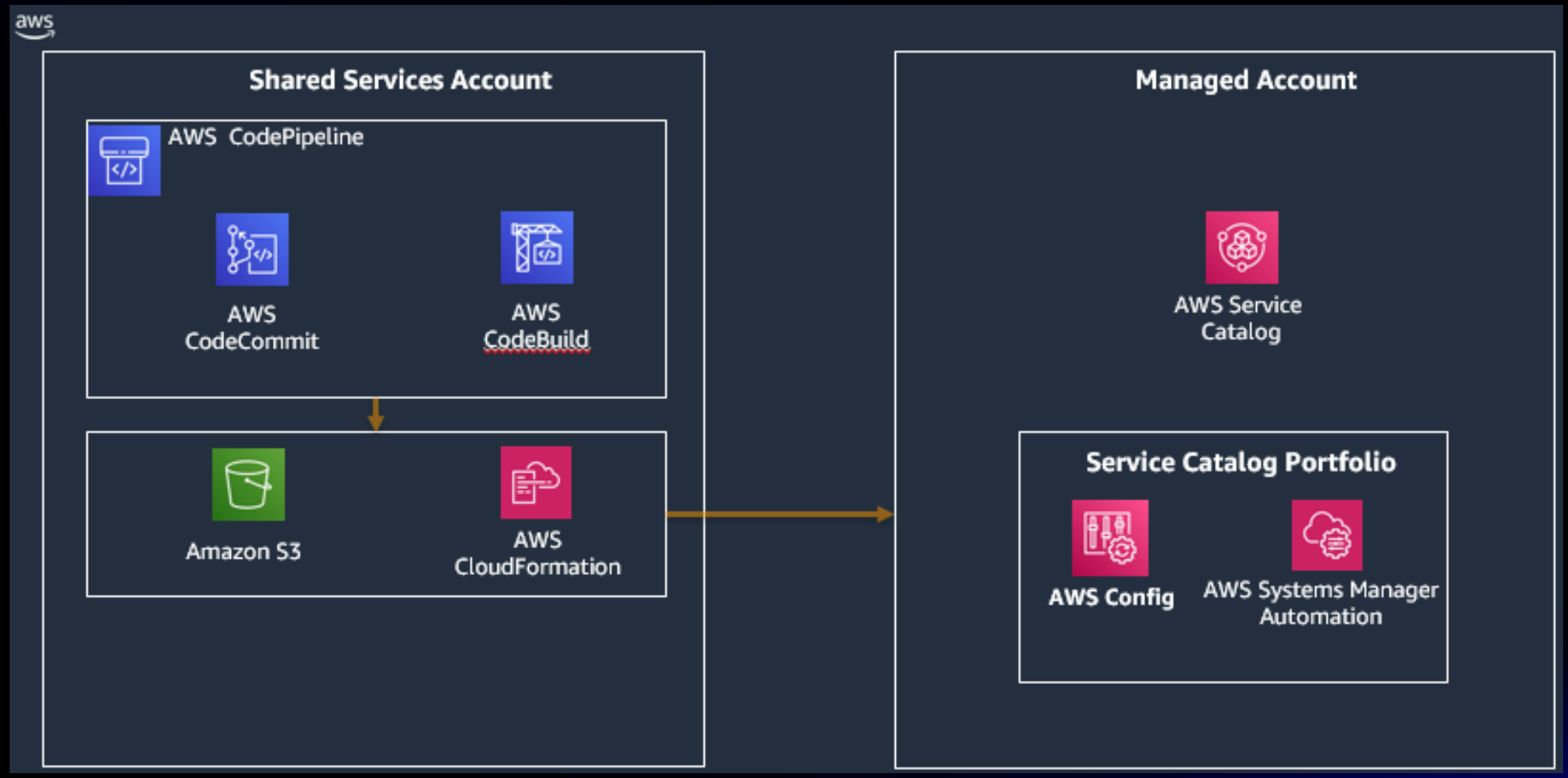
DEVELOPMENT WORKFLOW – GITHUB ACTIONS CI PIPELINE



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Demo: CodePipeline with AWS Service Catalog

COMPLIANCE AS CODE – PREVENTIVE CONTROLS WITH SERVICE CATALOG



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.