AWS re:Invent

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

COP310-R1

Cloud compliance and assurance

Isaiah Salinas
Sr WW CloudOps Specialist SA
AWS

Kanishk Mahajan
Sr Solutions Architect
AWS

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

Agenda

- Cloud compliance at scale
- Three lines model
- Hands-on labs – Overview
- References

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

Simplifying compliance at scale



AWS Security Hub

AWS License Manager

AWS Audit Manager

Amazon GuardDuty

AWS Config

Amazon Inspector

Amazon CloudWatch

AWS Systems Manager

AWS CloudTrail

AWS Control Tower

Amazon Macie

AWS Artifact

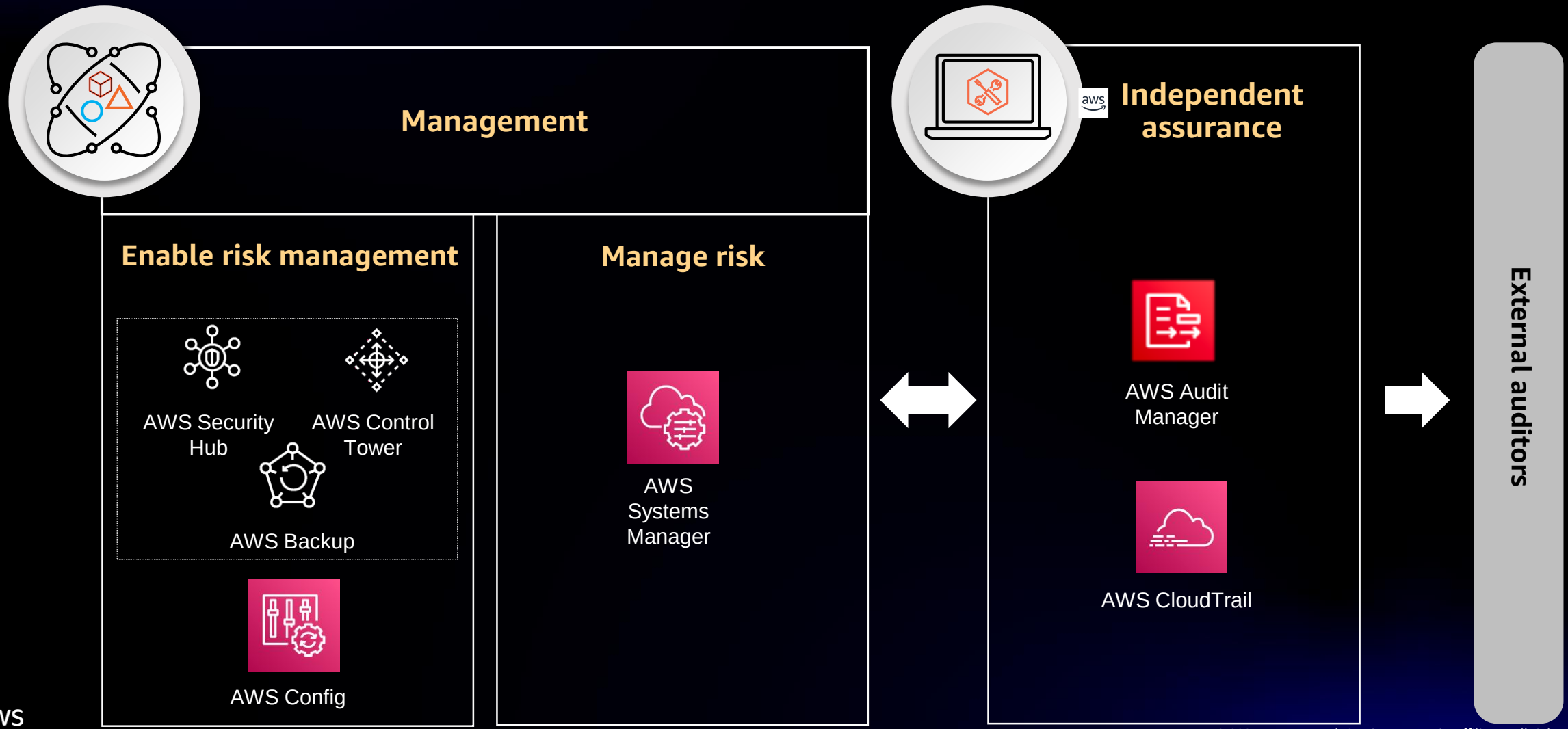
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Three lines model

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

How AWS enables cloud compliance and assurance

THE IIA'S 3 LINES MODEL



IIA = Institute of Internal Auditors

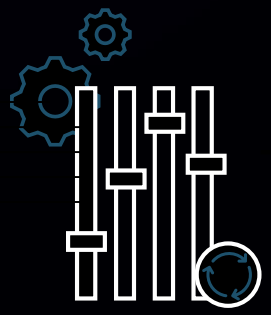
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable risk management – AWS Config

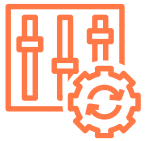


Identify

Identify control objectives across standards and regulations

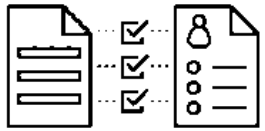


Configuration change occurs in your AWS resources



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 and console



Amazon SNS



Amazon CloudWatch



Amazon S3

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

aws

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

Enable risk management – Security hub



Monitor

Control effectiveness monitoring

AWS Security Hub
Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector
- AWS Firewall Manager
- IAM Access Analyzer
- Integrated partner solutions

Continuously aggregate and prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues

Conduct automated security checks

Use industry standards such as the CIS AWS Foundation Benchmark and PCI DSS

Take action

Investigate findings and/or take response and remediation actions

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

Manage risk management – AWS Systems Manager

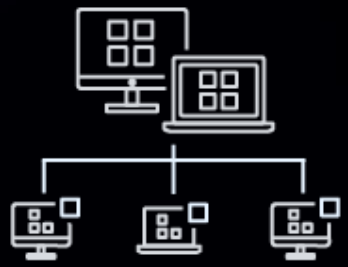


Design

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.

Independent assurance – AWS CloudTrail

AUTOMATE COMPLIANCE MANAGEMENT



Design

Control design and control evaluation

AWS CloudTrail
Track user activity and detect unusual API usage

Record
Record activity in AWS services as AWS CloudTrail events

Store
AWS CloudTrail delivers events to AWS CloudTrail console, Amazon S3 buckets, and optionally, Amazon CloudWatch logs

Act
Use Amazon CloudWatch events and alarms to take action when important events are detected

Review
View recent events in the AWS CloudTrail console or analyze log files with Amazon Athena

Compliance auditing

Operational troubleshooting

Security analysis

Automatic compliance remediation

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

Independent assurance – Audit manager



Assess

Control effectiveness assessment

AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance

Review, customize, or create framework

Review prebuilt frameworks and included controls, customize an existing framework, or define your own

Select a prebuilt or custom framework

Use a prebuilt framework or select your customized framework to begin an assessment

Define the scope of the assessment

Specify the accounts and services in scope in a Region for assessments

Activate assessment to continuously gather evidence

Conduct control reviews and/or delegate to resource owners to validate

Generate audit-ready reports

Assessment reports with links to evidence

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

Hands-on labs – Overview

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

Hands-on labs – Compliance at scale

Enable AWS Config Recorder with AWS CloudFormation StackSets

- Setup AWS Config recording in multiple regions

Setup AWS Config multi-account, multi-region data aggregation

- Setup AWS Config aggregation from multiple regions

AWS Config deploy custom conformance pack with AWS CloudFormation StackSets

- Deploy conformance packs (config rules mapped to frameworks) across multiple regions

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

Hands-on labs – Enable risk management

Using Open Policy Agent (OPA) to create AWS Config rules

- Write custom config rules in a declarative query language

Prescriptive compliance with service catalog and config

- Standardize compliance deployments in AWS

Visualizing AWS Config data using Amazon Athena and Amazon QuickSight

- Create dashboards in Quicksight to visualize AWS Config data

Using DevOps for continuous compliance in AWS Organizations

- Build and deploy compliance as code in your organization

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

Hands-on labs – Independent assurance

Automated remediations for CIS benchmarks using AWS Security Hub

- Deploy automated remediations for CIS violations detected by AWS Security Hub

Transform config conformance packs to audit manager assessments

- Extend audit assurance in AWS and convert conformance packs into audit manager assessments

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

References

- Webinar – Cloud Compliance and Assurance
- DevSecOps for auto-healing PCI compliance in AWS
- AWS Reference Solution - Cloud Compliance and Assurance
- Visualize AWS Config data using Amazon Athena and Amazon QuickSight
- Standardize compliance in AWS using DevOps and a Cloud Center of Excellence (CCOE) approach
- Automate configuration compliance at scale in AWS
- Integrate across the Three Lines Model



aws

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

Let’s get started . . .

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

Workshop

https://bit.ly/3FZ8vnk

Event Hash: 815a-16beeac4c4-0d

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

References

Next Steps



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

Thank you!

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