AWS re:Invent

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

COP301

Cloud compliance, assurance, and auditing

Andres Silva
Principal SA Cloud Operations
Amazon Web Services

Kaartik Viswanath
Sr. Software Dev Manager, AWS Config
Amazon Web Services

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

Agenda

- Challenges with compliance
- The Three Lines Model
- Managing risk
- Overseeing risk
- Assurance of risk management
- Key takeaways

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

Meet Ed



- Just hired as a cybersecurity engineer
- New to the cloud
- Eager to learn and explore
- Responsible for implementing compliance strategy

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

Challenges

- Dynamic landscape
- Pace of innovation
- Volume, variety, and velocity
- Familiarity with the cloud
- Global/ geographic
- Different compliance and security needs



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

Which one do you use for compliance?

WIDE RANGE OF AWS CAPABILITIES



AWS Config

Amazon GuardDuty

AWS Audit Manager

AWS License Manager

Amazon Inspector

AWS CloudTrail

Amazon CloudWatch

AWS Systems Manager

AWS Control Tower

Amazon Macie

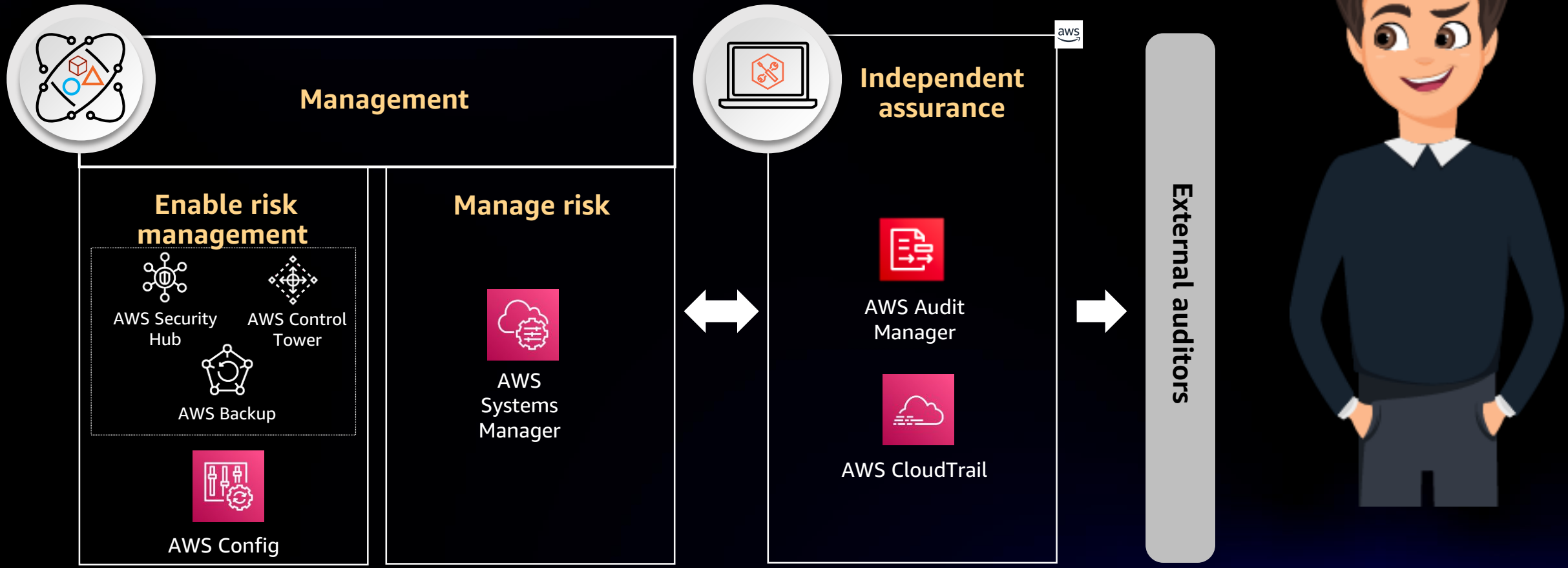
AWS Artifact

aws

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

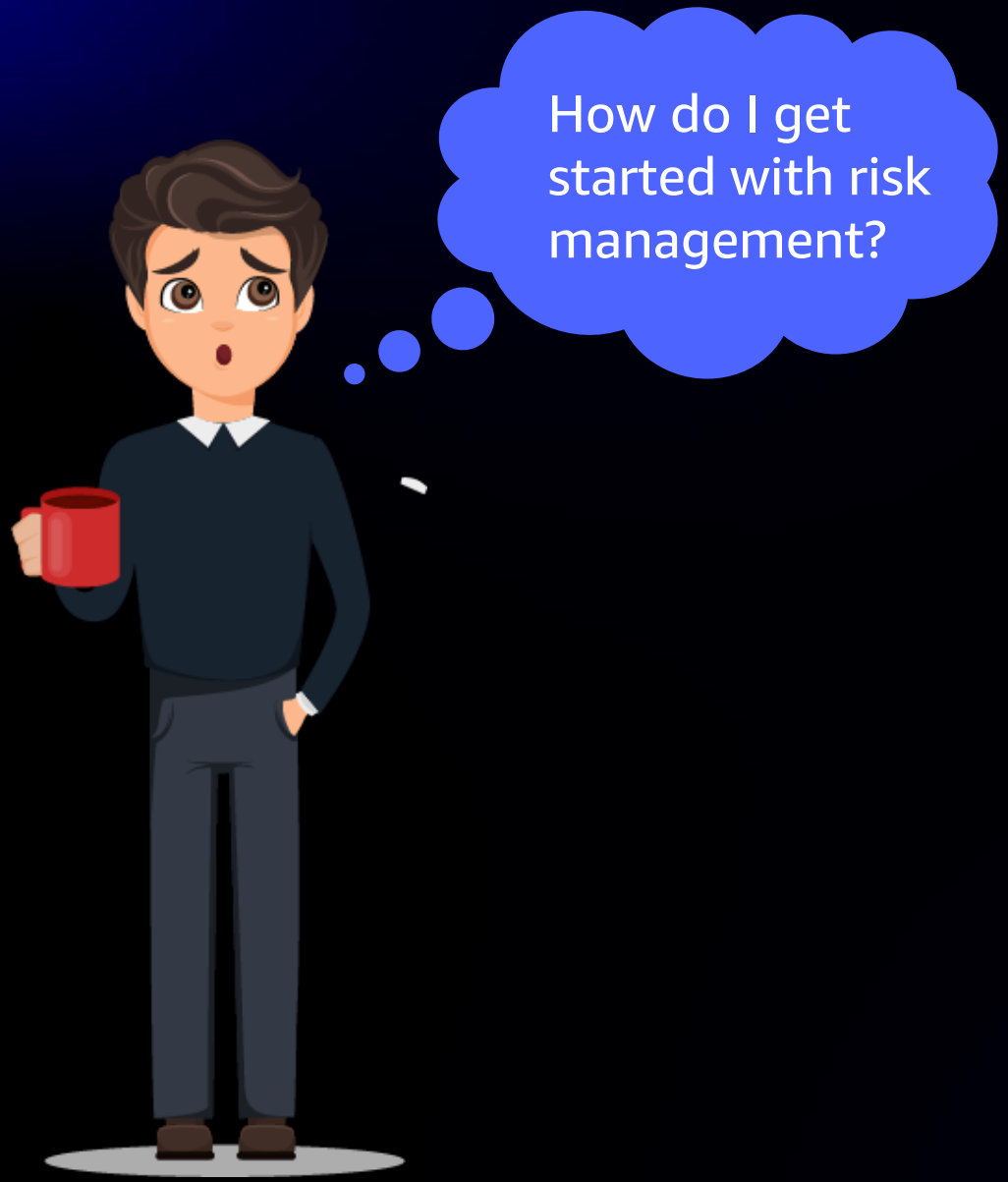
How AWS enables cloud compliance and assurance

THE IIA'S THREE LINES MODEL



IIA = Institute of Internal Auditors

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

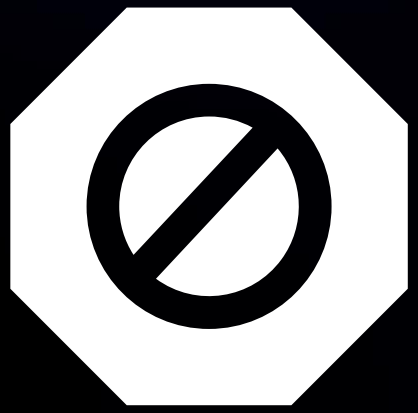


- Use AWS Control Tower – it's the right place to start
- Automate, automate, automate
- Compliance as code
- Establish preventive and detective controls



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

Manage risk – Define controls



Preventive controls



Detective controls

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

Manage risk – Preventive controls

Manage



AWS Organizations service control policies



AWS Identity and Access Management (IAM)



AWS Control Tower

Provision



AWS CloudFormation

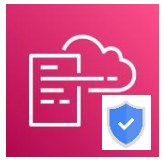


AWS Service Catalog



Terraform

Compliance



AWS CloudFormation Guard



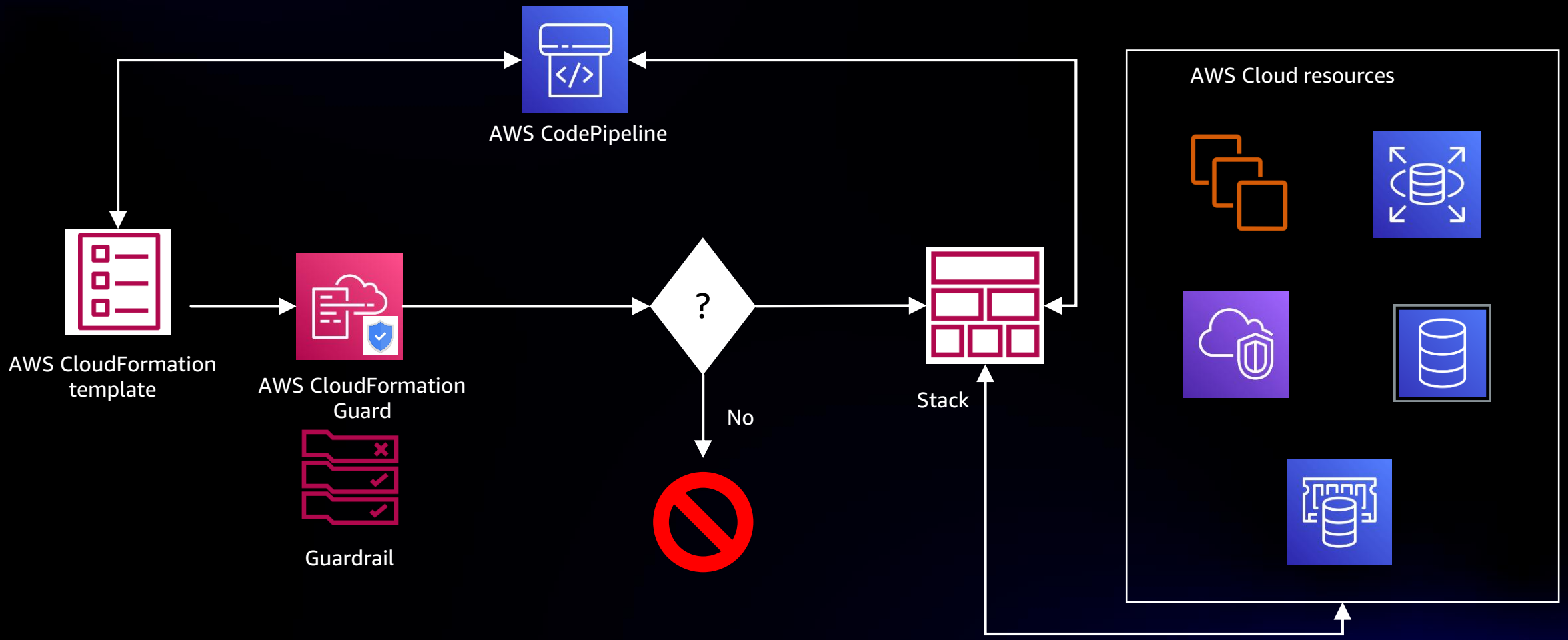
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Manage risk – AWS CloudFormation Guard

```
AWS::EC2::Volume {
    Properties {
        Encrypted == true
        Size <= 10
        VolumeType == 'gp2' OR
        VolumeType == 'gp3'
        AvailabilityZone == 'us-west-2b' OR
        AvailabilityZone == 'us-west-2c'
    }
}
```

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

Manage risk – AWS CloudFormation Guard



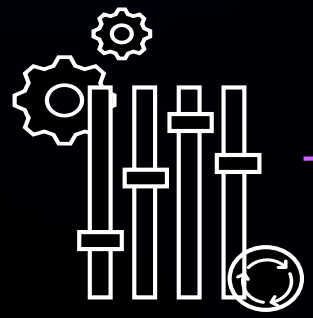
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Manage risk – AWS Config

ACCESS, AUDIT, AND EVALUATE



Access, audit, and evaluate



Configuration change occurs in your AWS resources

AWS Config

Records and normalizes the changes into a consistent format

Rules and conformance packs evaluate compliance

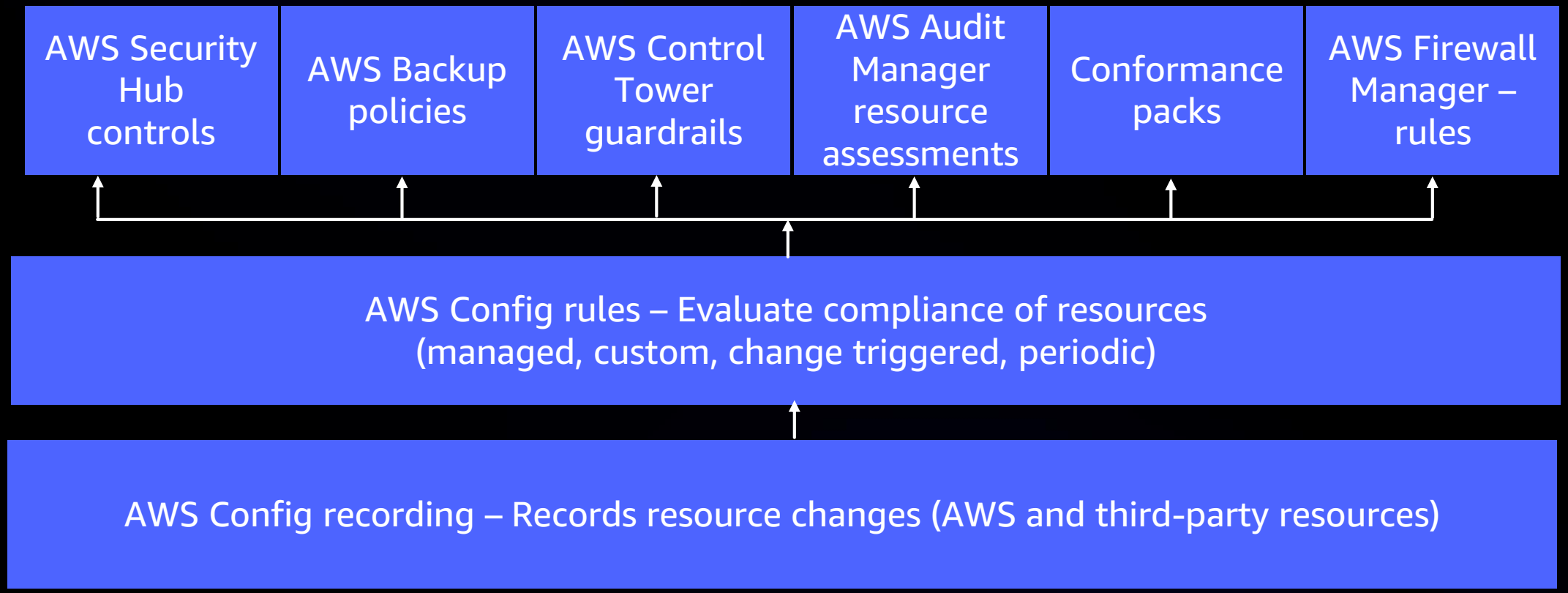
Sample conformance packs to get started: CIS, CMMC, FedRAMP, NIST, PCI, HIPAA, and more

- **AWS Config APIs and console**
- **Amazon SNS**
- **Amazon CloudWatch**
- **Amazon S3**

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

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

AWS Config – Core for compliance evaluations



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

Manage risk – Conformance packs

- A single ARN-able entity called a conformance pack
- Deploy the pack from the delegated admin account
- Create immutable rules
- Process check rules
- Simplify reporting
- Sample conformance pack templates

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

Manage risks – Detective controls

- AWS Config rules
  - Continuous compliance
  - Periodic audits
- Conformance pack
  - Scenario-based deployments
  - Configuration item for overall conformance pack compliance status
  - Security Hub standards vs. conformance packs

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

I get it . . .
I need to learn more about AWS Config.



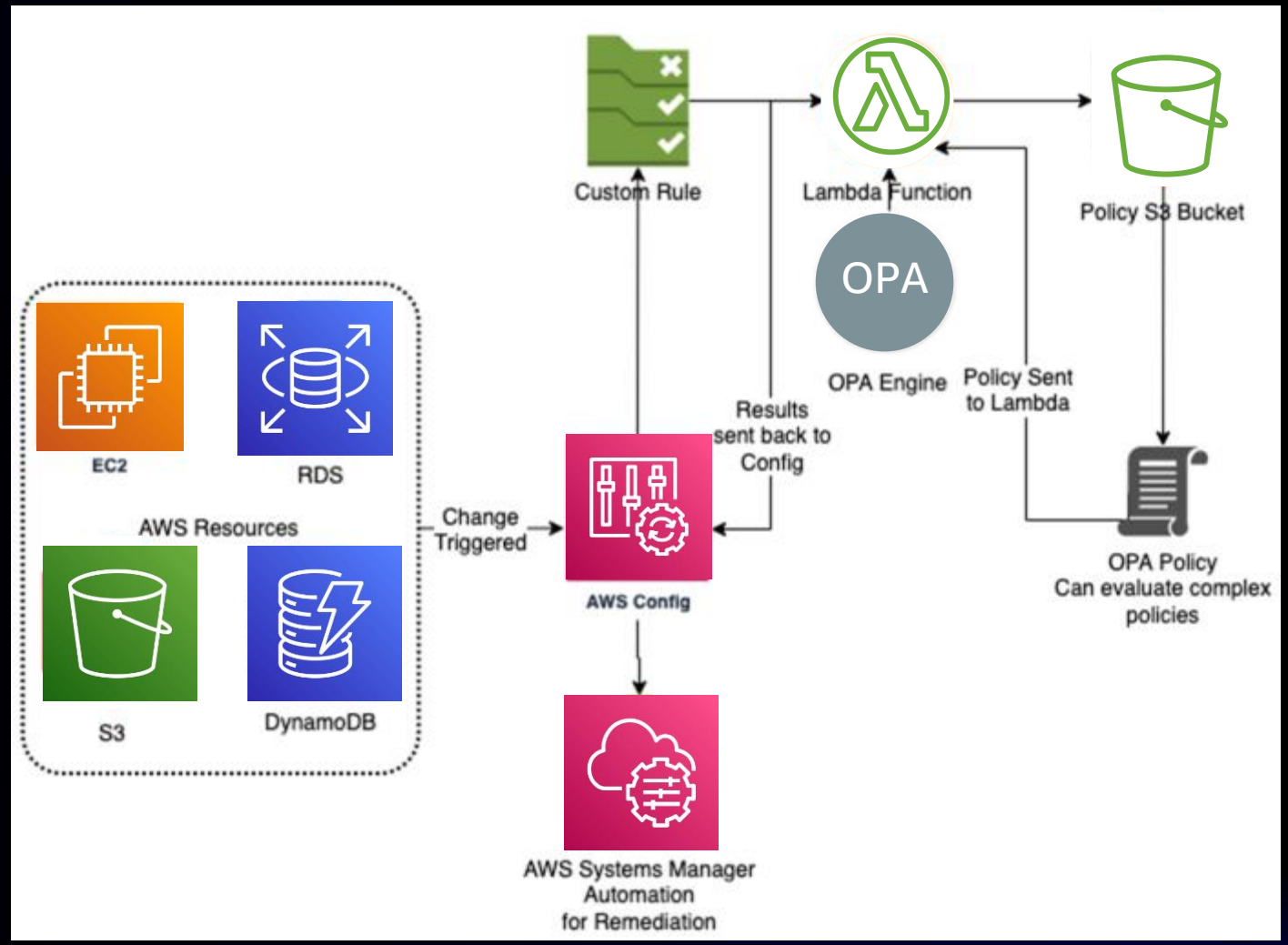
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config – Recent launches

- Recording – AWS KMS encryption support on Amazon S3 buckets
- Rules – New managed rules
- Conformance packs
  - Overall conformance packs compliance status
  - Conformance packs compliance as CI
- Aggregators
  - Support for conformance packs, conformance packs compliance status
- Advance query
  - Saved query
  - Pagination support

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

Manage risk – AWS Config and OPA



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

Manage risk – AWS Systems Manager

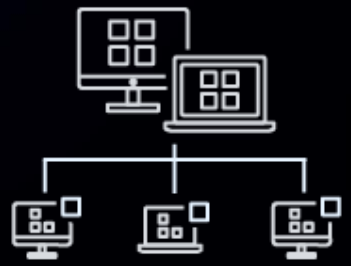
AUTOMATE COMPLIANCE MANAGEMENT



Operations hub for AWS

AWS 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



Quick setup



Automation



Run command



Inventory and patch manager

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

Manage risk – 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

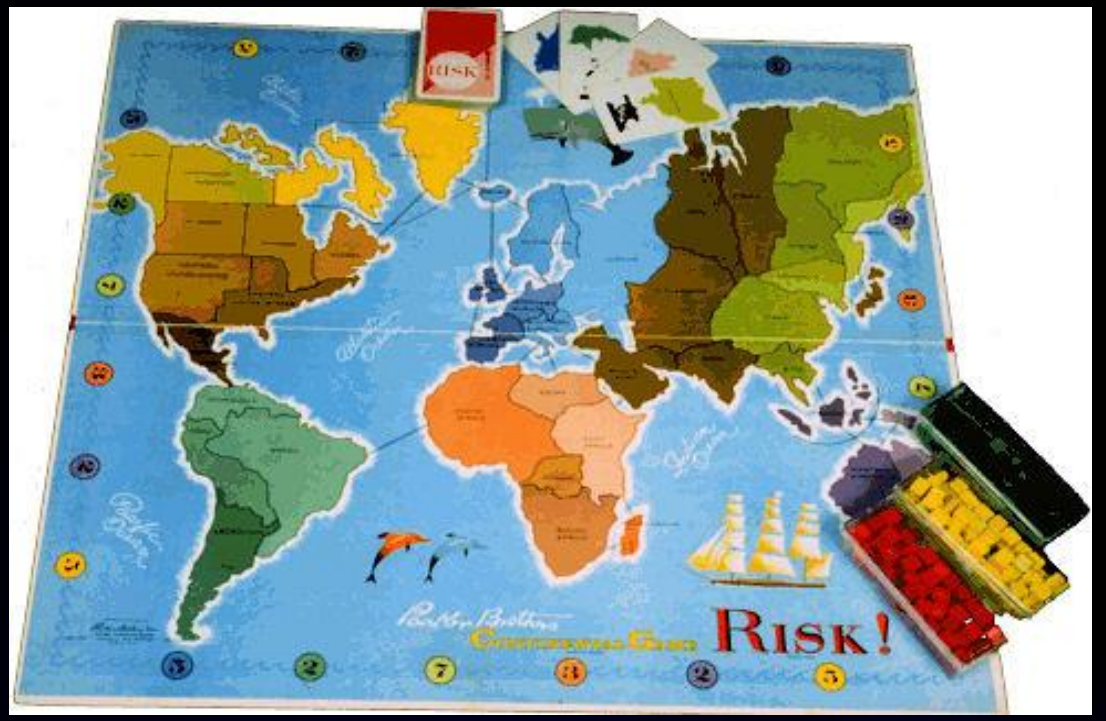
Operational troubleshooting

Security analysis

Automatic compliance remediation

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

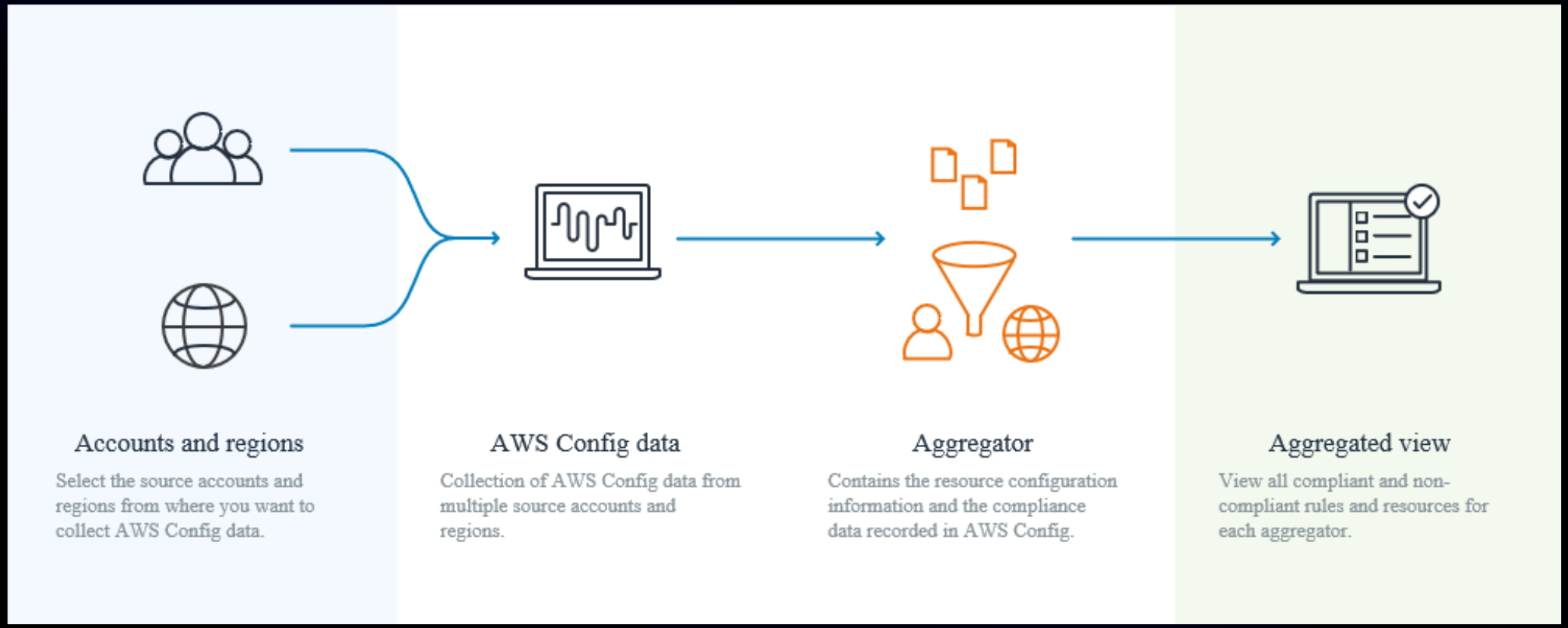




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Oversee risk – AWS Config

Implement continuous oversight



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

Oversee risk – AWS Security Hub

Implement continuous oversight



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
- AWS 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.





Auditor

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

Assurance of risk management – AWS Audit Manager



Assess

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.



Key takeaways

01

3 lines model

Helps you identify the right AWS service(s) for the right job

02

AWS Config is the core of compliance evaluations

AWS Config powers many other compliance features on AWS

03

Wide range of options for compliance

AWS offers a wide range of capabilities to help simplify cloud compliance and assurance

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

Resources



Cloud compliance and assurance samples



Cloud operations samples GitHub repo

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

Thank you!

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