Cloud compliance, assurance, and auditing

Andres Silva

Principal SA Cloud Operations
Amazon Web Services

Agenda

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

AWS Cloud Ops is fast and secure, built at cloud scale from the beginning

AWS Cloud Ops

GOVERNANCE

Security

Compliance

Operations

Spend management

AGILITY

Automated

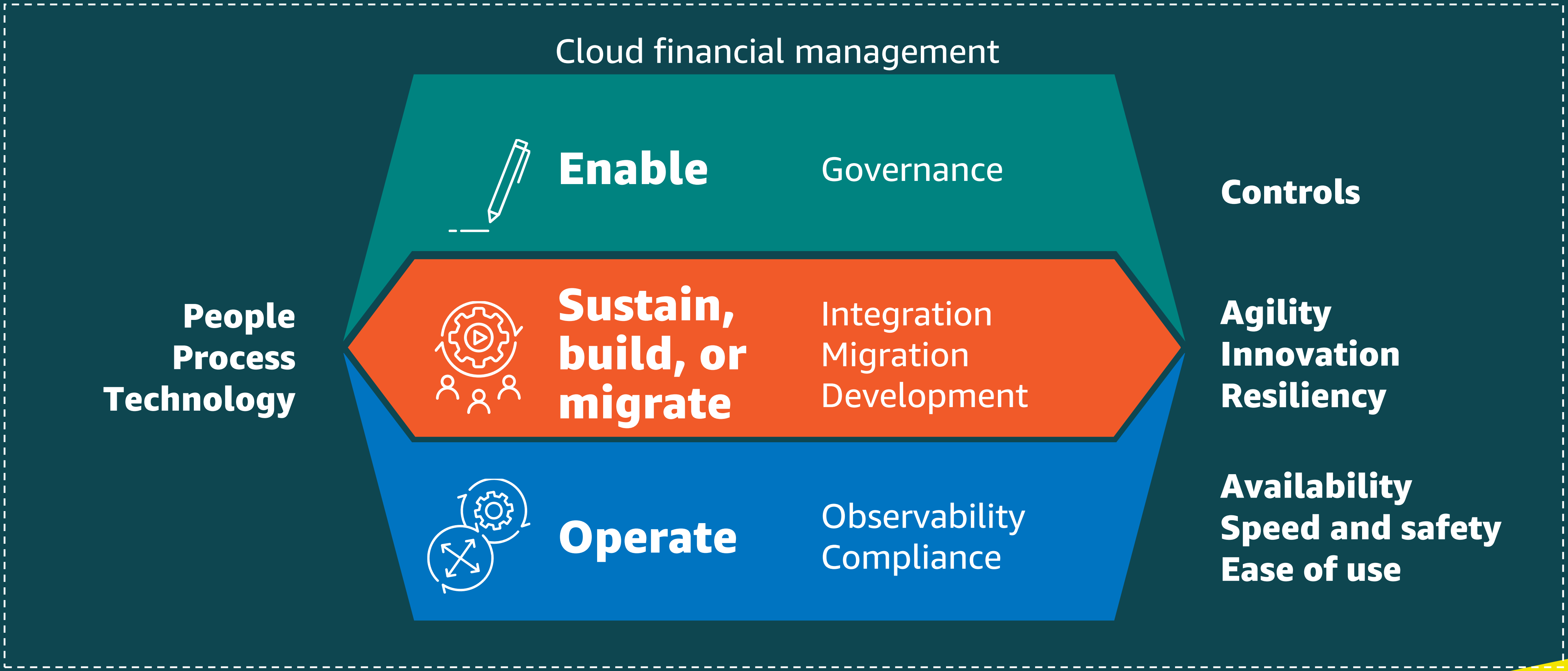
Self-service access

Experiment fast

Respond quickly to change

AWS Cloud Ops model

Speed up innovation by delivering operational outcomes in the cloud, on premises, and at the edge



Cloud financial management

People
Process
Technology

Enable Governance

Sustain, build, or migrate Integration
Migration
Development

Operate Observability
Compliance

Controls

Agility
Innovation
Resiliency

Availability
Speed and safety
Ease of use

Automation and security

Meet Ed

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

Challenges

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

Which one do you use for compliance?

- Wide range of AWS capabilities

AWS Config

Amazon GuardDuty

AWS Audit Manager

AWS CloudTrail

Amazon CloudWatch

Amazon Macie

AWS License Manager

Amazon Inspector

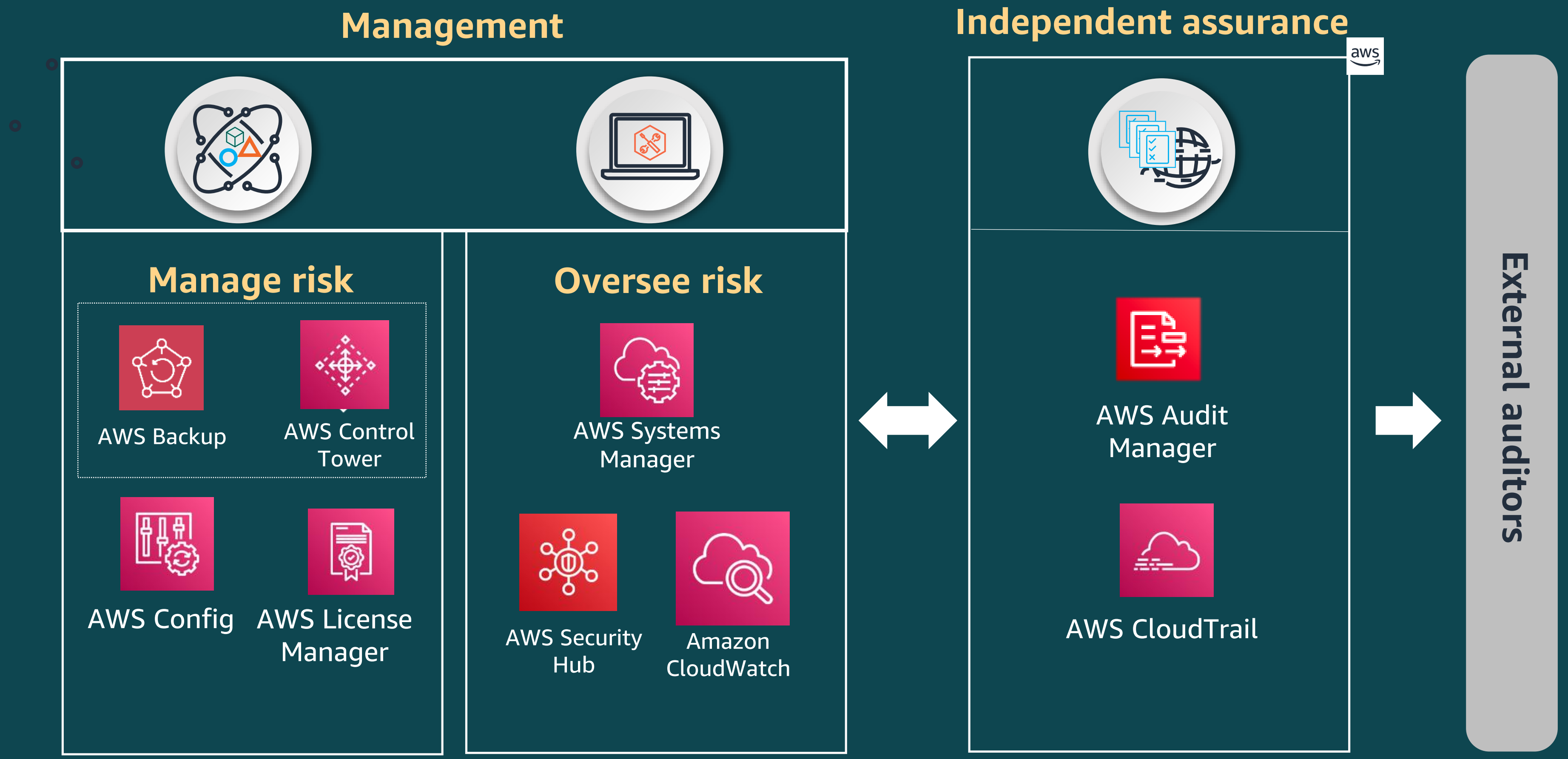
AWS Systems Manager

AWS Control Tower

AWS Artifact

How AWS enables cloud compliance and assurance

- The IIA’s three lines model



Management

Manage risk

AWS Backup

AWS Control Tower

AWS Config

AWS License Manager

Oversee risk

AWS Systems Manager

AWS Security Hub

Amazon CloudWatch

Independent assurance

AWS Audit Manager

AWS CloudTrail

External auditors

IIA = Institute of Internal Auditors

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

Manage risk – Define controls

Preventive controls

Detective controls

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

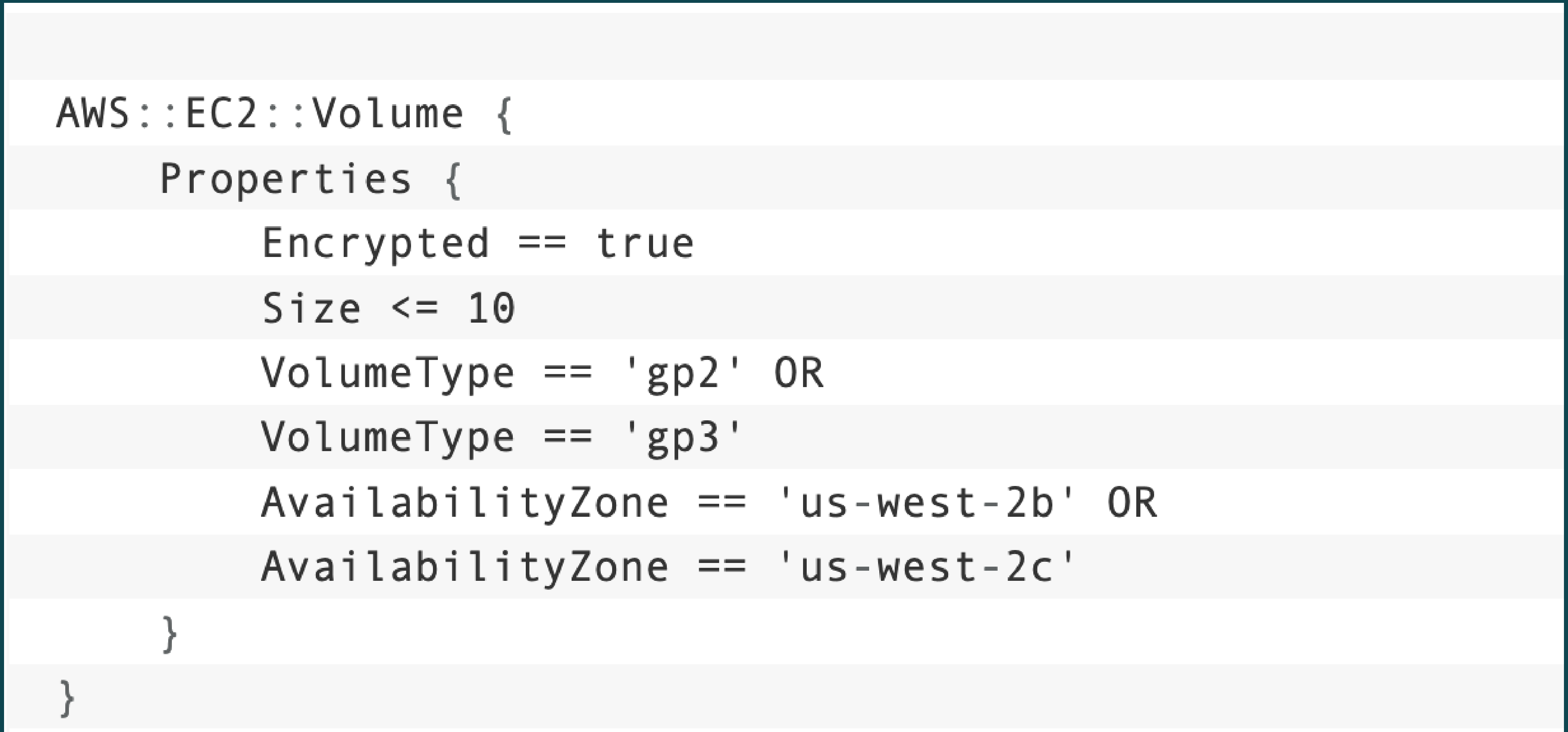
Compliance

AWS CloudFormation Guard

OPA

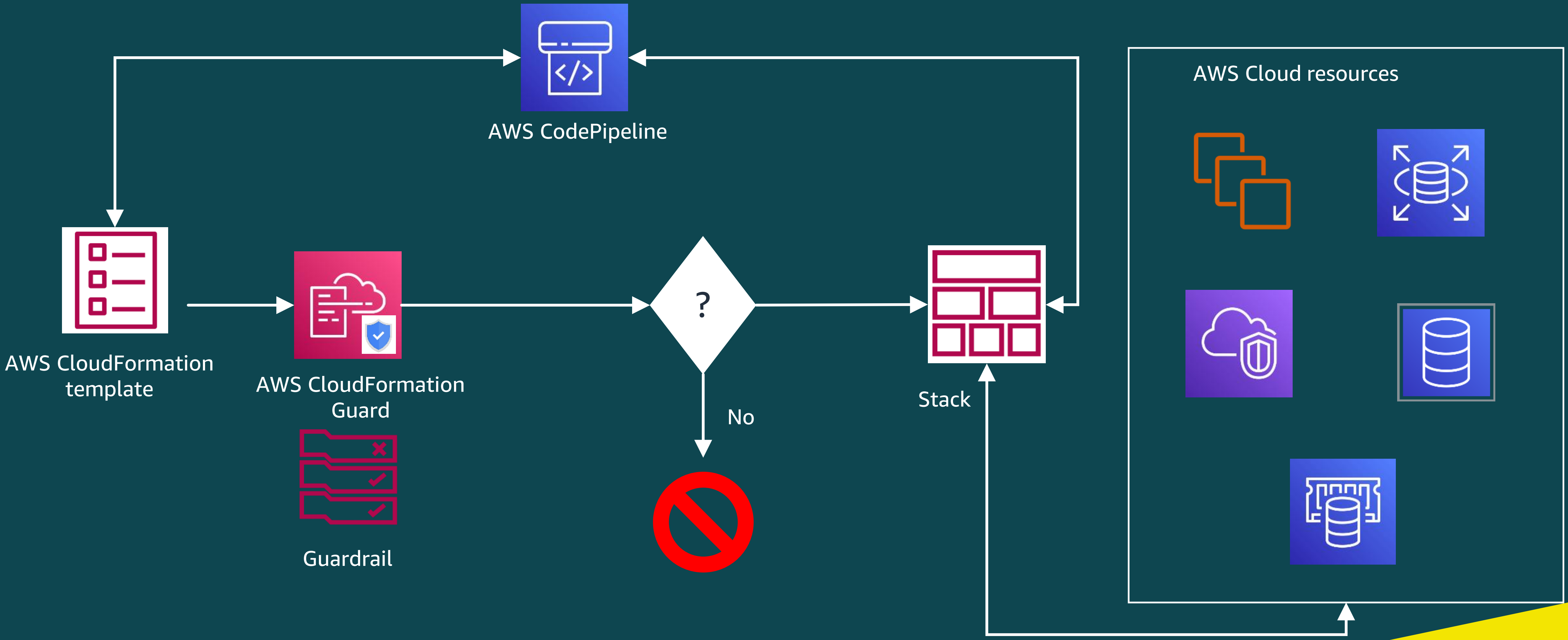
Open Policy Agent

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'
    }
}
```

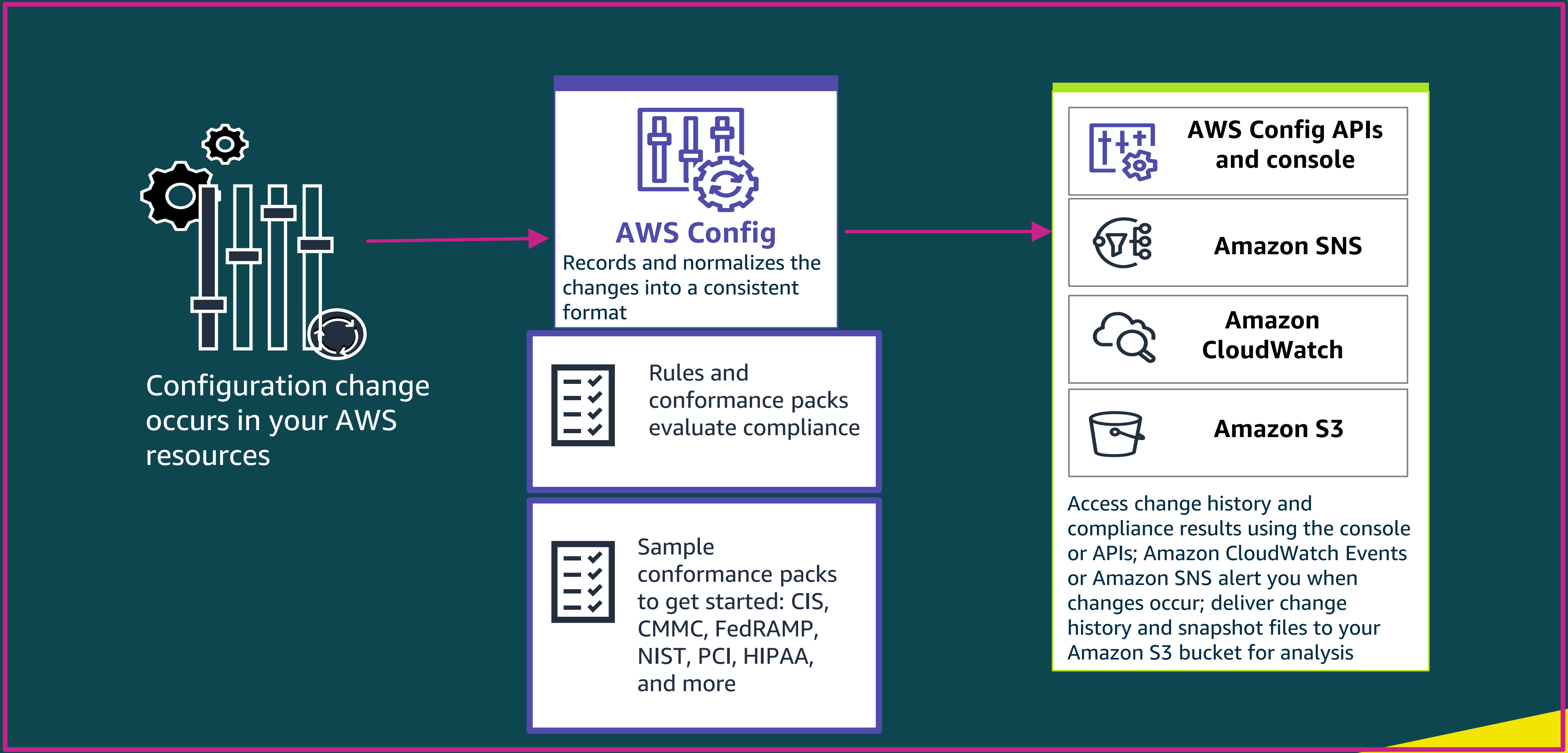
Manage risk – AWS CloudFormation Guard



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

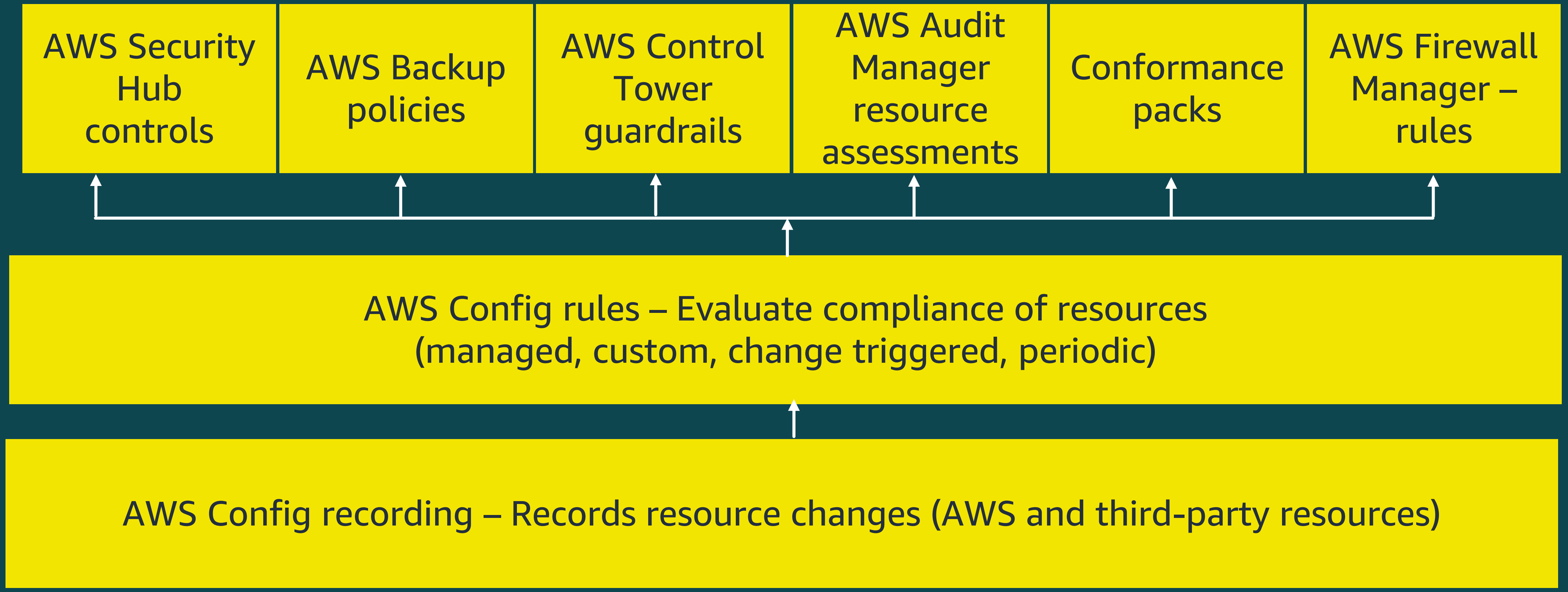
Amazon SNS

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

AWS Config – Core for compliance evaluations



AWS Security Hub controls

AWS Backup policies

AWS Control Tower guardrails

AWS Audit Manager resource assessments

Conformance packs

AWS Firewall Manager – rules

AWS Config rules – Evaluate compliance of resources (managed, custom, change triggered, periodic)

AWS Config recording – Records resource changes (AWS and third-party resources)

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

Manage risks – Detective controls

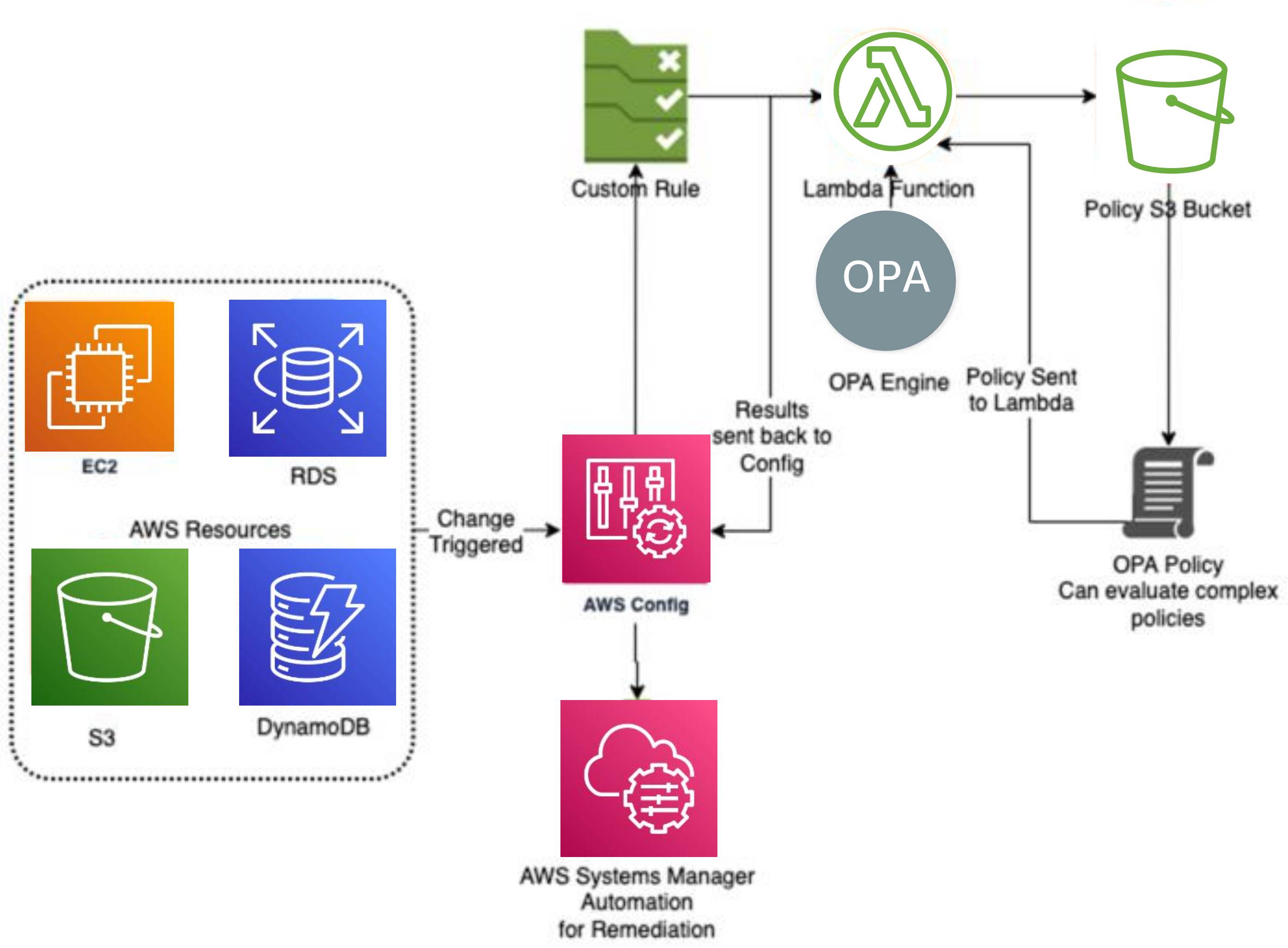
- AWS Config rules
  - Continuous compliance
  - Periodic audits
- Conformance pack
  - Scenario-based deployments
  - Configuration item for overall conformance pack compliance status
  - Security Hub standards vs. conformance packs

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

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

Manage risk – AWS Config and OPA



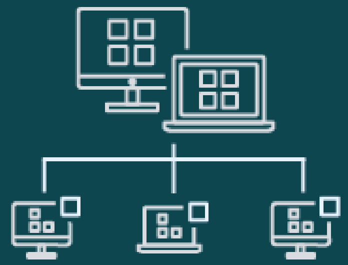
Manage risk – AWS Systems Manager

- 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

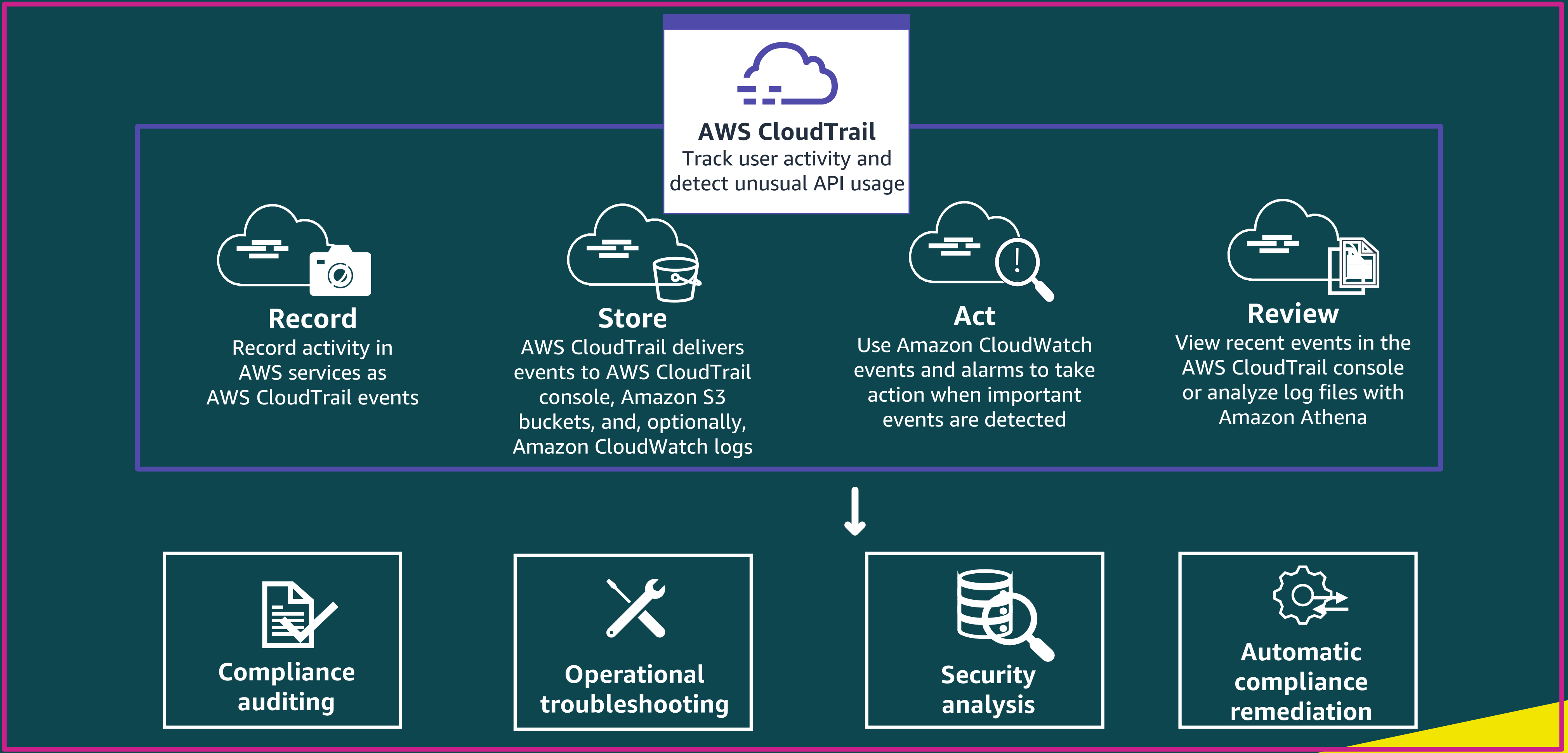
Inventory and patch manager

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

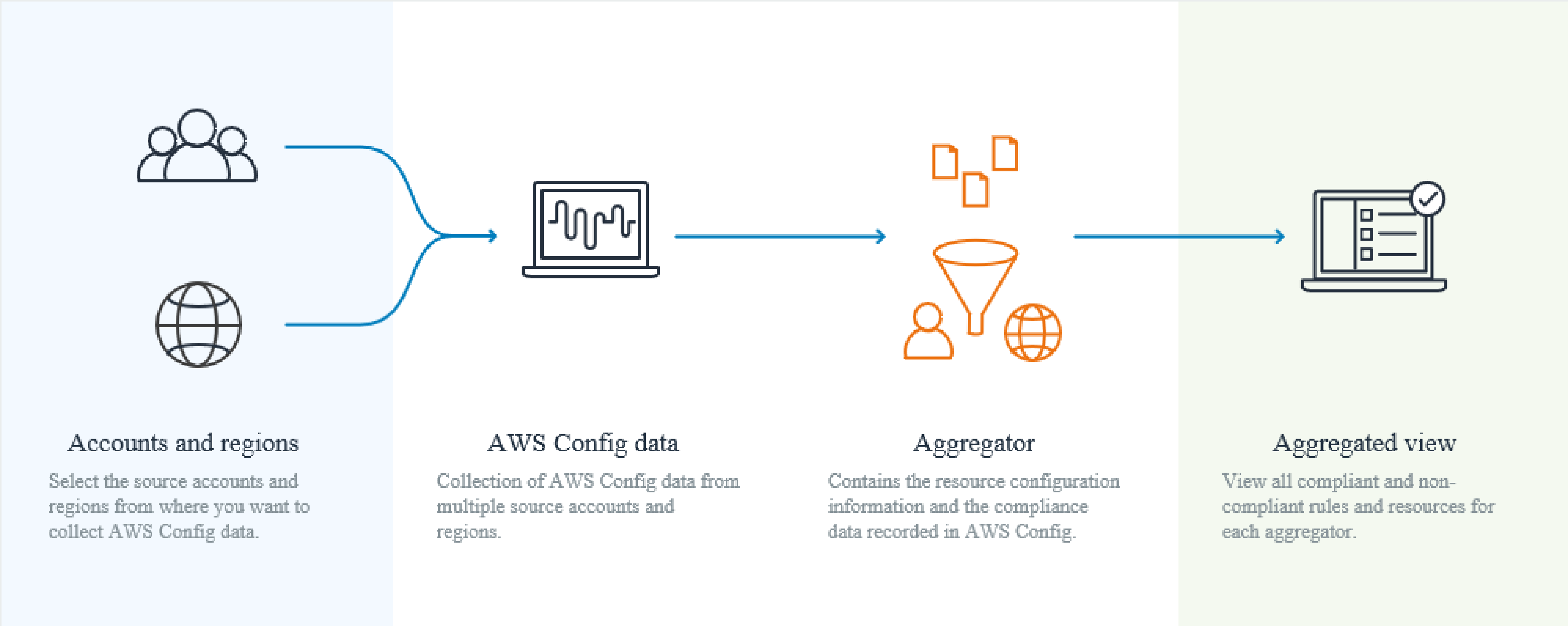
Demo

How do I get started with overseeing risk?

RISK!

Oversee risk – AWS Config

Implement continuous oversight and monitor risk



Accounts and regions

Select the source accounts and regions from where you want to collect AWS Config data.

AWS Config data

Collection of AWS Config data from multiple source accounts and regions.

Aggregator

Contains the resource configuration information and the compliance data recorded in AWS Config.

Aggregated view

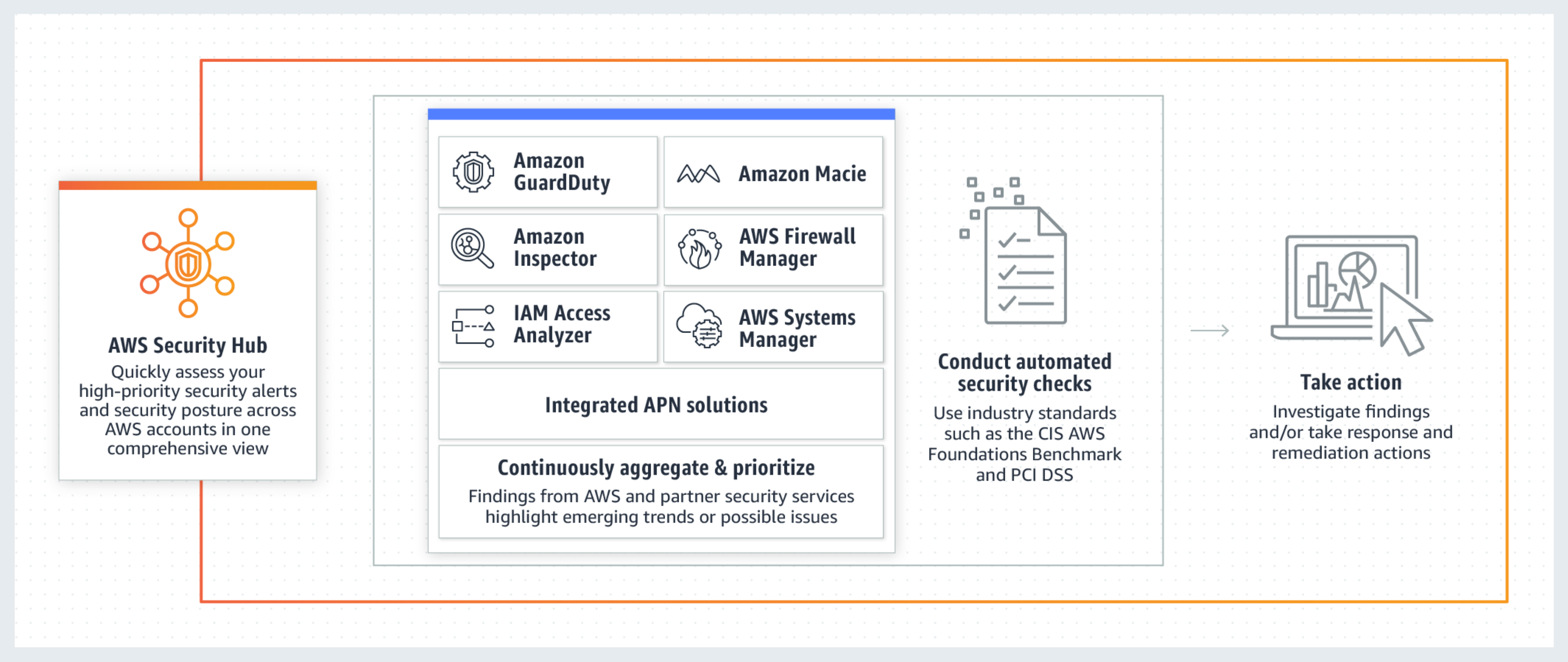
View all compliant and non-compliant rules and resources for each aggregator.

Oversee risk – AWS Security Hub

Implement continuous oversight and monitor risk

Monitor

Control effectiveness monitoring



AWS Security Hub

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

Continuously aggregate & 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 Foundations Benchmark and PCI DSS

Take action

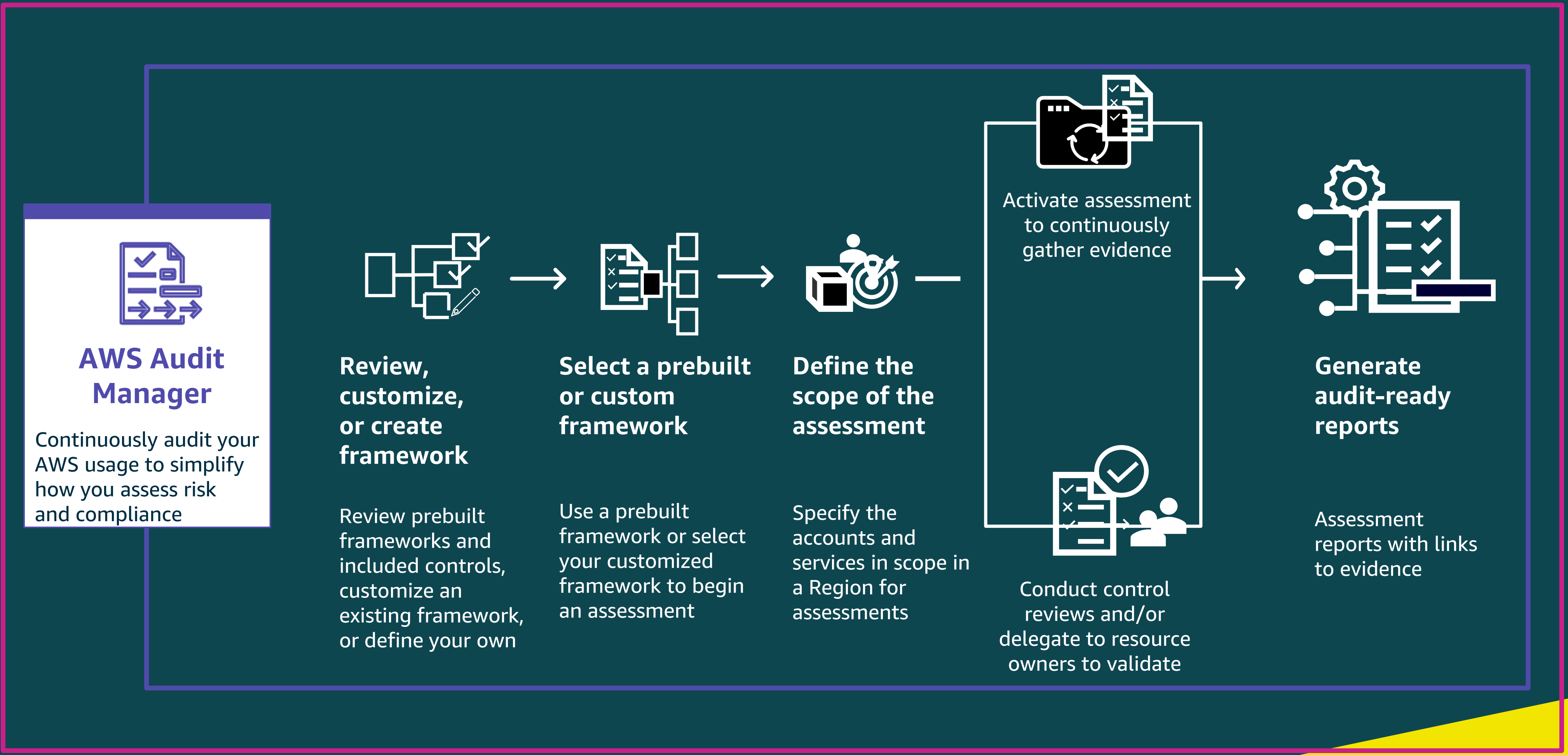
Investigate findings and/or take response and remediation actions

How do I get ready for my audits?
Auditor

Assurance of risk management – AWS 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

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

Resources

Cloud compliance and assurance samples

Cloud operations samples GitHub repo

Thank you!

Andres Silva

Principal SA Cloud Operations
Amazon Web Services