
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

STP207-R

Automating and evidencing key compliance security controls

Dani Traphagen (she/her)

Sr. Startup Solution Architect, Healthcare and Life Sciences
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- The compliance journey with bears
- 3 mental models
- Tooling
- Getting started guidance
- Customer example
- Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The compliance journey with bears



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Planning and preparation



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The situation

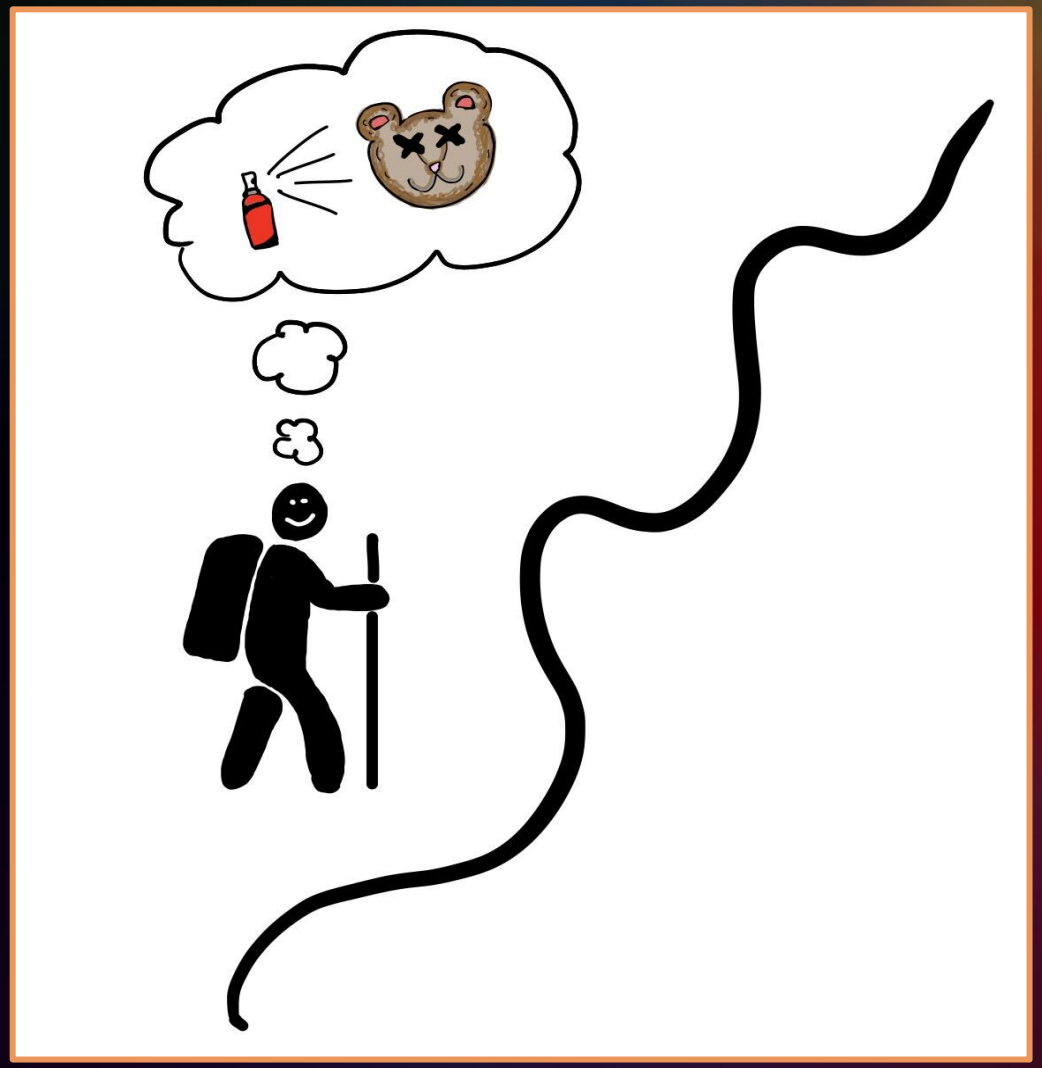


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bad things happen

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tooling



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tooling gone wrong

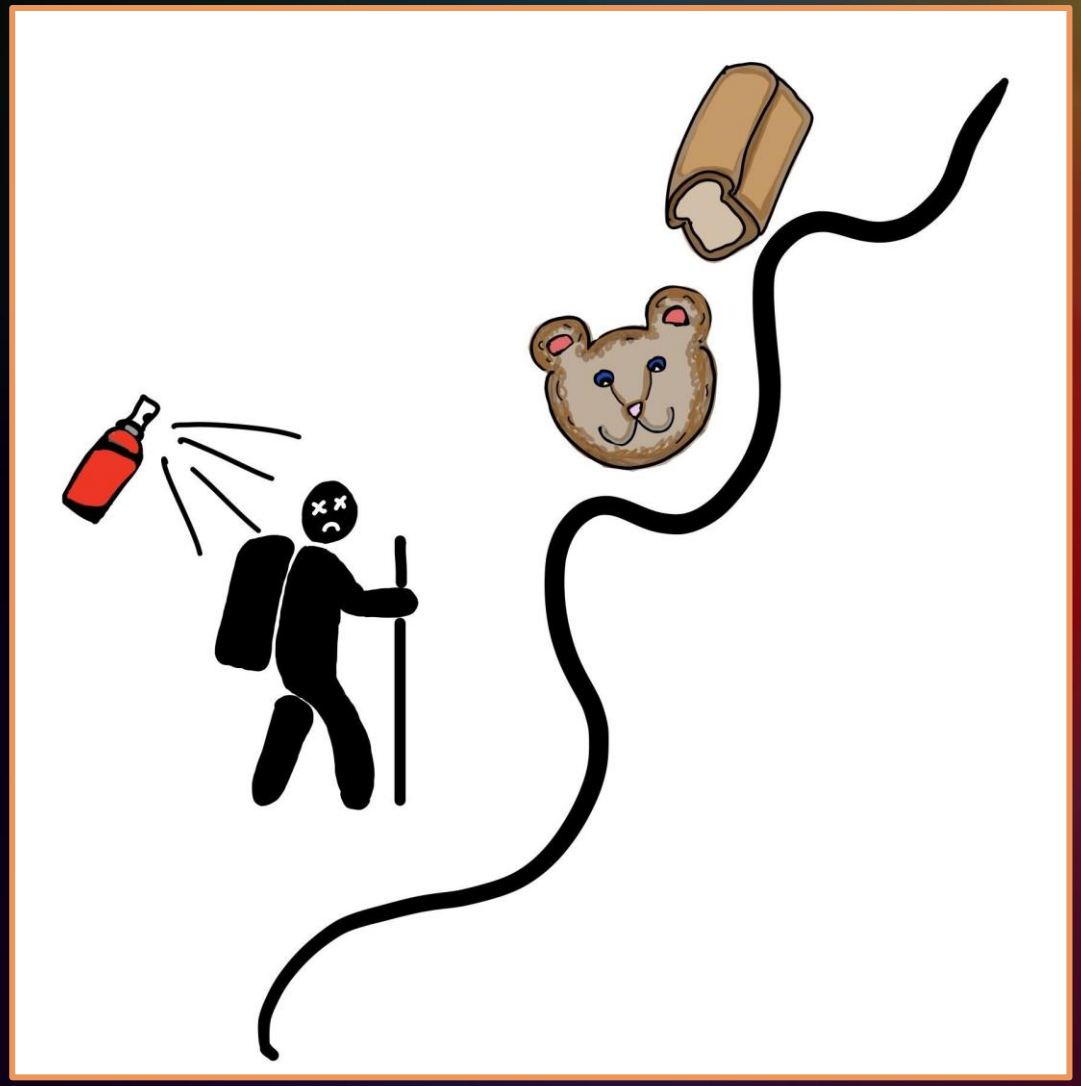


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bad things happen

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tooling gone wrong



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tooling gone wrong



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

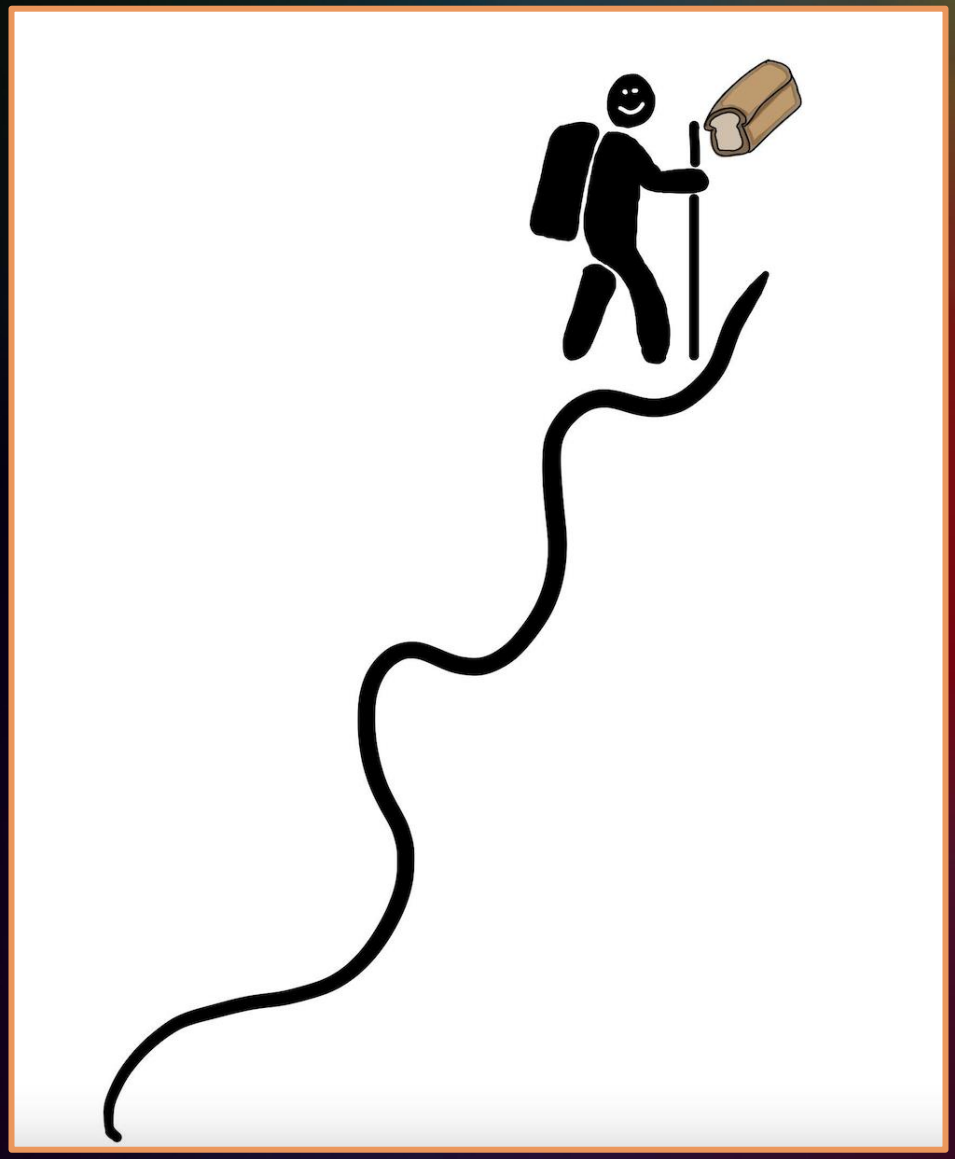
Photo credit: Leon Neal/Getty Images and OKWildlifeDept/Twitter

Tooling gone right



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Success!



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Good things happen

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common challenges with cloud compliance

1. 3 Vs
2. Cloud aptitude
3. Global distribution
4. Rate of innovation
5. Dynamic compliance needs
6. Choosing the right tools

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sheesh, there sure are a lot of tools...



Identity and access management

AWS Identity and Access Management (IAM)

AWS IAM Identity Center

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager



Detection

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender



Infrastructure protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF – Web application firewall

Amazon Virtual Private Cloud (Amazon VPC)

AWS PrivateLink

AWS Systems Manager



Data protection

Amazon Macie

AWS Key Management Service (AWS KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Amazon S3 server-side encryption



Incident response

Amazon Detective

AWS Elastic Disaster Recovery

AWS Config Rules

AWS Lambda



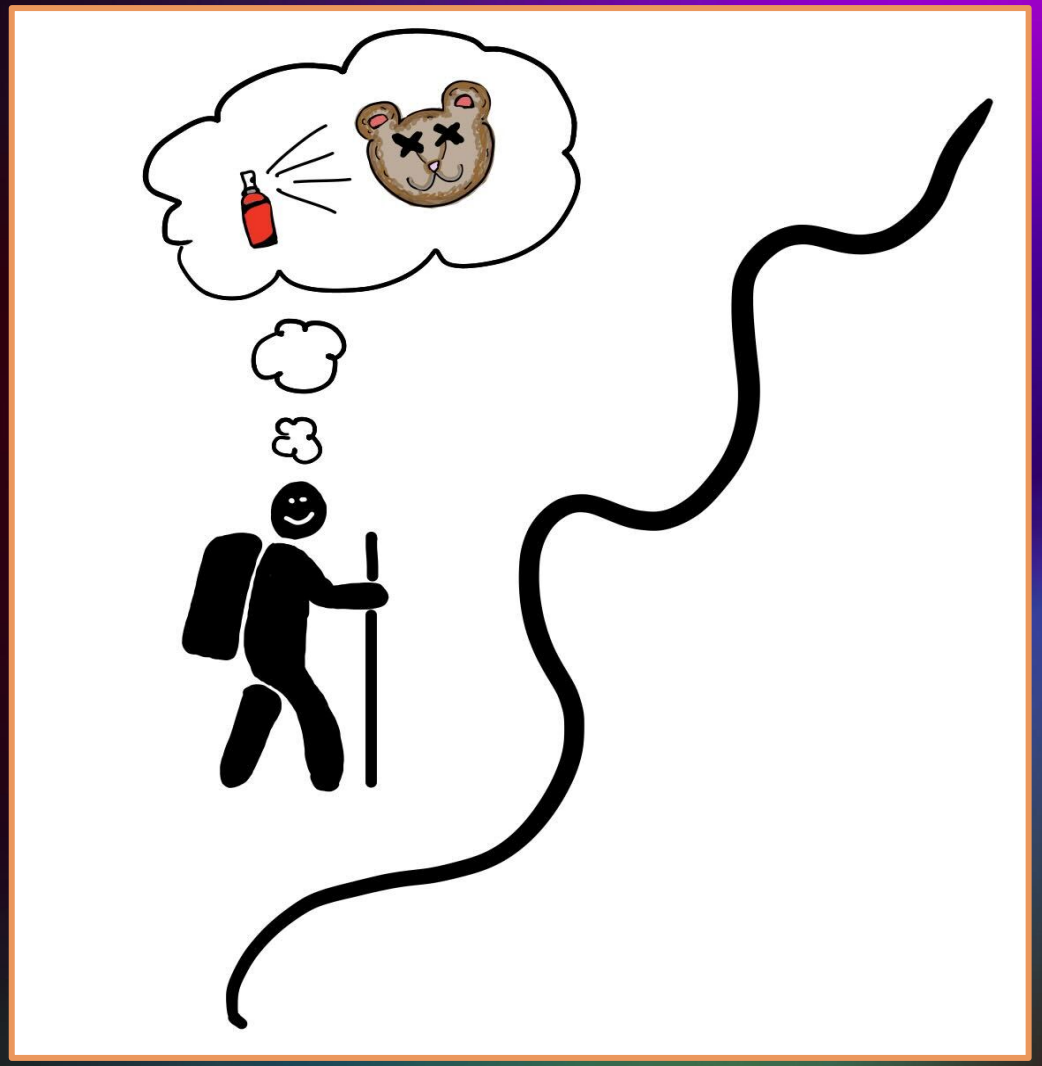
Compliance

AWS Artifact

AWS Audit Manager

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mental models



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

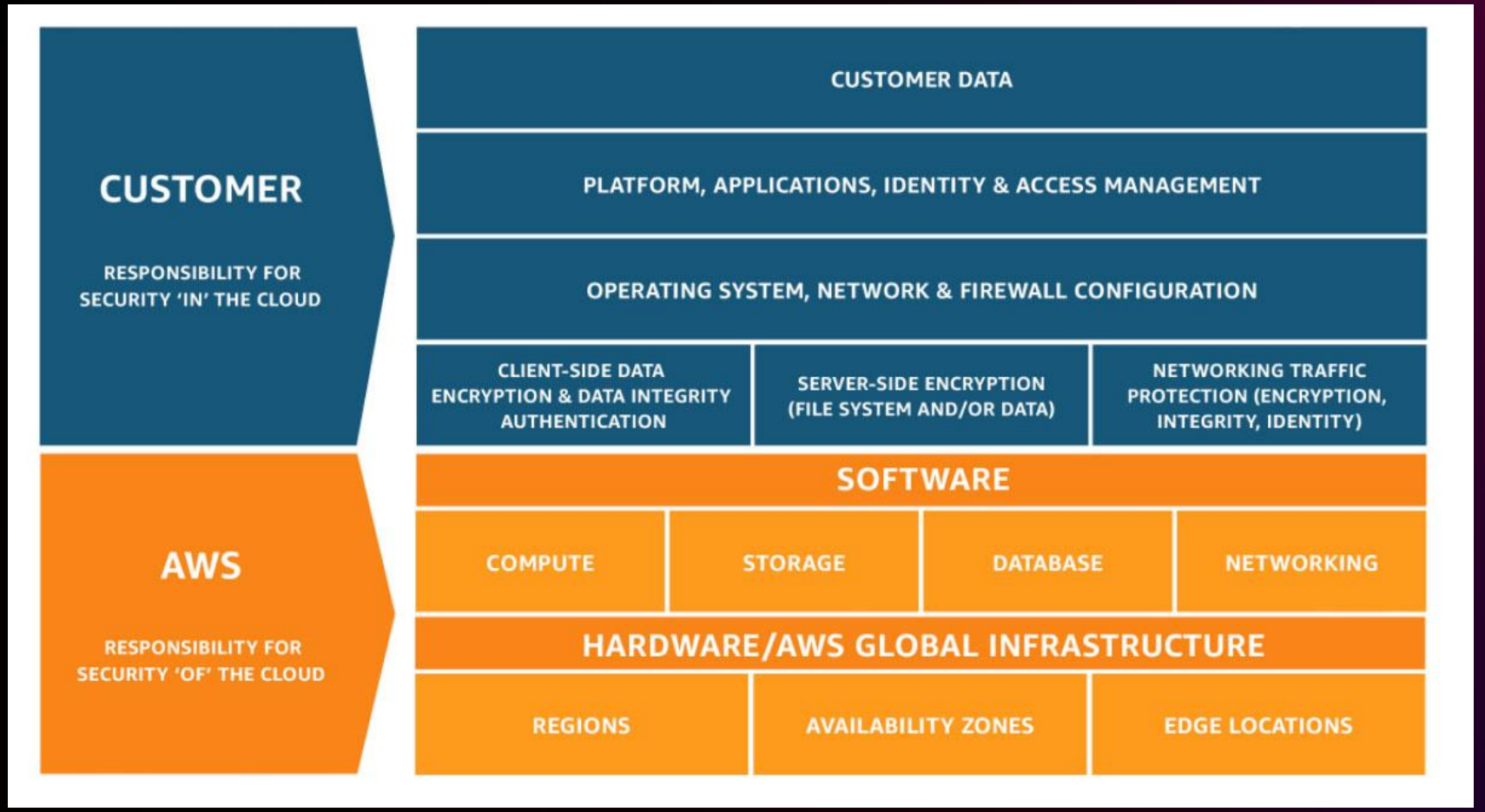
How to think about compliance on AWS

1. We need mental models for compliance
2. We need a plan for risk management
3. We need the support of tooling to:
    - Automate
    - Monitor
    - Evidence

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mental models

SHARED RESPONSIBILITY MODEL



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mental models

THE WELL-ARCHITECTED FRAMEWORK

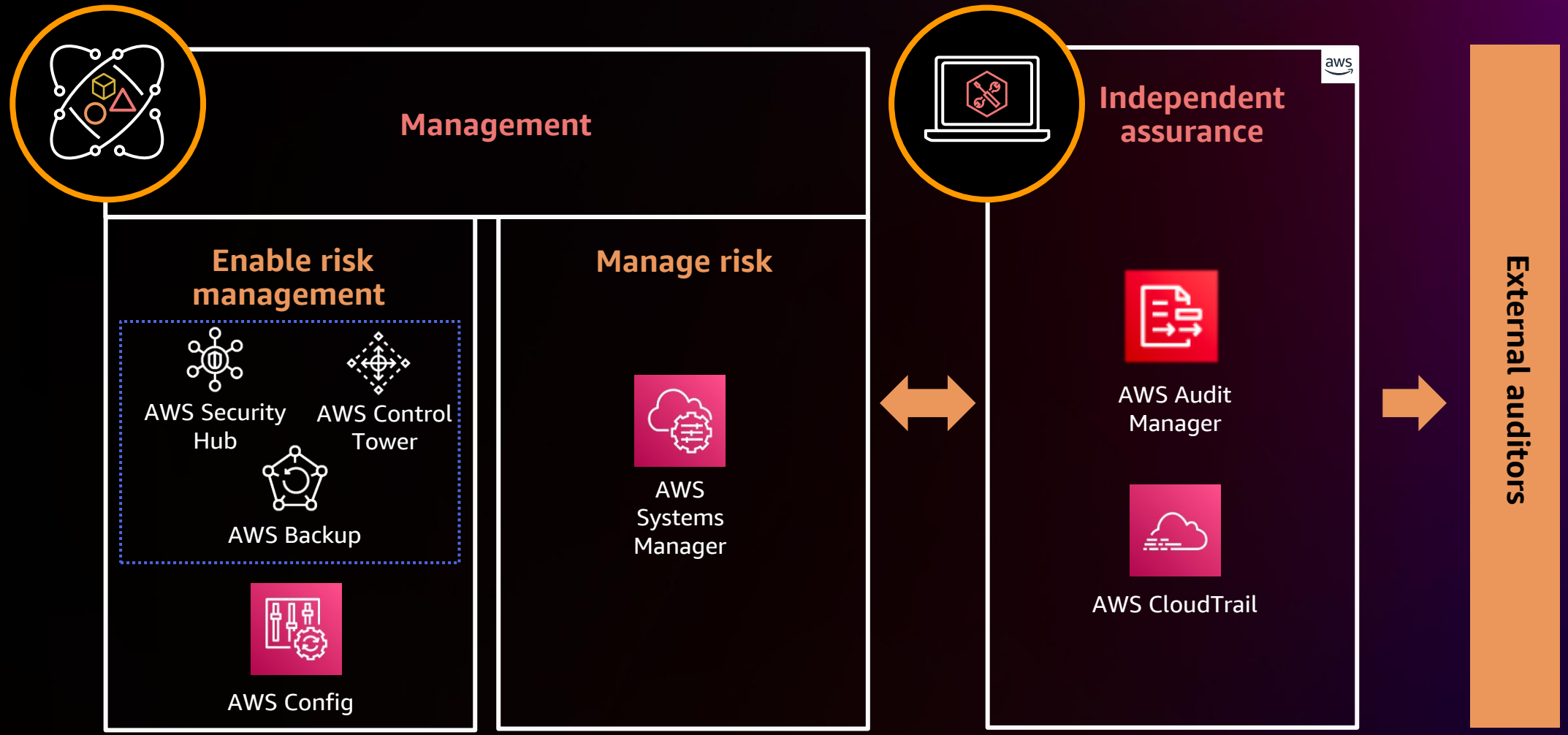


aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mental models

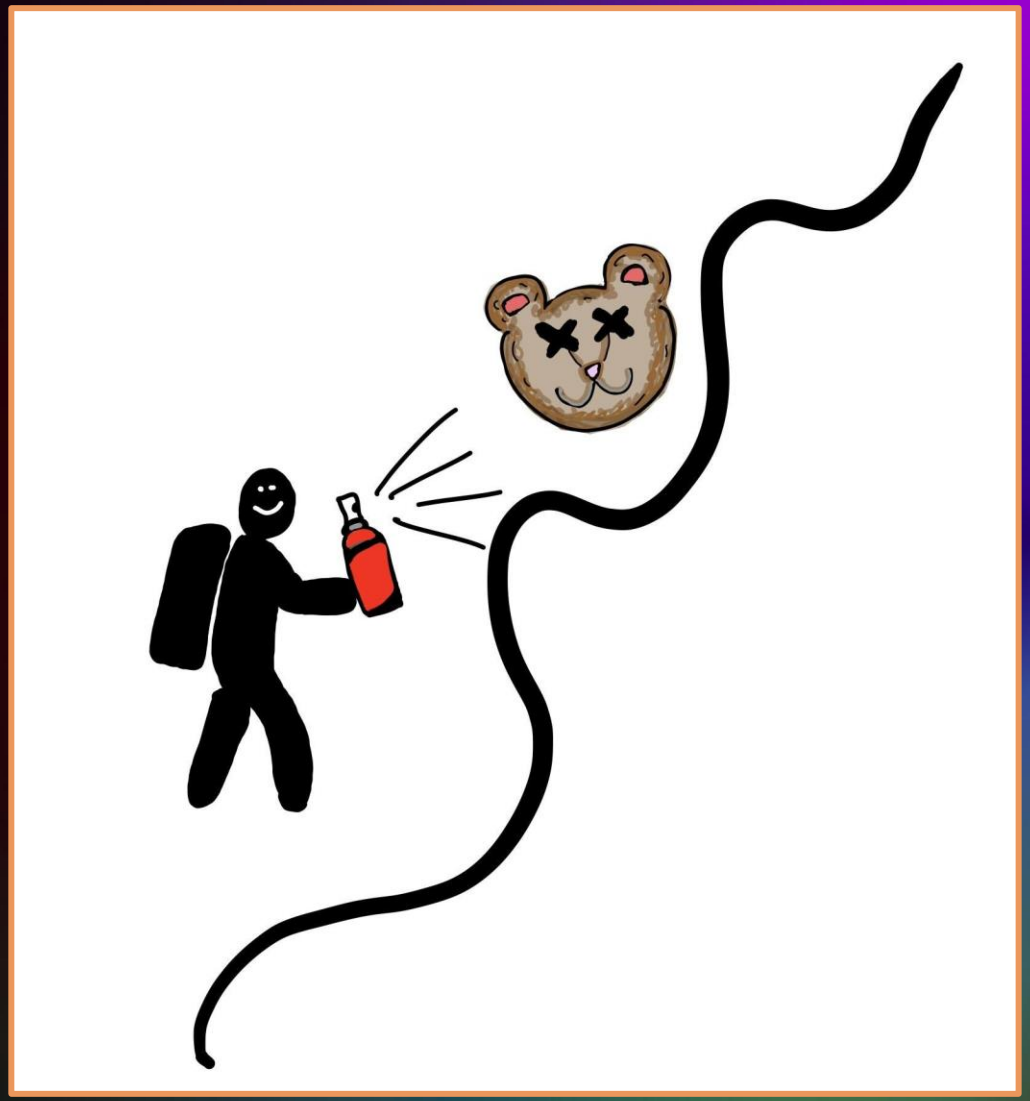
THE IIA'S "THREE LINES MODEL"



IIA = Institute of Internal Auditors

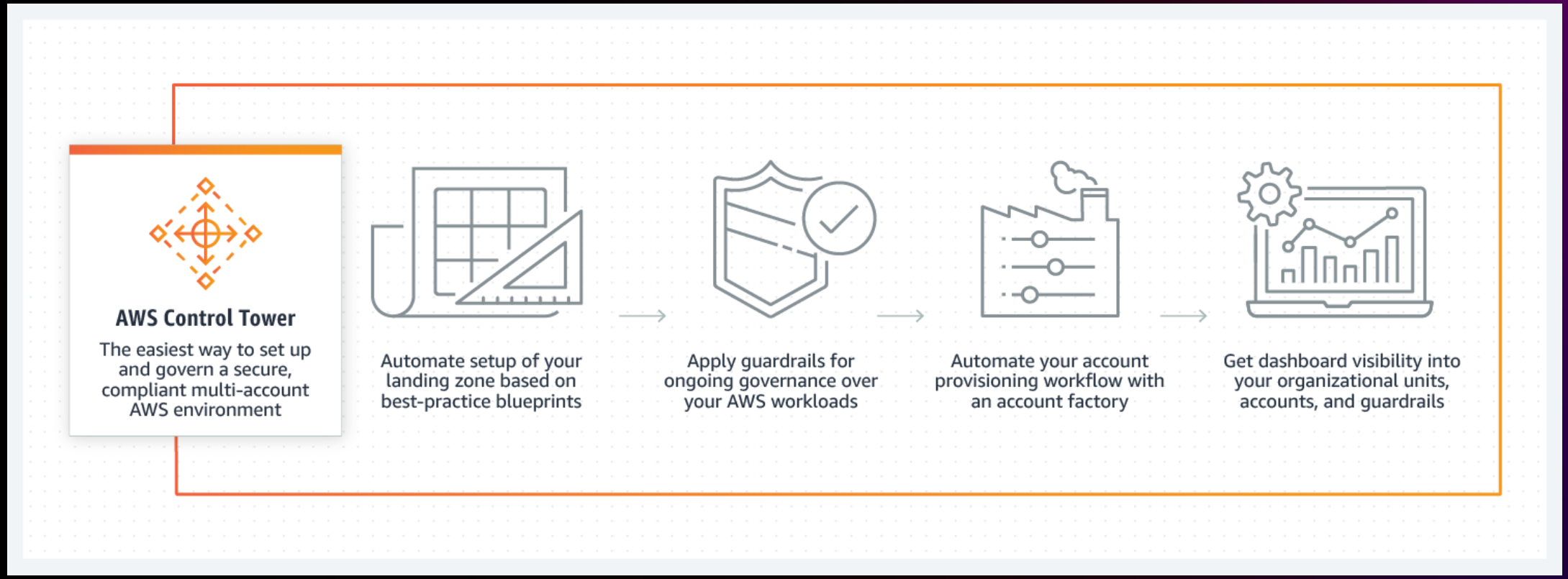
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tooling



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

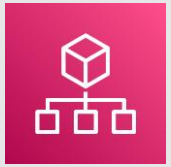
AWS Control Tower



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Preventative controls

Manage


AWS Organizations


AWS Identity and Access Management (IAM)


AWS Control Tower

Provision


AWS CloudFormation


AWS Service Catalog


Terraform (open source)

Compliance


AWS CloudFormation Guard


Open Policy Agent (open source)

aws

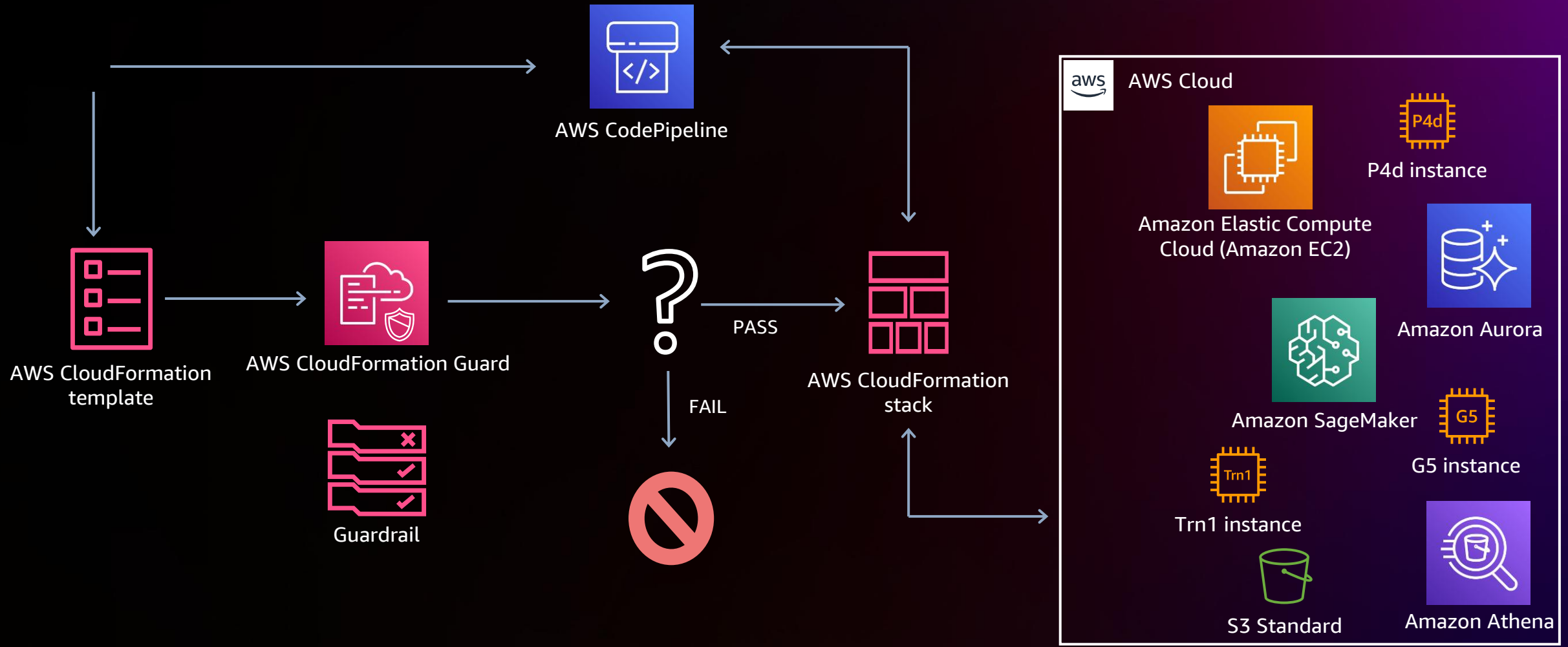
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using 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'
    }
}
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudFormation Guard for preventative controls



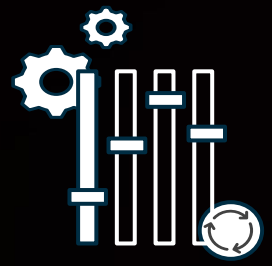
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config

ASSESS, AUDIT, AND EVALUATE



Assess, 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

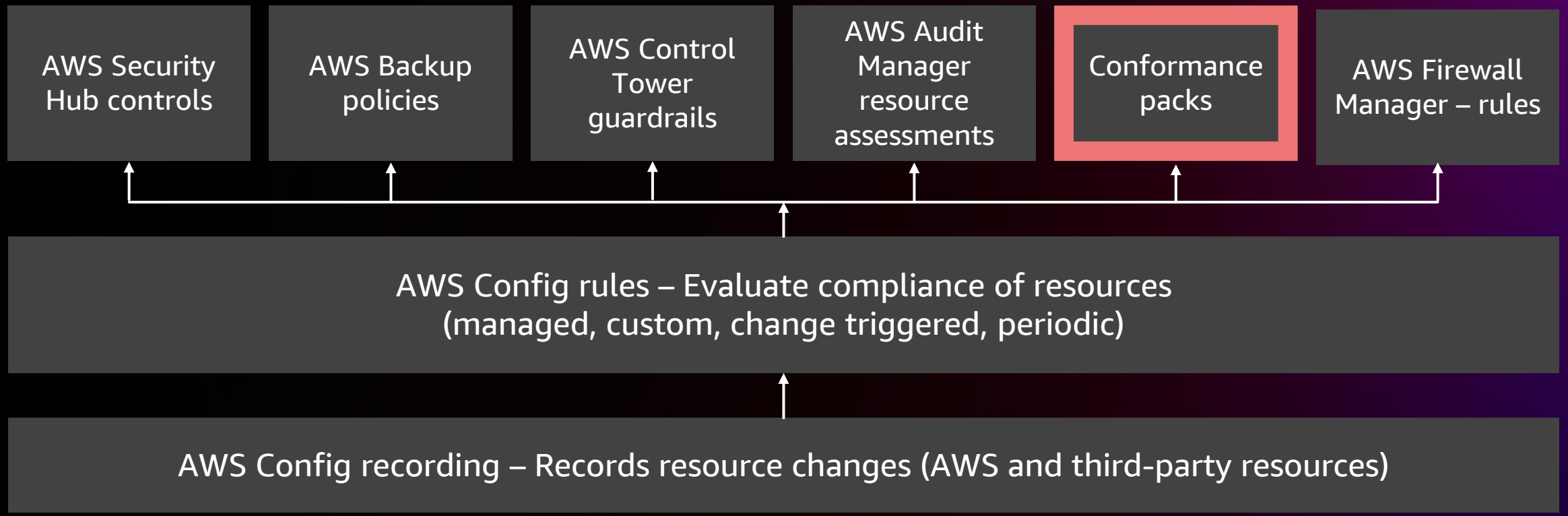
Amazon CloudWatch Events or Amazon SNS alert you when changes occur

deliver change history and snapshot files to your Amazon S3 bucket for analysis

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

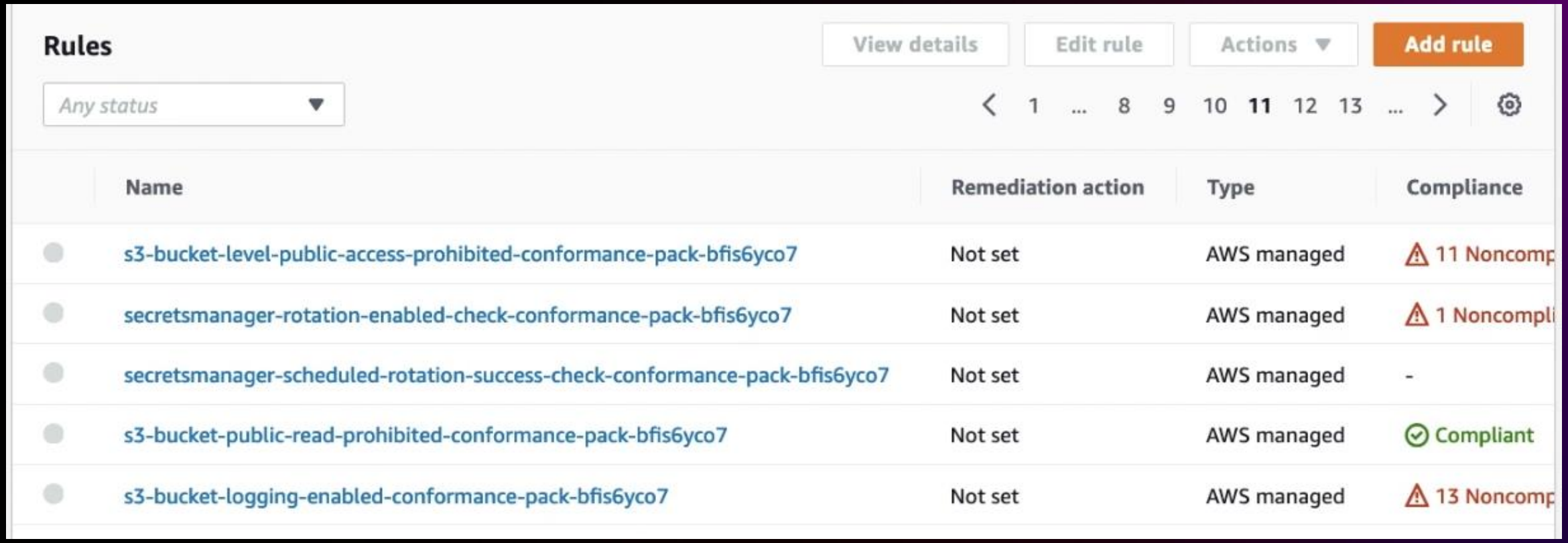
AWS Config

CORE FOR COMPLIANCE EVALUATIONS



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What it looks like in your console



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conformance packs

Use case – Deploy 100 rules into multiple accounts



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

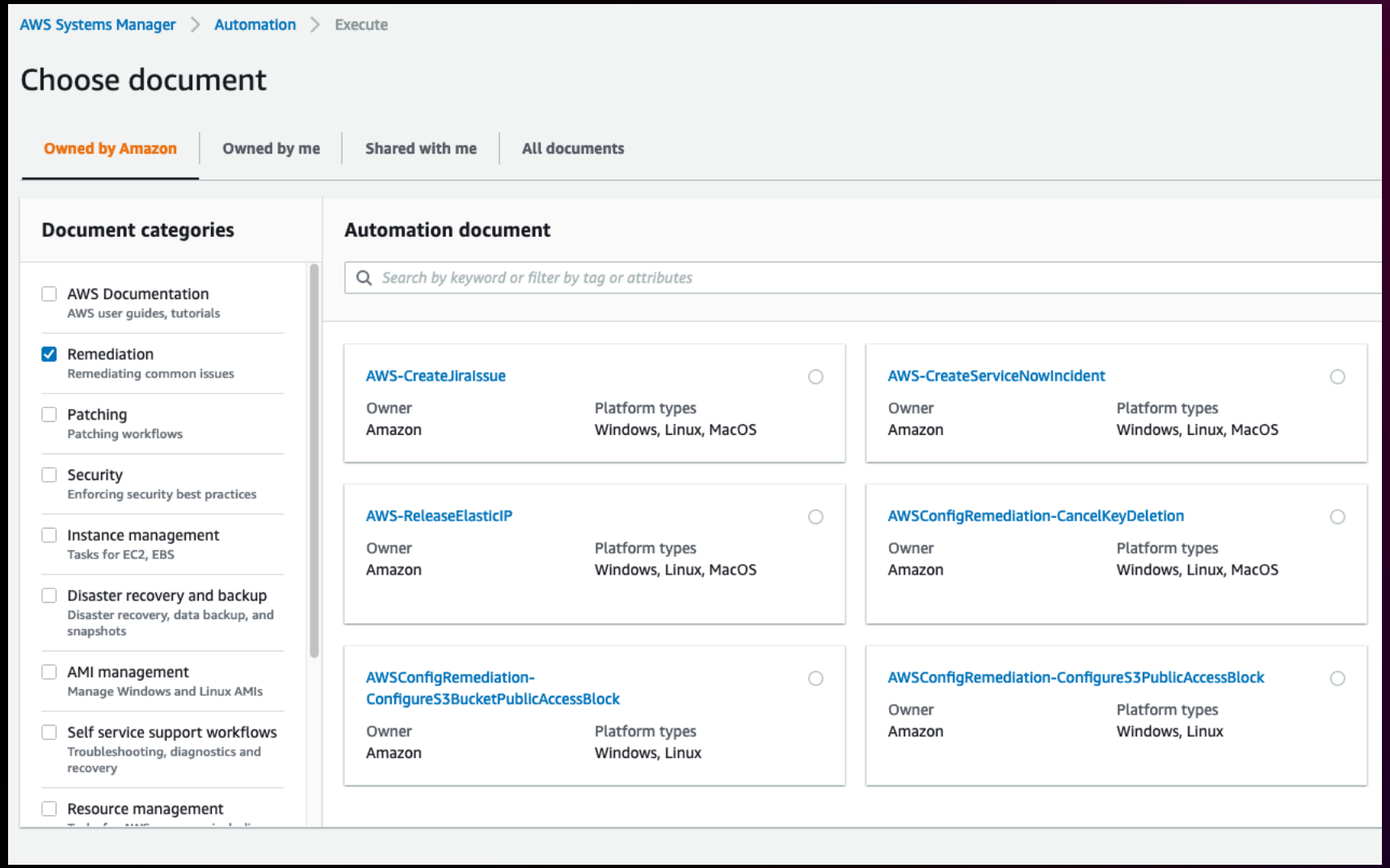
Detective controls

AWS Config Rules

Conformance Packs

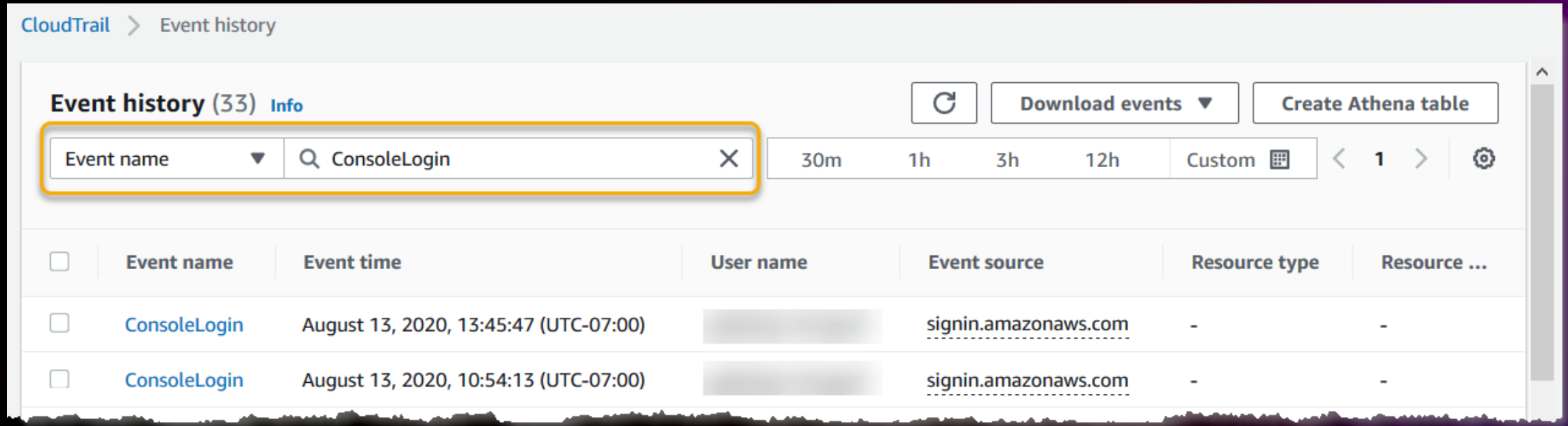
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Systems Manager



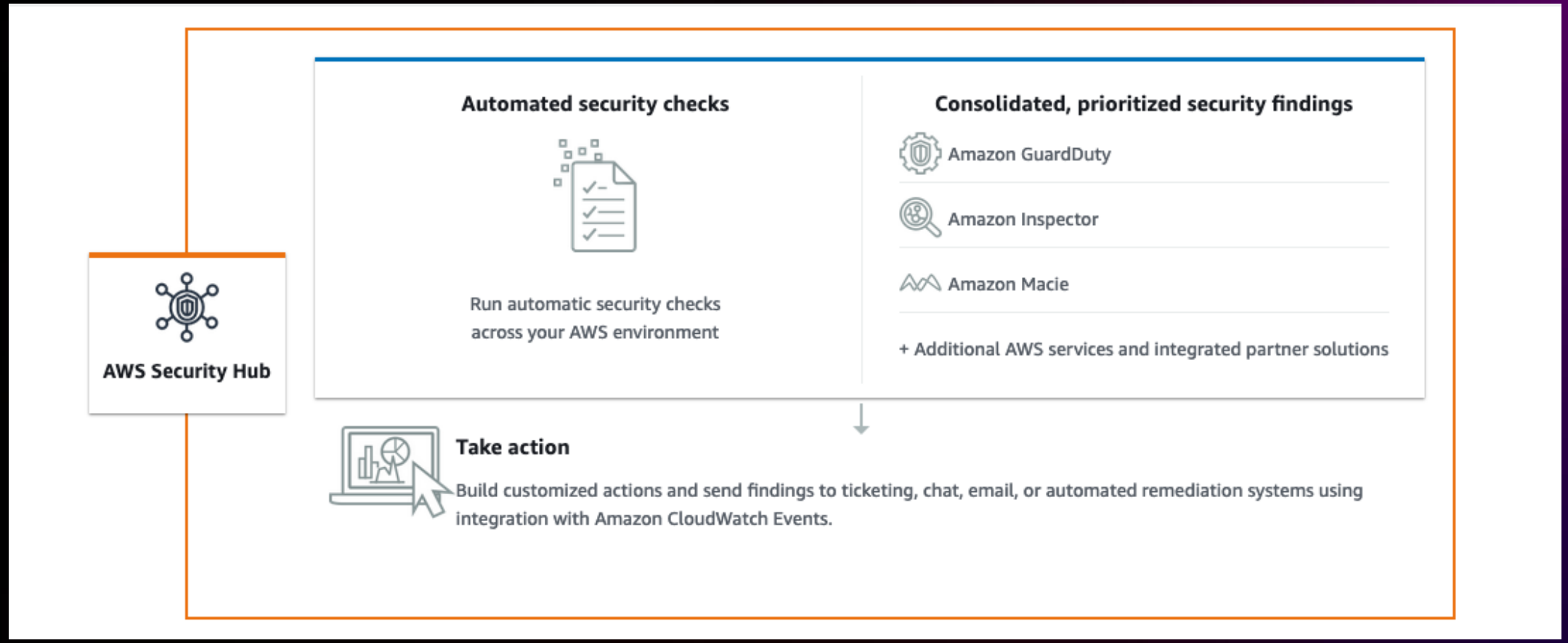
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudTrail



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Oversee risk with AWS Security Hub



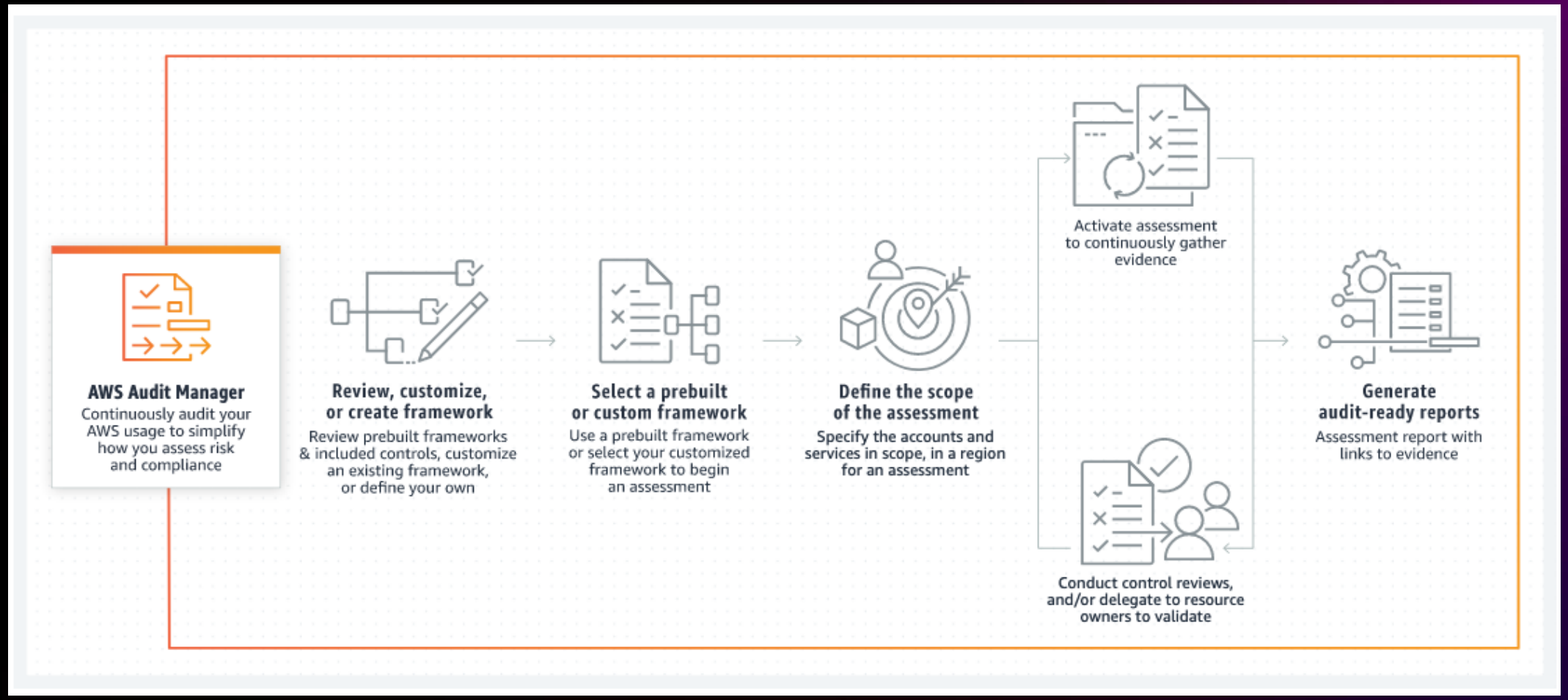
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting ready for an audit



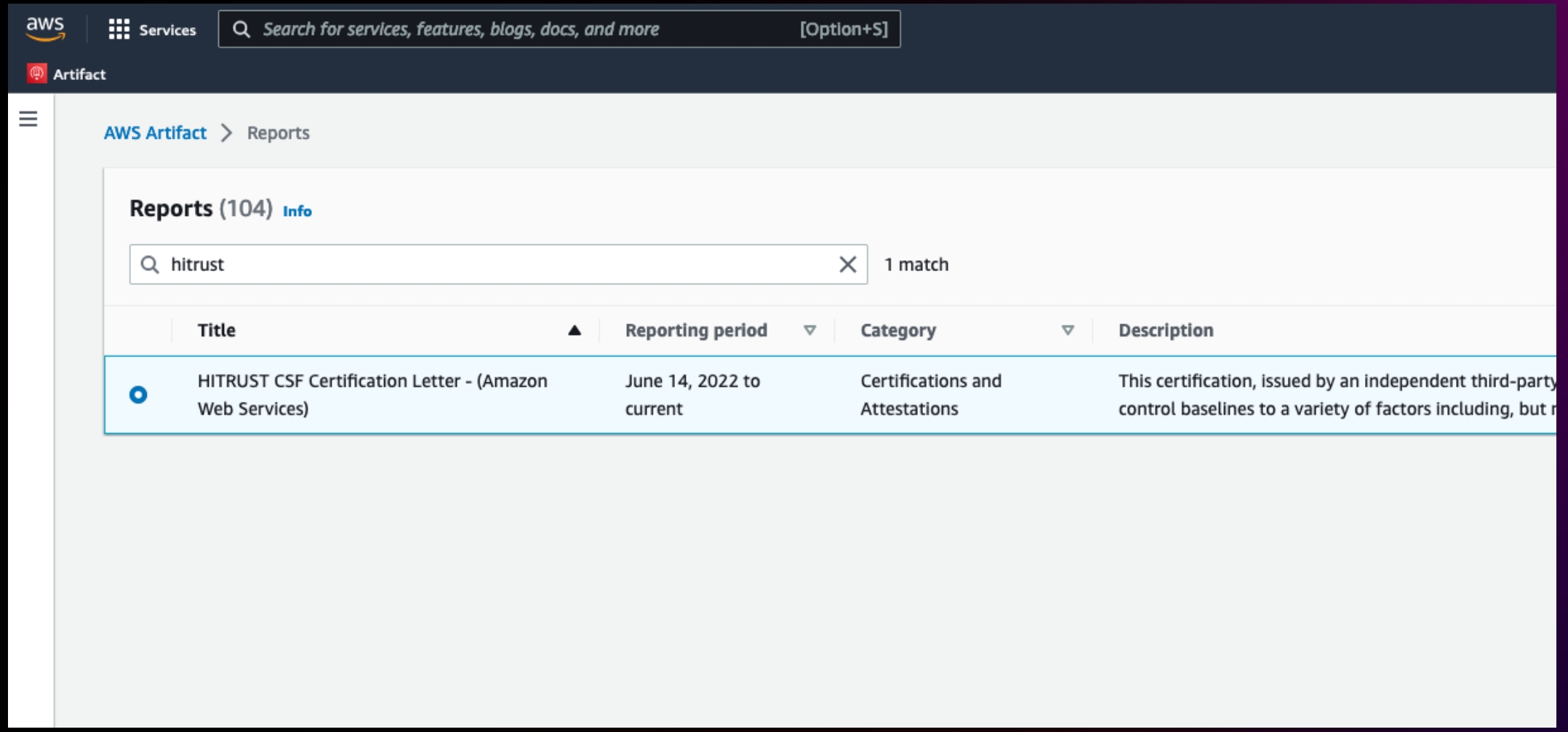
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Audit Manager



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Artifact



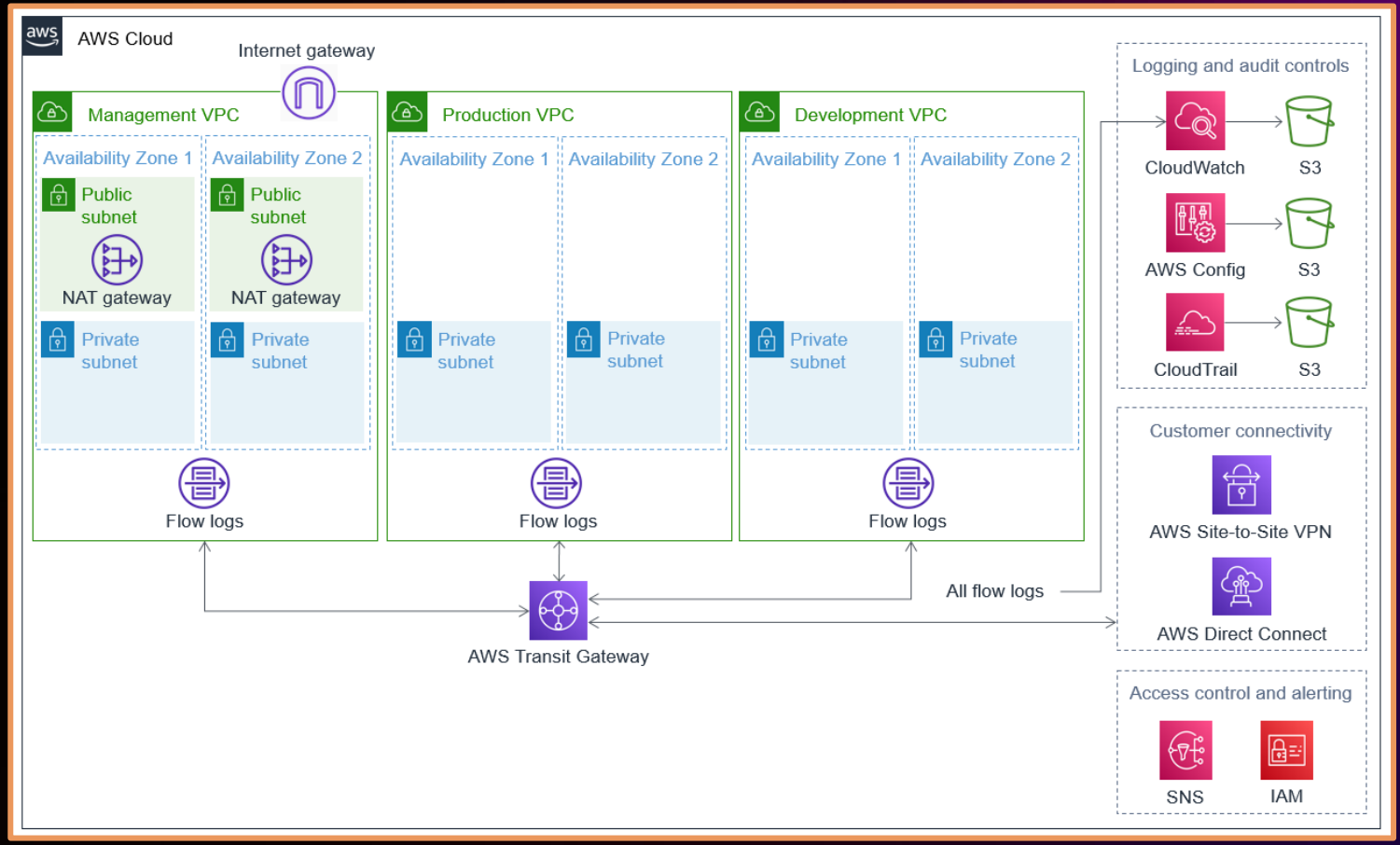
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started guidance



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

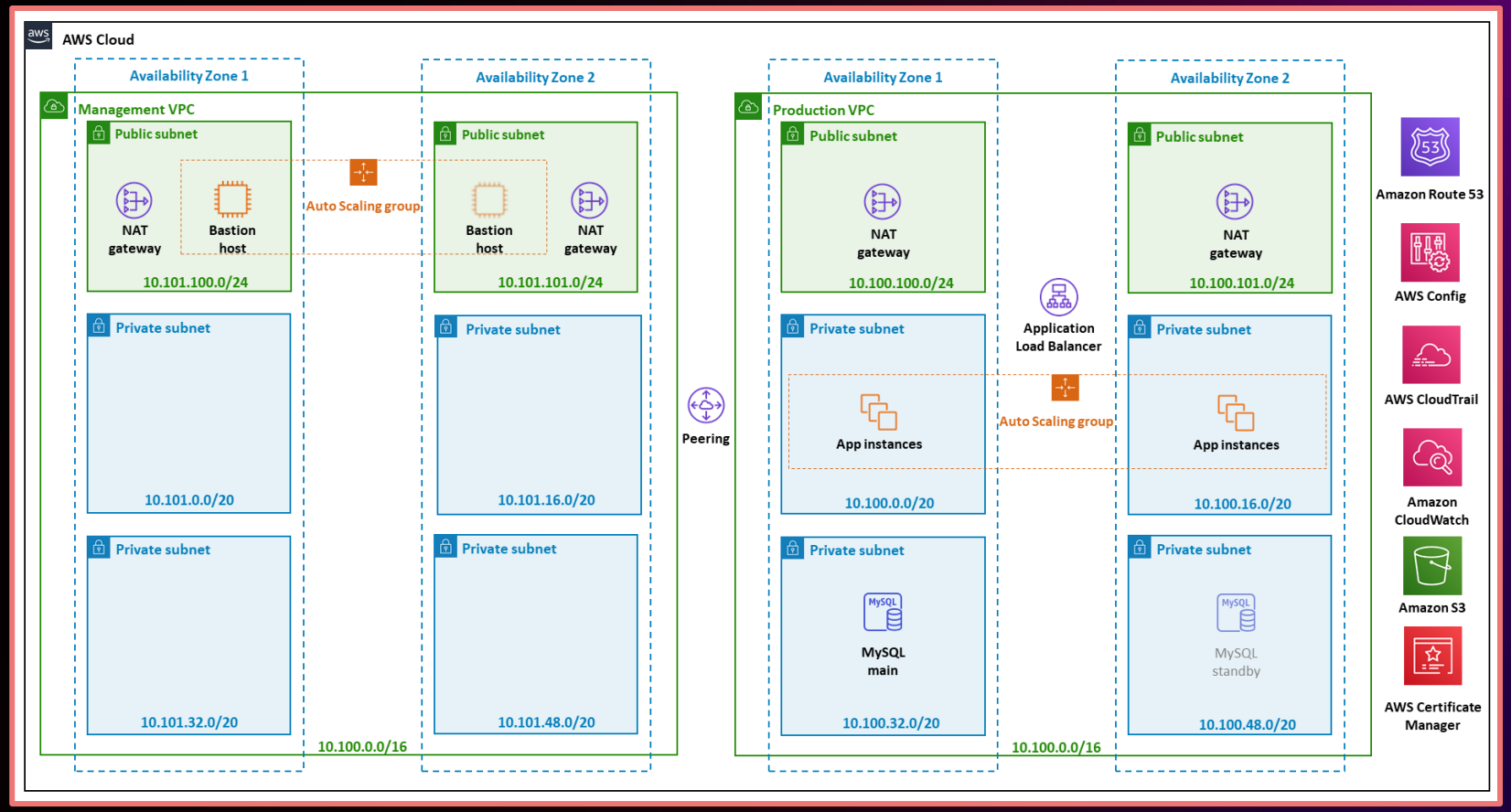
Quick Start – HIPAA reference architecture



https://aws.amazon.com/quickstart/architecture/compliance-hipaa/

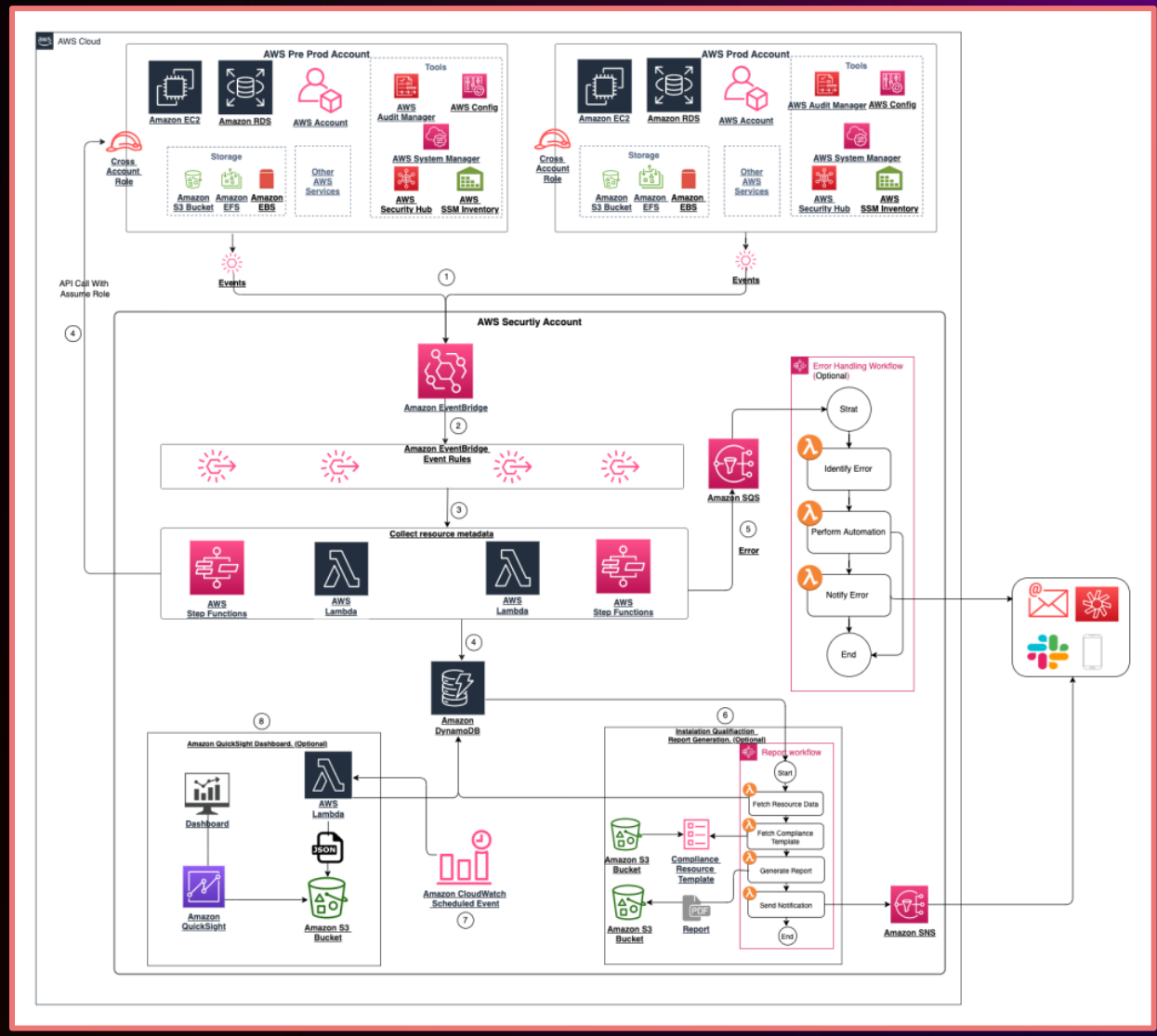
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Quick Start – HITRUST



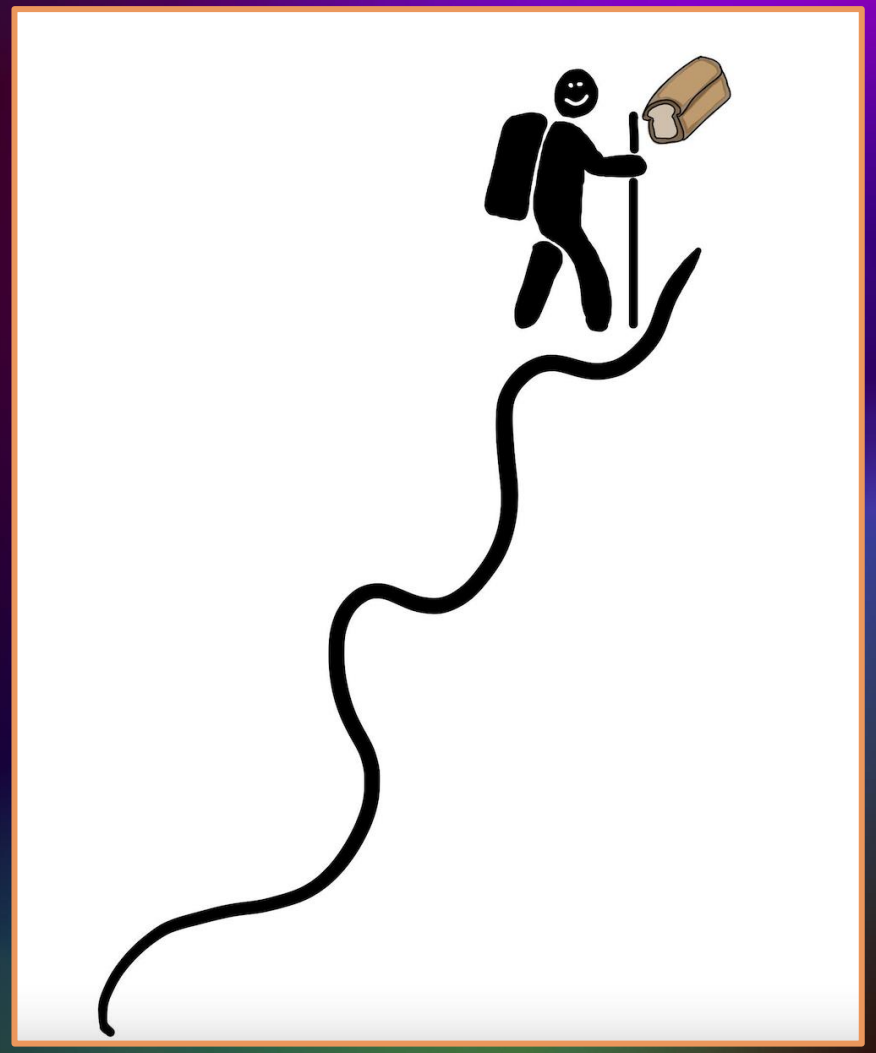
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GxP continuous compliance reference architecture



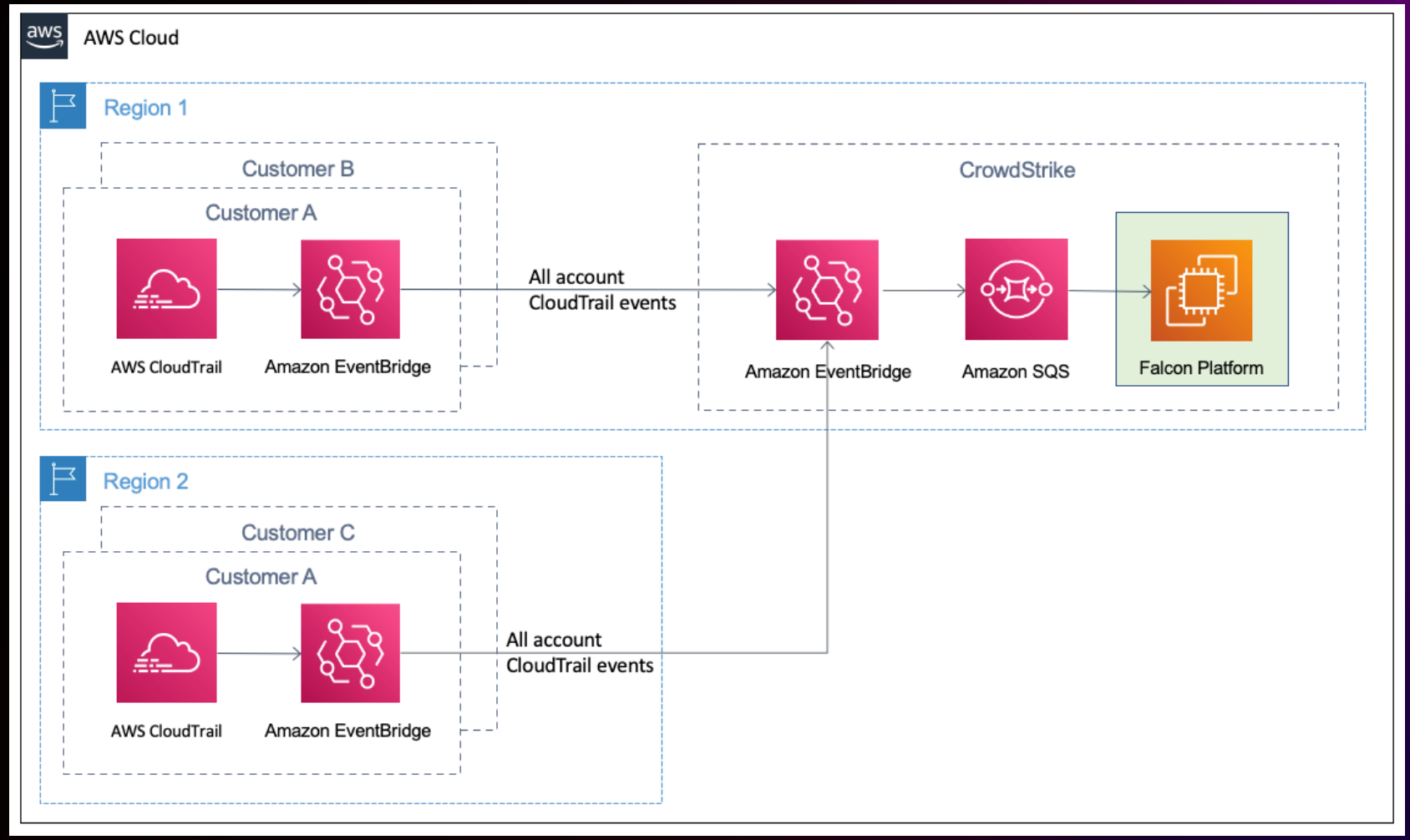
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer stories



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Event threat detection at CrowdStrike



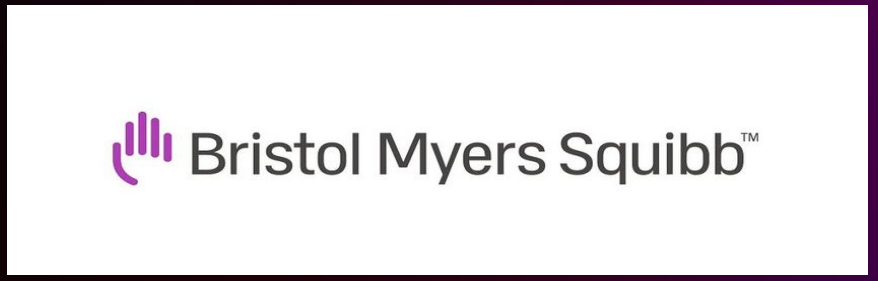
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer testimonials



"With AWS, DNAnexus enables enterprises worldwide to perform genomic analysis and clinical studies in a secure and compliant environment at a scale not previously not possible."

Richard Daly, CEO, DNAnexus



"Data residency in AWS Control Tower adds to our toolbox of programmatically setting up guardrails and data controls. As data regulations evolve, this capability will assist compliance and help us enable innovation to serve patients around the world."

William Taggart, Executive Director, Cloud Computing and DevOps, Bristol Myers Squibb

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Dani Traphagen
danitrap@amazon.com
@dtrapezoid on Twitter



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.