AWS re:Invent

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

SEC215

Evidence collection with AWS Audit Manager

John Fischer (he/him)
Senior Assurance Consultant, AWS Security Assurance Services
AWS

Kajal Deepak (she/her)
General Manager, AWS Audit Manager Service team
AWS

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

Agenda

What is continuous compliance?

What AWS services help facilitate continuous compliance?

AWS Audit Manager walk-through

Automation idea whiteboarding

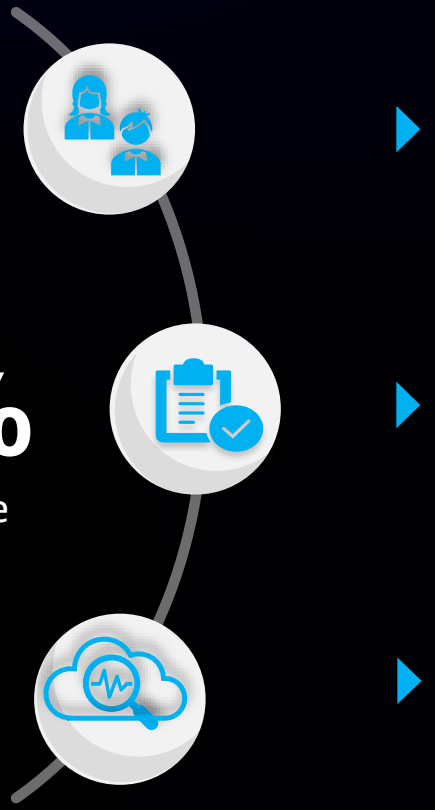
Q&A

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

Customer problems

80%
of the respondents

60%
of their time



"We are still doing cloud compliance audits the old-fashioned, manual way"

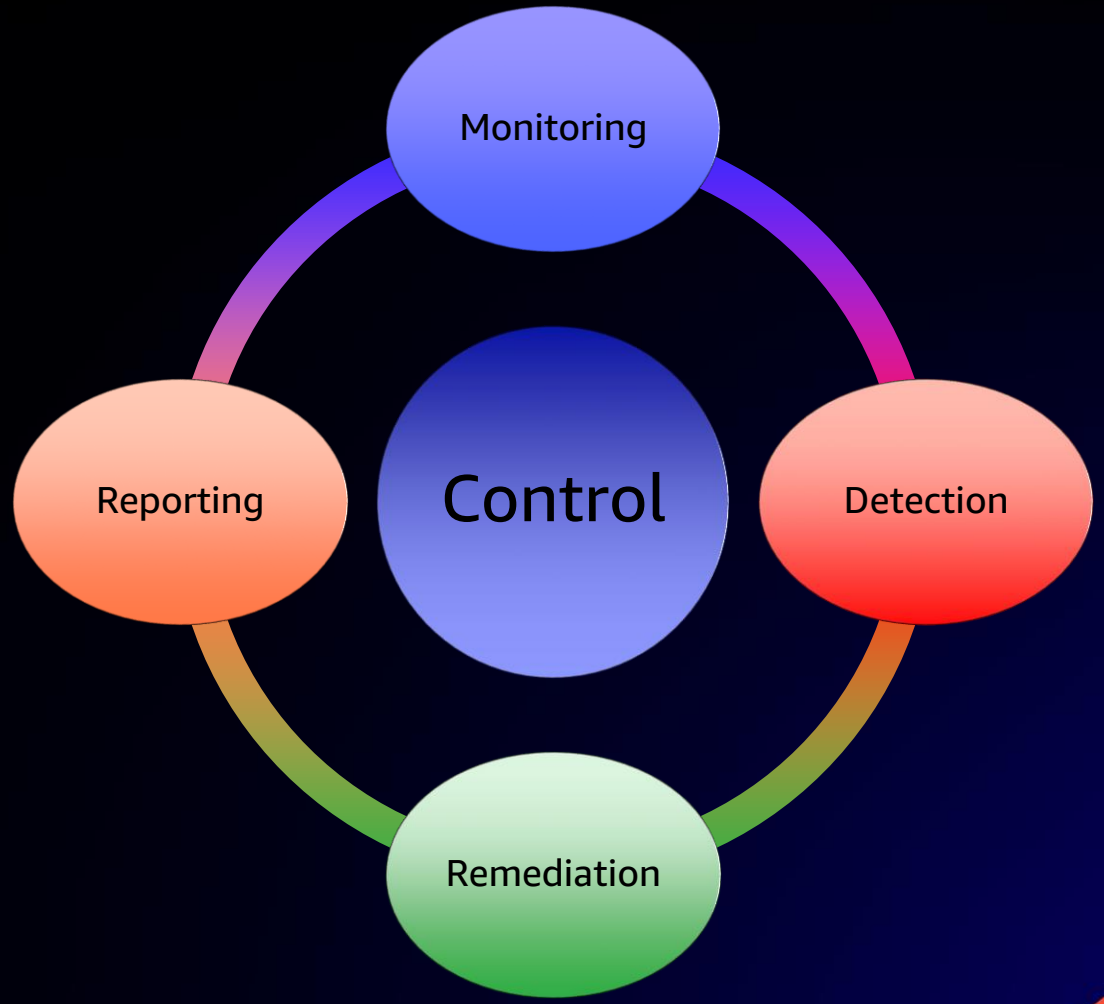
"We spend a lot of time collecting evidence for audits"

"We want to enhance our cloud compliance and audit capabilities in a cloud-native way"

Source: AWS 2010 internal survey; customer feedback

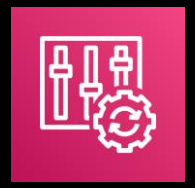
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is continuous compliance?



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

AWS services to enable continuous compliance



AWS Config

1. Evaluate



AWS Security Hub

2. Oversee

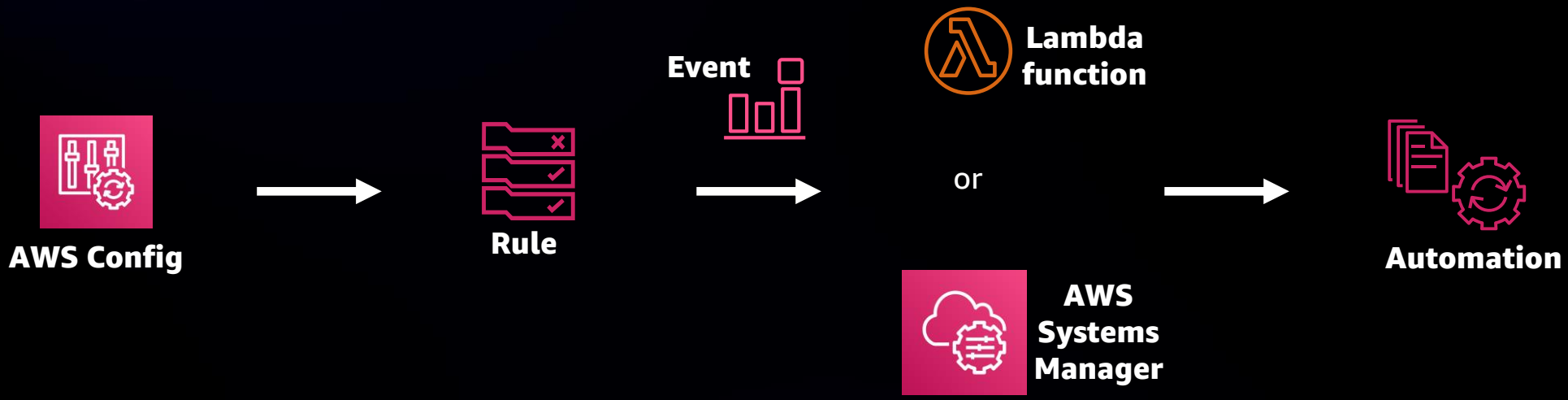


AWS Audit Manager

3. Report

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

Continuous compliance with AWS Config



1. AWS Config continuously records changes to AWS resources

2. A rule evaluation is triggered either periodically or when a resource configuration changes

   The evaluation will return a state of "compliant" or "noncompliant" based off of a set of criteria

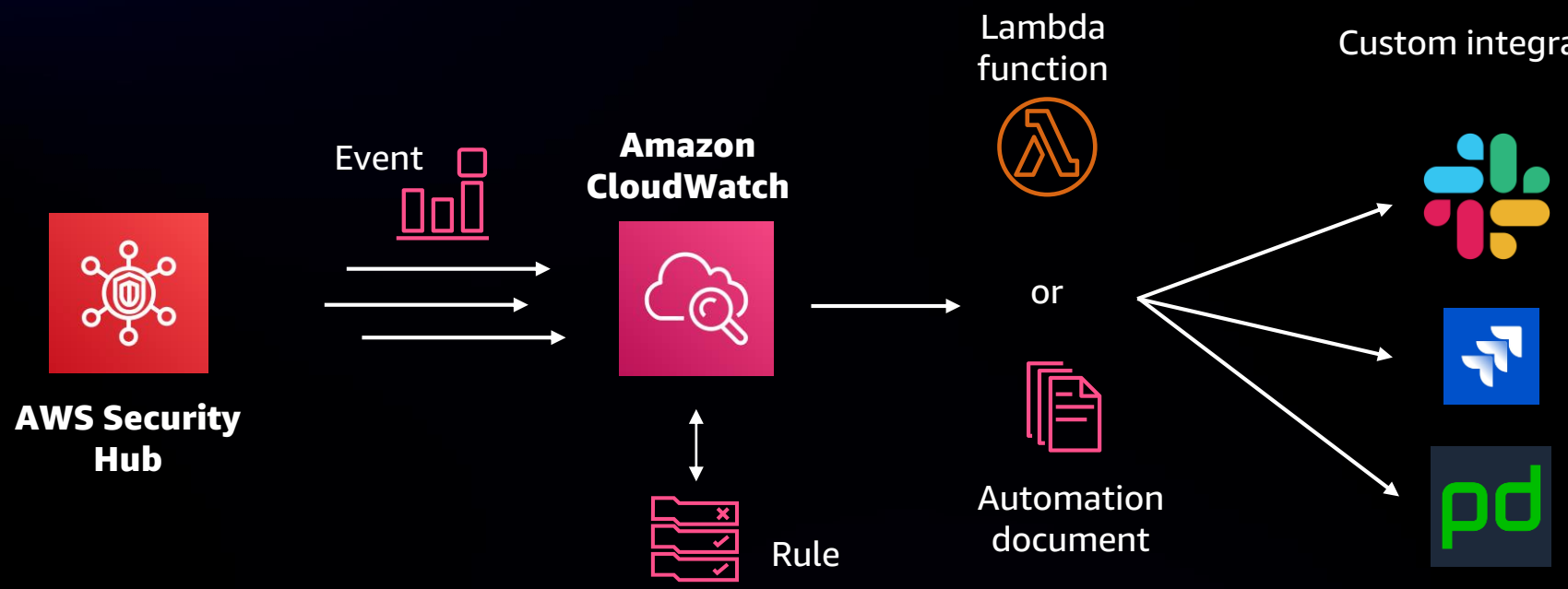
3. For "noncompliant" outcomes, an auto remediation via Lambda or SSM can be triggered

4. Lambda or SSM can perform the remediation

   After completion, the resource will return to a compliant state after the configuration change is made and the resource is re-evaluated

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

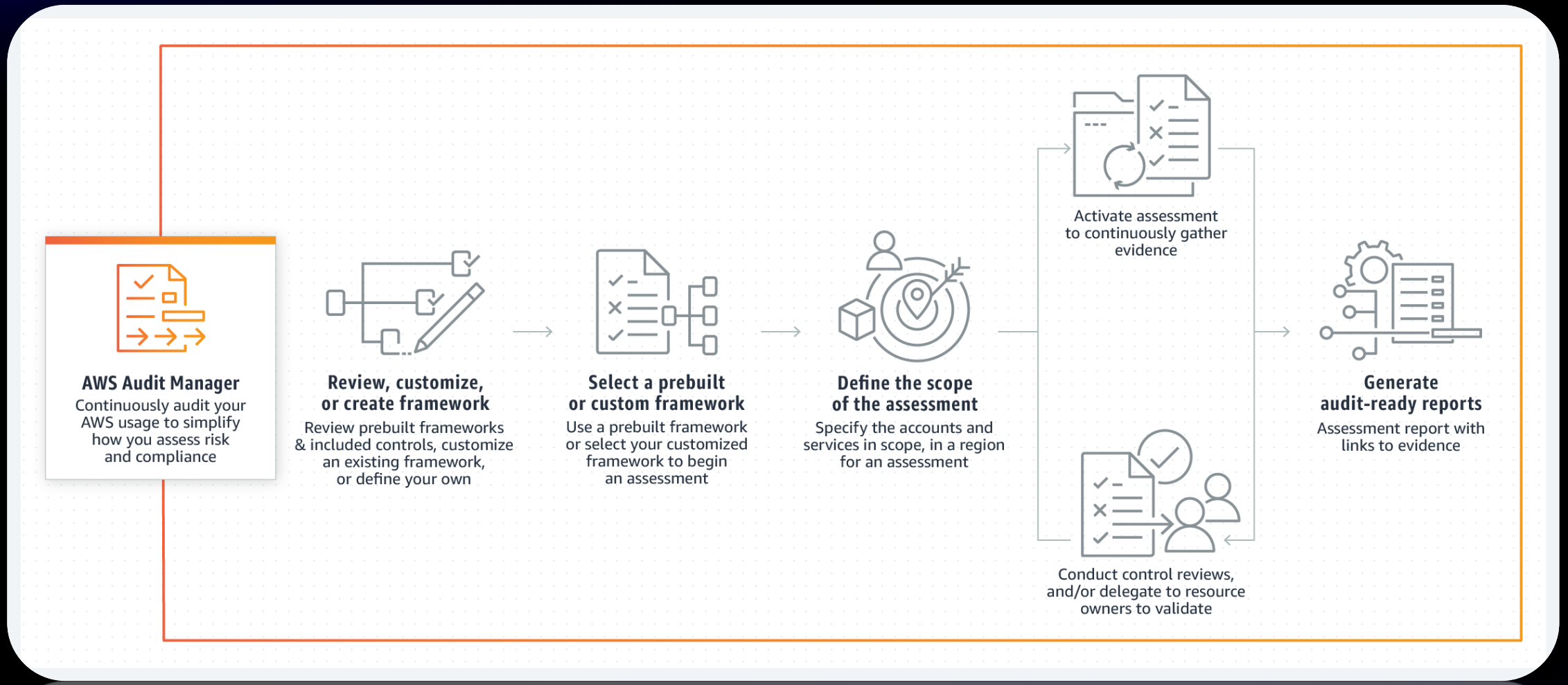
Continuous compliance with AWS Security Hub



1. All findings automatically sent to Amazon CloudWatch Events
2. Security Hub user selects findings in the console and takes custom action; findings sent to CloudWatch, decorated with a custom action ID
3. User creates CloudWatch Events rules to look for certain findings associated with a custom action ID or specific characteristics
4. The rule defines a target, typically a Lambda function, Step Function, or automation document
5. The target could be things like a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook

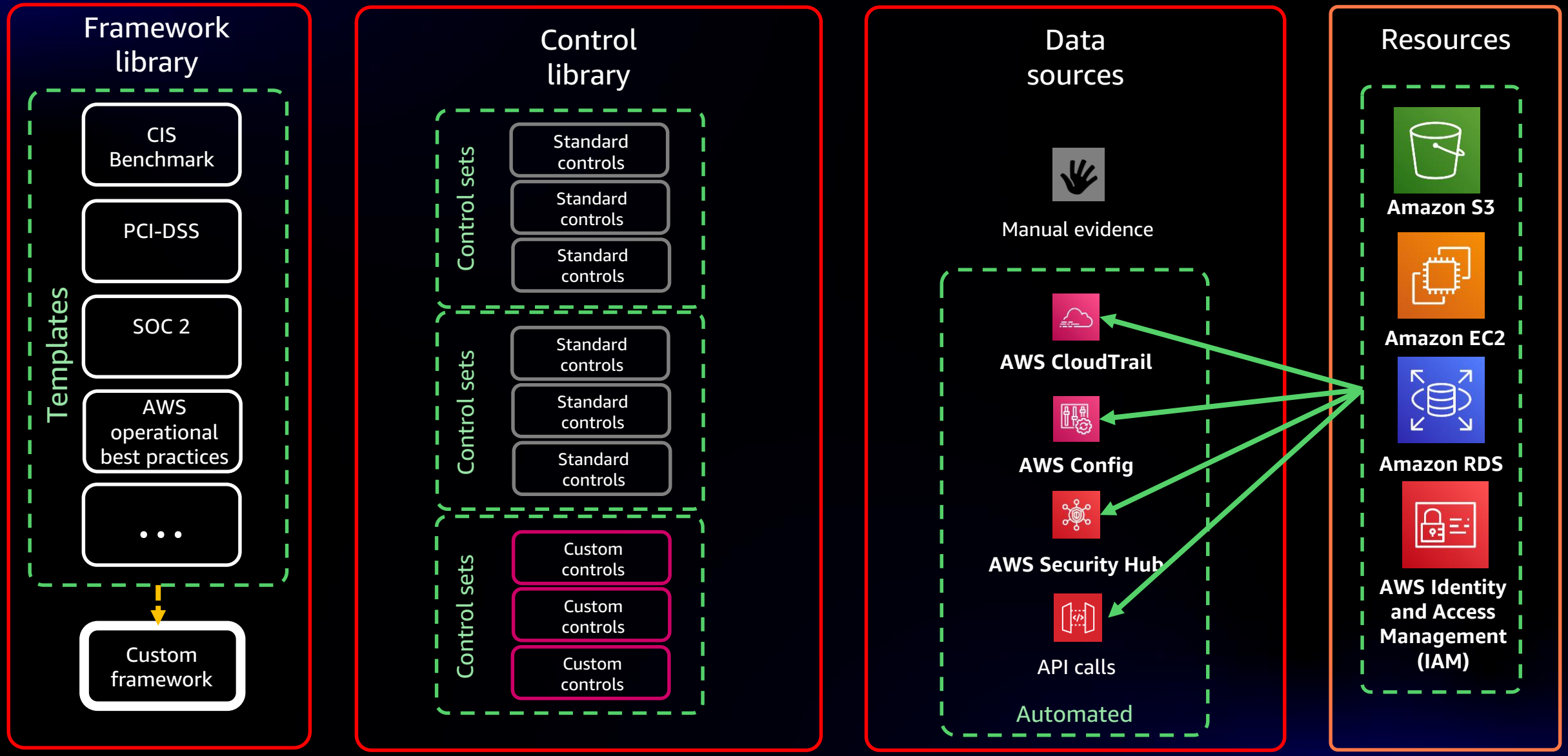
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How AWS Audit Manager works



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

AWS Audit Manager: Relationship



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

Whiteboard session

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

Additional resources

AWS Config (and conformance packs)

- https://aws.amazon.com/config/
- https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html

AWS Security Hub

- https://aws.amazon.com/security-hub/

AWS Audit Manager

- https://aws.amazon.com/audit-manager/

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

Thank you!

John Fischer
jofisc@amazon.com

Kajal Deepak
kajald@amazon.com

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