Security & Compliance

Visibility Review

George'son Tib.

Solutions Architect
AWS

Key Customer Asks

What security best practices should I follow within AWS?

How to identify resources that are noncompliant and create an action plan?

How to do I increase automation and reduce manual processes?

How do I get Started?

What are security best practices I should follow within AWS?

How do I perform asset inventory in AWS?

How do I patch and report on patch levels in AWS?

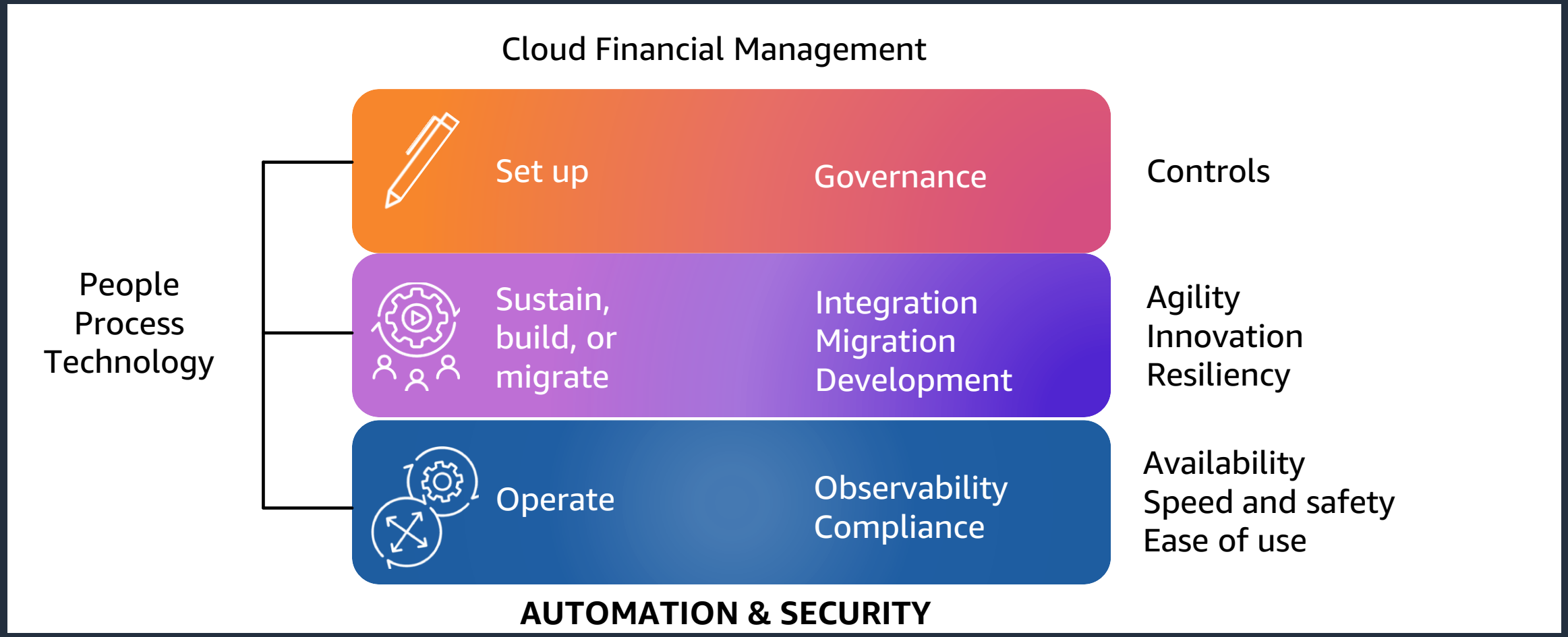
Which AWS Services should I use?

How do I know if my AWS Resources are configured securely or to a certain framework standard?

How do I prevent configurations that lead to security vulnerabilities and exposure?

AWS Cloud Operations

HELPS CREATE A SOLID CLOUD FOUNDATIONS BY DELIVERING OPERATIONAL OUTCOMES IN THE CLOUD, ON PREMISES, AND AT THE EDGE



Building a solid cloud foundation

4 DOMAINS, 10 SERVICES

Identity

AWS IAM Identity Center
Securely manage access to AWS services and resources

Governance

AWS Control Tower
Set up and govern a secure, mutli-account AWS environment

AWS Organizations
Policy-based management for multiple AWS accounts

Security

Amazon Guard Duty
Threat detection within AWS accounts and resources

AWS Key Management Service (KMS)
Easily create and control the keys used to encrypt your data

AWS Security Hub
Cloud security posture management

Operations

AWS Config
Assess, audit, and evaluated configurations of AWS resources

AWS CloudTrail
Track user activity and API usage in AWS accounts

Amazon CloudWatch
Visibility of your cloud resource and applications to collect metrics, logs, set alarm, and automatically react to change

AWS Systems Manager
Operational hub to view and control infrastructure

AWS Control Tower automatically turns on 5 superset services

Security & Compliance Visibility Review

Security & Compliance Visibility Review

Program

Helping customers gain visibility into their AWS environments and identify misconfigurations that can lead to security vulnerabilities by taking a proactive approach.

Goal

Starting point for recommendations and guidance for customer wanting to follow AWS security best practices.

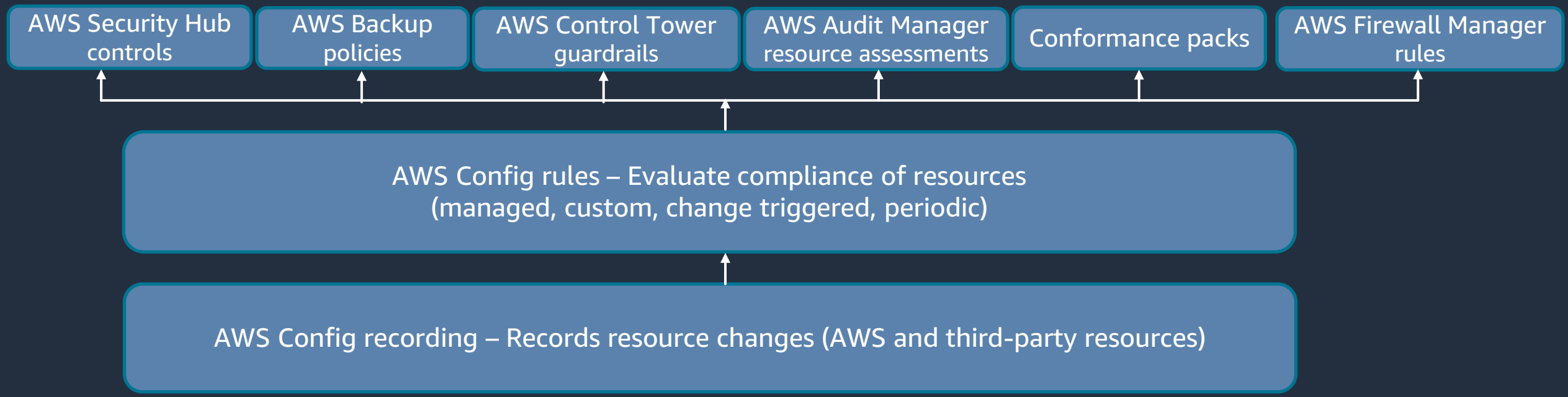
Services used

AWS Config Services
Assess, audit and evaluate configurations of AWS resources

AWS Security Hub
Cloud security posture management

AWS Config

CORE SERVICE FOR COMPLIANCE

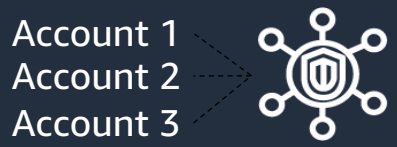


Use cases

Resource Management | Cloud CMBD | Audit Compliance | Security Analysis | Audit Compliance

AWS Security Hub

AUTOMATE AWS SECURITY CHECKS AND CENTRALIZE SECURITY ALERTS



Enable AWS Security Hub for all your accounts

Continuously aggregate and prioritise findings

Conduct automated compliance scans and checks

Take action based on findings

Better visibility into **security issues** → Easier to stay in **compliance**

[Hide or Keep] see notes

Enabling cloud foundations services at scale

Services enabled by AWS Control Tower

AWS Organizations

Policy-based management for multiple AWS accounts

AWS IAM Identity Center

Securely manage access to AWS services and resources

AWS CloudTrail

Track user activity and API usage in AWS Accounts

AWS Config

Assess, audit and evaluate configurations of AWS Resources

AWS Systems Manager

Operational Hub to view and control infrastructure

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

AWS Security Hub

Cloud security posture management

Amazon GuardDuty

Threat detection within AWS Accounts and Resources

Demo

Program Approach

Meeting #1 (30 Minutes) – FCD: Introduction of the Security & Compliance Visibility Review

Meeting #2 (30 Minutes) - Turn on AWS Config, AWS Security Hub to collect data on a single account, single region. Apply AWS Credits.

- Let the services collect data for no less than 24 hours, no more than a week. Schedule follow-up meeting.

Meeting #3 (1 hour) – Review scoring in AWS Security Hub, review 10 Checks

Resources

AWS Cloud Foundations
White paper

Security & Compliance
Visibility Review Workshop

AWS Foundational Security
Best Practices (FSBP) standard

Thank you!