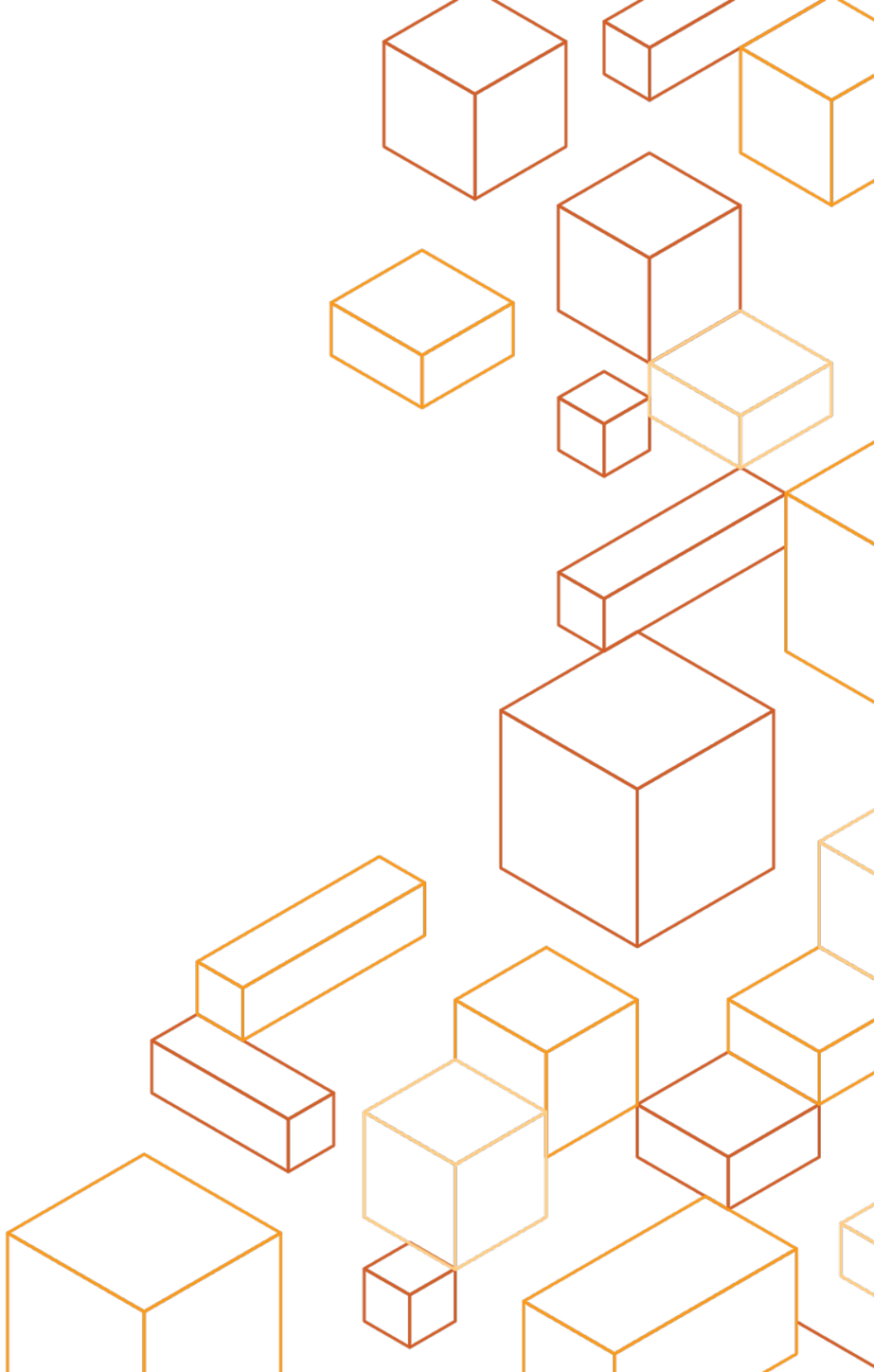
aws professional services

Security Governance & Strategy



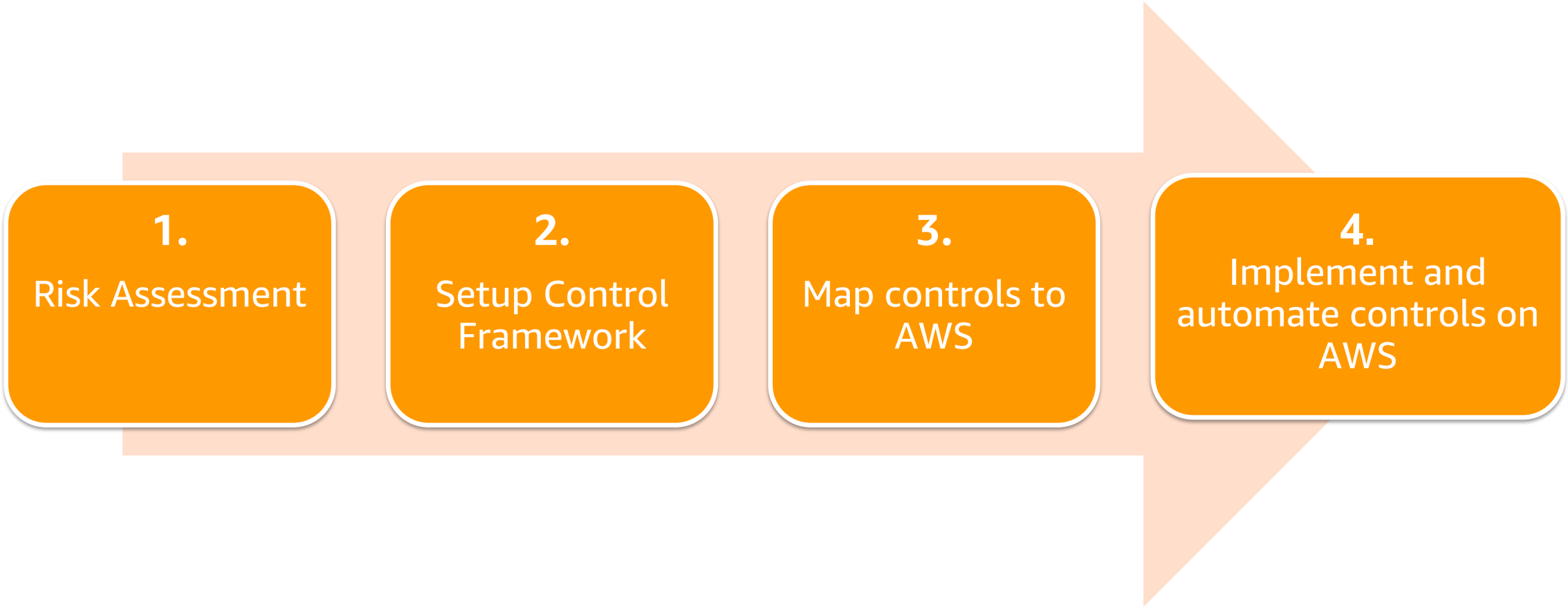
Agenda

- Governance & compliance in the cloud
- Modernize Technical Governance
- Defining your control environment
- Continuous Compliance

Goals

- Learn how to mitigate risk
- Discover tools to automate security enforcement at scale
- Realize that scale does not sacrifice granular security

Automating your governance and control framework



aws professional services

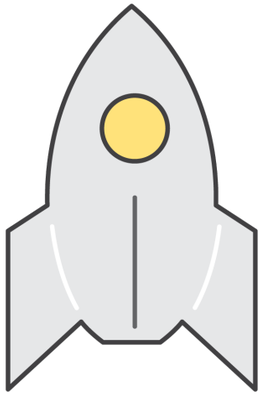
Why do you need a cloud security strategy?

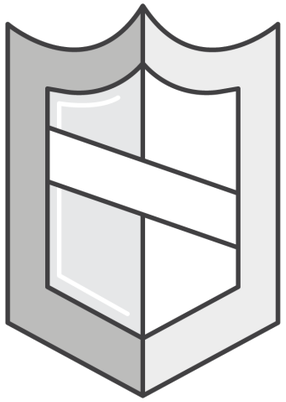
cloud adoption prompts updates to existing security strategy

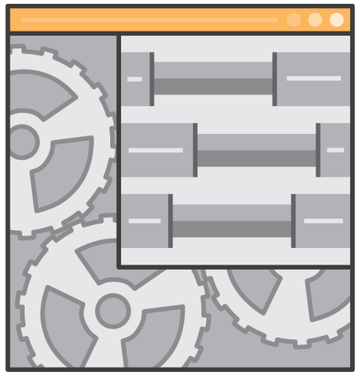
faster technology change in support of business outcomes

security risk is altered as a result of shared responsibility model

applications and third party vendors interact differently







move from protect/compliance posture to builder-friendly resilient environment

aws professional services

What is contained in a cloud security strategy?

Companies have differing needs although the building blocks are similar

develop & retain people with the skills for cloud security

risk modeling for cloud services and shared responsibility

technical pillars of cloud security (the AWS Security EPICs)

approach for using the cloud to secure assets and data

addressing security before steady state is achieved

framework of controls for compliance needs

framework for security governance

key performance indicators (monitor, maturity, visibility)

security in the development to production pipeline

aws professional services

Modernize technology governance

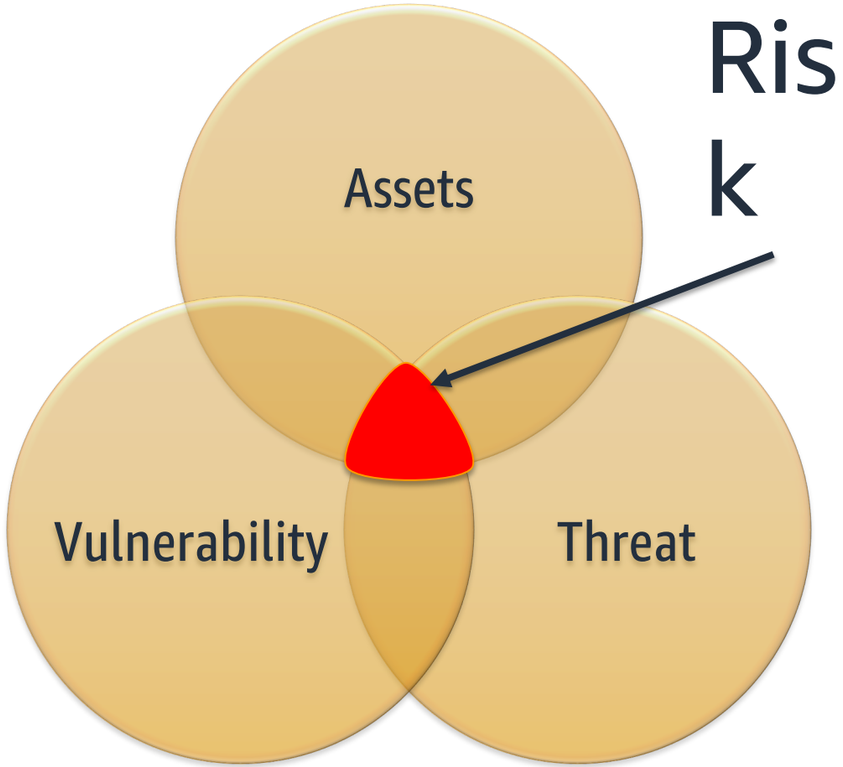
Security Governance & Strategy

aws professional services

Current State – Technology Governance

Issues – Technology Governance

The majority of technology governance processes relies predominantly on administrative and operational security controls with ***limited*** technology enforcement.



AWS has an opportunity to innovate and advance ***Technology Governance Services***.

aws professional services

Flexibility and Complexity

How many AWS accounts

Single VPC or Multiple VPCs

IAM groups or roles

Security groups or NACLs

Public or private subnets

Can we use S3 for this

What type of encryption

Who will manage the keys

Which AWS database

What is the regulatory requirement?

What's in-scope or out-of-scope?

How to verify the standards are met?

Security & Compliance then and now

aws professional services

Security by Design

Security by Design (SbD) is a security assurance approach that formalizes AWS account design, automates security controls, and streamlines auditing.

Instead of relying on auditing security retroactively, SbD provides security control built in throughout the AWS IT management process.

AWS Security Hub

AWS Identity and Access Management

Amazon CloudWatch

AWS Trusted Advisor

AWS CloudTrail

AWS Directory Service

AWS Key Management Service

AWS Config

aws professional services

Security by Design - Design Principles

Developing new risk mitigation capabilities, which go beyond global security frameworks, by treating risks, eliminating manual processes, optimizing evidence and audit ratifications processes through rigid automation

- Build security in every layer
- Design for failures
- Implement auto-healing
- Think parallel
- Plan for Breach
- Don't fear constraints
- Leverage different storage options
- Design for cost
- Treat Infrastructure as Code
  - Modular
  - Versioned
  - Constrained

SbD - Modernize Tech Governance (MTG)

Why?

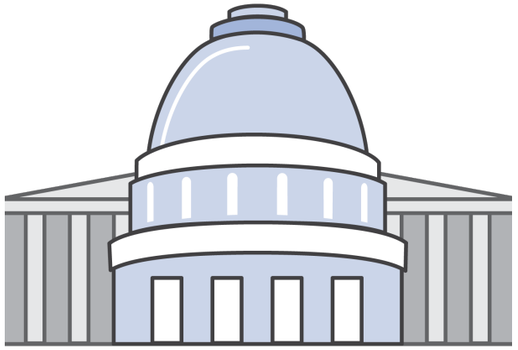
Complexity is growing, making the old way to govern technology obsolete

You need automation that AWS offers to manage security

Goal - Modernize Tech Governance (MTG)

Adopting "***Prevent***" controls, making "***Detect***" controls more powerful and comprehensive

SbD - Modernizing Technology Governance (MTG)



Automate Governance

Automate Deployments

Automate Security Operations

Continuous Compliance

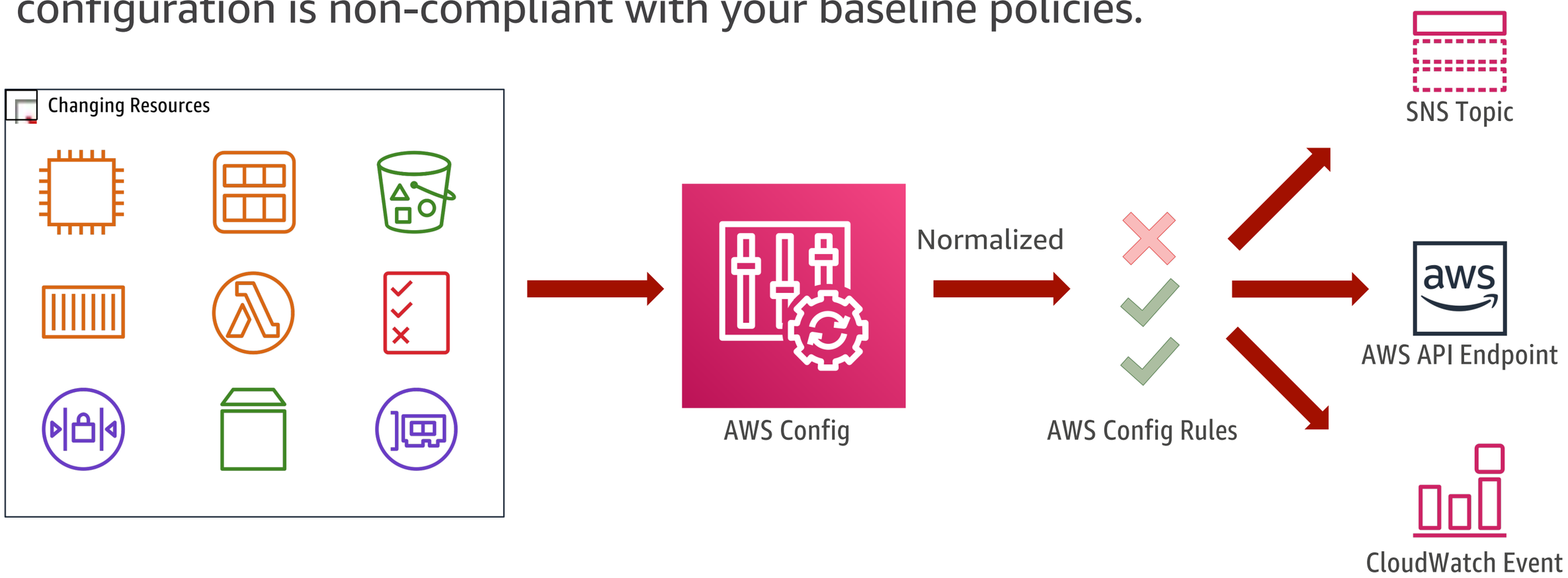
Continuous compliance

Security Governance & Strategy

aws professional services

Continuous Compliance

AWS Config is a continuous recording and continuous assessment service, that tracks configuration changes to AWS resources and alerts you if the configuration is non-compliant with your baseline policies.



Continuous Compliance - Eco-System

Security by Design

AWS Config Rules

AWS CloudFormation

Amazon Inspector

ALLGRESS

splunk>

VERIS GROUP

ALERT LOGIC®

CloudCheckr

CIS® Center for Internet Security®

Flux7

Symantec.

evident.io

aws professional services

aws professional services

Questions