



FINANCIAL SERVICES

Innovation and Transformation in Cloud Security and Risk: Continuous Compliance at Scale

Nick Dimtchev

Partner Sales Manager - Security, Compliance, and
Governance ISVs, AWS Global Financial Services (GFS)

Agenda

- What is continuous compliance?
- What does continuous compliance look like on the cloud?
- How AWS can help your continuous compliance journey

The fundamental underlying questions

How do you innovate and drive change while **maintaining your security and compliance posture** in a highly regulated sector?

How do you know when **you're not compliant**?

Continuous compliance requires insight and automation



Precise Visibility



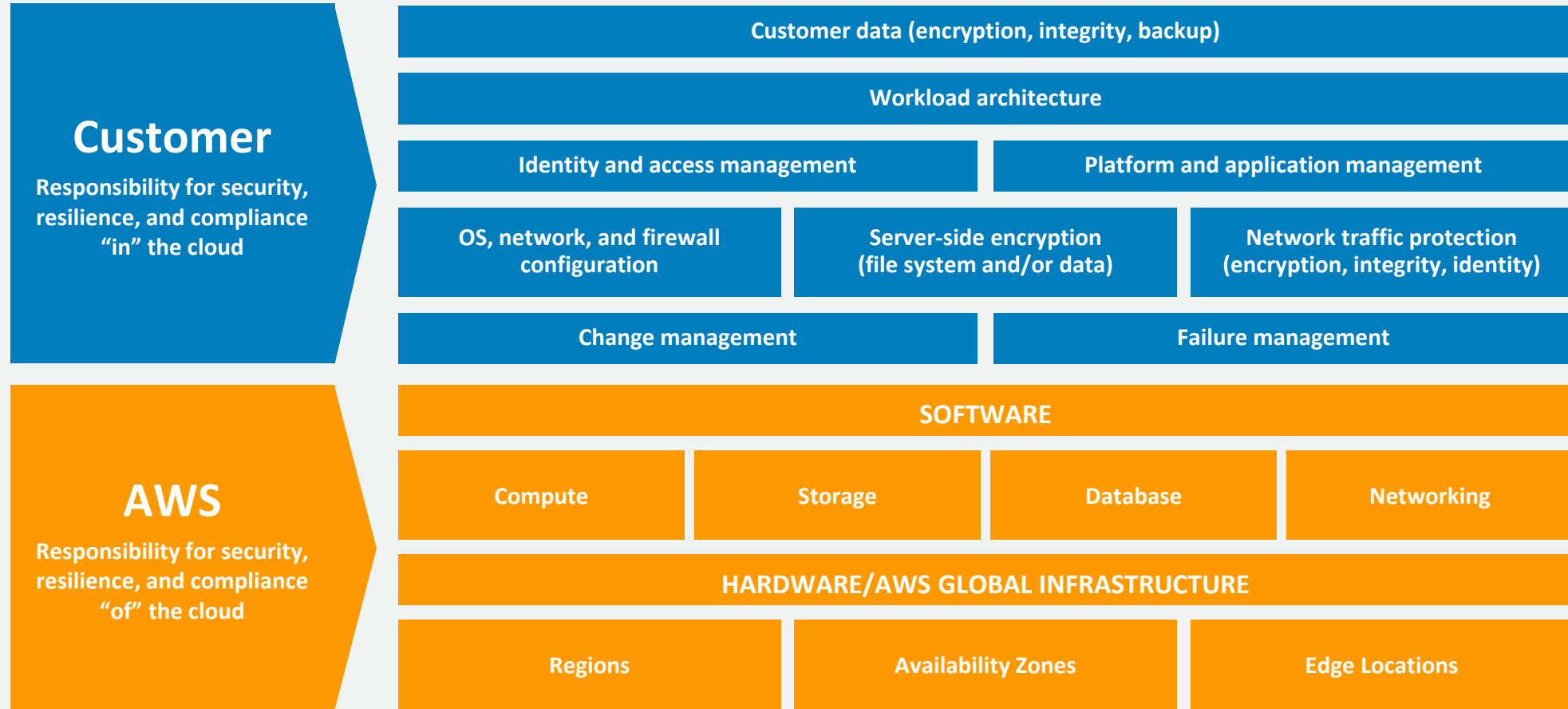
Near-Real-Time Automation



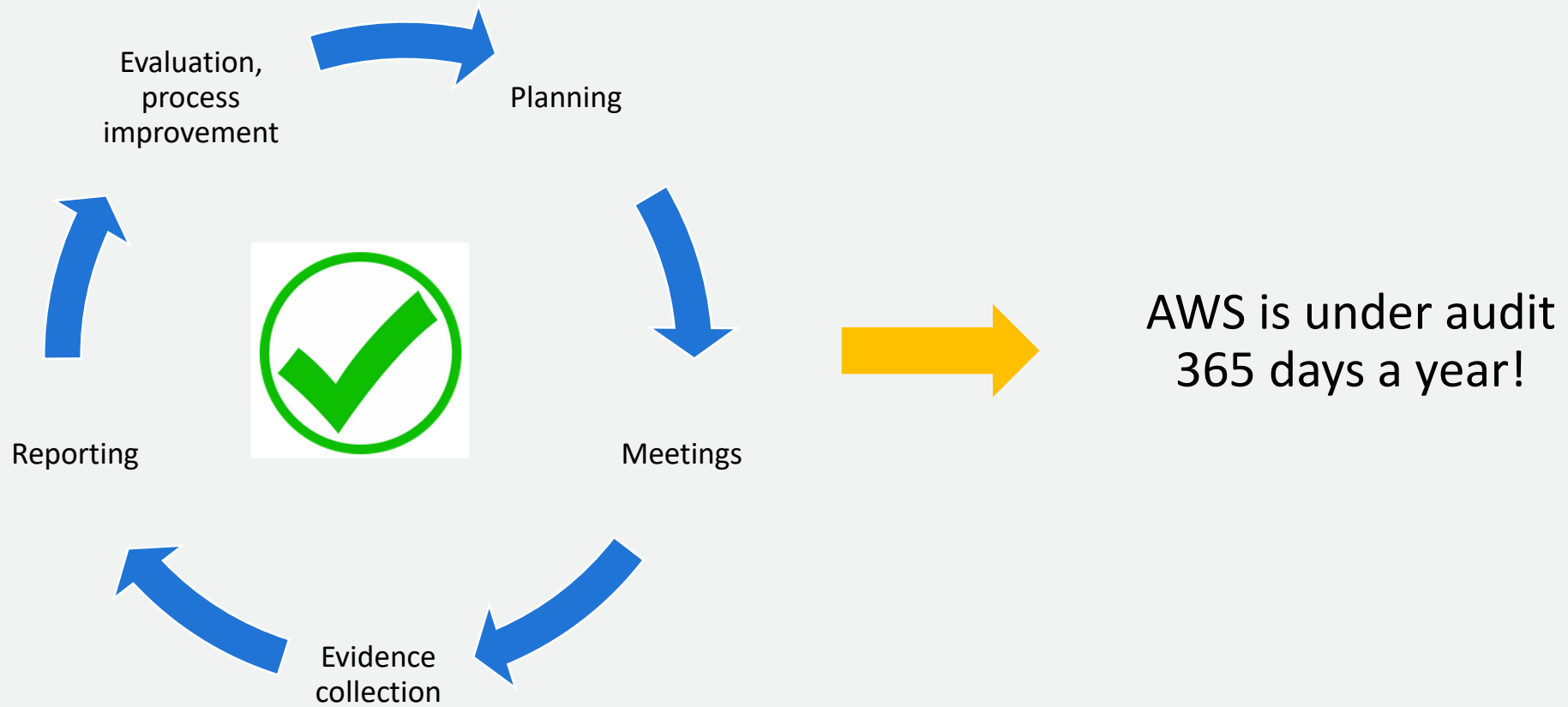
Continuous Compliance

Having the visibility into **WHO** made **WHAT** change from **WHERE** in near-real time enables you to **DETECT** mis-configurations and non-compliance and **RESPOND** quickly to **PREVENT** risks from materializing.

Cloud Compliance is a shared responsibility



AWS audit lifecycle



Customers rely on our compliance with global standards

Certifications & Attestations

- ✦ Cloud Computing Compliance Controls Catalogue (C5)
- ✦ CSA - STAR Level 2
- Cyber Essentials Plus
- DoD SRG
- ENS High
- FedRamp (Med & High)
- ✦ FINMA ISAE 3000
- FIPS
- HDS
- ISMAP
- IRAP
- ✦ ISO 22301
- ✦ ISO 27001, 27017, 27018, 27701
- ISO 9001
- K-ISMS
- ✦ MTCS – Tier 3
- ✦ OSPAR
- ✦ PCI-DSS Level 1
- ✦ PCI-3DS
- ✦ PiTukri ISAE-3000 Type II Report for Cloud Security
- ✦ SEC Rule 17-a-4(f)
- ✦ SOC 1, SOC 2, SOC 3

Laws, Regulations and Privacy

- | | | |
|----|---|----------------------------|
| DE | | CLOUD Act |
| 🌐 | ✦ | CISPE |
| GB | ✦ | GDPR |
| US | | FERPA |
| ES | ✦ | GLBA |
| US | | HIPAA |
| CH | | HITECH |
| US | | IRS 1075 |
| FR | | ITAR |
| JP | | My Number Act |
| AU | | Data Protection Act – 2018 |
| 🌐 | | VPAT / Section 508 |
| 🌐 | | PoPIA – South Africa |
| 🌐 | | Privacy Act - Australia |
| KR | | Privacy Act - New Zealand |
| SG | | PDPA: 2010 - Malaysia |
| SG | | PDPA: 2012 – Singapore |
| 📄 | | PIPEDA - Canada |
| 📄 | | PDPL – Argentina |
| FI | | LGPD – Brazil |
| US | | PDPA - Taiwan |
| 🌐 | | AAPI – Japan |

Alignments & Frameworks

- | | | | |
|----|---|------------------------------------|----|
| US | ✦ | CIS (Center for Internet Security) | 🌐 |
| EU | | CJIS (US FBI) | US |
| EU | | Cloud Security Principles | GB |
| US | ✦ | CSA (Cloud Security Alliance) | 🌐 |
| US | ✦ | FISC | JP |
| US | | FISMA | US |
| 🌐 | | G-Cloud | GB |
| US | | GxP (US FDA CFR 21 Part 11) | US |
| US | | HIPPA Quick Start Guide | US |
| JP | | HITRUST | US |
| GB | | IT Grundschutz | DE |
| US | | MITA 3.0 (US Medicaid) | US |
| ZA | ✦ | NIST 800-53 (Via FedRAMP ATO) | US |
| AU | ✦ | NIST Cybersecurity Framework (CSF) | US |
| NZ | ✦ | PCI-DSS Quick Start Guide | 📄 |
| MY | | SWIFT Client Connectivity Guide | 🌐 |
| SG | | | |
| CA | | | |
| AR | | | |
| BR | | | |
| TW | | | |
| JP | | | |

✦ = Financial Services Industry
 DE = Country of origin of compliance regime
 🌐 = industry or global standard



How AWS supports customer compliance and assurance

Manage and Oversee Risk



AWS Config



AWS Control Tower



AWS Security Hub



AWS Systems Manager



AWS Backup

Assurance of Risk Management



AWS CloudTrail



AWS Audit Manager

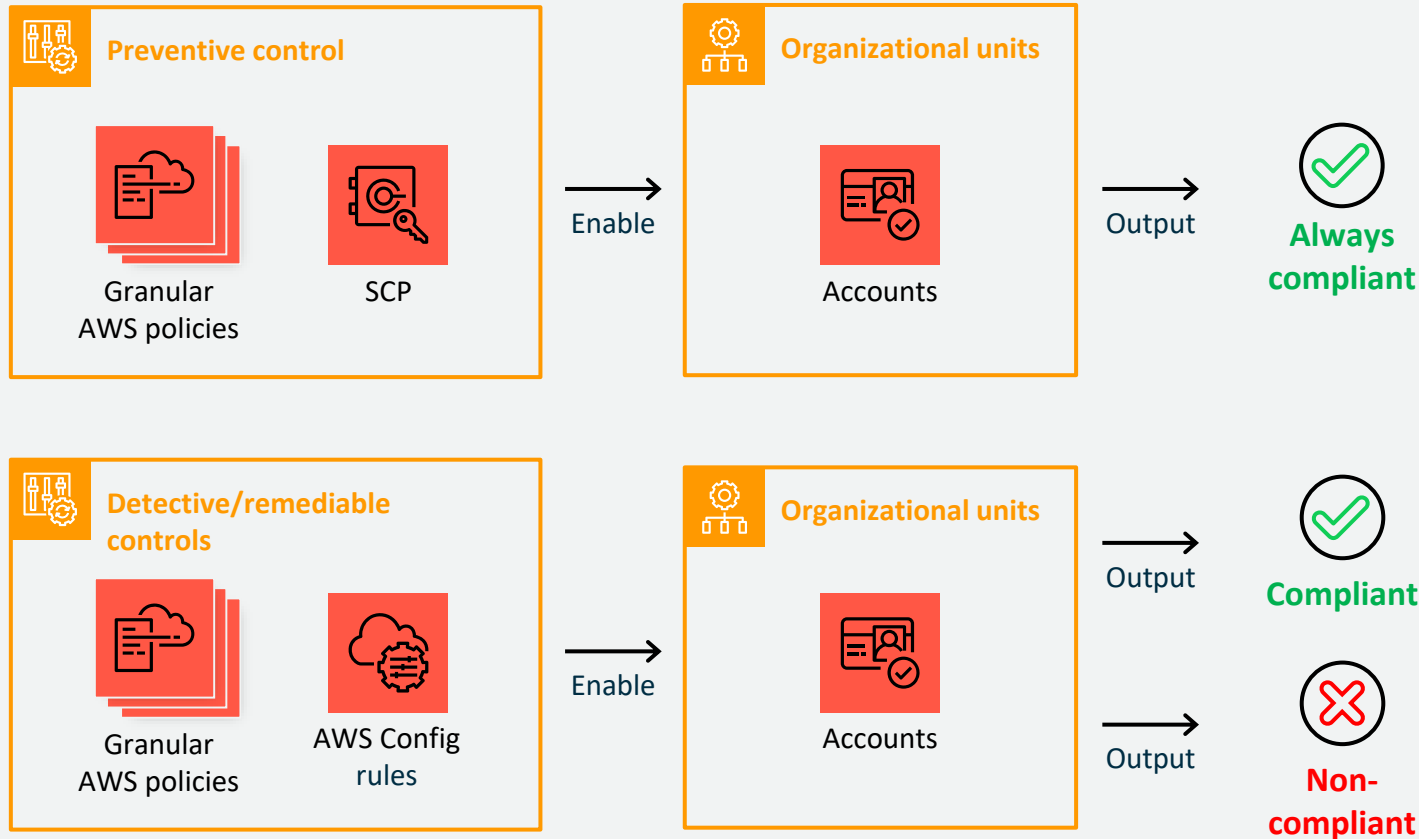


AWS Artifact

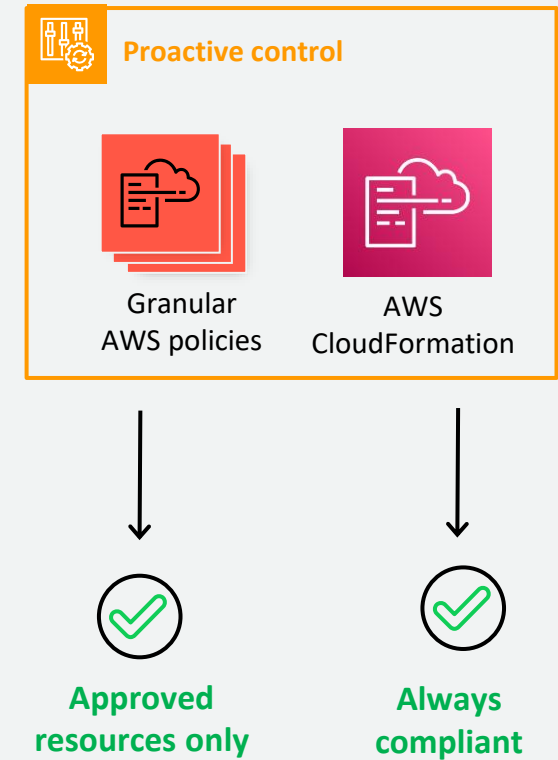


AWS Well-Architected Framework

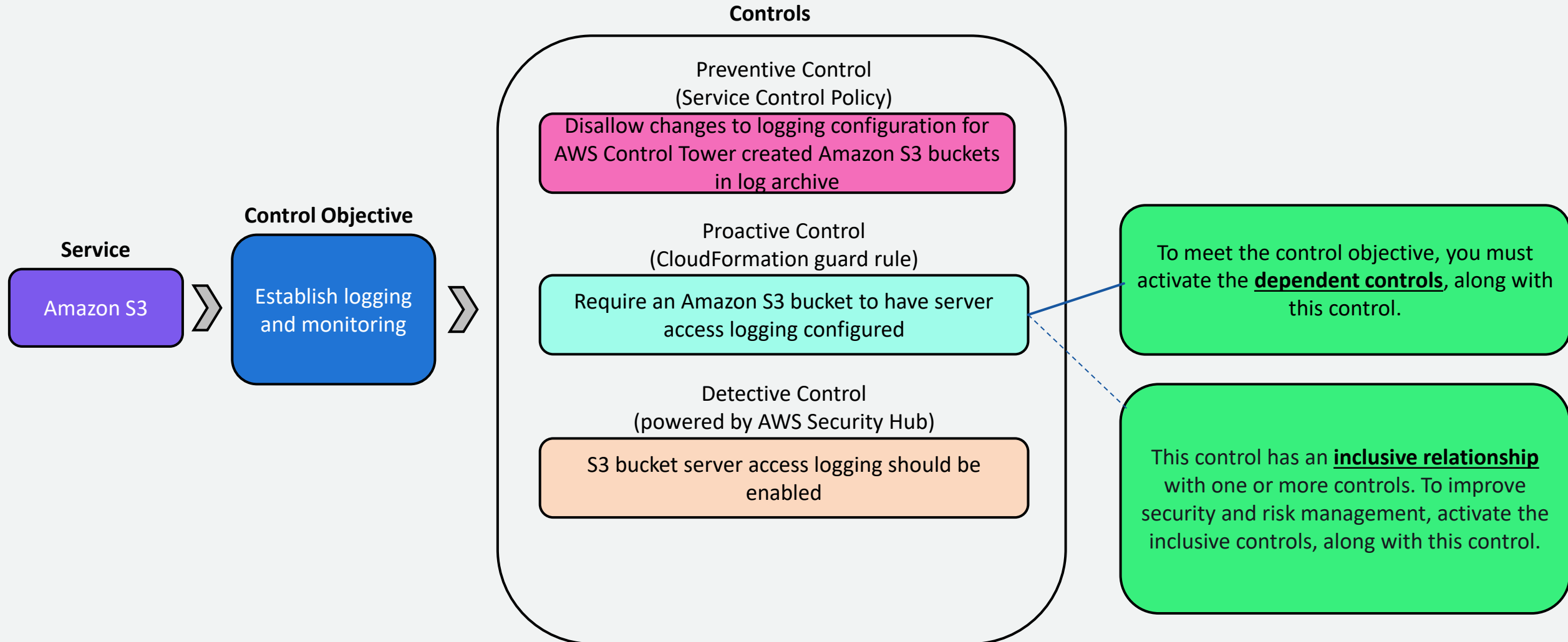
Control Tower Control Behaviors



NEW!





Example: Establish S3 logging and monitoring



Enable risk management and manage risk





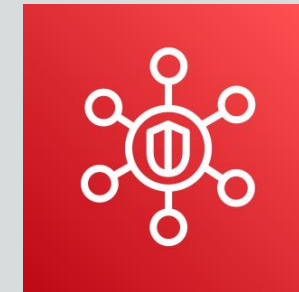
AWS Config

-  Enable AWS Config
-  Guard custom policy






AWS Systems Manager Automation

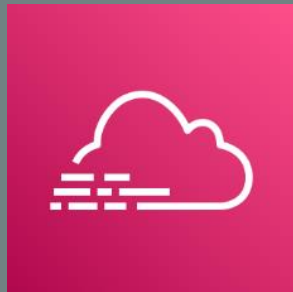
-  Automate with runbooks
-  Change manager remediation





AWS Systems Manager Change Manager

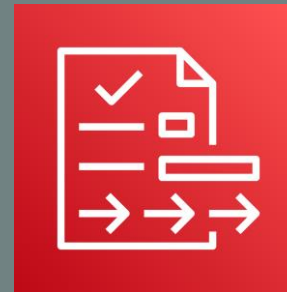
-  Enable AWS Security Hub
-  Aggregate findings
-  Automate remediation

Independent assurance





AWS CloudTrail

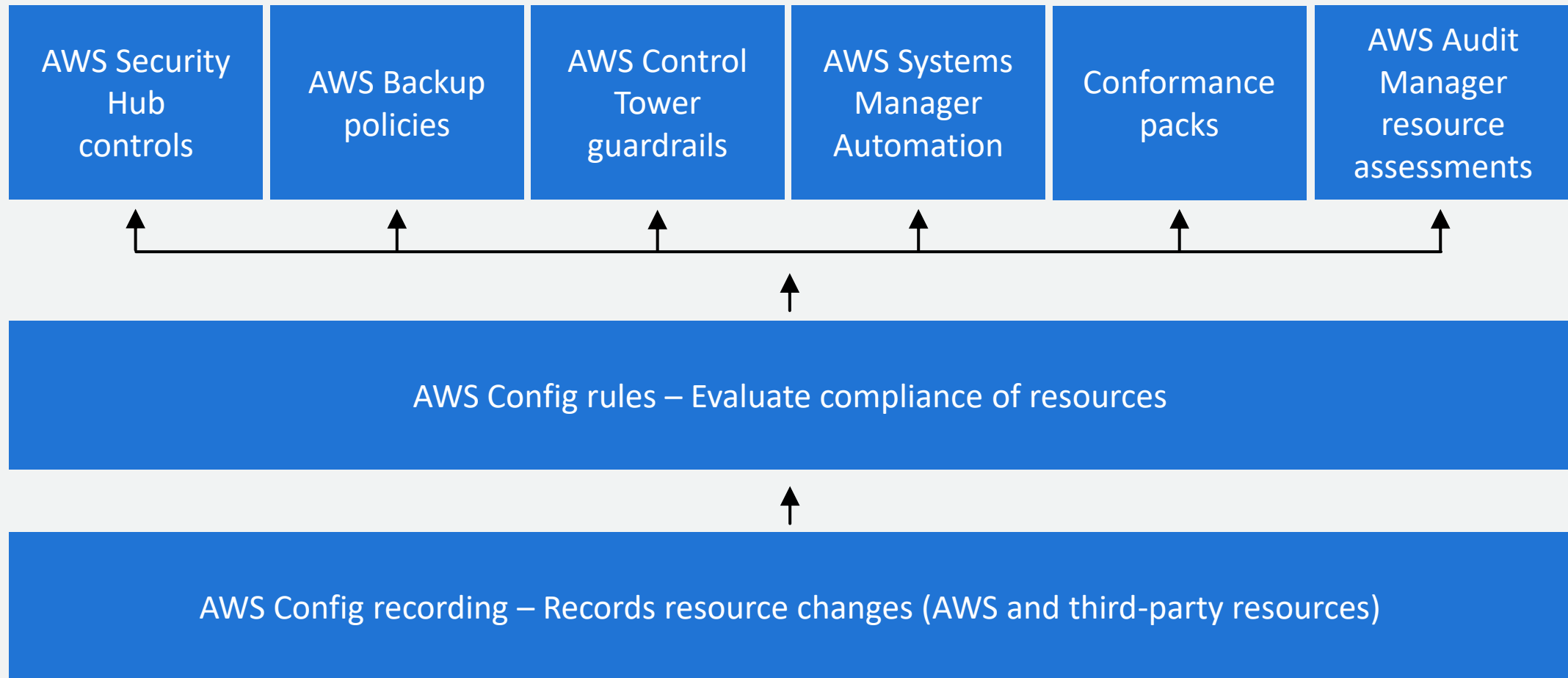
-  AWS CloudTrail Lake
-  Gather evidence



AWS Audit Manager

-  Assessment reports
-  Custom assessment reports

Controls Foundation



Continuous compliance requires insight and automation



Precise Visibility



Near-Real-Time Automation



Continuous Compliance

Having the visibility into **WHO** made **WHAT** change from **WHERE** in near-real time enables you to **DETECT** mis-configurations and non-compliance and **RESPOND** quickly to **PREVENT** risks from materializing.



Thank you!