AWS re:Invent

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

STP211-R2

Automating and evidencing key compliance security controls

Kristen Haught
Principal Security TPM
AWS

Megan O'Neil
Sr. Security SA
AWS

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

Agenda

Why are we here?

Automate and evidence common controls to scale

Putting it into practice

Demo

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

Why are we here?

HIPAA, PCI, ISO, SOC, HITRUST

Regulatory requirements

Customer requirements

Framework updates

Lessons learned

Product feature request (PFR) announcements

AWS service release notes (“What’s new”)

Evolving perspectives of cloud

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

Automate and evidence common controls

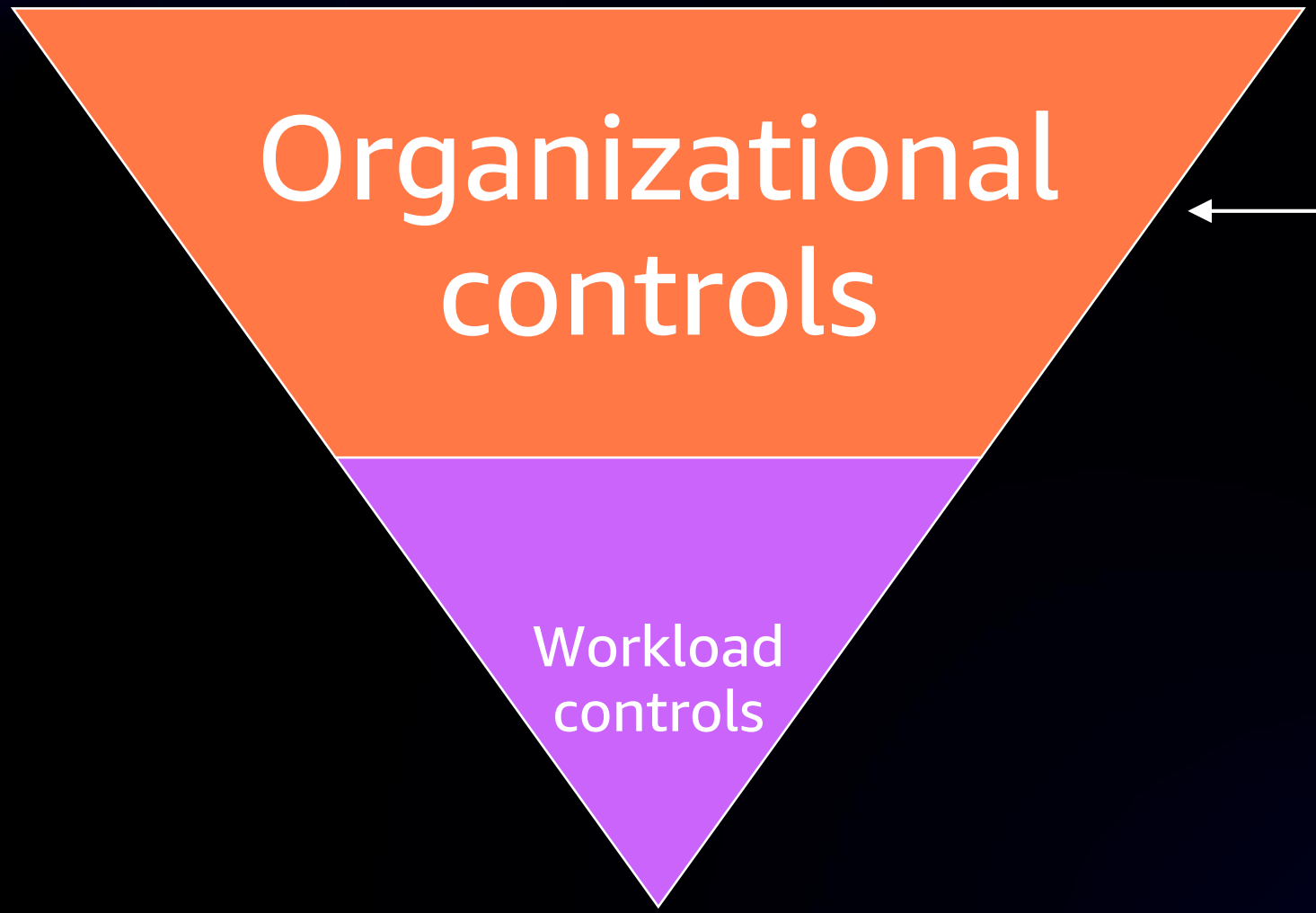
ORGANIZATIONAL AND WORKLOAD LEVEL CONTROLS



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

Automate and evidence common controls

ORGANIZATIONAL AND WORKLOAD LEVEL CONTROLS



What do you want to be **universally true** across every use of AWS?

Examples:
Enable organization-wide AWS CloudTrail
Enable Amazon GuardDuty across all accounts
Enable AWS Single Sign-On

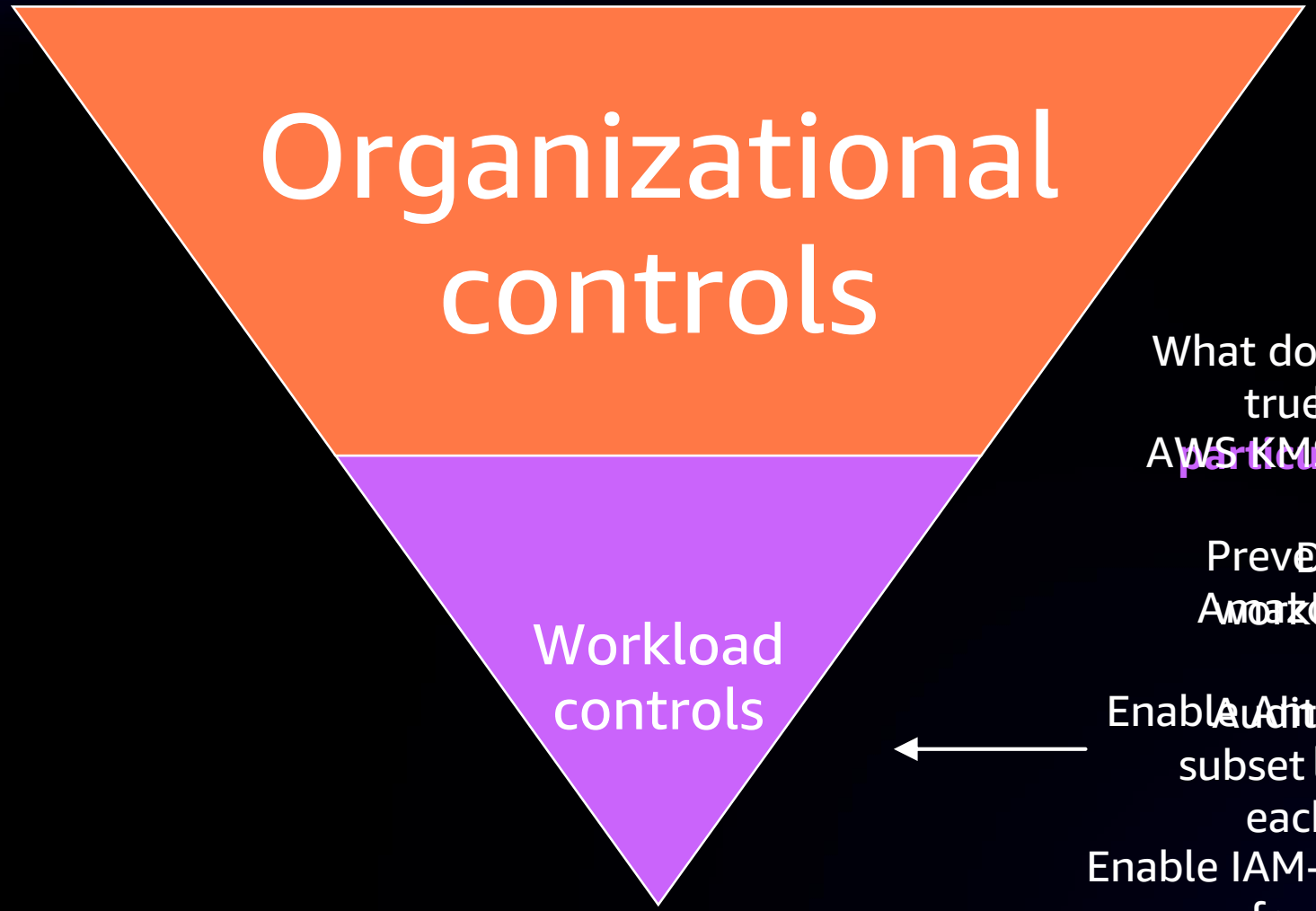
What do you want to be **universally true** across every use of AWS?

Examples:
Enable AWS KMS use
Deploy once, enforce everywhere
Encrypt Amazon RDS storage
Audit once, validate everywhere
Encrypt Amazon RDS snapshot

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

Automate and evidence common controls

ORGANIZATIONAL AND WORKLOAD LEVEL CONTROLS



What do you want to be true for any workload?

Examples:
Deploy in a particular workload account
Audit only a small subset of controls for each workload

Prevent unencrypted Amazon RDS instance
AWS KMS Key ID is defined

Enable Amazon S3 Object Lock legal hold

Enable IAM-based authentication for Amazon RDS

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

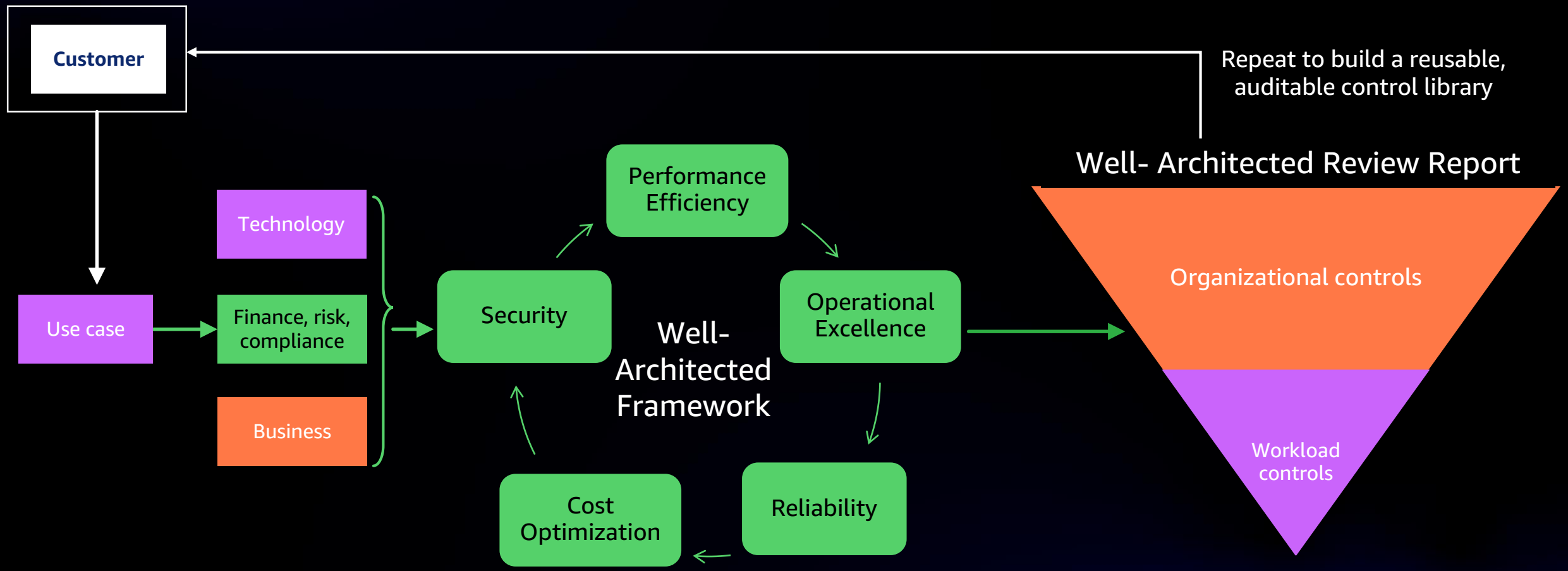
Putting this into practice…

- How do you determine the appropriate common controls for you?
- How do you build and deploy common controls?
- How do you know whether to deploy them at the organizational or workload layer?
- How do you audit these with minimal impact to your teams?

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

Mechanism to determine common controls

A MECHANISM TO ALIGN PEOPLE, PROCESS, AND TECHNOLOGY IS NECESSARY TO SCALE COMPLIANCE

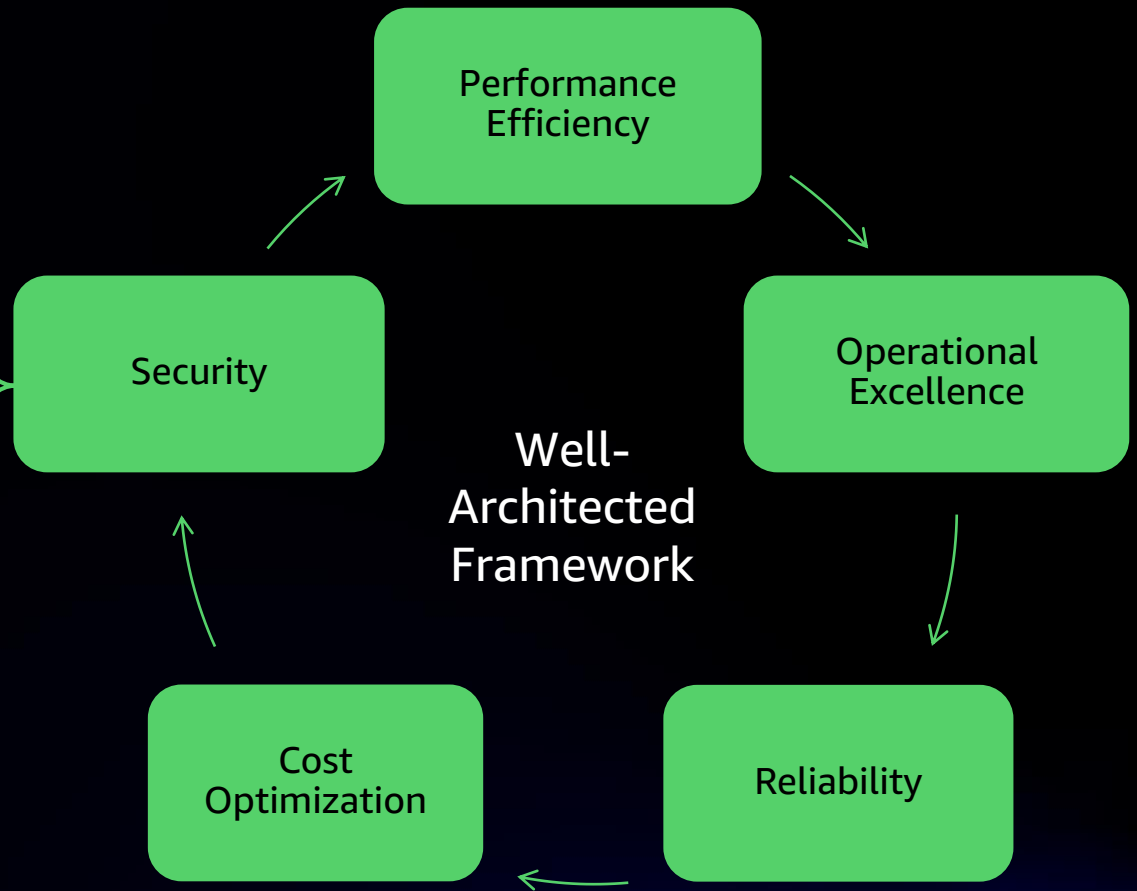


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use common framework to determine controls

LEVERAGE THE SECURITY PILLAR TO ALIGN WITH AWS SECURITY BEST PRACTICES

- Security, compliance, and governance
- Data protection
- Infrastructure protection
- Identity and access management
- Detection
- Incident response



https://wa.aws.amazon.com/wat.map.en.html

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

Well-Architected Framework Security Pillar

QUESTIONS CAPTURE CONTEXT TO HELP DETERMINE THE APPROPRIATE CONTROLS FOR YOUR USE CASE

Security, compliance, and governance	SEC 1: How do you securely operate your workload?
Identity and access management	SEC 2: How do you manage identities? SEC 3: How do you manage permissions?
Detection	SEC 4: How do you detect and investigate security events?
Infrastructure protection	SEC 5: How do you protect your network resources? SEC 6: How do you protect your compute resources?
Data protection	SEC 7: How do you classify your data? SEC 8: How do you protect your data at rest? SEC 9: How do you protect your data in transit?
Incident response	SEC 10: How do you anticipate, respond to, and recover from incidents?

aws

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

Well-Architected Framework Security Pillar

ASSOCIATED GUIDANCE HELPS YOU IDENTIFY AWS SERVICES AVAILABLE TO AUTOMATE CONTROLS

Security, compliance, and governance	SEC 1: How do you securely operate your workloads? AWS Control Tower, AWS CloudFormation, AWS Service Catalog
Identity and access management	SEC 2: How do you manage identities? SEC 3: How do you manage permissions for people and machines? AWS Identity and Access Management (IAM), developer and system tools, AWS SSO, AWS Organizations SCPs
Detection	SEC 4: How do you detect and investigate security events? AWS Security Hub, Amazon GuardDuty, Amazon CloudWatch, AWS Config/AWS Config rules, AWS CloudTrail
Infrastructure protection	SEC 5: How do you protect your network resources? SEC 6: How do you protect your compute resources? AWS WAF, AWS Systems Manager, VPC/VPC endpoints, Security Groups
Data protection	SEC 7: How do you classify your data? SEC 8: How do you protect your data at rest? SEC 9: How do you protect your data in transit? AWS KMS, AWS Certificate Manager (ACM)
Incident response	SEC 10: How do you anticipate, respond to, and recover from incidents? AWS Config rules, Amazon Detective, AWS Lambda

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

Well-Architected Framework Security Pillar

ASSOCIATED GUIDANCE HELPS YOU IDENTIFY AWS SERVICES AVAILABLE TO AUTOMATE CONTROLS

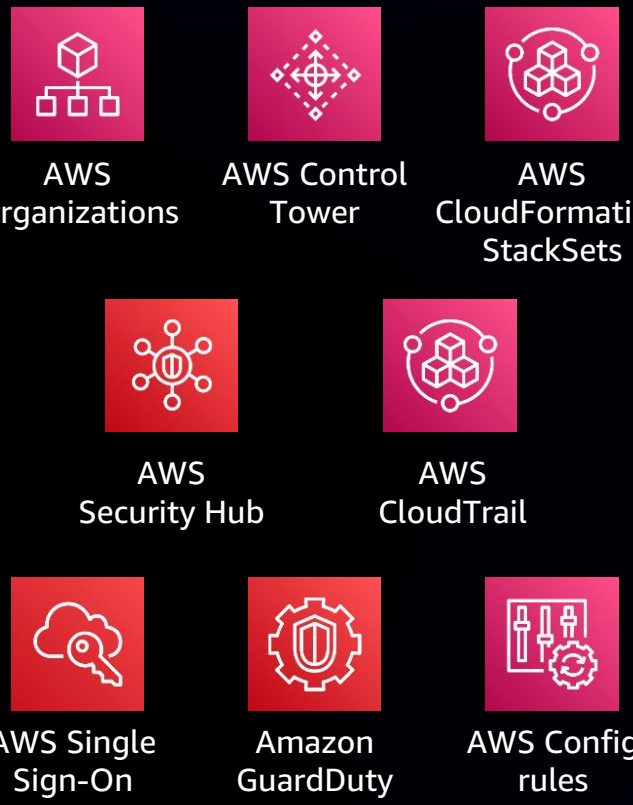
- Security, compliance, and governance
  - SEC 1: How do you securely operate your workload?
  - ISO A.8.1.1 Inventory of assets shall be drawn up and maintained.
- Identity and access management
  - SEC 2: How do you manage identities?
  - SEC 3: How do you manage permissions?
  - NIST 800-53: The information system implements multifactor authentication for local access to accounts.
- Detection
  - SEC 4: How do you detect and investigate security events?
  - HIPAA 164.308(a)(5)(ii)(c): Procedures for monitoring log-in attempts and reporting discrepancies.
- Infrastructure protection
  - SEC 5: How do you protect your network resources?
  - SEC 6: How do you protect your compute resources?
  - PCI 6.2: Install critical security patches within one month of release.
- Data protection
  - SEC 7: How do you classify your data?
  - SEC 8: How do you protect your data at rest?
  - SEC 9: How do you protect your data in transit?
  - SOC 2 Common Criteria 5.7: Entity data is protected during transmission.
- Incident response
  - SEC 10: How do you anticipate, respond to, and recover from incidents?
  - CIS SIM-05: Events which could represent a security incident are classified

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

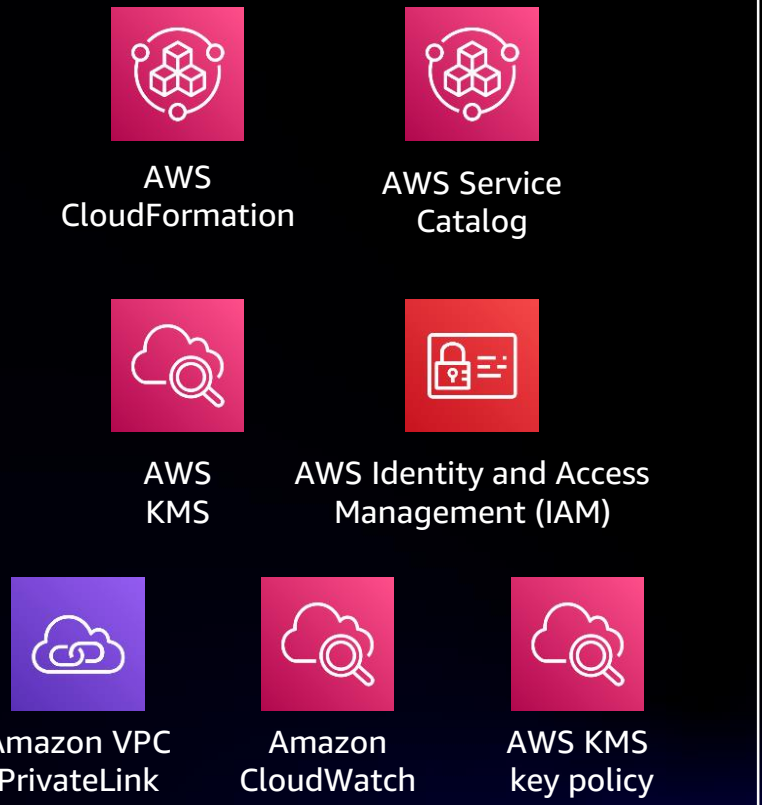
Build and deploy common controls

USE AWS SERVICES TO AUTOMATE ORGANIZATIONAL AND WORKLOAD LEVEL CONTROLS

Organizational controls

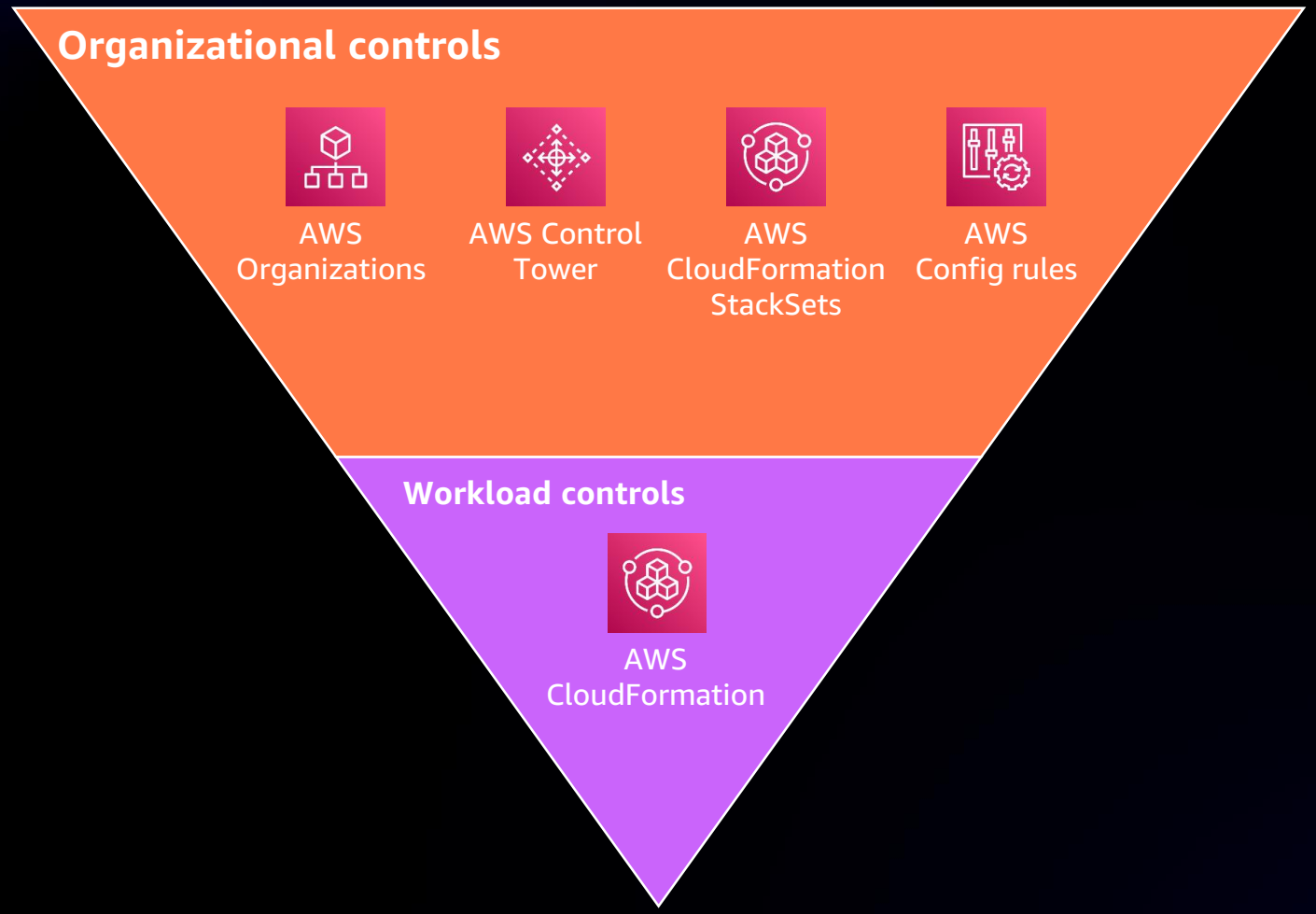


Workload controls



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

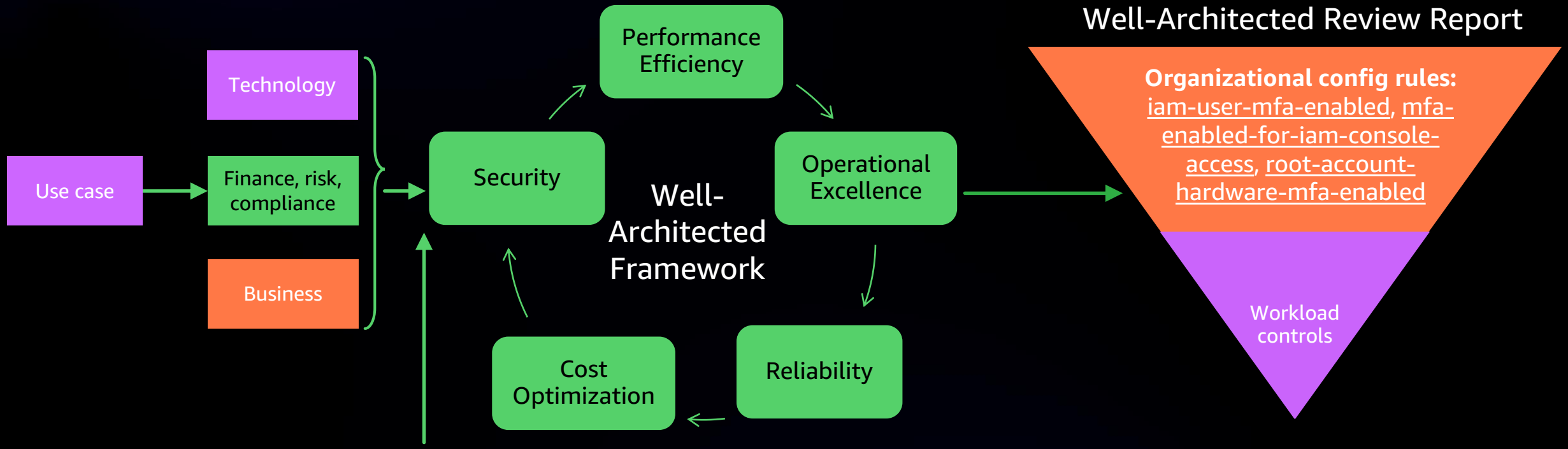
How do you audit & report on common controls?



1. Inspect configuration of controls
2. Sample once for automated controls
3. Assess remediation if noncompliance is detected
4. Report across audits, leveraging mappings to common framework

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

Now let’s tie it all together



Audit → NIST 800-53: The information system implements multifactor authentication for local access to accounts

aws

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

Thank you!

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