# aws INNOVATE

ONLINE CONFERENCE

INNOVATE
ONLINE CONFERENCE

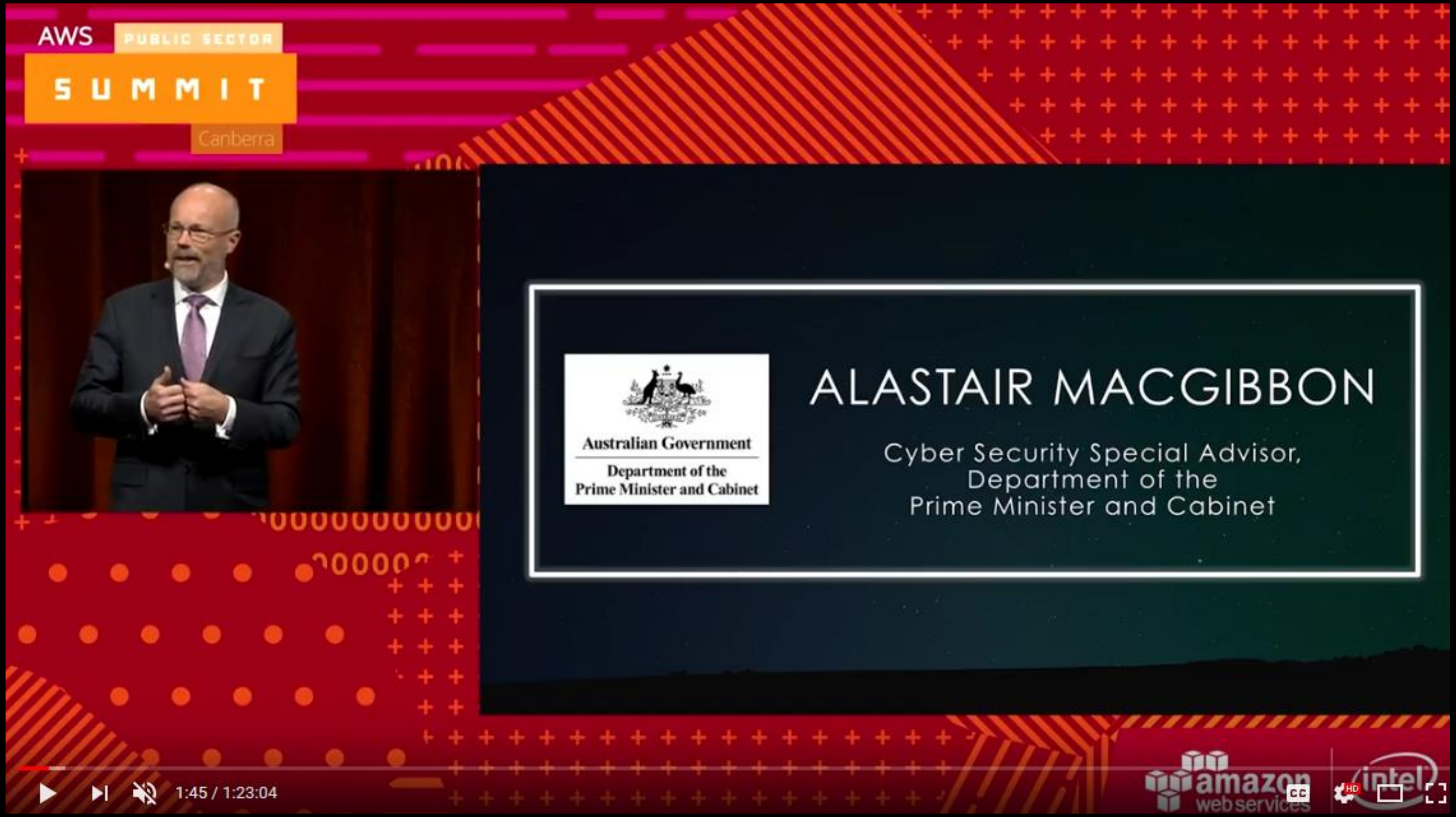
# Cloud security fundamentals

Phil Rodrigues
Principal Security Solutions Architect, AWS

# Voices of our **government customers**

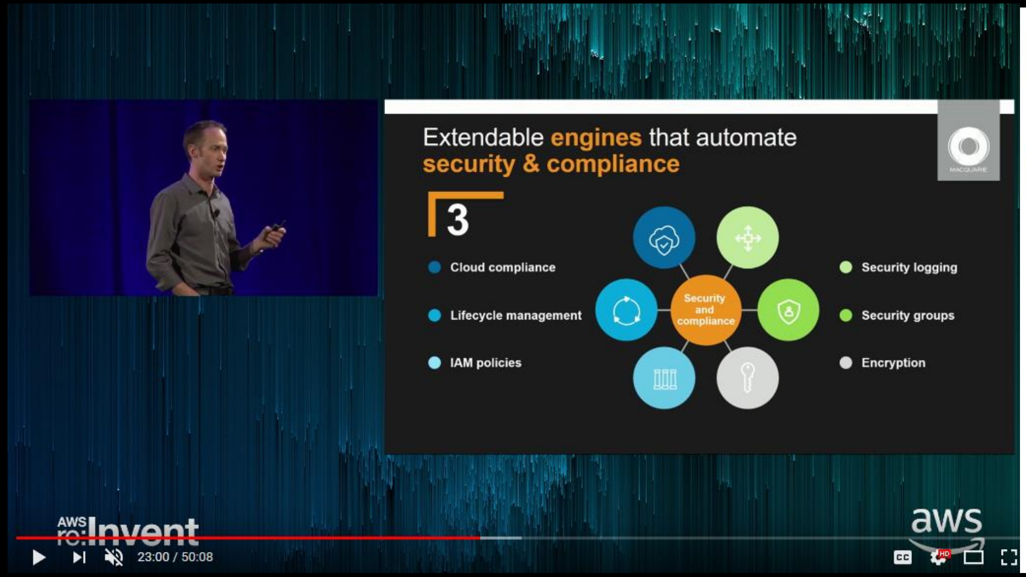
"Innovation and cloud help form the basis on which we will make the Australian government more secure.

Innovation is good. Cloud is good—because it helps us move off from legacy systems. Our biggest risk is indeed legacy systems."


AWS
PUBLIC SECTOR
SUMMIT
Canberra
Australian Government
Department of the Prime Minister and Cabinet
ALASTAIR MACGIBBON
Cyber Security Special Advisor, Department of the Prime Minister and Cabinet
1:45 / 1:23:04
amazon webservices
intel

# Voices of our banking customers

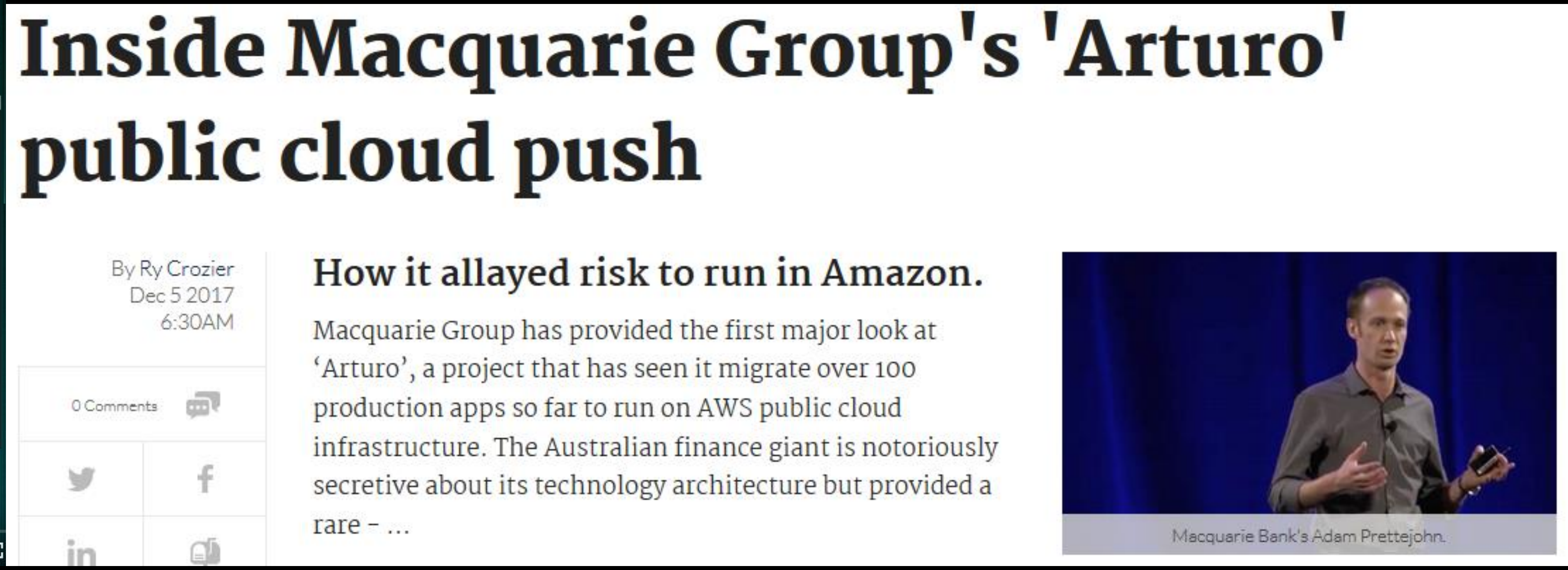
MACQUARIE
BANK



Extendable **engines** that automate **security & compliance**

3

- Cloud compliance
- Lifecycle management
- IAM policies
- Security logging
- Security groups
- Encryption



## Inside Macquarie Group's 'Arturo' public cloud push

By Ry Crozier
Dec 5 2017
6:30AM

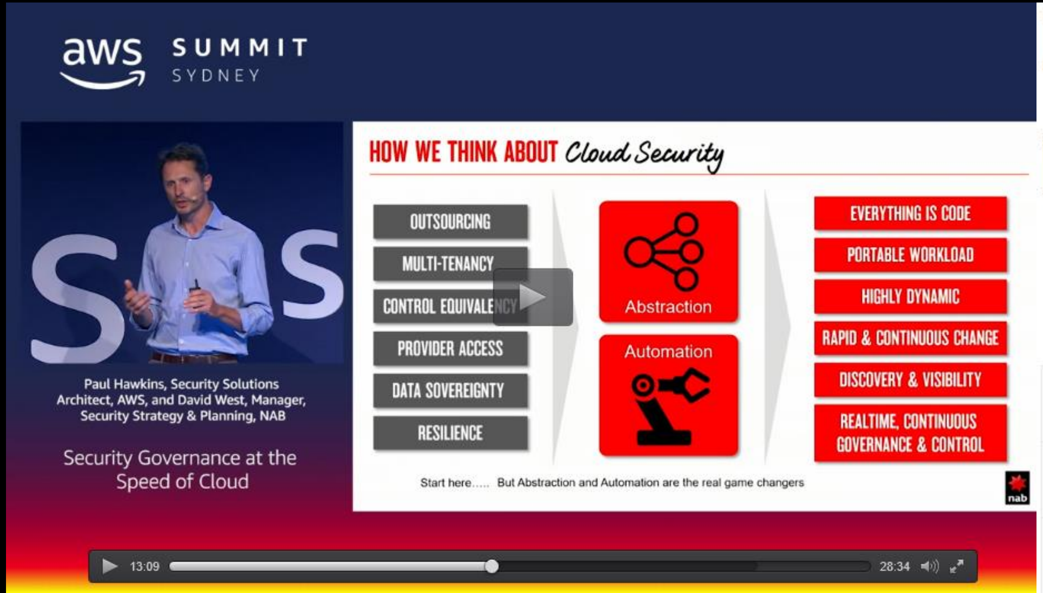
0 Comments

### How it allayed risk to run in Amazon.

Macquarie Group has provided the first major look at ‘Arturo’, a project that has seen it migrate over 100 production apps so far to run on AWS public cloud infrastructure. The Australian finance giant is notoriously secretive about its technology architecture but provided a rare - ...

Macquarie Bank's Adam Prettejohn.

nab



Paul Hawkins, Security Solutions Architect, AWS, and David West, Manager, Security Strategy & Planning, NAB

Security Governance at the Speed of Cloud

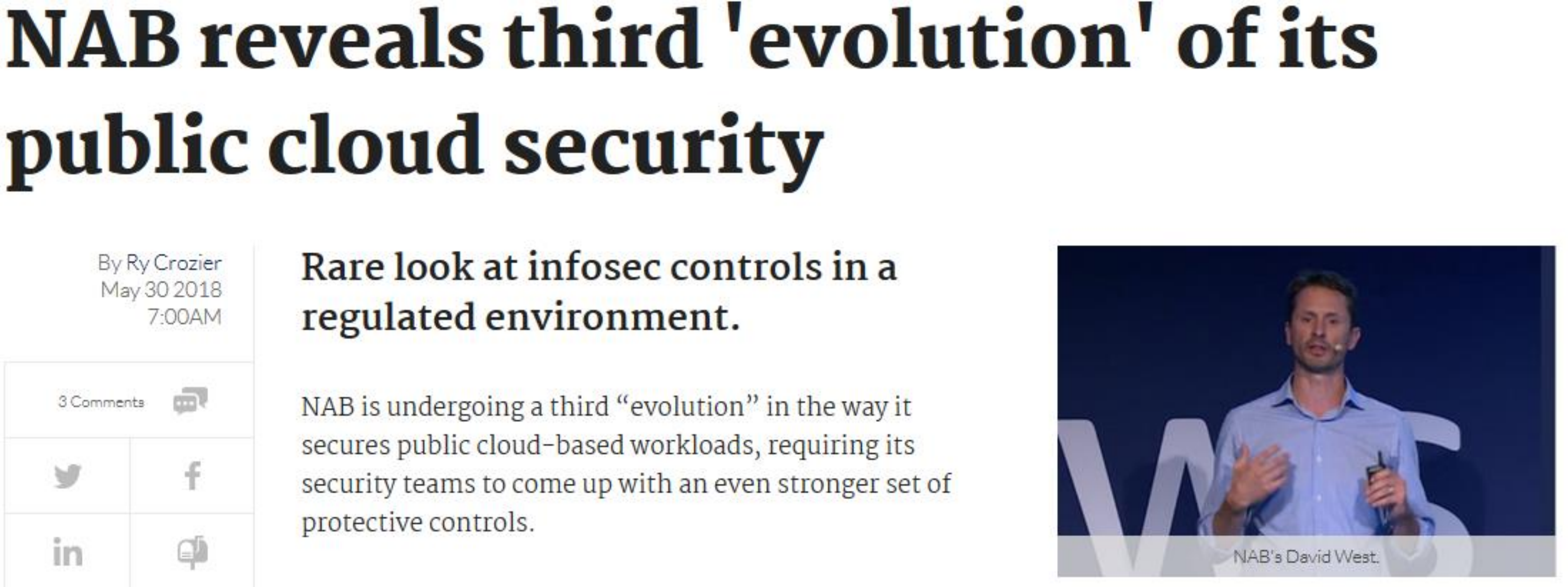
HOW WE THINK ABOUT *Cloud Security*

- OUTSOURCING
- MULTI-TENANCY
- CONTROL EQUIVALENCY
- PROVIDER ACCESS
- DATA SOVEREIGNTY
- RESILIENCE

- Abstraction
- Automation

- EVERYTHING IS CODE
- PORTABLE WORKLOAD
- HIGHLY DYNAMIC
- RAPID & CONTINUOUS CHANGE
- DISCOVERY & VISIBILITY
- REALTIME, CONTINUOUS GOVERNANCE & CONTROL

Start here..... But Abstraction and Automation are the real game changers



## NAB reveals third 'evolution' of its public cloud security

By Ry Crozier
May 30 2018
7:00AM

3 Comments

### Rare look at infosec controls in a regulated environment.

NAB is undergoing a third “evolution” in the way it secures public cloud-based workloads, requiring its security teams to come up with an even stronger set of protective controls.

NAB's David West.

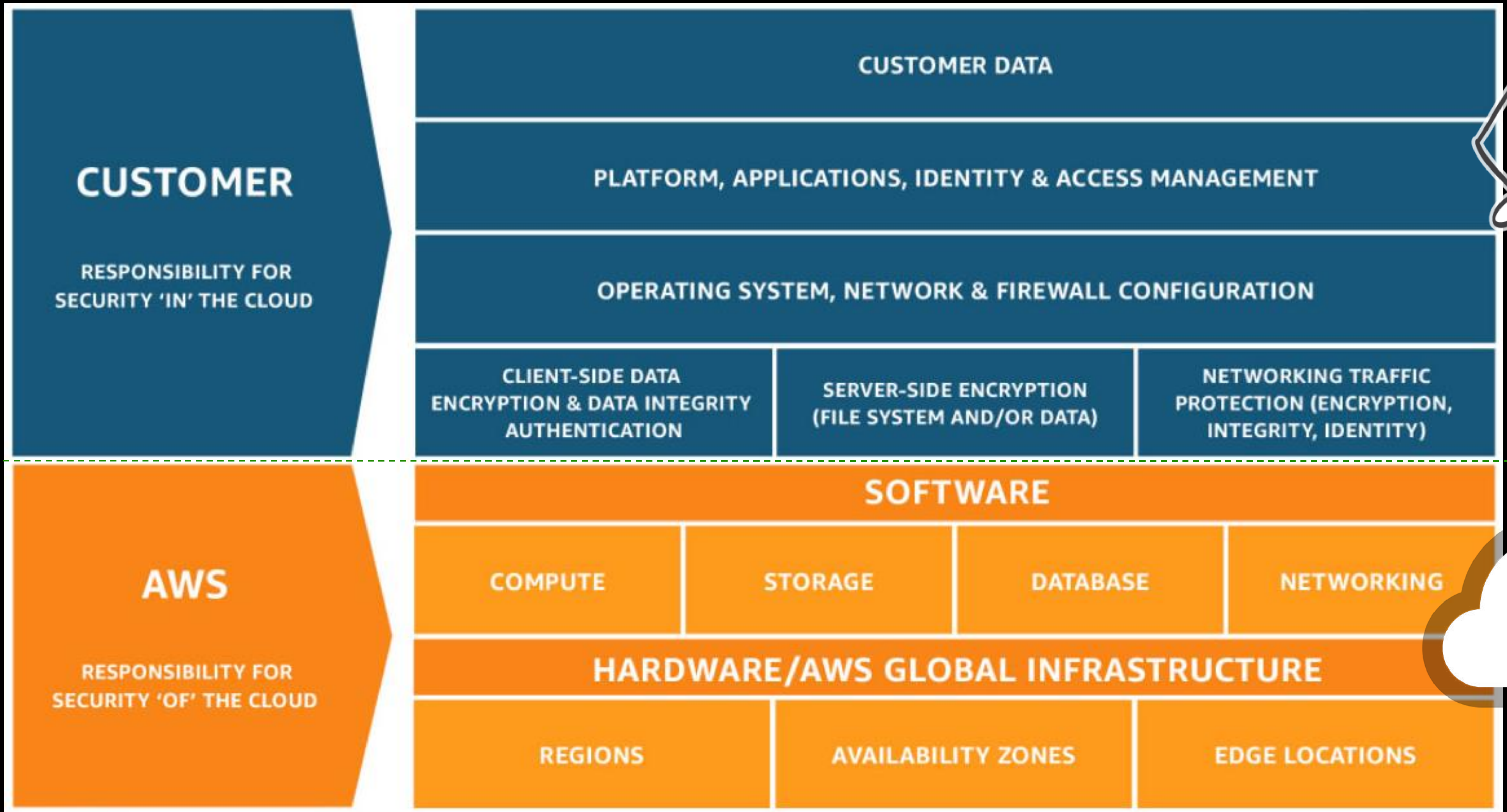
# Voices of all of our customers

AUSTRALIA POST
TELSTRA
ATLASSIAN
nib
carsales
REA Group
Transurban
origin
xero

# Agenda

- AWS **shared responsibility model**
- Security **of** the cloud
- Security **in** the cloud
- Resources

# AWS shared **responsibility model**



**CUSTOMER**

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

| | | |
|---|---|---|
| CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION | SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA) | NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY) |

**AWS**

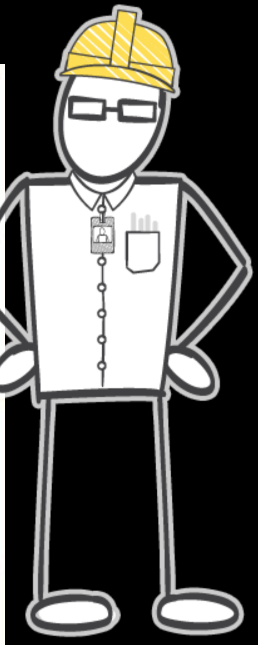
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

| | | | |
|---|---|---|---|
| COMPUTE | STORAGE | DATABASE | NETWORKING |

HARDWARE/AWS GLOBAL INFRASTRUCTURE

| | | |
|---|---|---|
| REGIONS | AVAILABILITY ZONES | EDGE LOCATIONS |



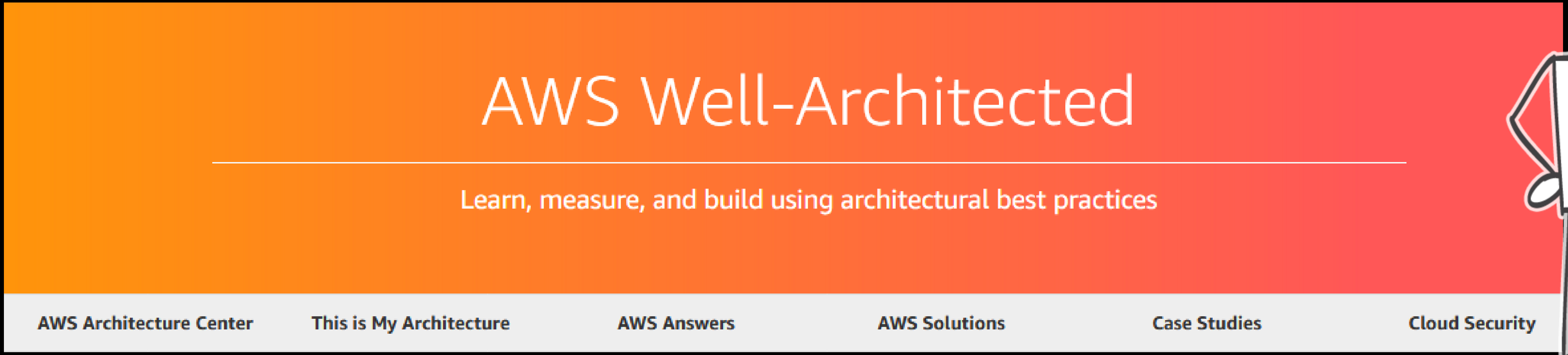
Security **in** the cloud

Managed by **customers**

Security **of** the cloud

Managed by **AWS**

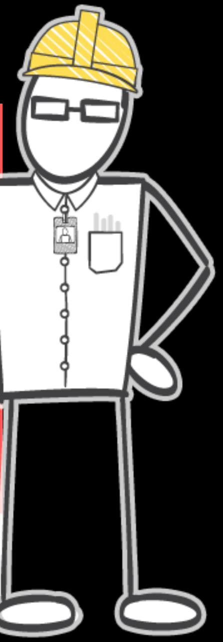
# AWS shared **responsibility model**



AWS Well-Architected

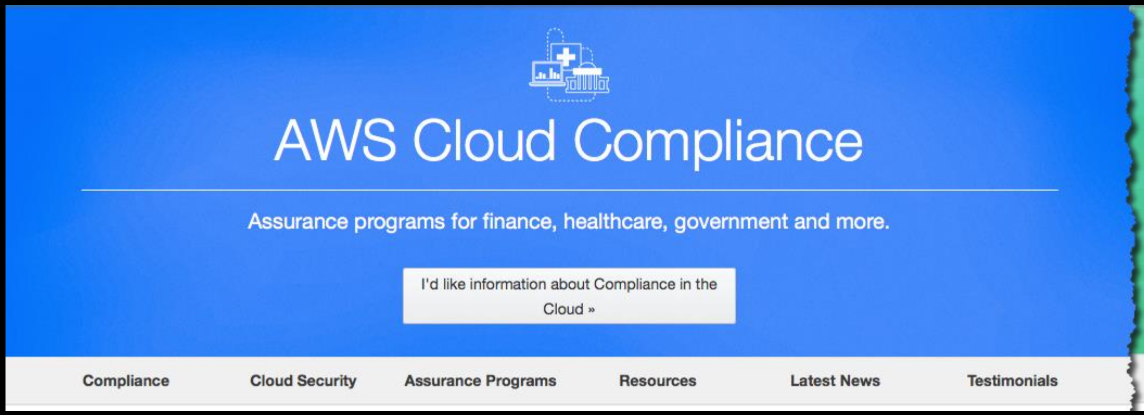
Learn, measure, and build using architectural best practices

AWS Architecture Center | This is My Architecture | AWS Answers | AWS Solutions | Case Studies | Cloud Security



Security **in** the cloud

Managed by **customers**

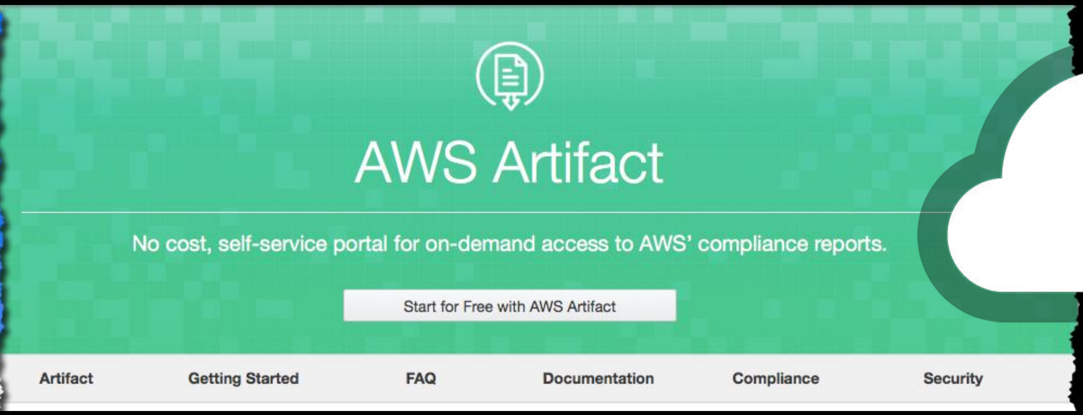


AWS Cloud Compliance

Assurance programs for finance, healthcare, government and more.

I'd like information about Compliance in the Cloud »

Compliance | Cloud Security | Assurance Programs | Resources | Latest News | Testimonials



AWS Artifact

No cost, self-service portal for on-demand access to AWS' compliance reports.

Start for Free with AWS Artifact

Artifact | Getting Started | FAQ | Documentation | Compliance | Security

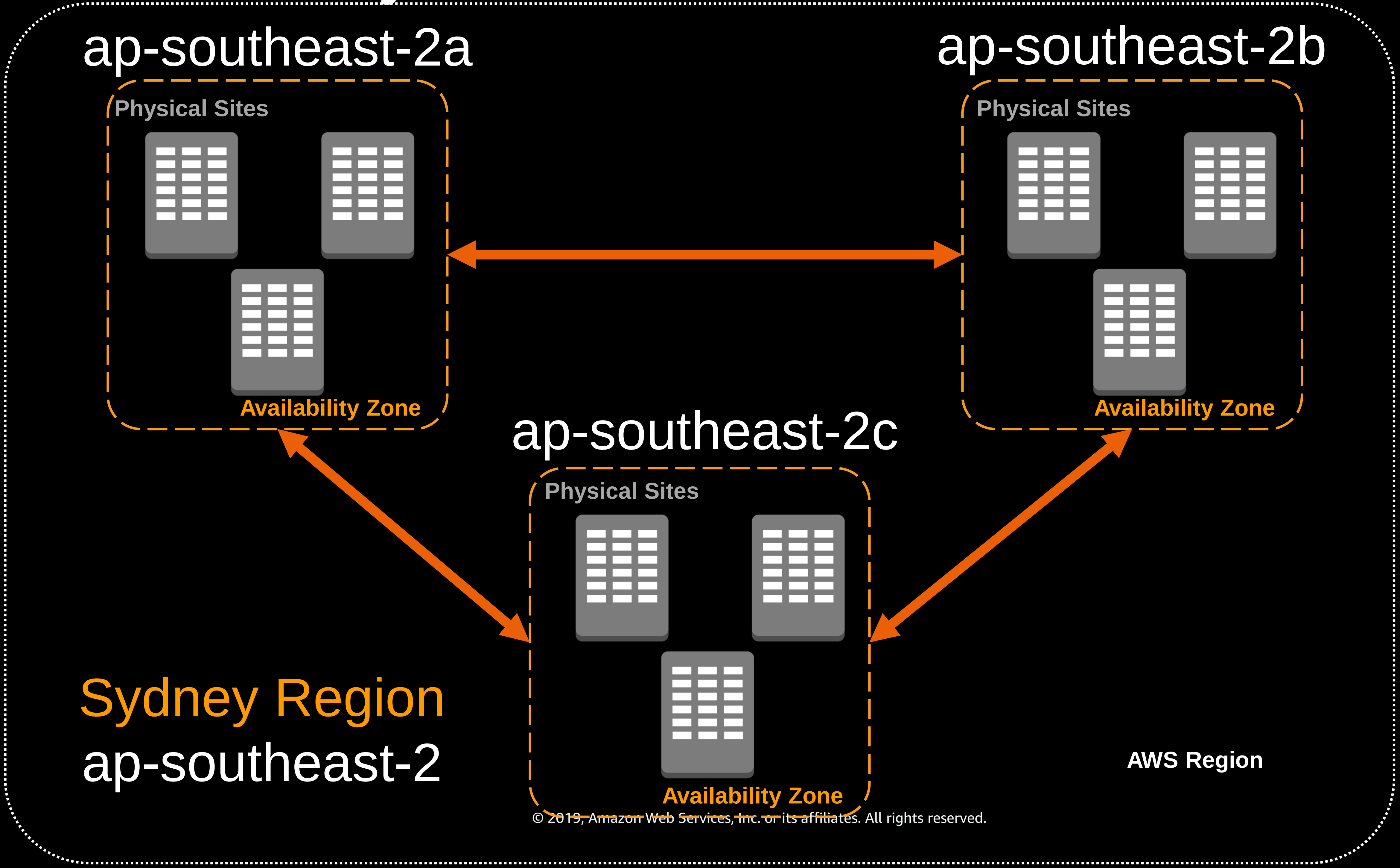
Security **of** the cloud

Managed by **AWS**

# Security of the cloud

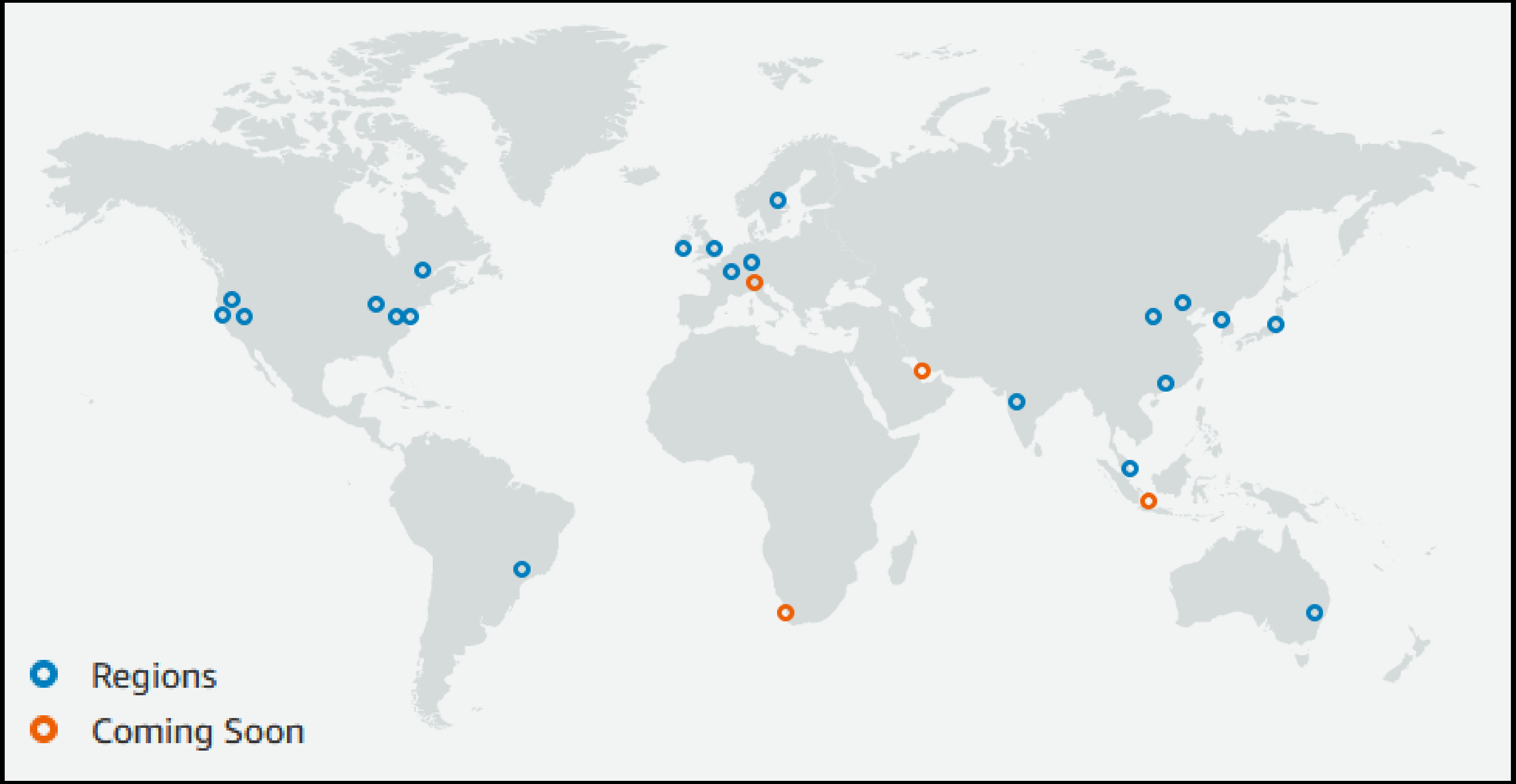
Managed by AWS

# AWS Availability Zones



# AWS global infrastructure

**21** Regions – **66** Availability Zones – **169** Network PoPs



https://aws.amazon.com/about-aws/global-infrastructure/

## Region & Number of Availability Zones

**AWS GovCloud (US)**

US-East (3)
US-West (3)

**US West**

Oregon (3)
Northern California (3)

**US East**

N. Virginia (6), Ohio (3)

**Canada**

Central (2)

**South America**

São Paulo (3)

**EU**

Ireland (3)
Frankfurt (3)
London (3)
Paris (3)
Stockholm (3)

**Asia Pacific**

Singapore (3)
Sydney (3), Tokyo (4)
Seoul (2), Mumbai (2)
Osaka (1)
Hong Kong (3)

**China**

Beijing (2)
Ningxia (3)

## Announced Regions

Bahrain, Cape Town, Jakarta, and Milan

# Does my content stay in the AWS Region?

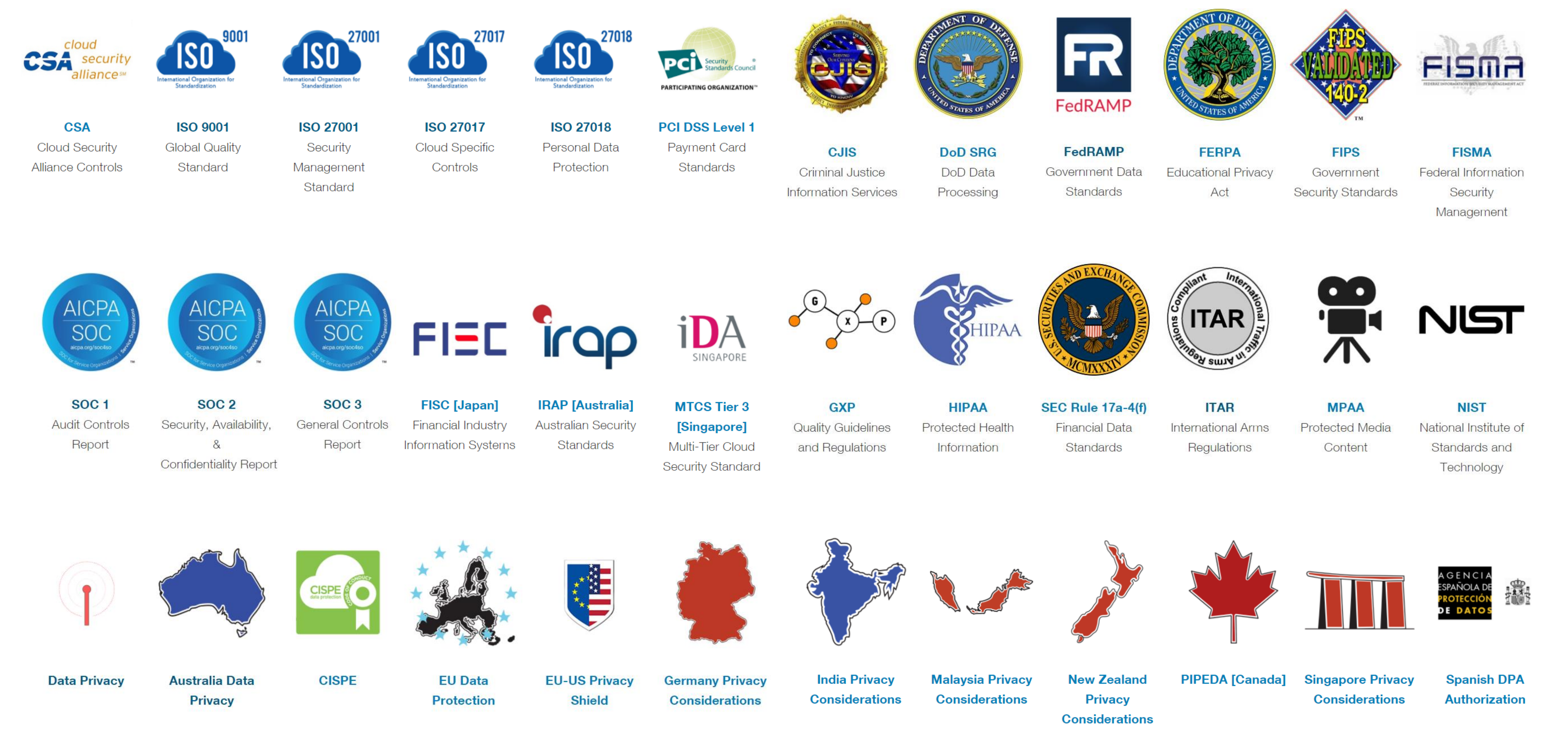
Choose an AWS Region and your customer content will not leave that country unless you move it

Control who can access content

Control format, accuracy, and encryption any way that you choose

Control content life cycle and disposal

# AWS compliance programs



CSA
Cloud Security Alliance Controls

ISO 9001
Global Quality Standard

ISO 27001
Security Management Standard

ISO 27017
Cloud Specific Controls

ISO 27018
Personal Data Protection

PCI DSS Level 1
Payment Card Standards

CJIS
Criminal Justice Information Services

DoD SRG
DoD Data Processing

FedRAMP
Government Data Standards

FERPA
Educational Privacy Act

FIPS
Government Security Standards

FISMA
Federal Information Security Management

SOC 1
Audit Controls Report

SOC 2
Security, Availability, & Confidentiality Report

SOC 3
General Controls Report

FISC [Japan]
Financial Industry Information Systems

IRAP [Australia]
Australian Security Standards

MTCS Tier 3 [Singapore]
Multi-Tier Cloud Security Standard

GXP
Quality Guidelines and Regulations

HIPAA
Protected Health Information

SEC Rule 17a-4(f)
Financial Data Standards

ITAR
International Arms Regulations

MPAA
Protected Media Content

NIST
National Institute of Standards and Technology

Data Privacy

Australia Data Privacy

CISPE

EU Data Protection

EU-US Privacy Shield

Germany Privacy Considerations

India Privacy Considerations

Malaysia Privacy Considerations

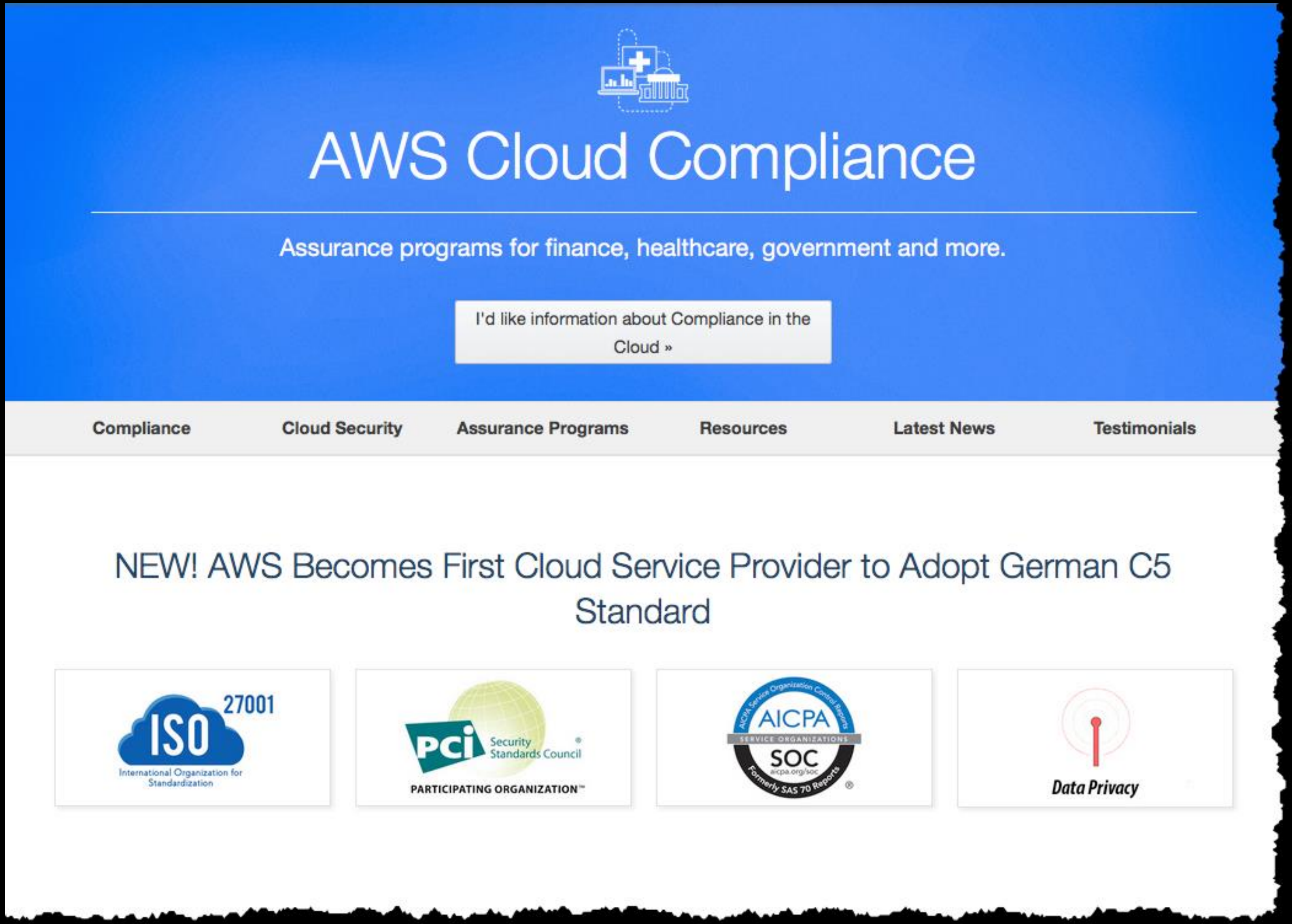
New Zealand Privacy Considerations

PIPEDA [Canada]

Singapore Privacy Considerations

Spanish DPA Authorization

# Accessing AWS compliance reports

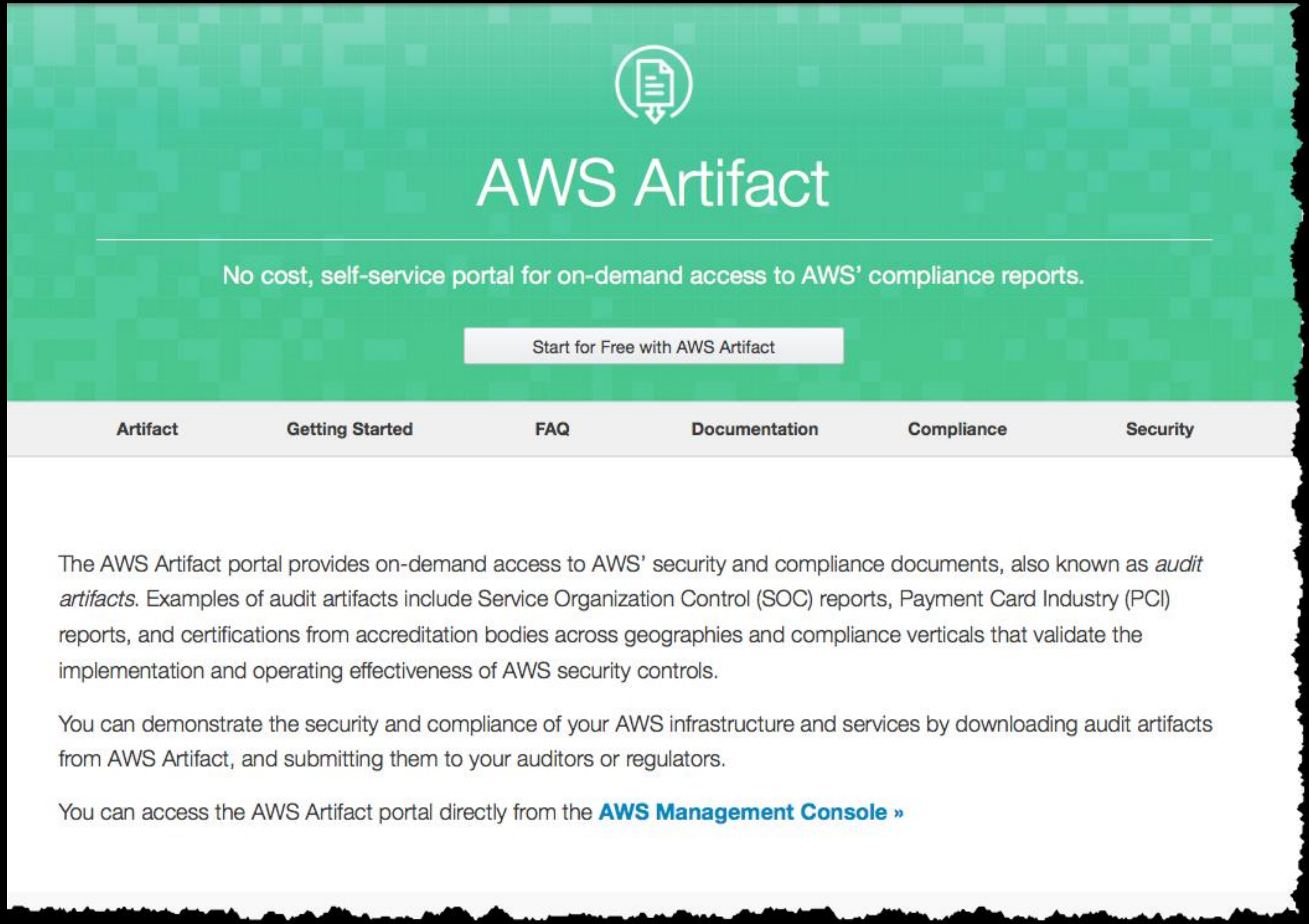


## AWS Cloud Compliance

Assurance programs for finance, healthcare, government and more.

NEW! AWS Becomes First Cloud Service Provider to Adopt German C5 Standard

ISO 27001
International Organization for Standardization
PCI Security Standards Council
PARTICIPATING ORGANIZATION™
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports
Data Privacy



## AWS Artifact

No cost, self-service portal for on-demand access to AWS' compliance reports.

The AWS Artifact portal provides on-demand access to AWS' security and compliance documents, also known as *audit artifacts*. Examples of audit artifacts include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

You can demonstrate the security and compliance of your AWS infrastructure and services by downloading audit artifacts from AWS Artifact, and submitting them to your auditors or regulators.

You can access the AWS Artifact portal directly from the **AWS Management Console »**

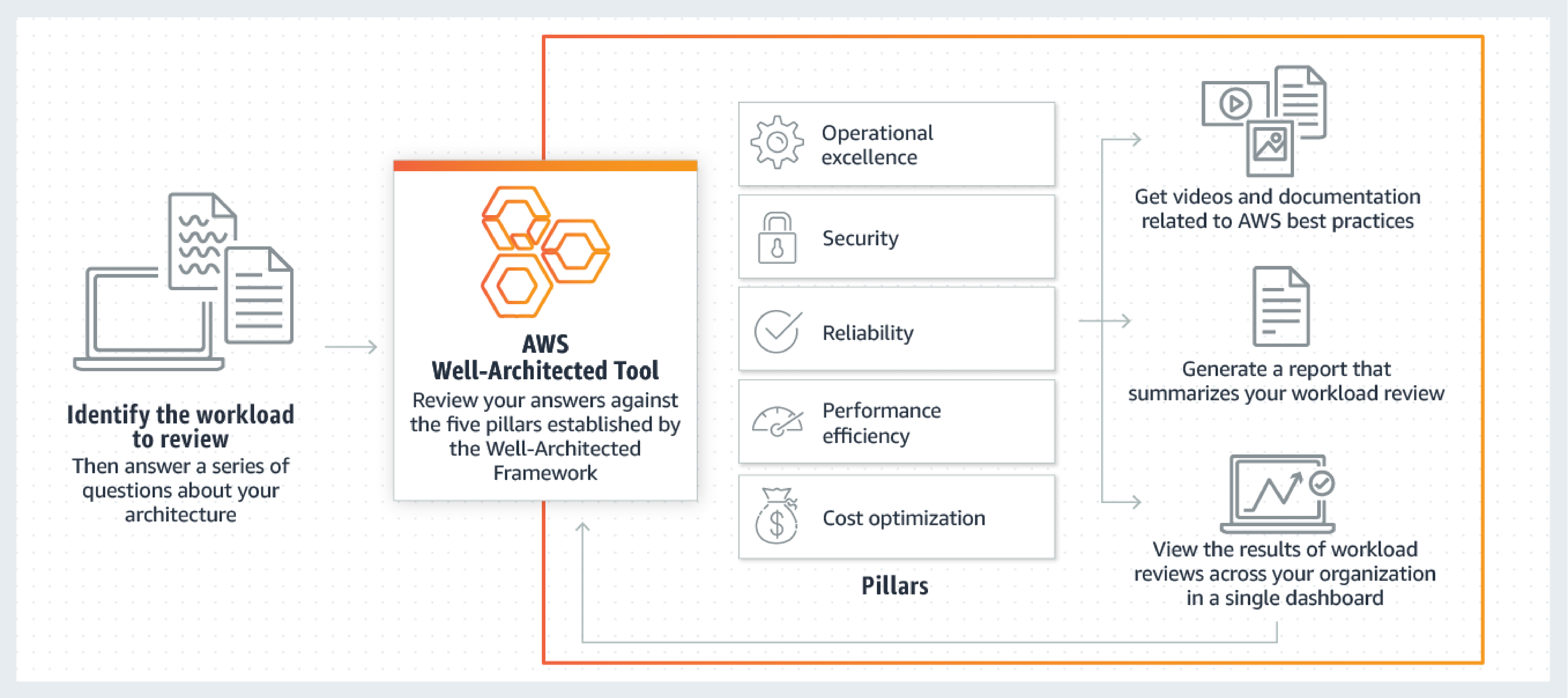
https://aws.amazon.com/compliance/

https://aws.amazon.com/artifact/

# Security in the cloud

Managed by customers

# AWS Well-Architected Framework



**Identify the workload to review**
Then answer a series of questions about your architecture

**AWS Well-Architected Tool**
Review your answers against the five pillars established by the Well-Architected Framework

Operational excellence

Security

Reliability

Performance efficiency

Cost optimization

**Pillars**

Get videos and documentation related to AWS best practices

Generate a report that summarizes your workload review

View the results of workload reviews across your organization in a single dashboard

# AWS security solutions

## Identity and access management

- AWS Identity and Access Management (IAM)
- AWS Organizations
- Amazon Cognito
- AWS Directory Service
- AWS Secrets Manager
- AWS Single Sign-On

## Detective control

- AWS CloudTrail
- AWS Config
- Amazon CloudWatch
- Amazon GuardDuty
- VPC Flow Logs

## Infrastructure security

- AWS Systems Manager
- AWS Shield
- AWS WAF – Web application firewall
- AWS Firewall Manager
- Amazon Inspector
- Amazon Virtual Private Cloud (Amazon VPC)

## Data protection

- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- Amazon Macie
- AWS Certificate Manager (ACM)
- Server-side encryption

## Incident response

- AWS Config Rules
- AWS Lambda

## Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources.

### AWS Identity and Access Management (IAM)

Securely control access to AWS services and resources

### AWS Organizations

Leverage policy-based management for multiple AWS accounts

### Amazon Cognito

Add user sign-up, sign-in, and access control to your web and mobile apps

### AWS Directory Service

Use Managed Microsoft Active Directory in the AWS Cloud

### AWS Secrets Manager

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

### AWS Single Sign-On

Centrally manage single sign-on (SSO) access to multiple AWS accounts and business applications

## Detective control

Gain the visibility you need to spot issues before they impact the business; further, improve your security posture and reduce the risk profile of your environment.

## AWS CloudTrail

Enable governance, compliance, and operational/risk auditing of your AWS account

## AWS Config

Record and evaluate configurations of your AWS resources; enable compliance auditing, security analysis, resource change tracking, and troubleshooting

## Amazon CloudWatch

Monitor AWS Cloud resources and your applications on AWS to collect metrics, monitor log files, set alarms, and automatically react to changes

## Amazon GuardDuty

Employ intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads

## VPC Flow Logs

Capture information about the IP traffic going to and from network interfaces in your VPC; flow log data is stored using Amazon CloudWatch Logs

## Infrastructure security

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS.

### AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure operating systems

### AWS Shield

Make use of this managed DDoS protection service, which safeguards web applications running on AWS

### AWS WAF – Web application firewall

Protect your web applications from common web exploits, ensuring availability and security

### AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications

### Amazon Inspector

Employ automation of security assessments to help improve the security and compliance of applications deployed on AWS

### Amazon Virtual Private Cloud (Amazon VPC)

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define

## Data protection

In addition to using our automatic data encryption and management services, employ more features for data protection.

### AWS Key Management Service (AWS KMS)

Easily create and control the keys used to encrypt your data

### AWS CloudHSM

Use a managed hardware security module (HSM) in the AWS Cloud

### Amazon Macie

Use this machine learning-powered security service to discover, classify, and protect sensitive data

### AWS Certificate Manager (ACM)

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

### Server-Side Encryption

Take advantage of flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys

## Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides these tools to automate aspects of this best practice.

### AWS Config Rules

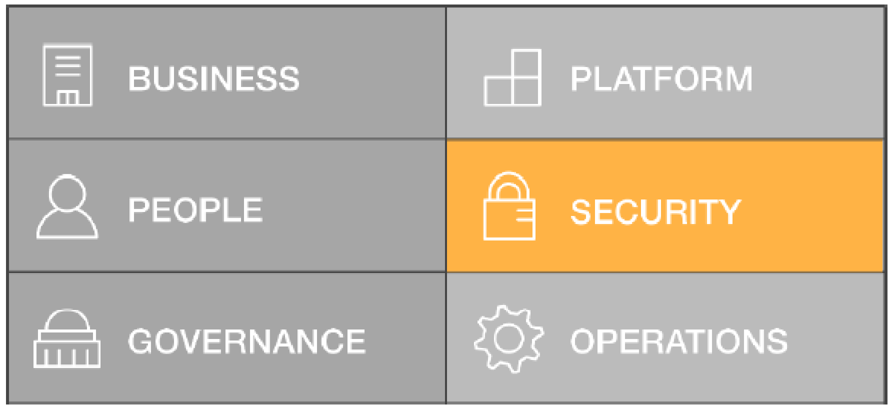
Create rules that automatically take action in response to changes in your environment, such as isolating resources, enriching events with additional data, or restoring configuration to a known good state

### AWS Lambda

Use our serverless compute service to run code without provisioning or managing servers so you can scale your programmed, automated response to incidents

# Align to cloud security **best practices**

## AWS Cloud Adoption Framework (CAF)



How to move to the cloud securely, including the “five core epics”:

- Identity and access management
- Logging and monitoring
- Infrastructure security
- Data protection
- Incident response

## AWS security best practices

Whitepaper with 44 best practices including:

- Identity and access management (10 best practices)
- Logging and monitoring (4)
- Infrastructure security (15)
- Data protection (15)

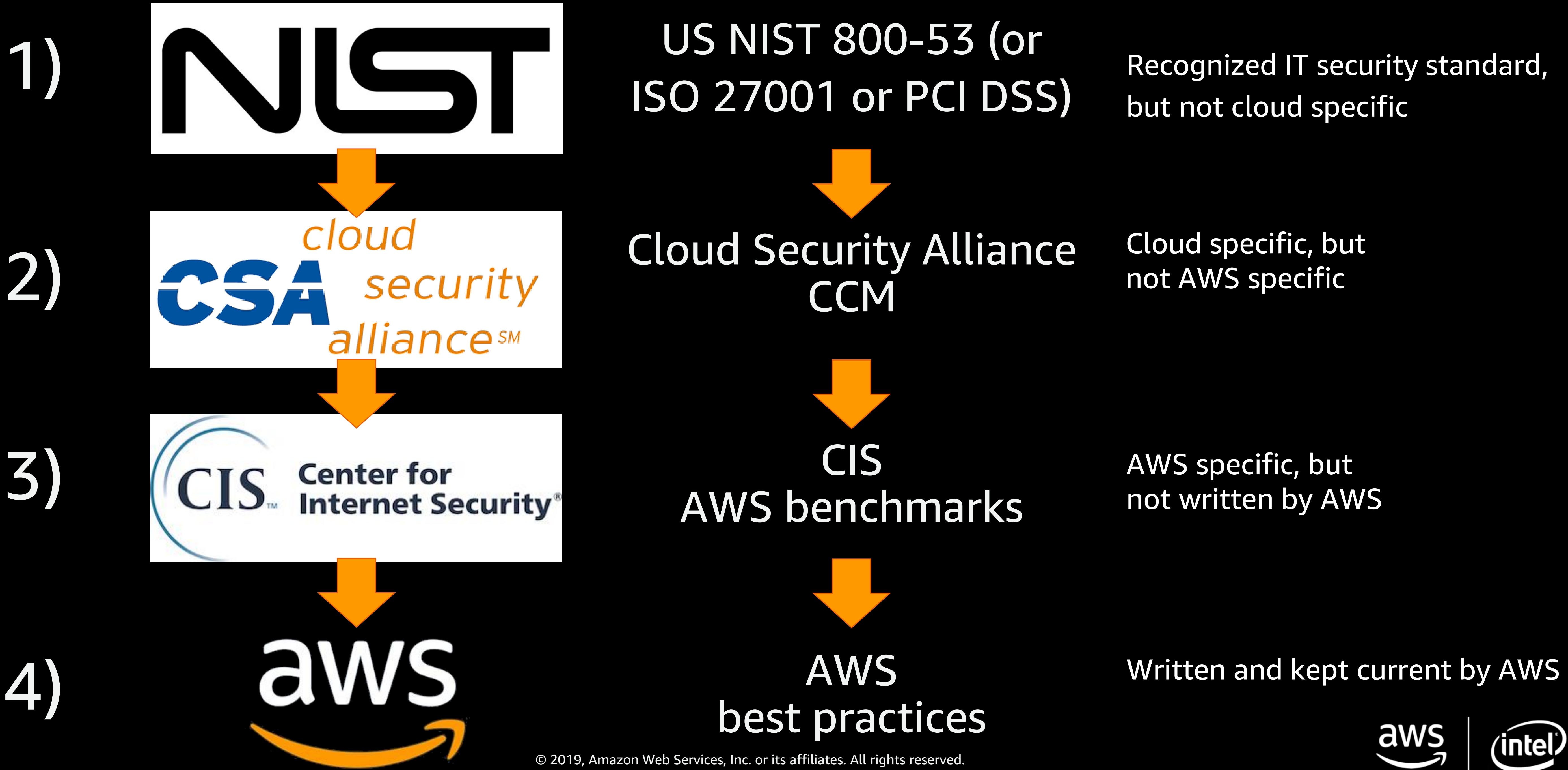
## Center for Internet Security (CIS) Benchmarks

CIS™ Center for Internet Security®

148 detailed recommendations for configuration and auditing covering:

- “AWS Foundations” with 52 checks aligned to AWS best practices
- “AWS Three-Tier Web Architecture” with 96 checks for web applications

# Align AWS controls with **global frameworks**



1) US NIST 800-53 (or ISO 27001 or PCI DSS)

Recognized IT security standard, but not cloud specific

2) Cloud Security Alliance CCM

Cloud specific, but not AWS specific

3) CIS AWS benchmarks

AWS specific, but not written by AWS

4) AWS best practices

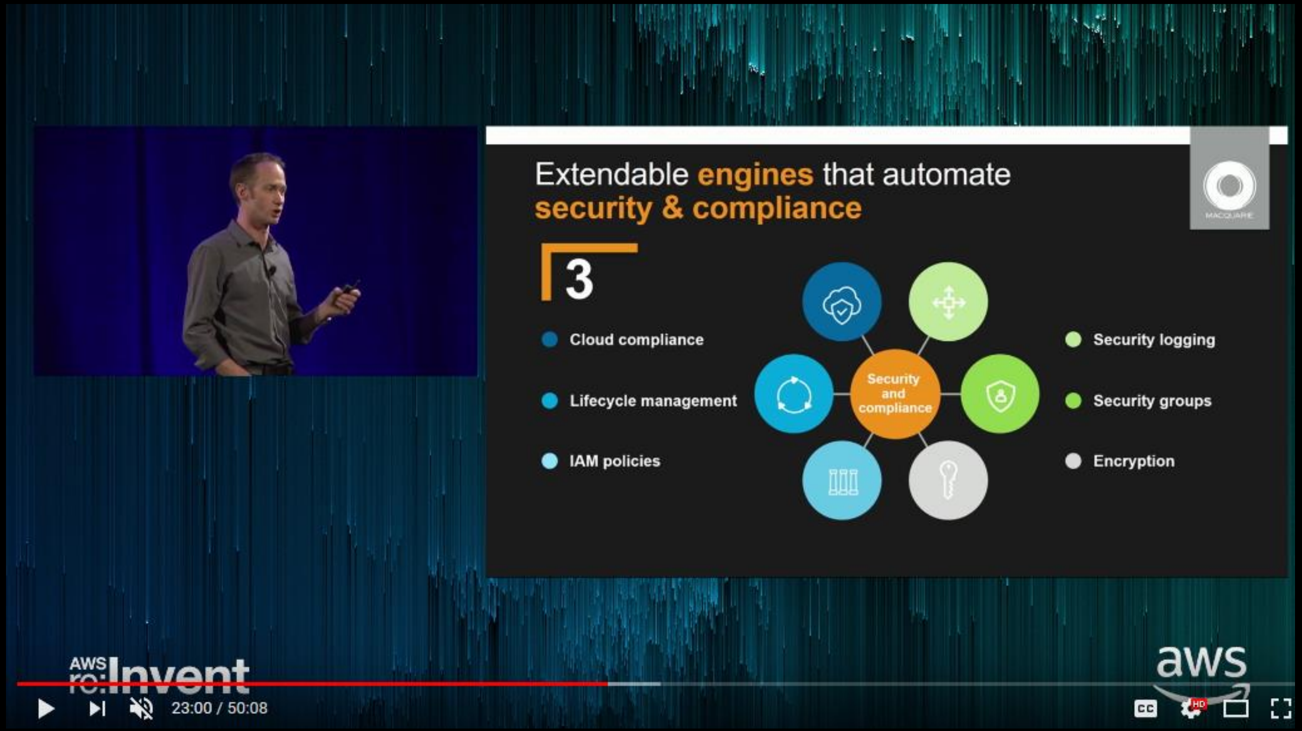
Written and kept current by AWS

# Resources

# Videos

## AWS Channel on YouTube

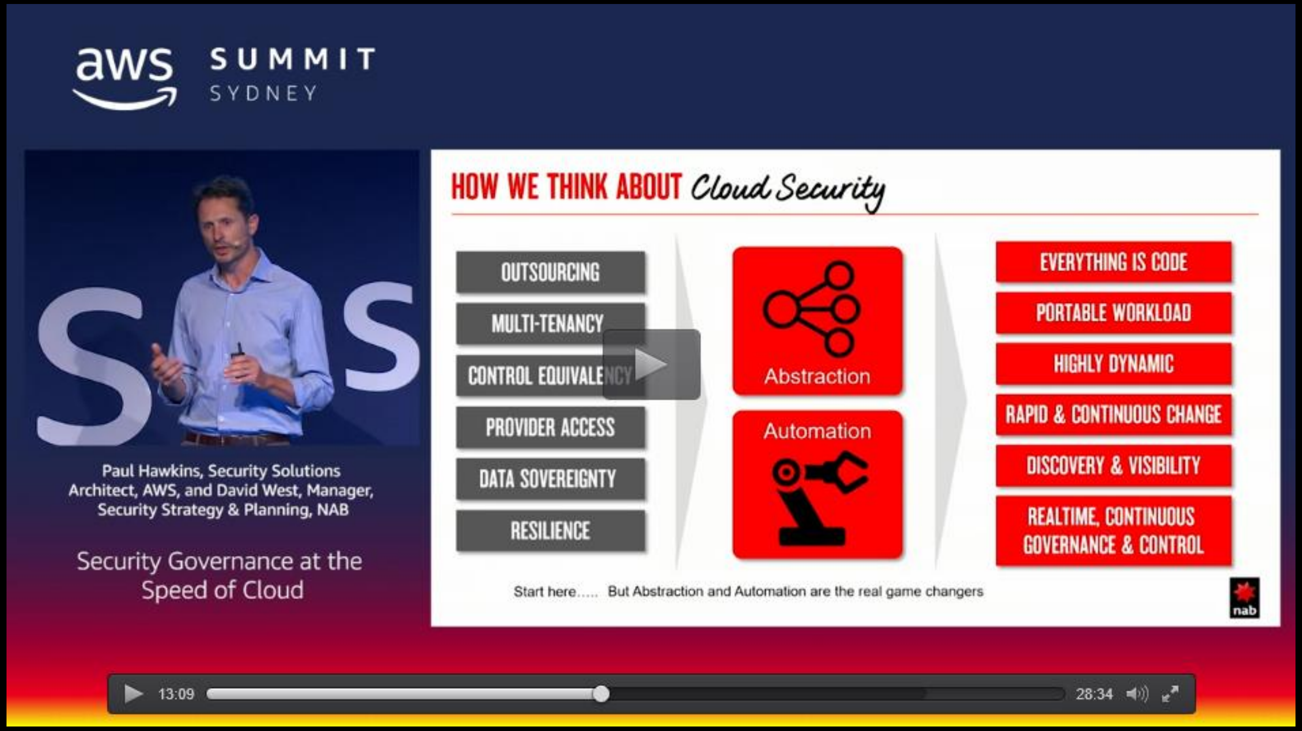
### AWS re:Invent 2017



https://aws.amazon.com/blogs/security/videos-and-slide-decks-from-the-aws-reinvent-2017-security-compliance-identity-track/

## AWS On-Demand

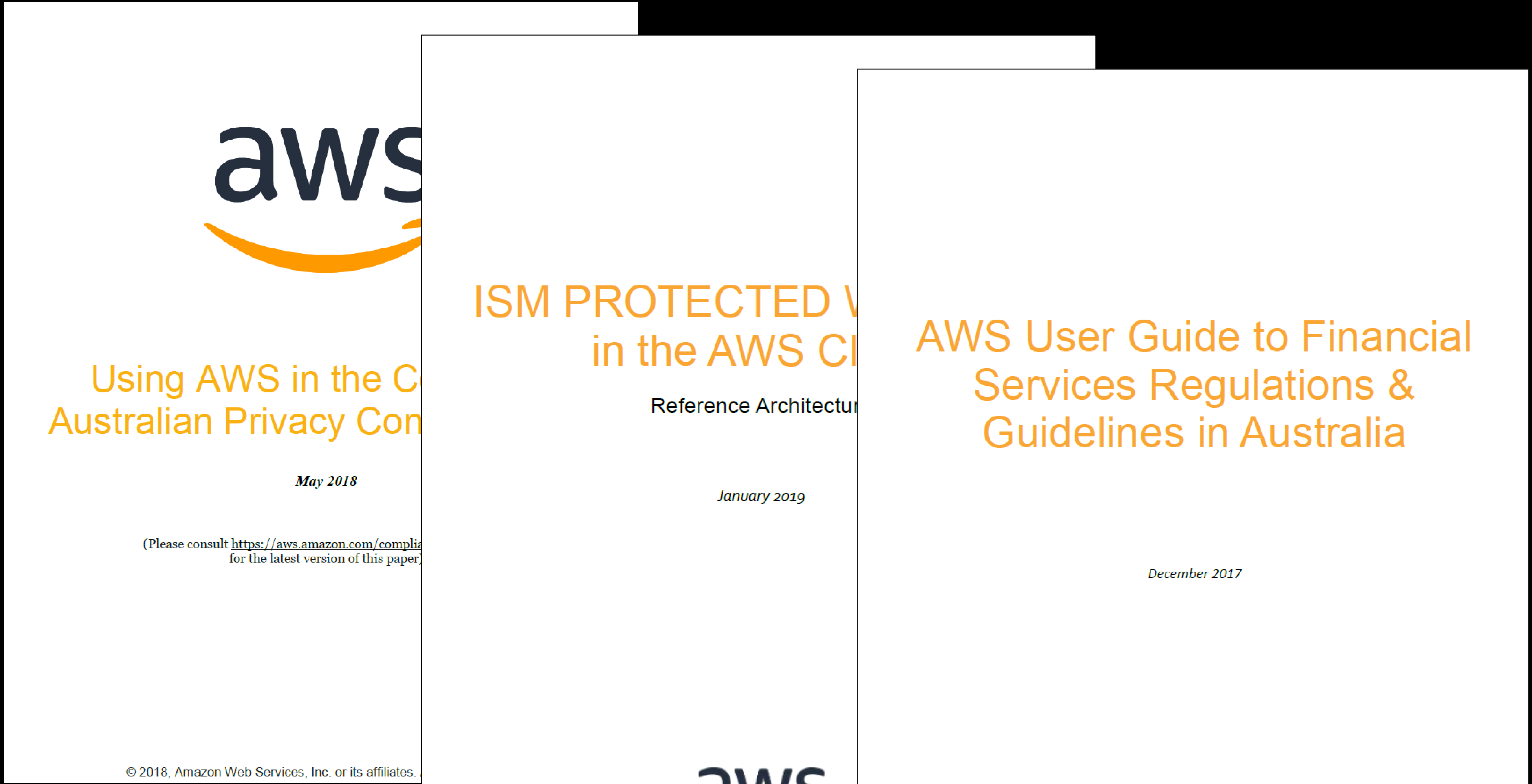
### AWS Summit Sydney 2018



aws SUMMIT SYDNEY
HOW WE THINK ABOUT Cloud Security
OUTSOURCING
MULTI-TENANCY
CONTROL EQUIVALENCY
PROVIDER ACCESS
DATA SOVEREIGNTY
RESILIENCE
Abstraction
Automation
EVERYTHING IS CODE
PORTABLE WORKLOAD
HIGHLY DYNAMIC
RAPID & CONTINUOUS CHANGE
DISCOVERY & VISIBILITY
REALTIME, CONTINUOUS GOVERNANCE & CONTROL
Start here..... But Abstraction and Automation are the real game changers
nab
Paul Hawkins, Security Solutions Architect, AWS, and David West, Manager, Security Strategy & Planning, NAB
Security Governance at the Speed of Cloud
13:09
28:34

https://aws.amazon.com/summits/sydney/on-demand/Tracks/secure/

# Whitepapers: https://aws.amazon.com/whitepapers/#security



Using AWS in the C
Australian Privacy Con

*May 2018*

(Please consult https://aws.amazon.com/complia
for the latest version of this paper)

ISM PROTECTED V
in the AWS Cl

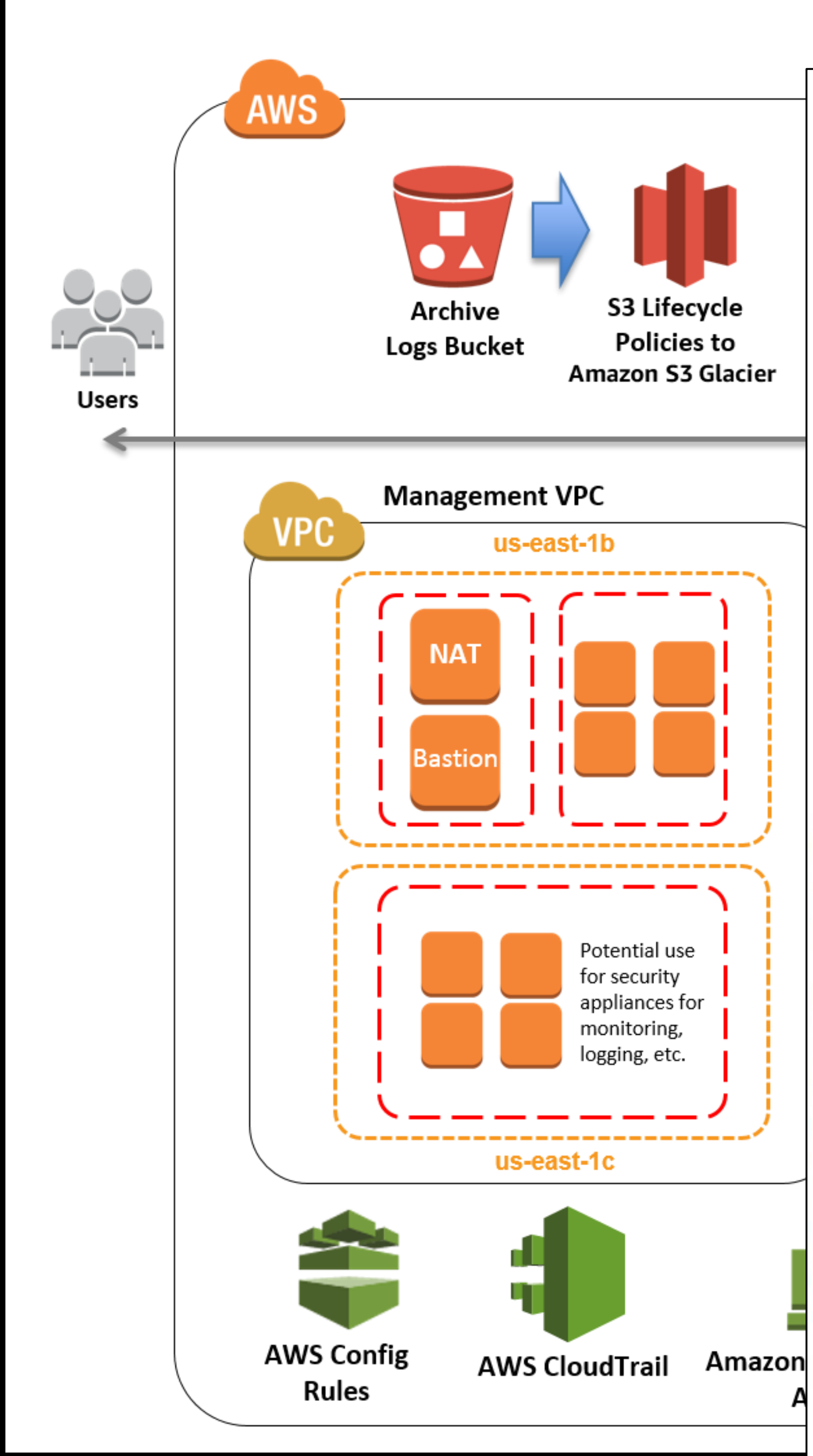
Reference Architectur

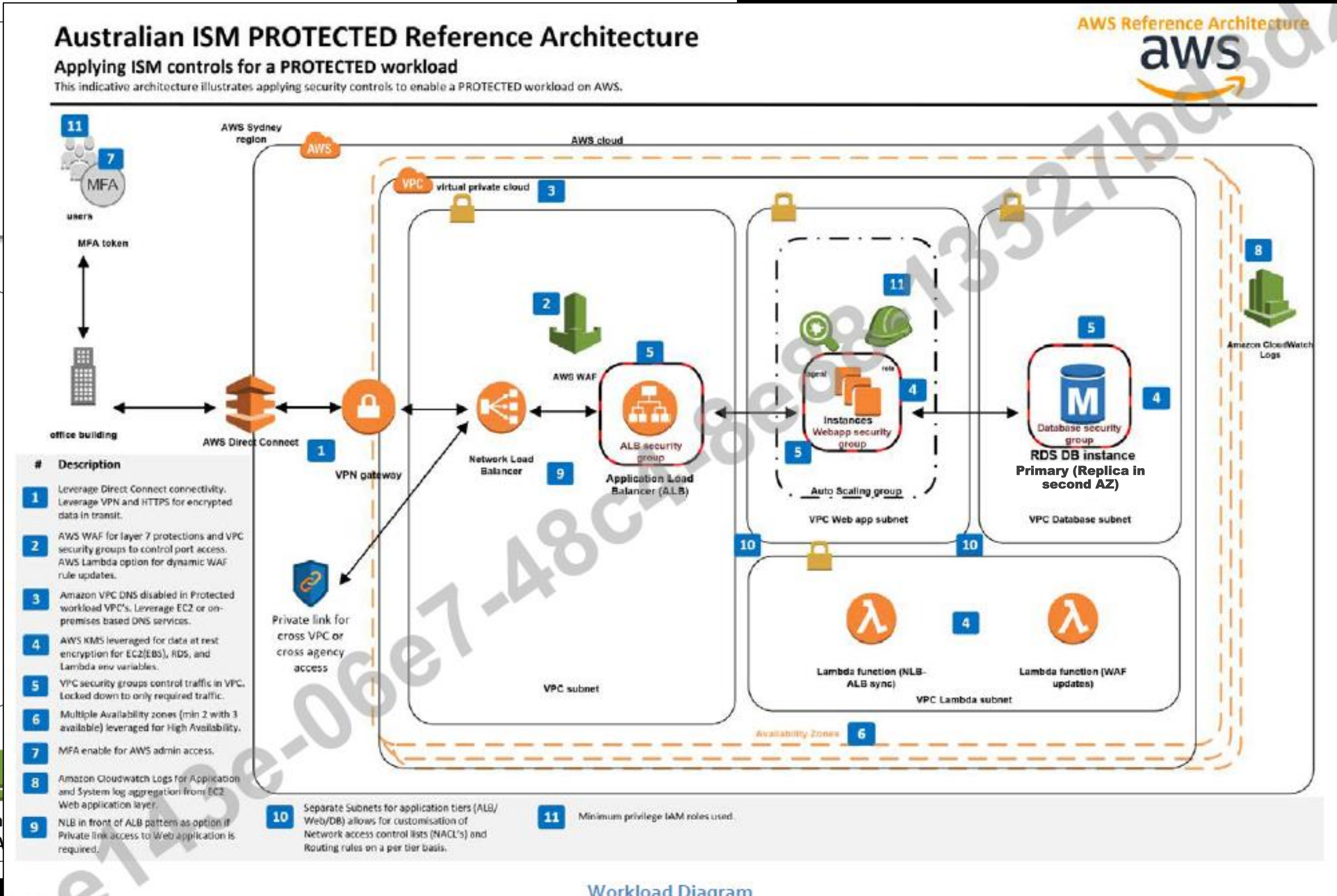
*January 2019*

AWS User Guide to Financial Services Regulations & Guidelines in Australia

*December 2017*

# Architecture: https://aws.amazon.com/architecture/





## Australian ISM PROTECTED Reference Architecture

### Applying ISM controls for a PROTECTED workload

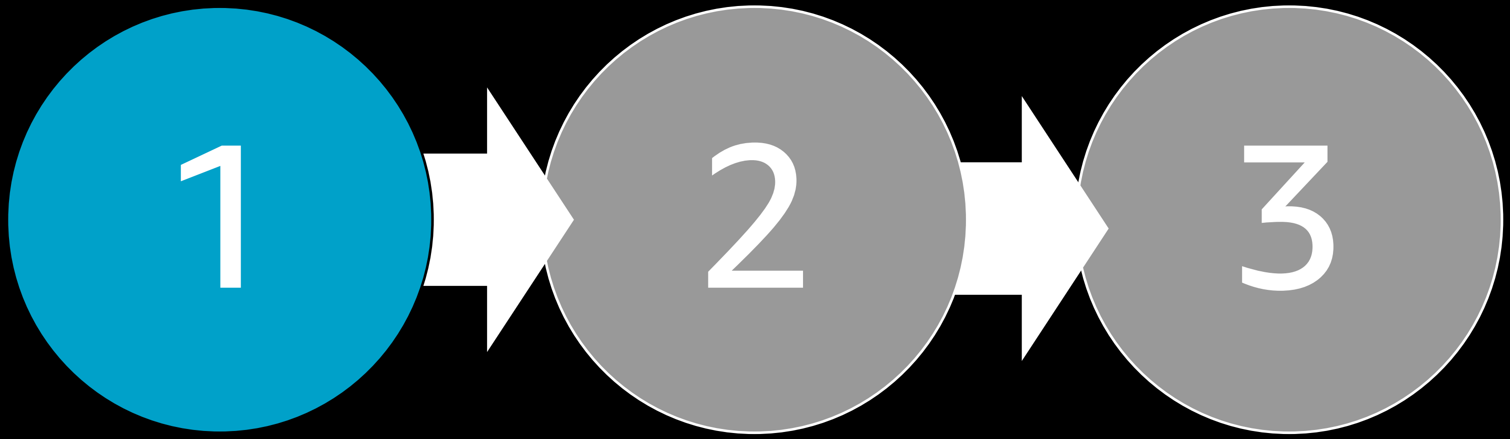
This indicative architecture illustrates applying security controls to enable a PROTECTED workload on AWS.

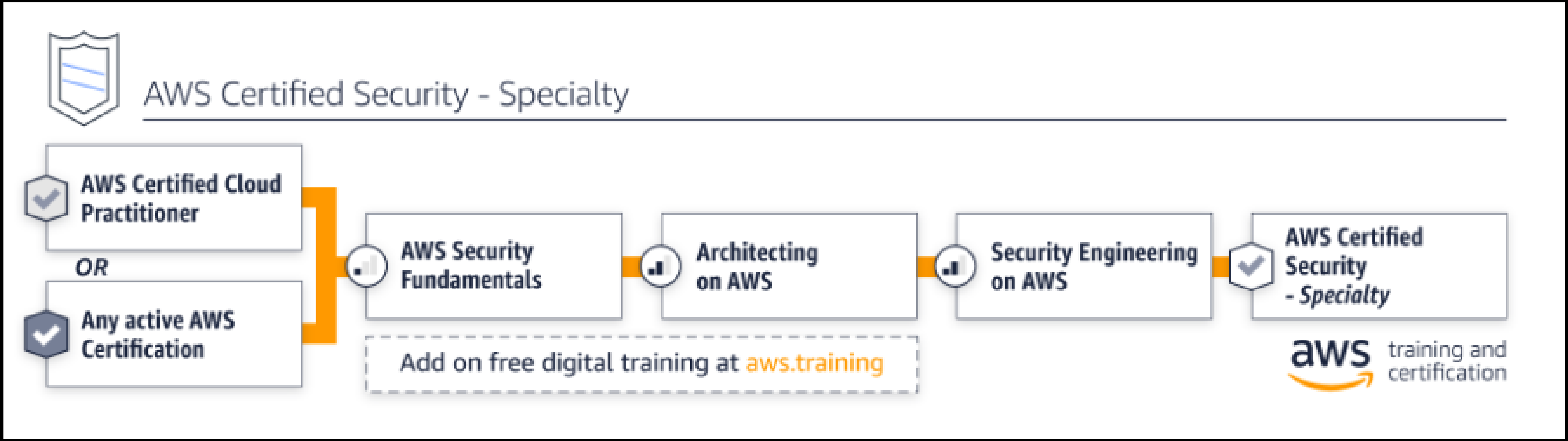
| # | Description |
|---|---|
| 1 | Leverage Direct Connect connectivity. Leverage VPN and HTTPS for encrypted data in transit. |
| 2 | AWS WAF for layer 7 protections and VPC security groups to control port access. AWS Lambda option for dynamic WAF rule updates. |
| 3 | Amazon VPC DNS disabled in Protected workload VPC's. Leverage EC2 or on-premises based DNS services. |
| 4 | AWS KMS leveraged for data at rest encryption for EC2(EBS), RDS, and Lambda env variables. |
| 5 | VPC security groups control traffic in VPC. Locked down to only required traffic. |
| 6 | Multiple Availability zones (min 2 with 3 available) leveraged for High Availability. |
| 7 | MFA enable for AWS admin access. |
| 8 | Amazon Cloudwatch Logs for Application and System log aggregation from EC2 Web application layer. |
| 9 | NLB in front of ALB pattern as option if Private link access to Web application is required. |
| 10 | Separate Subnets for application tiers (ALB/ Web/DB) allows for customisation of Network access control lists (NACL's) and Routing rules on a per tier basis. |
| 11 | Minimum privilege IAM roles used. |

Workload Diagram

# Next steps

## Educate: AWS security curriculum





AWS Certified Security - Specialty

AWS Certified Cloud Practitioner

*OR*

Any active AWS Certification

AWS Security Fundamentals

Architecting on AWS

Security Engineering on AWS

AWS Certified Security - *Specialty*

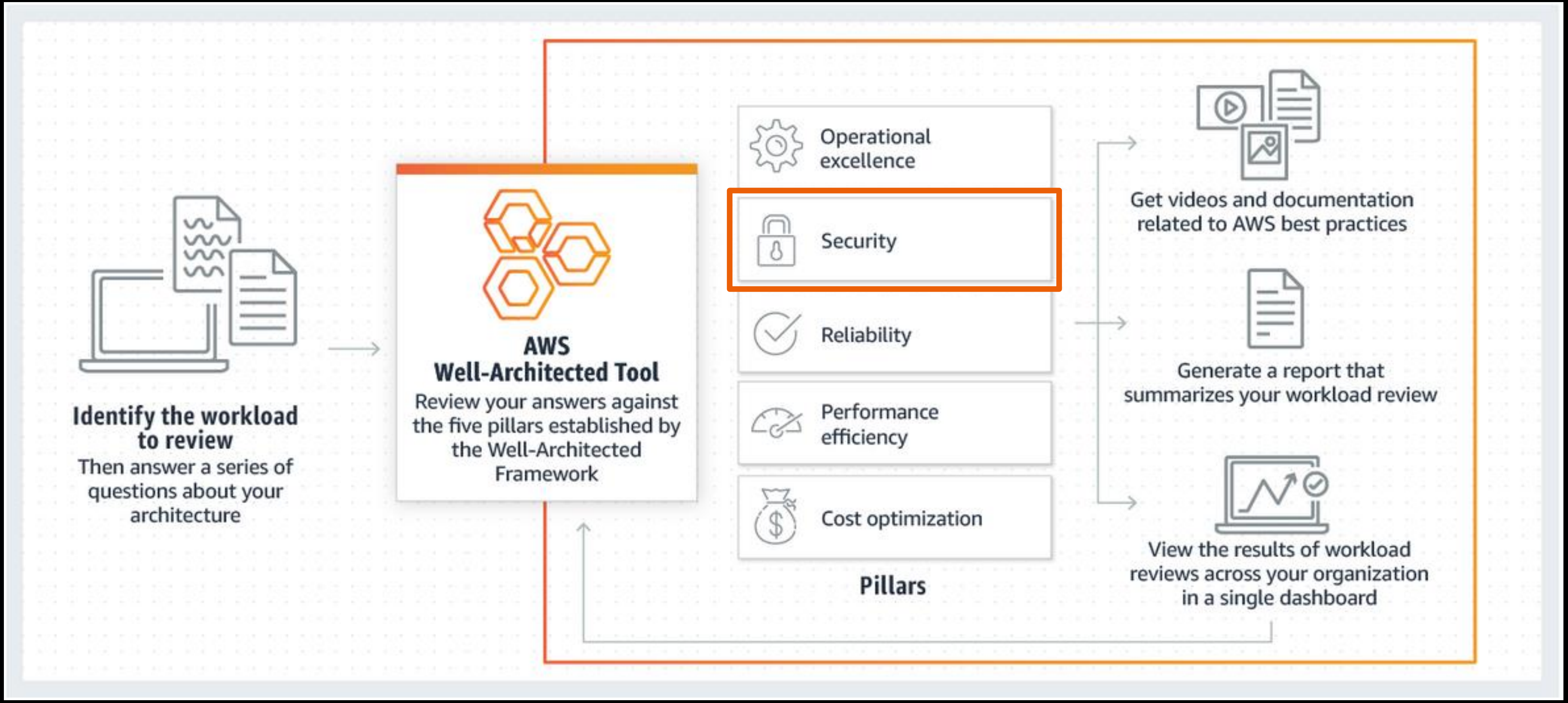
Add on free digital training at aws.training

aws training and certification

# Next steps

## Assess: AWS Well-Architected

1 → 2 → 3



**Identify the workload to review**

Then answer a series of questions about your architecture

**AWS Well-Architected Tool**

Review your answers against the five pillars established by the Well-Architected Framework

Get videos and documentation related to AWS best practices

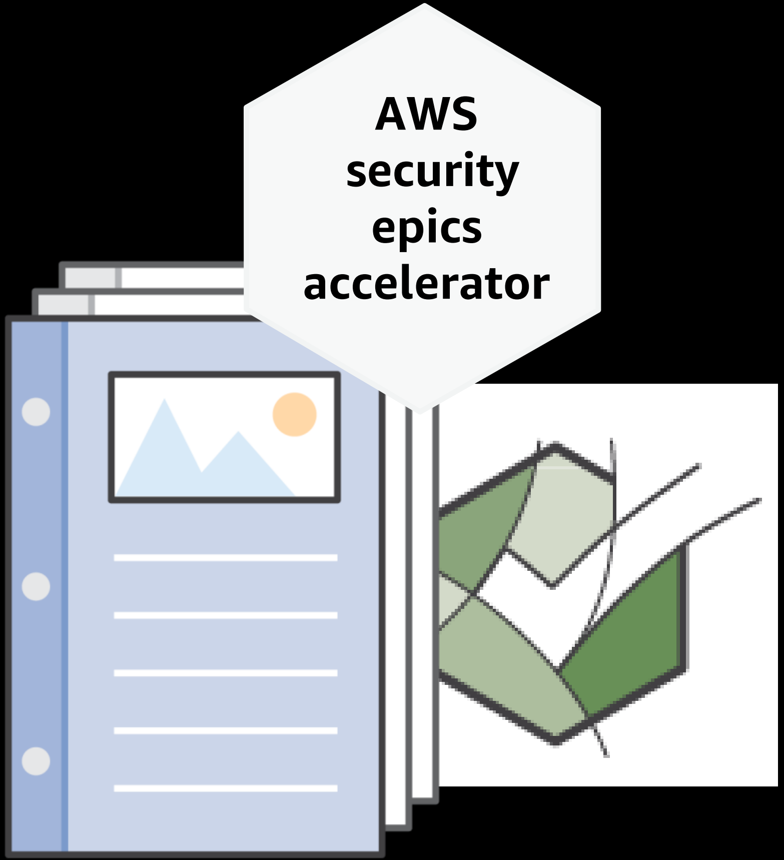
Generate a report that summarizes your workload review

View the results of workload reviews across your organization in a single dashboard

# Next steps

## Advise: AWS Professional Services

AWS enterprise security, risk & compliance blueprint


AWS security epics accelerator

AWS security incident response simulation

# Learn from AWS experts. Advance your skills and knowledge. Build your future in the AWS Cloud.

**Digital Training**

Free, self-paced online courses built by AWS experts

**Classroom Training**

Classes taught by accredited AWS instructors

**AWS Certification**

Exams to validate expertise with an industry-recognized credential

**Ready to begin building your cloud skills?**
**Get started at: [https://www.aws.training/](https://www.aws.training/)**

aws | intel

# Why work with an APN Partner?

**APN Partners are uniquely positioned to help your organization at any stage of your cloud adoption journey, and they:**

- Share your goals—focused on your success
- Help you take full advantage of all the business benefits that AWS has to offer
- Provide services and solutions to support any AWS use case across your full customer life cycle

**APN Partners with deep expertise in AWS services:**

**AWS Managed Service Provider (MSP) Partners**

APN Partners with cloud infrastructure and application migration expertise

**AWS Competency Partners**

APN Partners with verified, vetted, and validated specialized offerings

**AWS Service Delivery Partners**

APN Partners with a track record of delivering specific AWS services to customers

**Find the right APN Partner for your needs:** https://aws.amazon.com/partners/find/

# Thank you for attending AWS Innovate

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.

- aws-apac-marketing@amazon.com
- twitter.com/AWSCloud
- facebook.com/AmazonWebServices
- youtube.com/user/AmazonWebServices
- slideshare.net/AmazonWebServices
- twitch.tv/aws