Managing Encryption Keys in Multi-cloud to Secure Your Cloud Assets

Wood Lam

Security Consultant
Wood.lam@thalesgroup.com

Year 2020 - Beginning of the New Normal

IAAS

</>
DaaS

PaaS

SaaS

Is Maintaining Security in the Cloud so Difficult ?

Lesson learnt from new normal

- Think proactively
  - Multi-cloud strategy?
  - What goal do I want to achieve?

Avoid human error

- Automation

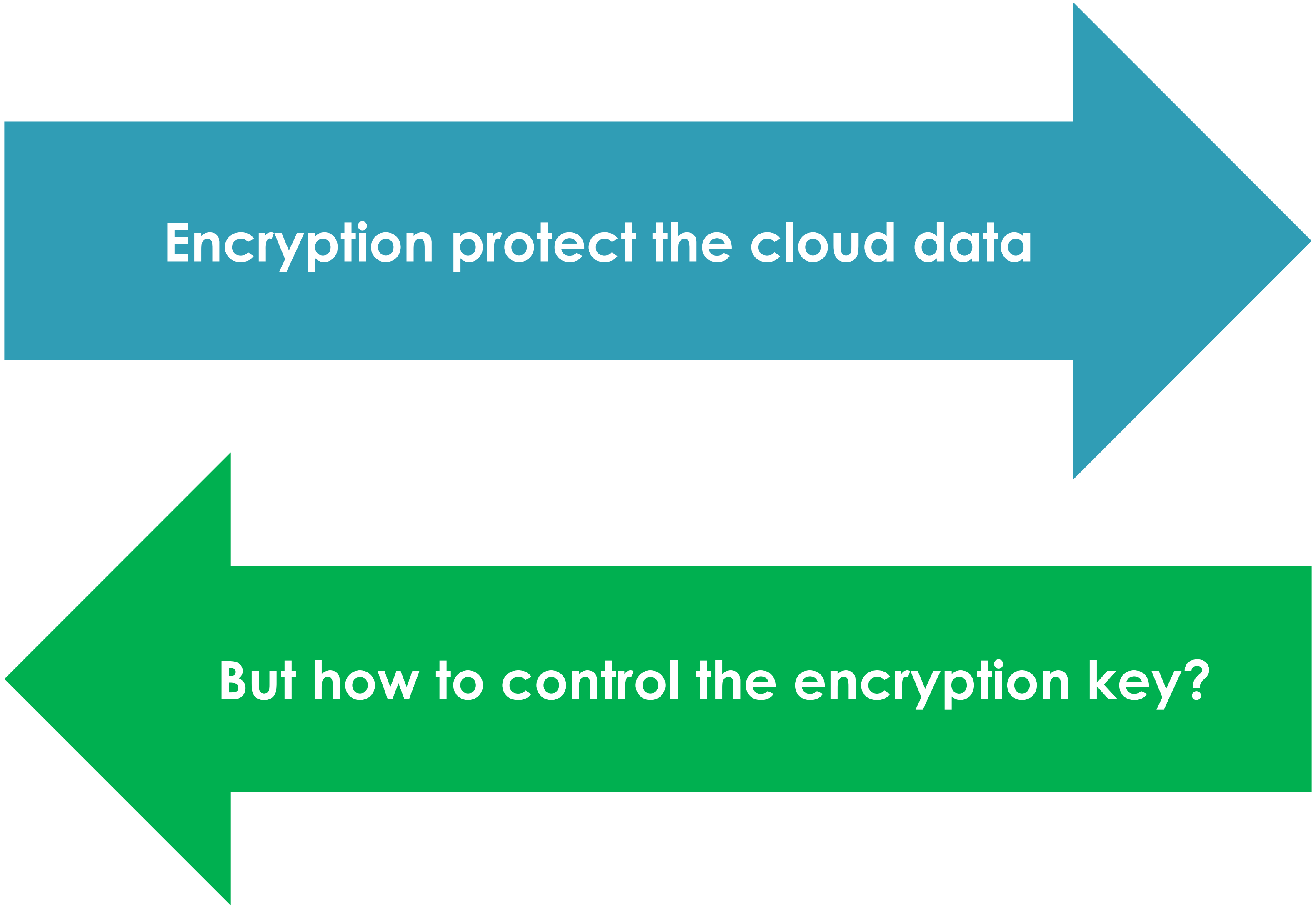
Compliance thinking

- Control and logs

Secured by design

- Leverage cloud service provider
- Data security

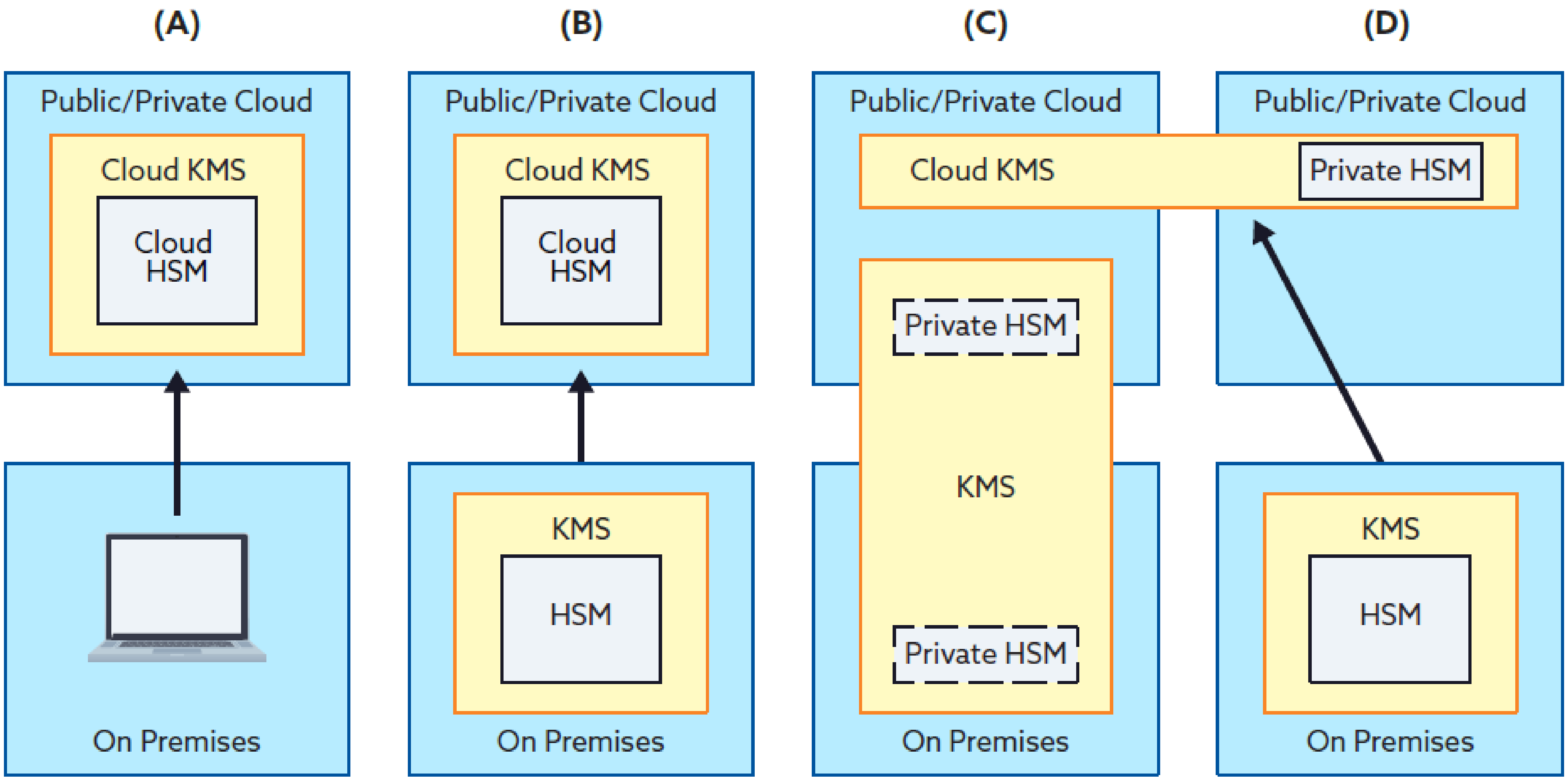
Encryption and Encryption Keys



Encryption protect the cloud data

But how to control the encryption key?

Cloud Services and Key Management Systems



Key Management in Cloud Services: Understanding Encryption's Desired Outcomes and Limitations

Industry Standard on Cloud Key Management

Cloud Controls Matrix v4

Release Date: 01/20/2021

CEK-08

[CSC Key Management Capability]

"CSPs must provide the capability for CSCs to manage their own data encryption keys. "

CEK-10	Key Generation
CEK-11	Key Purpose
CEK-12	Key Rotation
CEK-13	Key Revocation
CEK-14	Key Destruction
CEK-15	Key Activation
CEK-16	Key Suspension
CEK-17	Key Deactivation
CEK-18	Key Archival
CEK-19	Key Compromise
CEK-20	Key Recovery

CEK-09

[Encryption and Key Management Audit]

Audit encryption and key management systems, policies, and processes

Practice Guide for Cloud Computing Security

- provides the practical guidance and reference for the secure adoption of cloud computing technology in the Government.

5.4 Asset Management - [Protect data by encryption]

Data encryption is a way to enhance data confidentiality. B/Ds should confirm that encryption capabilities provided on cloud service are adequate with the cryptographic policy on the use of cryptographic controls. … The **encryption key should also be properly protected and managed.**

5.6 Cryptography - [Manage and protect cryptographic keys]

Cryptographic keys should be **managed** and **protected** properly in accordance with security regulations and policies. Key management on storage should be enforced and **keys should be managed in the custody of the B/Ds**. Processes for a key management lifecycle should be defined: how keys are generated, used, stored, backed up, recovered, rotated, and deleted… B/Ds may adopt encryption to protect unclassified information when using public cloud service with **cryptographic keys management** and protection.

5.9.2 Virtualisation Security - [Enforce least privilege and segregation of duties]

Administrators of cloud, hypervisor, storage, network and system should perform their own duties without being able to gain access to the sensitive data residing on the systems they manage.

BYOK, Key lifecycle management and challenges

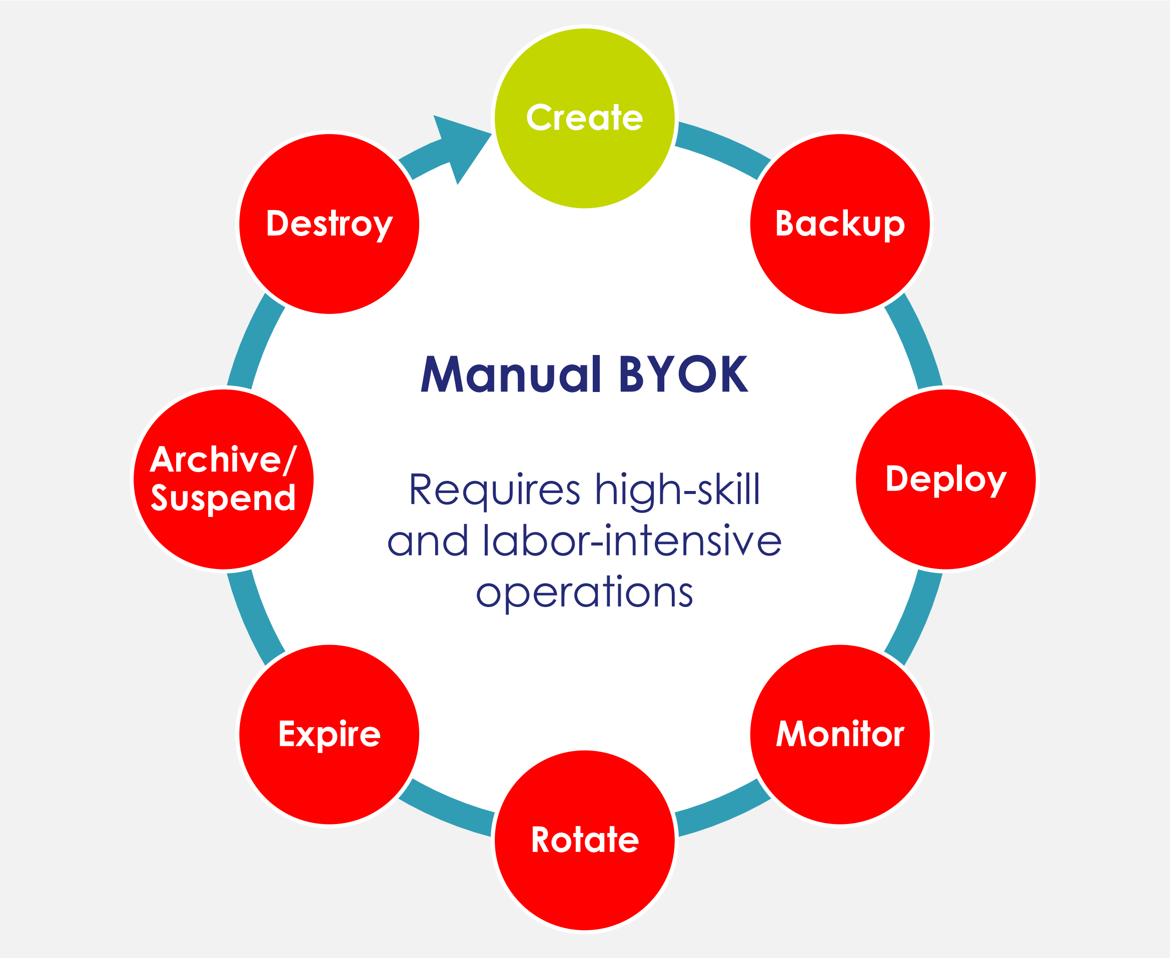
- Different clouds with different security procedures
  - Hard to realise Multi-cloud deployment?

- Risk concerns during the BYOK procedures

- Key lifecycle management

BYOK vs Key Lifecycle Management and Centralized Key Management

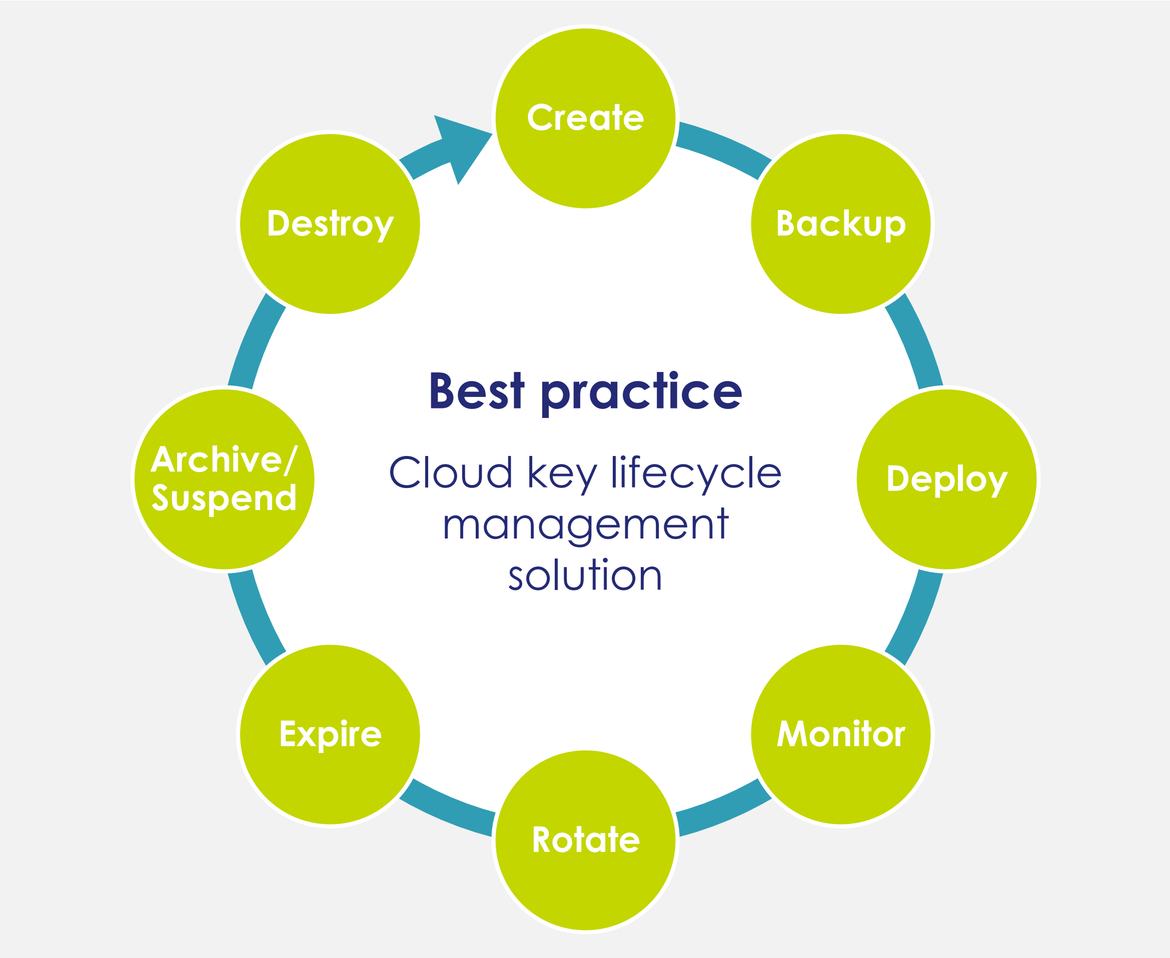
Bring Your Own Key



Manual BYOK

Requires high-skill and labor-intensive operations

Key Lifecycle Management



Best practice

Cloud key lifecycle management solution

Use case 1 - Multinational energy corporation (Americas/US)

Background

- The corporation had been heavily consuming cloud for the daily operations and workloads
- Multiple cloud native KMSs

Business challenges

- Company IT Security mandated that all keys to be controlled and generated on-premises.
- For key rotation, it took several hours to rotate keys with native tools.
- Audit challenges

How Thales help

- Several **hours** vs few **minutes**
- Add-on **automation**, schedule and **auditable** logs
- Key recovery mechanism

Use case 2 – Retail industry (APAC)

Background

- The company wishes to migrate to SaaS provided by different CSPs
- Highly concerned of the security of the business secret

Business challenges

- Management concern about the cloud exit plan
- Lack of experts on multi-cloud operations and key management
- Market ready products

How Thales help

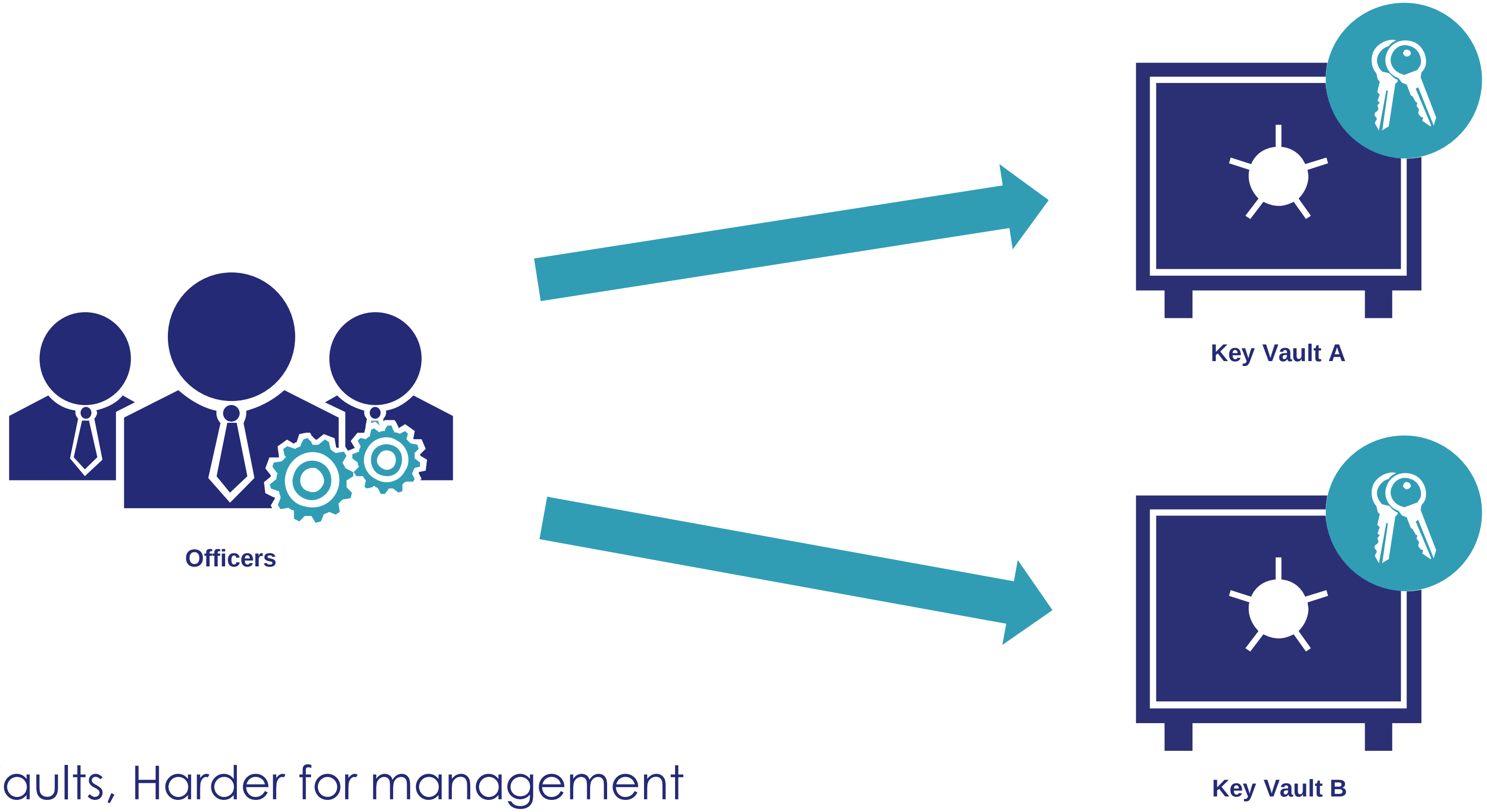
- BYOK with Key lifecycle management on **multi-clouds**
- **Ready** to support for different clouds and strong references
- Fulfill cloud exit plans

Demo

Demo 1 – Managing Multiple KMSs

Demo 2 – Multiple Cloud Key Management

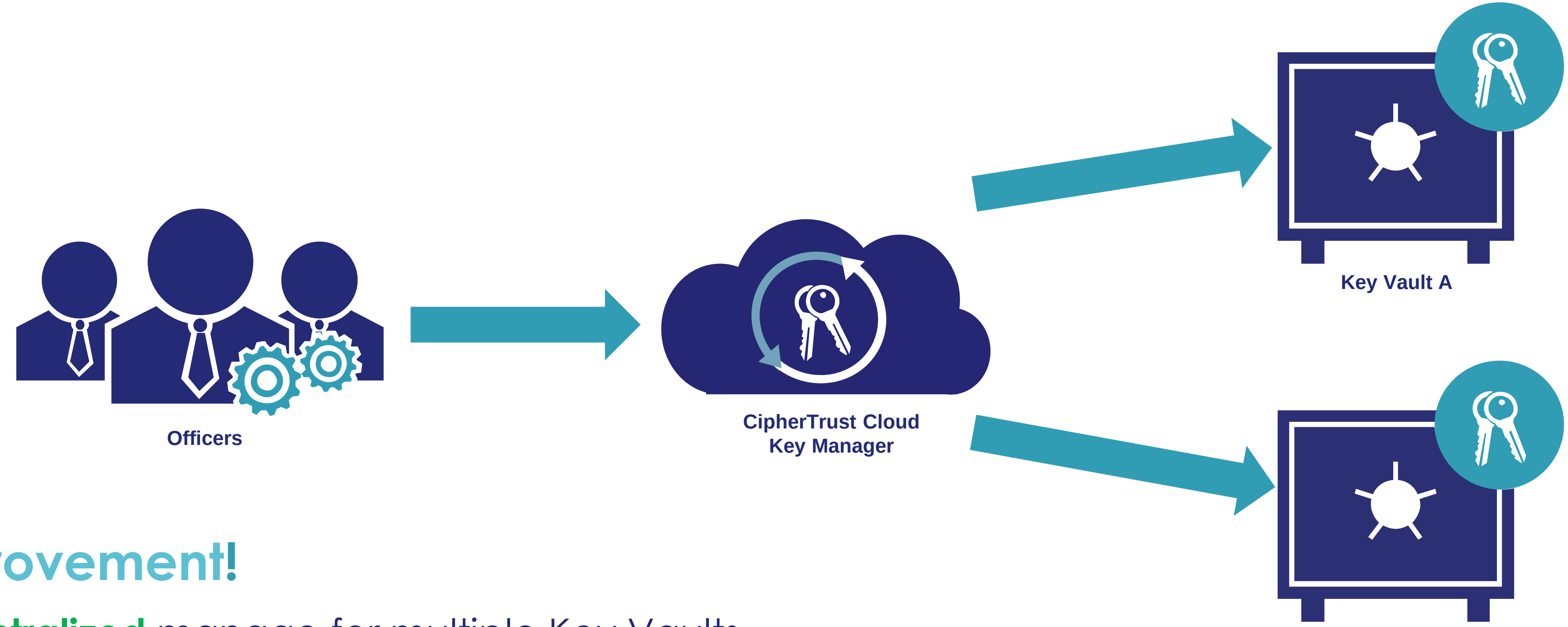
Demo 1 – Managing Multiple Key Vaults (Before)



Difficulties

- More Key Vaults, Harder for management
- Limited key lifecycle management
- Human errors

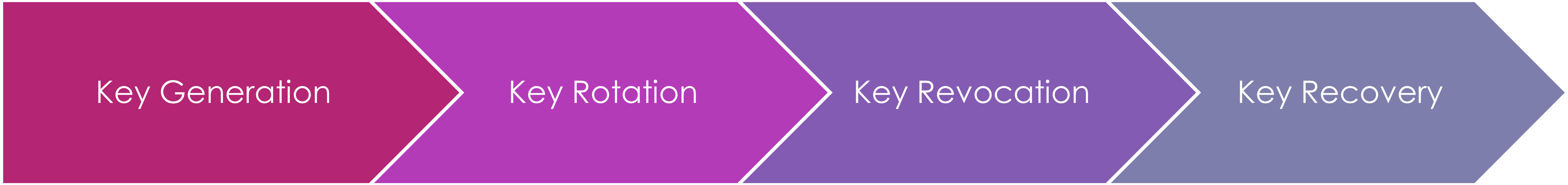
Demo 1 – Managing Multiple Key Vaults (After)



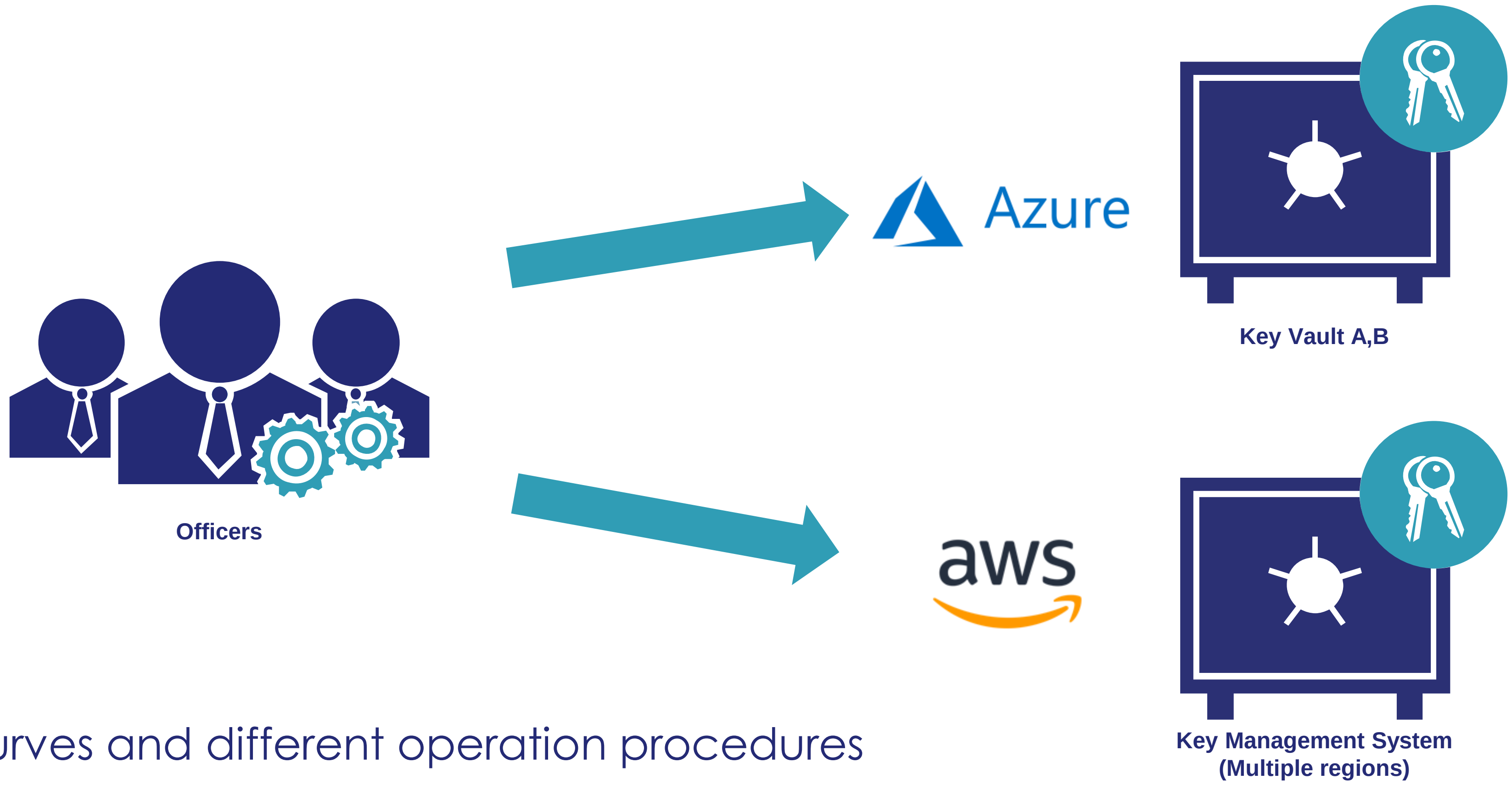
Improvement!

- **Centralized** manage for multiple Key Vaults
- **Full** key lifecycle management from on-premise to cloud
- **Automation** with audit trails

Demo 1 – Key Lifecycle Management



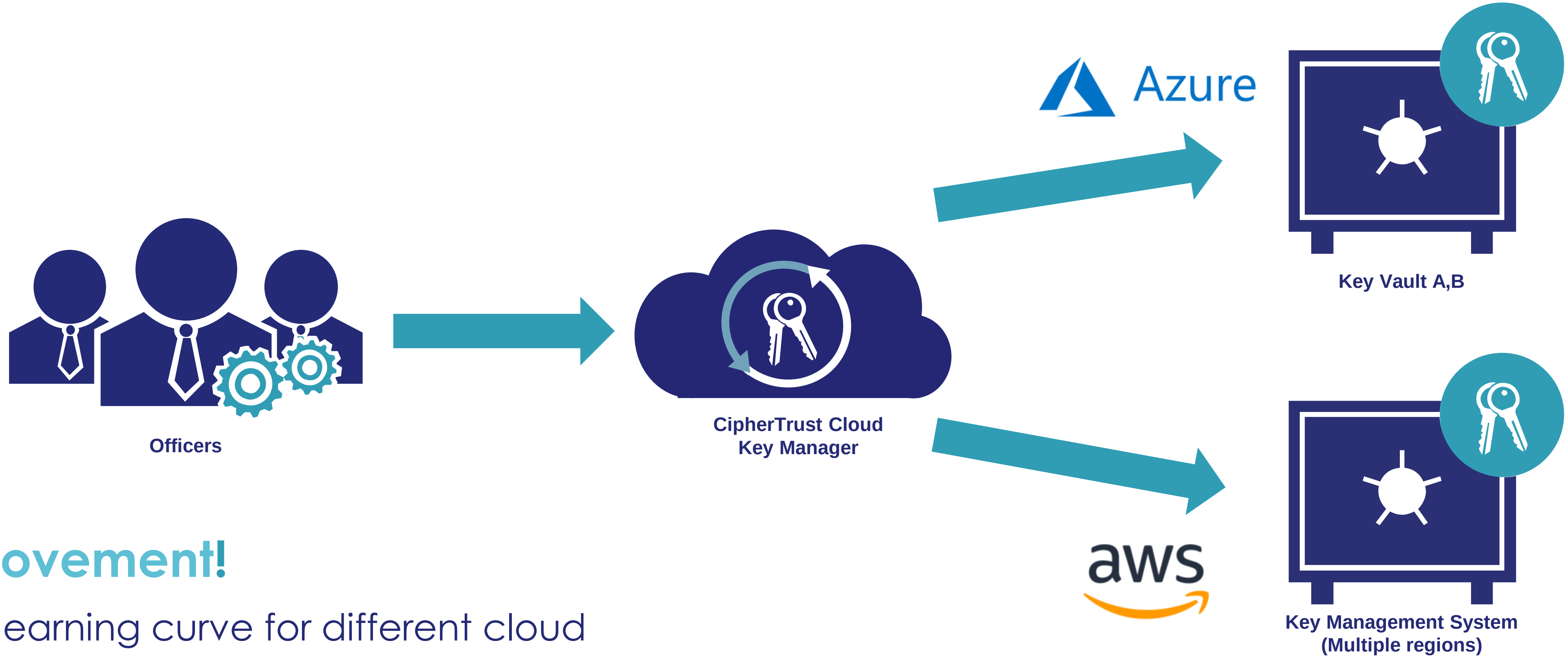
Demo 2 – Multiple Cloud Key Management (Before)



Difficulties

- Learning curves and different operation procedures
- Different portals for different cloud
- Human error during different KMS BYOK

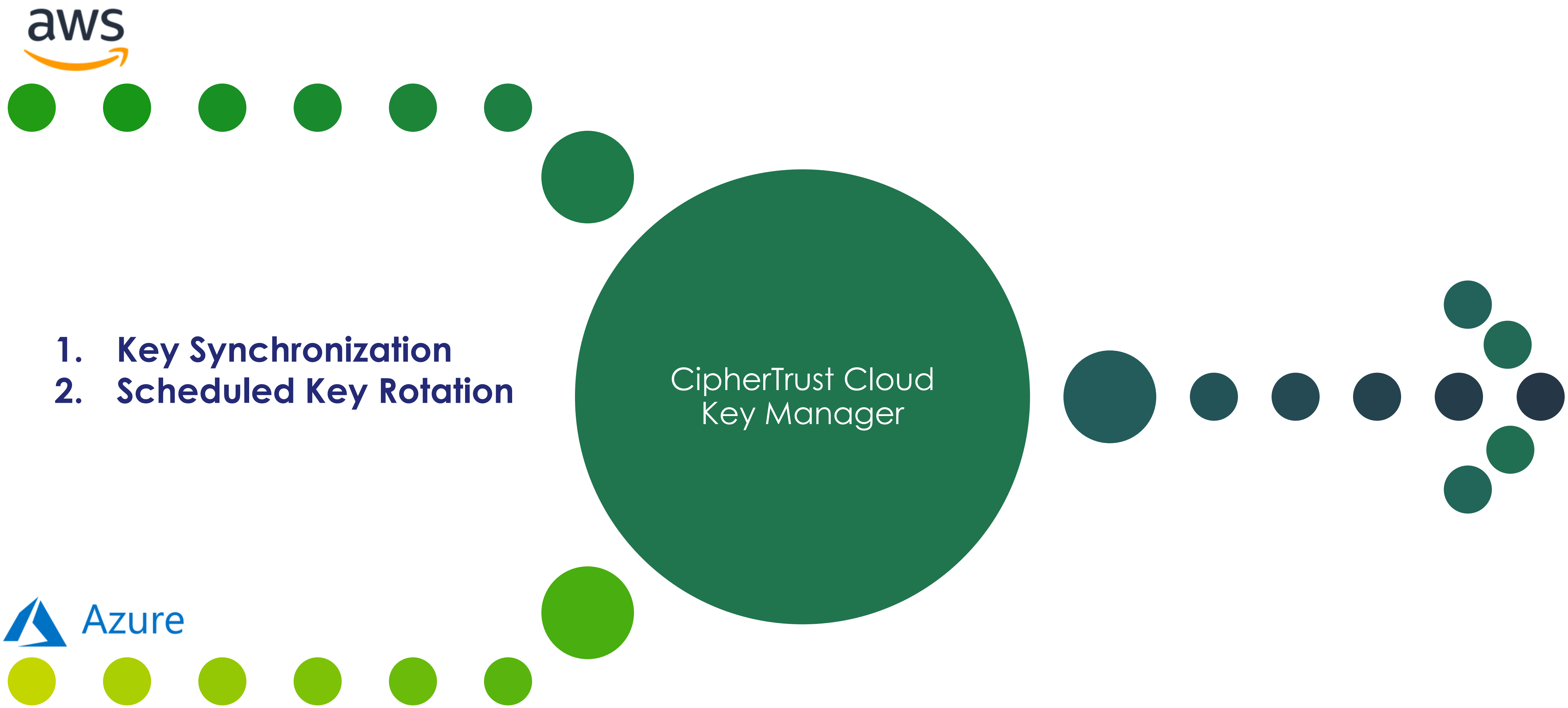
Demo 2 – Multiple Cloud Key Management (After)


Officers
CipherTrust Cloud Key Manager
Azure
Key Vault A,B
aws
Key Management System (Multiple regions)

Improvement!

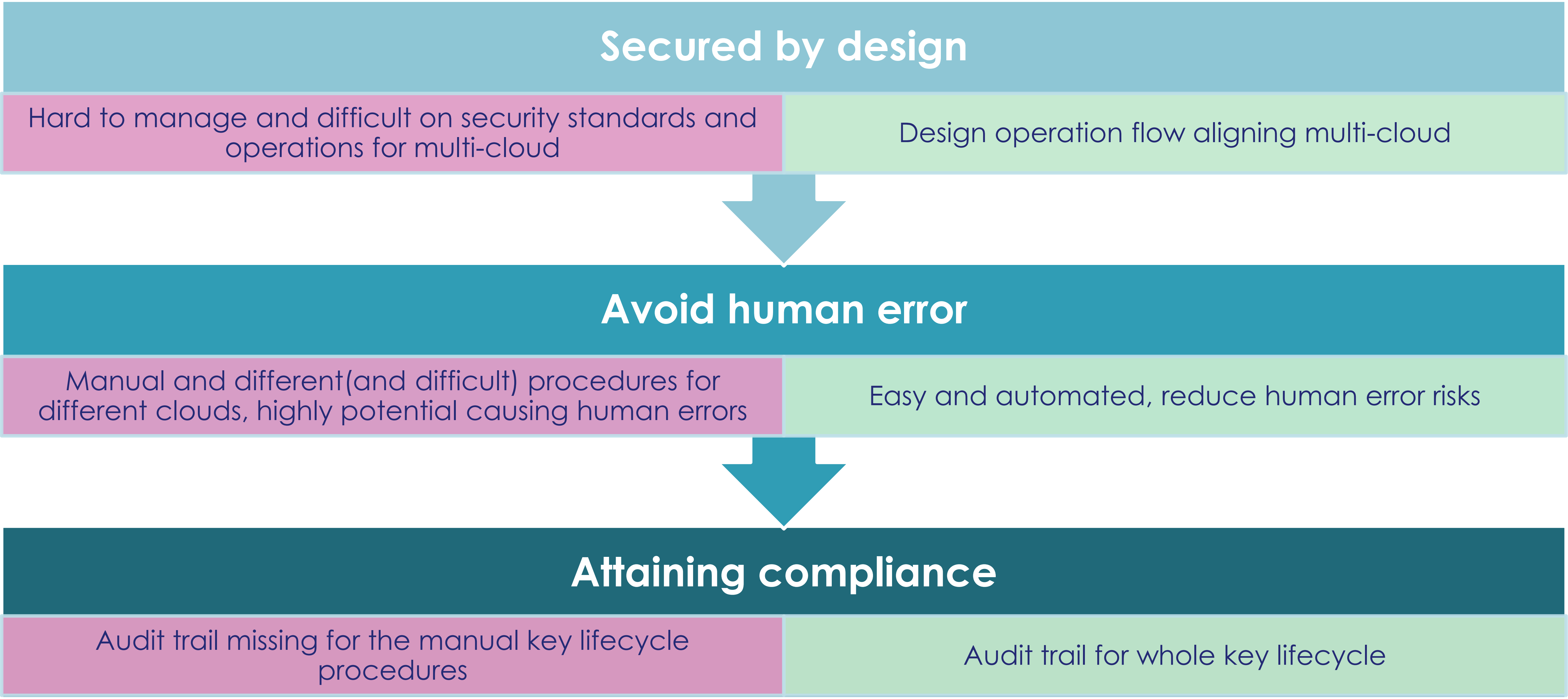
- No learning curve for different cloud
- **Single** portal for different cloud
- Few clicks and automation for different cloud BYOK

Demo 2 – Multi-Cloud Security Operation / Management



1. **Key Synchronization**
2. **Scheduled Key Rotation**

Conclusion – Operation, Control and Compliance



Secured by design

Hard to manage and difficult on security standards and operations for multi-cloud

Design operation flow aligning multi-cloud

Avoid human error

Manual and different(and difficult) procedures for different clouds, highly potential causing human errors

Easy and automated, reduce human error risks

Attaining compliance

Audit trail missing for the manual key lifecycle procedures

Audit trail for whole key lifecycle

Scan to Redeem

Answer FOUR simple questions to receive a KeySmart

*Shipping to HONG KONG only

Wood Lam

Security Consultant
Wood.lam@thalesgroup.com

Thank you

Gracias شكرا لكم

धन्यवाद Merci

Danke 謝謝

ありがとうございました