AWS VIRTUAL BANKING USER GUIDE

Background

At AWS, we understand the compliance needs of Authorized Institutions (AI) and strive to help them migrate to the cloud in a secure manner. The Hong Kong Monetary Authority (HKMA) has recently revised the **Guideline on Authorization of Virtual Banks**[1], and confirmed that the virtual banks will be subject to the same set of supervisory requirements applicable to conventional banks.

This User Guide focuses on the following key considerations for Virtual Banks using AWS, described in the Guideline of Authorization of Virtual Banks and with reference to the **AWS User Guide to Financial Services Regulations & Guidelines in Hong Kong**[2].

Information Security

"14. Technology related risk, especially information security, system resilience and business continuity management, is of vital importance to a virtual bank. Security breaches and unauthorized tampering with the systems of the bank could result in financial loss as well as loss of reputation. The general principle is that the security and technology related controls in place should be "fit for purpose", i.e. appropriate to the type of transactions which the virtual bank intends to carry out." - **Banking Ordinance, Authorization of Virtual Banks, HKMA**

Information security is our highest priority. Using AWS, AIs benefit from a datacenter and network architecture built to meet the requirements of the most security-sensitive organizations. Under the AWS shared responsibility model, AWS provides a global secure infrastructure and foundational compute, storage, networking and database services. AWS provides a range of security services and features that AIs can use to secure their cloud environment. The following are key security domains with examples of complementary AWS services that enable customers to build compliant applications and environments on AWS.

Identity	AWS Identity & Access Management AWS Organizations AWS Cognito AWS Directory Service AWS Single Sign-On
Dectective Control	AWS CloudTrail AWS Config Amazon CloudWatch Amazon GuardDuty VPC Flow Logs
Infrastructure Security	Amazon EC2 Systems Manager AWS Shield AWS Web Application Firewall (WAF) Amazon Inspector Amazon Virtual Private Cloud (VPC)
Data Protection	AWS Key Management Service (KMS) AWS CloudHSM Amazon Macle Certificate Manager Service Side Encryption
Incident Response	AWS Config Rules AWS Lambda

System Resilience and Business Continuity Management

The global AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). An AWS Region is a physical location in the world where AWS has multiple AZs. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. These AZs offer customers the ability to operate production applications and databases which are more highly available, more fault tolerant and more scalable than would be possible from a single data center.

AWS provides AIs with the capability to implement a robust business continuity plan, including frequent server instance backups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic regions as well as across multiple AZs within each region.

Assessment

> *"15. .... A more detailed independent assessment of the actual design, implementation and effectiveness of its computer hardware, systems, security, procedures and controls should be undertaken and the report of the assessment should be provided to the MA before the virtual bank commences operation...."*- **Banking Ordinance, Authorization of Virtual Banks, HKMA**

AWS has established a formal audit program to validate the implementation and effectiveness of the AWS control environment. The AWS audit program includes internal and third-party accreditation audits. The objectives of these audits are to evaluate the operating effectiveness of the AWS control environment. Internal audits are planned and performed periodically. Audits by third party accreditation are conducted to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities.

Compliance reports from these assessments, which includes ISO 27001, ISO 27017, ISO 27018, ISO 9001, PCI DSS Level and SOC, are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications. Some key audit programs and certifications are described in the section entitled "AWS Compliance Assurance Programs". For a full list of audits, certifications and attestations, see the AWS Assurance Programs webpage.

Exit Plan

AIs own and manage access to their data and use of AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Import/Export Snowball to transfer large amounts of data into and out of AWS using physical storage appliances

Additionally, AWS offers AWS Database Migration Service, a web service that AIs can use to migrate a database from an AWS service to an on-premises database. AWS also provides the ability to delete your data. Because AIs retain control and ownership of your data, it is their responsibility to manage data retention according to their requirements.

AWS Services can be used in connection with the transfer of company IT resources in the course of the sale or divestiture of a company's assets or businesses. One notable example is AWS's role in helping Hess Corporation divest of its downstream business. More information of this Case Study can be found here: **AWS Case Study of Hess Corporation[3].**

Next Steps

AWS has published a User Guide to Financial Services Regulations & Guidelines in Hong Kong to assist AIs in their cloud adoption journey by examining the following:

- **HKMA Supervisory Policy Manual on General Principles for Technology Risk Management (TM-G-1)**
- **HKMA Supervisory Policy Manual on Outsourcing (SA-2)**

It provides information that will help companies conduct their due diligence and implement an appropriate information security, risk management and governance program for their use of AWS.

The User Guide to Financial Services Regulations & Guidelines in Hong Kong can be downloaded from **https://d1.awsstatic.com/whitepapers/compliance/HKMA_User_Guide.pdf**

If you have questions or need more information, please contact your Account Manager, or visit

https://aws.amazon.com/contact-us/.

[1] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/guideline_eng_virtual_bank_20180608.pdf

[2] https://d0.awsstatic.com/whitepapers/compliance/HKMA_User_Guide.pdf

[3] https://aws.amazon.com/solutions/case-studies/hess-corporation/