AWS is committed to offering AWS financial institutions customers in Hong Kong SAR a strong compliance framework and advanced tools and security measures which they can use to evaluate, meet, and demonstrate compliance with applicable legal and regulatory requirements.

This document provides AWS financial institution customers with information about the legal and regulatory requirements in Hong Kong SAR which may apply to their use of AWS services.

Who is the financial regulator in Hong Kong SAR?

The Hong Kong Monetary Authority (HKMA) regulates and supervises Authorized Institutions (AIs) including banks and deposit-taking companies as well as retail payment systems and stored-value facilities.

The Hong Kong Insurance Authority (HKIA) regulates and supervises authorized insurers including insurance companies.

The Securities and Futures Commission (SFC) regulates and supervises the securities and futures markets including brokers, investment advisers, fund managers and intermediaries.

What regulations apply to financial institutions in Hong Kong SAR using AWS?

Financial institutions in Hong Kong SAR may be subject to a number of different legal and regulatory requirements when they use cloud services. Guidelines issued by the Hong Kong SAR financial services regulators provide a framework for financial institutions in Hong Kong SAR when they are planning to use cloud services. Some of the key guidelines include:

- HKMA Customer Data Protection Circular (2014)
- HKMA Risk Assessment Form on Technology-related Outsourcing (including Cloud Computing) [document not publicly available - available to AIs only]
- HKIA GL14 Guideline on Outsourcing (2017)
- SFC Use of External Electronic Data Storage Circular (2019)
- SFC Media Release on IOSCO Principles on Outsourcing (2005)

In general, the above guidance covers a variety of contractual and operational areas, including due diligence, risk management, business continuity, and monitoring and oversight. The following AWS whitepapers provide further information on these issues in the context of AWS services:

- AWS User Guide to Financial Services Regulations & Guidelines in Hong Kong SAR – Hong Kong Monetary Authority
- AWS User Guide to Financial Services Regulations & Guidelines in Hong Kong SAR – Hong Kong Insurance Authority
Customers that have questions about the applicable regulations, and how these may apply to their use of AWS services, can reach out to their account representative or contact us.

Regulations are changing rapidly in this space, and AWS is working to help customers proactively respond to new rules and guidelines. AWS encourages its financial institutions customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including other local regulations, guidelines and laws.

**Key considerations for financial institutions in Hong Kong SAR using AWS**

AWS is committed to offering customers a strong compliance framework and advanced tools and security measures which customers can use, to evaluate, meet, and demonstrate compliance with applicable legal and regulatory requirements.

Financial institutions who are using or planning to use AWS services can take the following steps to better understand their compliance needs:

1. Consider the purpose of the workload(s) under consideration and the relevant categories of data in order to anticipate which legal and regulatory requirements may apply.

   Assess the materiality or criticality of the relevant workload(s) in light of local requirements. For example, the HKMA Authorized Institutions should notify the HKMA prior to entering a material outsourcing arrangement with AWS. Authorized Insurers should notify the HKIA prior to entering into a new material outsourcing arrangement or significantly varying an existing one. SFC-Licensed Corporations should seek SFC approval if regulatory records are stored exclusively with an external Electronic Data Storage Provider (EDSP) such as AWS.

2. Review the AWS [Shared Responsibility Model](#) and map AWS responsibilities and customer responsibilities according to each AWS service that will be used. Customers can also use [AWS Artifact](#) to access AWS’ audit reports and conduct their assessment of the control responsibilities.

3. Customers that have further questions about how AWS services can enable their security and compliance needs, or that would like more information, can contact their account representative or contact us.

---

**Key data privacy and protection considerations for financial institutions in Hong Kong SAR using AWS**

Financial institutions in Hong Kong SAR using AWS services should also consider applicable privacy requirements, including the [Hong Kong Personal Data (Privacy) Ordinance (Cap. 486)](#). More information on these requirements are included in the AWS whitepaper, [Using AWS in the Context of Hong Kong SAR Privacy Considerations](#). If customers process or are planning to process the personal data of data subjects in the European Union (EU), they should visit [AWS’ General Data Protection Regulation (GDPR) Center](#). More information on these requirements are included in the AWS whitepaper, [Navigating GDPR Compliance on AWS](#).
Additional AWS Resources

The following resources are publicly available:

- **AWS Compliance Quick Reference Guide**
- **AWS User Guide to Financial Services Regulations and Guidelines in Hong Kong SAR – Hong Kong Monetary Authority**
- **AWS User Guide to Financial Services Regulations and Guidelines in Hong Kong SAR – Hong Kong Insurance Authority**
- **Navigating GDPR Compliance on AWS**
- **Using AWS in the Context of Hong Kong SAR Privacy Considerations**

The following resources are available for download through [AWS Artifact](#). Please note that an [AWS account](#) will be required to access AWS Artifact.

- **HKMA TM-G-1 General Principles for Technology Risk Management Workbook**
- **HKMA TM-G-2 Business Continuity Planning Workbook**
- **HKIA GL20 Guideline on Cybersecurity Workbook**

AWS Compliance Programs

This document is provided for informational purposes only. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.