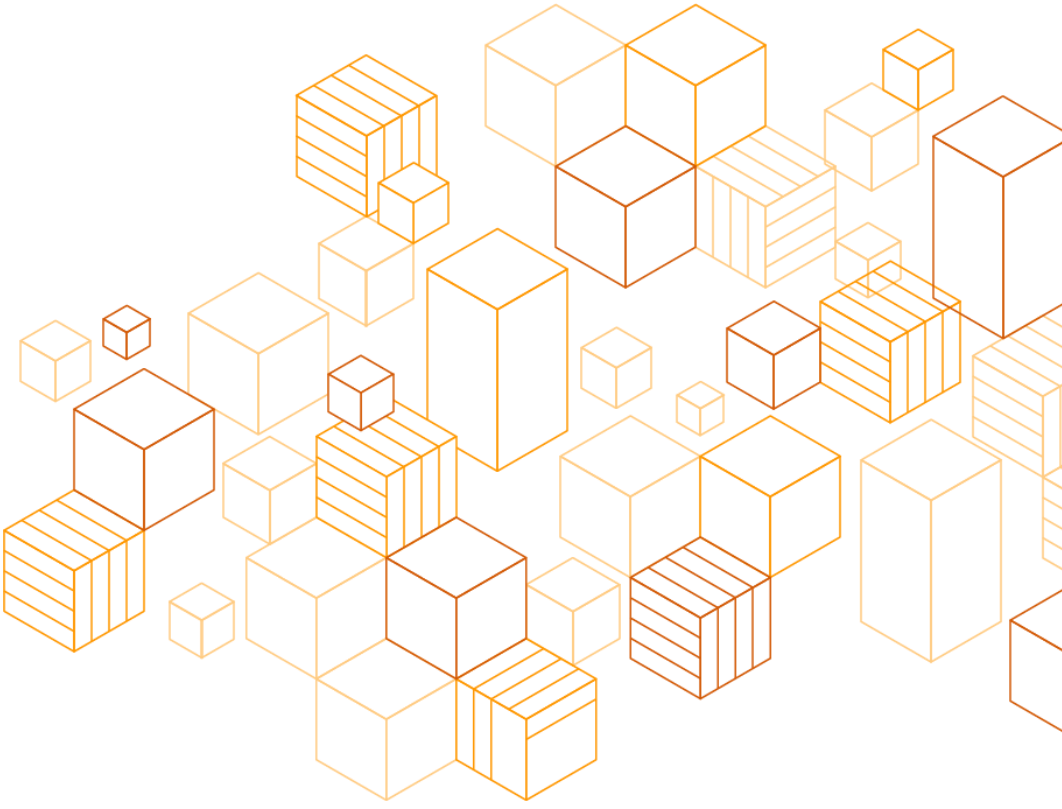
AWS User Guide to the Hong Kong Monetary Authority on Outsourcing and General Principles for Technology Risk Management Supervisory Policy Manuals

April 2020



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. 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.

Contents

About this Guide

This document provides information to assist Authorized Institutions (AIs) in Hong Kong regulated by the Hong Kong Monetary Authority (HKMA) as they accelerate their use of Amazon Web Services' (AWS) Cloud services

Overview

The Hong Kong Monetary Authority (HKMA) issues guidelines to provide the Hong Kong banking industry with practical guidance to facilitate compliance with regulatory requirements. The guidelines relevant to the use of outsourced services instruct Authorized Institutions (AIs) to perform risk assessments, perform due diligence reviews of service providers, ensure controls are in place to preserve information confidentiality, have sufficient monitoring and control oversight on the outsourcing arrangement, and establish contingency arrangements.

The following sections provide considerations for AIs as they assess their responsibilities with regards to the following guidelines:

- Supervisory Policy Manual on Outsourcing (SA-2) - This Supervisory Policy Manual sets out the HKMA's supervisory approach to outsourcing and the major points which the HKMA recommends AIs to address when outsourcing their activities, including the use of cloud services.
- Supervisory Policy Manual on General Principles for Technology Risk Management (TM-G-1) - This Supervisory Policy Manual provides AIs with guidance on general principles which AIs are expected to consider in managing technology-related risks.

Taken together, AIs can use this information to perform their due diligence and assess how to implement an appropriate information security, risk management, and governance program for their use of AWS. For a list of the guidelines, see the Regulatory Resources – Regulatory Guides section on the HKMA website.

Security and the Shared Responsibility Model

Cloud security is a shared responsibility. At AWS, we maintain a high bar for security *OF* the cloud through robust governance, automation, and testing and validates our approach through compliance with global and regional regulatory requirements and best practices. Security *IN* the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems, and networks. Customers should carefully consider how they will manage the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. We

recommend that customers think about their security responsibilities on a service-by-service basis because the extent of their responsibilities may differ between services.

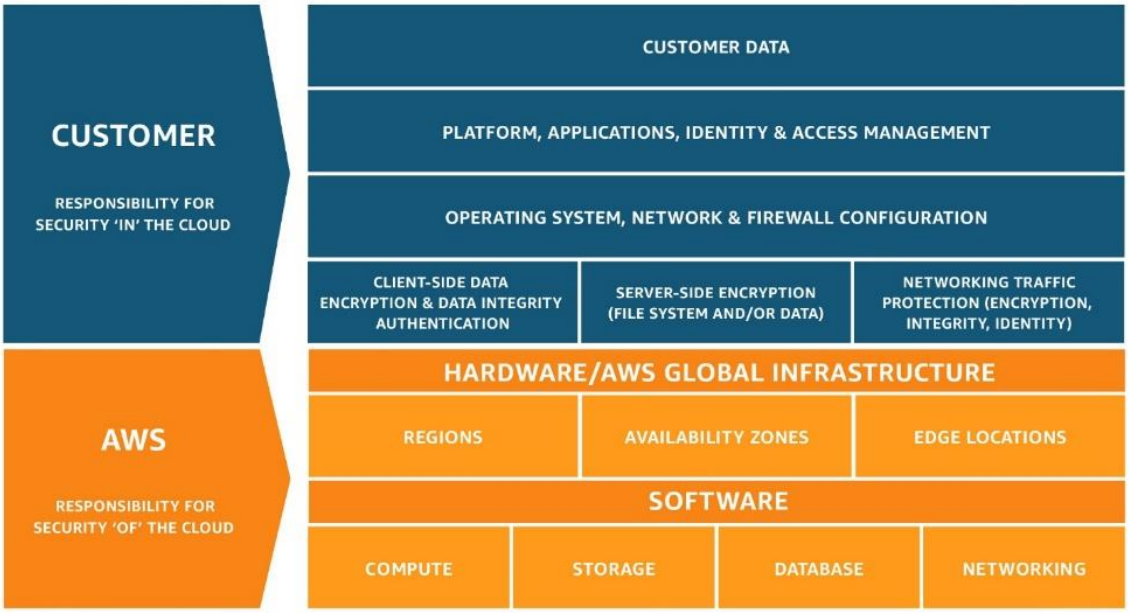


Figure 1 – Shared Responsibility Model

Security IN the Cloud

Customers are responsible for their security in the cloud. For services such as Amazon Elastic Compute Cloud (Amazon EC2), the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. Customers can also use managed services, such as databases, directory, and web application firewall services, which provide customers the resources they need to perform specific tasks without having to launch and maintain virtual machines. For example, a customer can launch an Amazon Aurora database, which Amazon Relational Database Service (Amazon RDS) manages to handle tasks such as provisioning, patching, backup, recovery, failure detection, and repair.

It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS.
- The AWS services that are used with the content.

- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their content is encrypted and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customers are responsible for the security of the content they put on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platforms, databases, or other services.

Security OF the Cloud

For many services, such as EC2, AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In order to provide assurance about security of the AWS Cloud, we continuously audit our environment. AWS infrastructure and services are validated against multiple compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that can be implemented, and to better assist customers with managing their control environment.

- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.
- **Monitor** that AWS maintains compliance with global standards and best practices, through the use of thousands of security control requirements.

AWS Compliance Assurance Programs

In order to help customers establish, operate, and leverage the AWS security control environment, AWS has developed a security assurance program that uses global privacy and data protection best practices. These security protections and control processes are independently validated by multiple third-party independent assessments. The followings are of particular importance to Hong Kong AIs:

ISO 27001 – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System that defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

ISO 27017 – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

ISO 27018 – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by

the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

ISO 9001 - ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

PCI DSS Level 1 - The Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

SOC – AWS System & Organization Controls (SOC) Reports are independent third-party audit reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls established to support operations and compliance. For more information, see the SOC Compliance webpage. There are three types of AWS SOC Reports:

- **SOC 1**: Provides information about the AWS control environment that may be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
- **SOC 3**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information.

By tying together governance-focused, audit-friendly service features with such certifications, attestations and audit standards, AWS Compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.

For more information about other AWS certifications and attestations, see AWS Compliance Programs.

AWS Artifact

Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting tool available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS's security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Regions

The AWS Cloud infrastructure is built around AWS Regions and Availability Zones. An AWS Region is a physical location in the world that is made up of multiple Availability Zones. Availability Zones consist of one or more discrete data centers that are housed in separate facilities, each with redundant power, networking, and connectivity. These Availability Zones offer customers the ability to operate production applications and databases at higher availability, fault tolerance, and scalability than would be possible from a single data center. For current information on AWS Regions and Availability Zones, see https://aws.amazon.com/about-aws/global-infrastructure/.

HKMA Supervisory Policy Manual on Outsourcing (SA-2)

The HKMA Supervisory Policy Manual on Outsourcing (SA-2) provides guidance and recommendations on prudent risk management practices for outsourcing, including use of cloud services by AIs. AIs that use the cloud are expected to carry out due diligence, evaluate and address risks, and enter into appropriate outsourcing agreements. Section 2.2 of the SA-2 states that the AI's risk assessment should include a determination of the importance and criticality of the services to be outsourced, the cost and benefit of the outsourcing, and the impact on the AI's risk profile (in respect of operational, legal

and reputation risks) of the outsourcing. AIs should be able to demonstrate their observance of the guidelines to the HKMA through the submission of the HKMA Risk Assessment Form on Technology-related Outsourcing (including Cloud Computing) six weeks before target implementation date.

A full analysis of the SA-2 is beyond the scope of this document. However, the following sections address the considerations in the SA-2 that most frequently arise in interactions with AIs.

Outsourcing Notification

Under Section 1.3.2 of the SA-2, AIs are required to notify the HKMA via a Notification Letter prior to implementing solutions which leverage public cloud services in respect of banking-related business areas, including in cases where the AI is outsourcing a banking activity to a service provider who is providing services using the public cloud. In general, a notification letter should be submitted to the HKMA 3 months prior to the commencement of the outsourcing activity. The AI must affirm specific compliance with controls related to outsourcing and cloud operation, together with general compliance with other relevant HKMA guidelines such as the Supervisory Policy Manual on General Principles for Technology Risk Management (TM-G-1).

The HKMA expects AIs to fully comply with all relevant regulatory control requirements prior to launching any new outsourced services, including when deploying on AWS cloud.

Assessment of Service Providers

Sections 2.1, 2.2 and 2.3 of the SA-2 set out a list of topics that should be evaluated in the course of due diligence when an AI is considering an outsourcing arrangement, including use of cloud services. The following table includes considerations for each component of Section 2.3.1 of the SA-2.

Due Diligence Requirement	Customer Considerations
Financial soundness	The financial statements of Amazon.com Inc. include AWS's sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website.

Due Diligence Requirement	Customer Considerations
Reputation	Since 2006, AWS has provided flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, allowing us to provide new services that help millions of active customers.
Managerial skills	AWS management has developed a strategic business plan, which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.
Technical capabilities, operational capability and capacity	The AWS Cloud operates a global infrastructure with multiple Availability Zones within multiple geographic AWS Regions around the world. For more information, see AWS Global Infrastructure. AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and data. Maintaining customer trust and confidence is of the utmost importance to AWS. AWS performs a continuous risk assessment process to identify, evaluate, and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months.
Compatibility with the AI's corporate culture and future development strategies	AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure that the quality and security requirements are met with each release. The AWS strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements.

Due Diligence Requirement	Customer Considerations
Familiarity with the banking industry and capacity to keep pace with innovation in the market.	For a list of case studies from financial services customers that have deployed applications on the AWS Cloud, see Financial Services Customer Stories. For a list of financial services cloud solutions provided by AWS, see Financial Services Cloud Solutions. The AWS Cloud platform expands daily. For a list of the latest AWS Cloud services and news, see What's New with AWS.

Outsourcing Agreement

Section 2.4 of the SA-2 clarifies that the type and level of services to be provided and the contractual liabilities and obligations of the service provider must be clearly set out in a service agreement between the AI and their service provider. HKMA expect AIs to regularly review their outsourcing agreements.

AWS customers may have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit your organization's needs. For more information about AWS Enterprise Agreements, contact your AWS representative.

Information Confidentiality

Under Section 2.5 of the SA-2, AIs need to ensure that as part of the outsourcing, AIs can continue to comply with local and regional data protection requirements. The following table lists what you should consider.

Requirement	Customer Considerations
Section 2.5.2: AIs should have controls in place to ensure that the requirements of customer data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of customer information.	**Data Protection** – You choose how your data is secured. AWS offers you strong encryption for your data in transit or at rest, and AWS provides you with the option to manage your own encryption keys. If you want to tokenize data before it leaves your organization, you can engage a number of AWS partners with relevant expertise. **Data Integrity** – For access and system monitoring, AWS Config provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. Config rules enable you to create rules that automatically check the configuration of AWS resources recorded by AWS Config. When your resources are created, updated, or deleted, AWS Config streams these configuration changes to Amazon Simple Notification Service (Amazon SNS), which notifies you of all configuration changes. AWS Config represents relationships between resources, so that you can assess how a change to one resource might impact other resources. **Data Segregation** – Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. **Access Rights** – AWS provides a number of ways for you to identify users and securely access your AWS Account. A complete list of credentials supported by AWS can be found in the AWS Management Console by choosing your user name in the navigation bar and then choosing **My Security Credentials**. AWS also provides additional security options that enable you to further protect your AWS Account and control access using the following: AWS Identity and Access Management (IAM), key management and rotation, temporary security credentials, and multi-factor authentication (MFA).

Requirement	Customer Considerations
Section 2.5.4: In the event of a termination of outsourcing agreement, for whatever reason, AIs should ensure that all customer data is either retrieved from the service provider or destroyed	AWS provides you with the ability to delete your data. Because you retain control and ownership of your data, it is your responsibility to manage data retention to your own requirements. If you decide to leave AWS, you can manage access to your data and AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Import/Export to transfer large amounts of data into and out of AWS using physical storage appliances. For more information, see Cloud Storage with AWS. Additionally, AWS offers AWS Database Migration Service, a web service that you can use to migrate a database from an AWS service to an on-premises database. In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent your organization's data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. For more information, see ISO 27001 standards, Annex A, domain 8. AWS has been validated and certified by an independent auditor to confirm alignment with the ISO 27001 certification standard. For additional details, see AWS Cloud Security. Also, see the Section 7.3 of the Customer Agreement which is available at AWS Customer Agreement.

Monitoring and Control

Under Section 2.6 of the SA-2, AIs need to ensure that they have sufficient and effective procedures for monitoring the performance of the service provider, the relationship with the service provider and the risks associated with the outsourced activity.

AWS has implemented a formal, documented incident response policy and program, this can be reviewed in the SOC 2 report via AWS Artifact. You can also see security notifications on the AWS Security Bulletins website. AWS provides you with various

tools you can use to monitor your services, including those already noted and others you can find on the AWS Marketplace.

Contingency Planning

Under Section 2.7 of the SA-2, AIs should maintain contingency plans that take the following into consideration: the service provider's contingency plan, a breakdown in the systems of the service provider, and telecommunication problems in the host country. Section 2.7.2 of the SA-2 states that contingency arrangements in respect of daily operational and systems problems would normally be covered in the service provider's own contingency plan. AIs should ensure that they have an adequate understanding of their service provider's contingency plan and consider implications for their own contingency planning in the event that the outsourced service is interrupted.

AWS and regulated AIs share a common interest in maintaining operational resilience, i.e., the ability to provide continuous service despite disruption. Continuity of service, especially for critical economic functions, is a key prerequisite for financial stability. For more information about AWS operational resilience approaches, see the AWS whitepaper Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond. The AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been developed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach ensures that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions. For more information, see the AWS whitepaper Amazon Web Services: Overview of Security Processes and the SOC 2 report in the AWS Artifact console.

AWS provides you with the capability to implement a robust 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 Availability Zones within each Region. For more information about disaster recovery approaches, see Disaster Recovery.

Access to Outsourced Data

The SA-2 clarifies that an AI's outsourcing arrangements should not interfere with the ability of the AI to effectively manage its business activities or impede the HKMA in carrying out its supervisory functions and objectives.

You retain ownership and control of your data when using AWS services. You have complete control over which services you use and whom you empower to access your content and services, including what credentials will be required. You control how you configure your environments and secure your data, including whether you encrypt your data (at rest and in transit), and what other security features and tools your use and how you use them. AWS does not change your configuration settings, as these settings are determined and controlled by you. You have the complete freedom to design their security architecture to meet your compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers you to decide when and how security measures will be implemented in the cloud, in accordance with your business needs. For example, if a higher availability architecture is required to protect your data, you may add redundant systems, backups, locations, network uplinks, etc. to create a more resilient, high availability architecture. If restricted access to your data is required, AWS enables you to implement system-level access rights management controls and data level encryption. For more information, see Using AWS in the Context of Hong Kong Privacy Considerations.

You can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 27018 certifications and PCI DSS compliance reports. These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls.

For more information about the AWS approach to audit and inspection, please contact your AWS representative.

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

The HKMA Supervisory Policy Manual on General Principles for Technology Risk Management (TM-G-1) sets out risk management principles and best practice standards to guide AIs in meeting their legal obligations. The HKMA expects AIs to have an effective technology risk management framework in place to ensure the adequacy of IT controls and quality of their computer systems.

AWS has produced a TM-G-1 Workbook that covers the six domains documented within the TM-G-1. For shared controls, where AWS is expected to provide information as part of the Shared Responsibility Model, AWS controls are mapped against the control requirements of the TM-G-1.

The following table shows the AWS response to guidelines Sections 2.1.1 and 3.3.2 of the TM-G-1:

ID	Guideline	Responsibility	Customer Considerations
2.1.1	Achieving a consistent standard of sound practices for IT controls across an AI requires clear direction and commitment from the Board and senior management. In this connection, senior management, who may be assisted by a delegated sub-committee, is responsible for developing a set of IT control policies which establish the ground rules for IT controls. These policies should be formally approved by the Board or its designated committee and properly implemented among IT functions and business units.	Customer Specific	Not Applicable

ID	Guideline	Responsibility	Customer Considerations
3.3.2	Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorized activities being performed by the security administration function.	Shared	**Identity & Access Management: Segregation of Duties** Privileged access to AWS systems by AWS employees are allocated based on least privilege, approved by an authorized individual prior to access provisioning, and assigned a different user ID than used for normal business use. Duties and areas of responsibility (for example, access request and approval, change management request and approval, change development, testing and deployment, etc.) are segregated across different individuals to reduce opportunities for an unauthorized or unintentional modification or misuse of AWS systems. Customers retain the ability to manage segregation of duties of their AWS resources by using AWS Identity and Access Management (IAM). IAM enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

You can get a copy of the TM-G-1 Workbook by accessing AWS Artifact within the AWS Management Console.

To use the TM-G-1 Workbook, you should review the AWS responses and then enrich them with your own organizational controls. Let's use the previous controls statements as an example. Section 2.2.1 of the TM-G-1 discusses the sound practices for IT controls oversight by the AI's board of directors/senior management. This is a principle that would only apply to you and is not specific to cloud or particular applications. This control can only be fulfilled by you, the AI. In contrast, Section 3.3.2 of the TM-G-1 is a shared control. This control requires formal procedures for administering the access rights to system resources and application systems. This is a shared control because

AWS administers the access rights to the system resources AWS uses to operate the cloud services and you administer the system resources that you create using our services.

The Workbook also positions you to more clearly consider whether and how to add supplementary technology risk controls that are specific to your line-of-business or application teams, or your particular needs.

Note that it is important to appreciate the implications of the shared security responsibility model, and understand which party is responsible for a particular control. Where AWS is responsible, the AI should identify which of the AWS Assurance reports, certifications or attestations are used to establish or assess that the control is operating.

Next Steps

Each organization's cloud adoption journey is unique. In order to successfully execute your adoption, you need to understand your organization's current state, the target state, and the transition required to achieve the target state. Knowing this will help you set goals and create work streams that will enable staff to thrive in the cloud.

The AWS Cloud Adoption Framework (AWS CAF) offers structure to help organizations develop an efficient and effective plan for their cloud adoption journey. Guidance and best practices prescribed within the framework can help you build a comprehensive approach to cloud computing across your organization, throughout your IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find more about such workshops, please contact your AWS representative. Alternatively, AWS provides access to tools and resources for self-service application of the AWS CAF methodology at AWS Cloud Adoption Framework.

For AIs in Hong Kong, next steps typically also include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, as well as AWS Solution Architects, Professional Services teams and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us at https://aws.amazon.com/contact-us/.

- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the AWS Artifact portal (accessible via the AWS Management Console).
- Consider the relevance and application of the CIS AWS Foundations Benchmark available here and here, as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the Additional Resources section below.
- Speak with your AWS representative to learn more about how AWS is helping Financial Services customers migrate their critical workloads to the cloud.

Additional Resources

For additional information, see:

- AWS Cloud Security Whitepapers & Guides
- AWS Compliance
- AWS Cloud Security Services
- AWS Best Practices for DDoS Resiliency
- AWS Security Checklist
- Cloud Adoption Framework - Security Perspective
- AWS Security Best Practices
- AWS Risk & Compliance
- Using AWS in the Context of Hong Kong Privacy Considerations

Document Revisions

Date	Description
April 2020	Updates to *Additional Resources*.
February 2020	Revision and updates.
November 2017	Style and content updates.
August 2017	First publication.