Navigating HKMA Compliance on AWS

February 2024

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

Abstract

This document provides information to assist authorized institutions (AIs) in Hong Kong that are regulated by the Hong Kong Monetary Authority (HKMA) as they accelerate their use of Amazon Web Services (AWS).

This guide:

- Describes the respective roles that the customer and AWS each play in managing and securing the cloud environment.
- Provides an overview of the regulatory requirements and guidance that AIs can consider when using AWS.
- Provides additional resources that can help AIs design and architect their AWS environment to be secure and meet regulatory expectations, including those under HKMA guidelines.

Introduction

The AWS Well-Architected Framework helps you understand the pros and cons of the decisions you make when building systems on Amazon Web Services (AWS). The six pillars of the Framework allow you to learn architectural best practices for designing and operating reliable, secure, efficient, cost-effective, and sustainable systems. AWS also provides a service known as the AWS Well-Architected Tool, available at no additional charge in the AWS Management Console, so you can review your applications and workloads against these best practices by answering a set of questions for each pillar. The Financial Services Industry Lens for the AWS Well-Architected Framework specifies best practices for security, data privacy, and resiliency that are intended to address requirements of financial institutions. For more expert guidance and best practices for your cloud architecture—reference architecture deployments, diagrams, and whitepapers—see the AWS Architecture Center.

AWS provides financial services institutions across multiple industries including banking, payments, capital markets, and insurance the secure, resilient global cloud infrastructure and services they need to differentiate themselves today and adapt to the needs of tomorrow. Through continuous innovation, AWS delivers security capability, breadth and depth of services, deep industry expertise, and an expansive partner network.

Building on AWS empowers organizations to modernize their infrastructure, meet rapidly changing customer behaviors and expectations, and drive business growth. AWS offers IT services in categories ranging from compute, storage, database, and networking to artificial intelligence and machine learning. Across the world, financial institutions have used AWS services to build their own applications for mobile banking, regulatory reporting, and market analysis.

Financial services institutions are regulated by different regulators in Hong Kong based on business natures. The Hong Kong Monetary Authority (HKMA) is Hong Kong's central banking institution. One of the HKMA's primary functions is to regulate and supervise banking business and the business of taking deposits with a view to promoting the stability and integrity of the financial system (including the banking system). Authorized institutions (AIs) regulated by the HKMA, including licensed banks, restricted license banks, and deposit-taking companies, typically consider the following HKMA guidelines to be relevant to their use of AWS services:

- HKMA Supervisory Policy Manual module on Outsourcing (SA-2) – This module sets out the HKMA's supervisory approach to outsourcing and the key points that the HKMA recommends AIs to address when outsourcing their activities.

- HKMA Supervisory Policy Manual module on Operational Resilience (OR-2).

- HKMA Supervisory Policy Manual module on General Principles for Technology Risk Management (TM-G-1) – This module provides AIs with guidance on general principles that AIs are expected to consider in managing technology-related risks.

- Guidance on Cloud Computing – This circular provides AIs with guidance on the HKMA's supervisory expectations with respect to the adoption of cloud computing.

This guide is intended to be a resource to help AIs understand the technical and operational requirements of the HKMA guidelines that might apply to them when using AWS. This guide includes a description of the AWS compliance framework, advanced tools, and security measures, which AIs can use to evaluate and help demonstrate compliance with their applicable regulatory requirements under the HKMA guidelines.

For a full list of the HKMA guidelines, see the Regulatory Resources section on the HKMA website.

Security and the AWS Shared Responsibility Model

It's important that AIs understand the AWS Shared Responsibility Model before exploring the specific requirements under the HKMA guidelines.

Cloud security is a shared responsibility. AWS manages security of the cloud by making sure that AWS Cloud infrastructure adheres to global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer.

This means that customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems, and networks, as they would for applications in an on-premises data center.

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security principles. 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 AWS services operate.

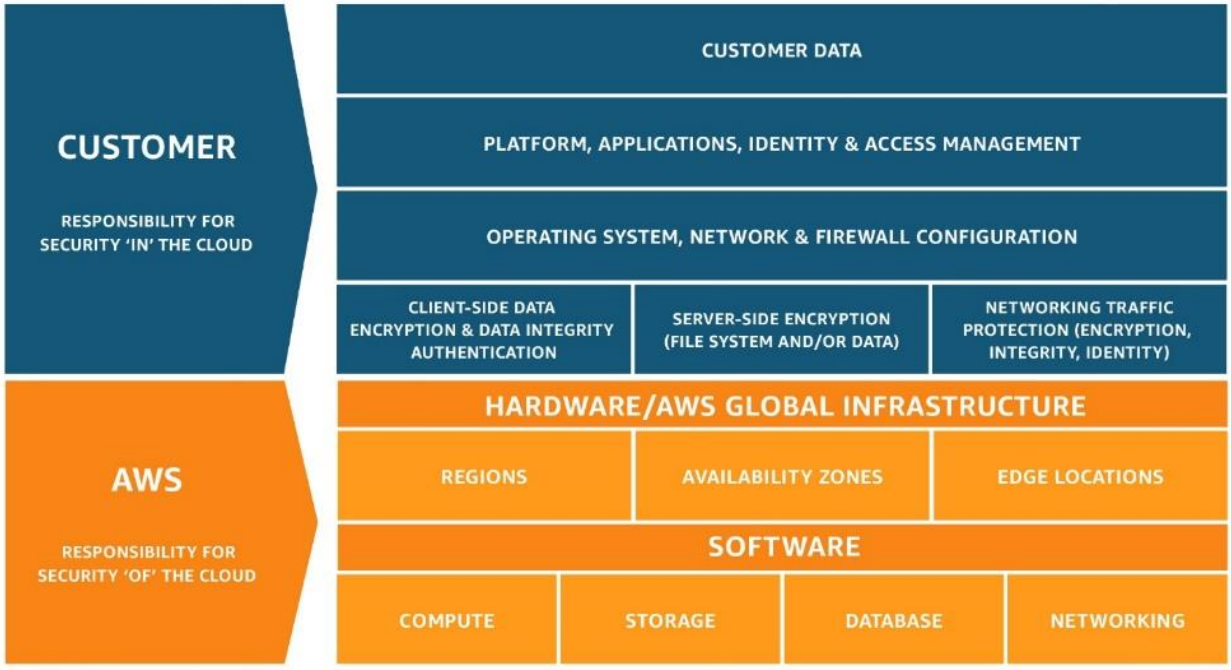

Figure 1 – AWS Shared Responsibility Model

Security in the cloud

Customers are responsible for their security in the cloud. Customers can also use managed services, such as databases, directory, and web application firewall services, which provide the resources needed to perform specific tasks without having to maintain the virtual machines layer. 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's important to note that when using AWS services, customers maintain control of 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.
- Where their content is stored.
- The format and structure of their content and whether it's 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. Customer responsibility is determined by the AWS services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security

responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as infrastructure as a service (IaaS) and so requires the customer to perform all of the necessary security configuration and management tasks.

Customers that deploy an EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For abstracted AWS services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, operating system, and environments, and customers access the endpoints to store and retrieve data. Whether the customer is using IaaS or an abstracted service, customers are responsible for managing their data (including encryption options), classifying their assets, and using AWS Identity and Access Management (IAM) tools to apply the appropriate permissions.

Security of the cloud

AWS infrastructure and services are backed by several compliance standards and industry certifications across geographies and industries. Customers can use compliance certifications held by AWS 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:

- **Validation** 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 customers can implement, and to better assist customers with managing their control environment.

- **Demonstrating** the AWS compliance posture to help enable 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.

- **Monitoring** through applicable security controls, which AWS maintains in alignment with global standards and best practices.

AWS compliance programs

AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can use the AWS compliance programs to help satisfy their regulatory requirements. For more information about these third-party certifications and audit reports, see the AWS Compliance Programs webpage.

Certifications and third-party attestations

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads. However, the following are of particular importance to 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's 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 22301:2019** – ISO 22301:2019 specifies requirements to implement, maintain and improve a business continuity management system (BCMS). AWS alignment with and independent third-party assessment of this internationally recognized code of practice demonstrates the commitment of AWS to the business continuity and resiliency of AWS global services and assures compliance with international standards. For more information, or to download the AWS ISO 22301:2019 certification, see the ISO 22301:2019 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 the 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 (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) 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 and Organization Controls (SOC) Reports are independent third-party examination 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 might be relevant to a customer's internal controls over financial reporting (ICOFR) as well as information for assessment and opinion of the effectiveness of 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, confidentiality, and privacy.

    - **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, confidentiality, and privacy without disclosing AWS internal information.

By tying together governance-focused, audit-friendly service features with 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 the AWS Compliance Programs webpage. For information about general AWS security controls and service-specific security, see Best Practices for Security, Identity, and Compliance.

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 security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Compliance Center

Customers can use the AWS Compliance Center to research cloud-related regulatory requirements in over 50 countries. AWS Compliance Center helps customers access country-specific compliance resources such as compliance guides or whitepapers, identify local regulatory requirements and regulators, and view AWS compliance programs that might apply to a specific country.

AWS Global Cloud Infrastructure

The AWS Global Cloud Infrastructure comprises of AWS Regions and Availability Zones. A Region is a physical location in the world consisting of multiple Availability Zones.

Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities.

Availability Zones offer customers the ability to operate applications and databases in a way that's more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment.

AWS customers choose the AWS Regions in which their content and servers are located. This allows customers to establish environments that help meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in the locations of their choice. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

HKMA Supervisory Policy Manual module on Outsourcing (SA-2)

The HKMA Supervisory Policy Manual module on Outsourcing (SA-2) provides guidance and recommendations on prudent risk management practices for outsourcing, including the use of cloud services by AIs. AIs that use cloud services are expected to observe the SA-2 and perform appropriate risk assessment for use of the cloud. Section 2.2 of the SA-2 states that an AI's risk assessment should assess 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 to operational, legal, and reputation risks) of the outsourcing.

Prior to cloud implementation, AIs should demonstrate their compliance of the SA-2 and the relevant technology risk requirements through the submission of the HKMA Risk Assessment Form on Technology-related Outsourcing (including cloud computing). 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 our interactions with AIs.

Outsourcing notification

Under Section 1.3.2 of the SA-2, AIs are required to notify the HKMA through a notification letter prior to implementing solutions that use public cloud services in respect to banking-related business areas, including in cases where the AI is outsourcing a banking activity to a service provider that is providing services using the public cloud. In general, a notification letter should be submitted to the HKMA three 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 module 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 the 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 the use of cloud services. The following table includes considerations for each component of Section 2.3.1 of the SA-2.

Due diligence areas	Considerations
Financial soundness	The financial statements of Amazon.com, Inc. include AWS sales and income, permitting assessment of its financial position and ability to service its debts and liabilities. These financial statements are available from the US Securities and Exchange Commission (SEC) or at Amazon's Investor Relations website.
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.

Due diligence areas	Considerations
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.
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.

Due diligence areas	Considerations
	The AWS Cloud environment 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 states that the contractual liabilities and obligations of the service provider must be clearly set out in a service agreement. HKMA also expects AIs to regularly review their outsourcing agreements with the service provider. Customers regulated by the HKMA have the option to enroll in an Enterprise Agreement with AWS. We also offer a Financial Services Addendum to support our customers to address the HKMA contractual requirement. For more information about AWS Enterprise Agreements and the Financial Services Addendum, contact your AWS representative.

Information confidentiality

Under Section 2.5 of the SA-2, AIs should ensure the outsourcing arrangement complies with the relevant data protection requirements. The following table lists some of the considerations.

Data protection requirements	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. AWS 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 configuration changes. AWS Config represents relationships between resources so that you can assess how a change to one resource might impact other resources.

Data protection requirements	Considerations
	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).
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 (AWS DMS), a web service that you can use to migrate a database from an AWS service to an on-premises database.

Data protection requirements	Considerations
	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 should ensure there are effective procedures for monitoring and managing the performance and the relationship with the service providers, and the risks associated with the outsourced activities. This includes establishing reporting procedures to escalate events or problems related to the outsourcing activities.

AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub, and AWS Config rules to track, monitor, analyze, and audit events. If these tools identify an event that is analyzed and determined to be an incident, that *qualifying event* will raise an incident and start the incident management process and the appropriate response actions necessary to mitigate the incident.

Regarding the AWS incident management process, AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.

Contingency planning

Under Section 2.7 of the SA-2, AIs should maintain contingency plans to ensure business continuity. AIs should ensure that there is an adequate understanding of their service provider's contingency plan and consider implications to the AI's operations if the outsourced service is interrupted.

AWS and AIs share a common interest in maintaining operational resilience, that is, the ability to provide continuous services despite disruption. Continuity of services, especially for critical financial 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. 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 makes sure 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 customers 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 Availability Zones within each Region. For more information about disaster recovery approaches, see Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

Access to outsourced data

The SA-2 states that an AI's outsourcing arrangements should not interfere with the AI's ability to access their data and to maintain up-to-date records.

Understanding the cloud shared responsibility model is important when it comes to understanding the access to the AI's data. The customer retains ownership and control of their data when using AWS services. They have complete control over which services they use and whom they allow to access their content and services, including what credentials will be required. The customer controls how they configure their environments and secure their data, including whether they encrypt their data (at rest and in transit), and what other security features and tools they use and how they use them. AWS doesn't change customers' configuration settings, as these settings are determined and controlled by the customer. Customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers customers to decide when and how security measures will be implemented in the AWS Cloud, in accordance with their business needs. For example, if a higher availability architecture is required to protect a customer's data, the customer can add redundant systems, backups, locations, network uplinks, and so on, to create a more resilient, high availability architecture. If restricted access to the data is required, AWS enables the customer 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.

Customers 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, contact an AWS representative.

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

The HKMA Supervisory Policy Manual module 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. You can get a copy of the TM-G-1 Workbook by accessing AWS Artifact within the AWS Management Console.

HKMA Supervisory Policy Manual module on Operational Resilience (OR-2)

The HKMA Supervisory Policy Manual module on Operational Resilience (OR-2) sets out the general principles that AIs are expected to consider when developing their operational resilience framework.

AWS customers can use the features of the AWS infrastructure and AWS services to help meet a wide range of resiliency goals.

Using multiple Availability Zones, even within a single Region, can enhance resiliency as compared to an on-premises environment.

Availability Zones are designed to mitigate against the risk of natural disaster and other disruptions that might occur. Availability Zones are physically separated within a metropolitan region and are in different flood plains. Each Availability Zone is also designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of failure.

Customers can achieve extremely high recovery time and recovery point objectives by using multiple Availability Zones and data replication.

For more details, see Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

HKMA guidance on cloud computing

The HKMA circular Guidance on Cloud Computing sets out the HKMA's supervisory expectations for the use of the cloud. A full analysis of the HKMA Guidance on Cloud Computing is beyond the scope of this document. However, the following sections address the considerations that most frequently arise in our interactions with AIs.

The following table is organized into two columns, namely:

- **Supervisory expectations** – This column lists the technical and operational expectations that might be applicable to each of the scenarios outlined in the HKMA guidance.
- **Considerations** – This column explains the AWS considerations for addressing the expectations set out in the HKMA guidance. It might refer to the security of the cloud, and how AWS implements and manages the controls and AWS services AIs can use to address these expectations.

Supervisory expectations	Considerations
1. Maintaining an effective governance framework for cloud computing.	AWS customers are responsible for maintaining adequate governance over their entire IT control environment, regardless of how or where IT is deployed. Leading practices include: • Understanding the required compliance objectives and requirements (from relevant sources) • Establishing a control environment that meets those objectives and requirements • Understanding the validation required based on the organization's risk tolerance • Verifying the operating effectiveness of their control environment Deployment in the AWS Cloud gives enterprises different options to apply various types of controls and various verification methods.

Supervisory expectations	Considerations
	Strong customer compliance and governance might include the following basic approach: 1. Reviewing the AWS Shared Responsibility Model, AWS Security Documentation, AWS compliance reports, and other information available from AWS, together with other customer-specific documentation. Understand as much of the entire IT environment as possible, and then document all compliance requirements into a comprehensive cloud control framework. 2. Designing and implementing control objectives to meet the enterprise compliance requirements as laid out in the AWS Shared Responsibility Model. 3. Identifying and documenting controls owned by outside parties. 4. Verifying that all control objectives are met and all key controls are designed and operating effectively. Approaching compliance governance in this manner will help customers gain a better understanding of their control environment and will help clearly delineate the verification activities to be performed.
2. Conducting proper due diligence on Cloud Service Providers (CSPs) before and during engagement.	Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the 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 these third-party certifications and audit reports, see the AWS Compliance Programs webpage. 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.

Supervisory expectations	Considerations
	See the following AWS audit reports and certifications for additional details: SOC 2, PCI DSS, ISO 27001 and ISO 27017. **Logical separation of environment and multi-tenancy** Customers are responsible for the separation of the environments and data they create on AWS. AIs must manage access to their content and resources through users, groups, permissions, and credentials that customers control. The Logical Separation Handbook and the Security Design of AWS Nitro System will help AIs understand logical separation in the cloud and demonstrates its advantages over a traditional physical separation model. Customer environments are logically segregated to help prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services that provide virtualized operational environments to customers (such as Amazon EC2) make sure that customers are segregated from one another and help prevent cross-tenant privilege escalation and information disclosure through hypervisors and instance isolation.
3. Understanding the institution's roles and responsibilities under the CSP agreement.	Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS Cloud Infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer. See the **Security and the Shared Responsibility Model** section of this document for more details.
4. Maintaining effective risk management procedures for cloud operations.	The HKMA Supervisory Policy Manual module 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 make sure the adequacy of IT controls and quality of their computer systems.

Supervisory expectations	Considerations
	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. Customers can get a copy of the TM-G-1 Workbook by accessing AWS Artifact within the AWS Management Console. **Cloud portability** Understanding the cloud shared responsibility model is important when it comes to understanding cloud portability. Some key concepts of the shared responsibility model include: • Customers own their data. • Customers have the ability to store content in the format they choose. • Customers choose the geographic locations in which to store their data, and it doesn't move unless the customer decides to move it. • Customers can download or delete their data whenever they like. AWS services are built to support data migration into and out of AWS. Additionally, AWS provides tools and documented techniques to make it easy to do both. AWS Cloud infrastructure is built on open standards. This means that customers have the freedom to move their own data wherever they want. The same tools AWS offers to migrate into the AWS cloud can be used to help customers migrate out of it.
5. Adopting effective measures to protect information deployed to cloud.	AWS customers retain control and ownership of their data and are responsible for managing critical content security requirements. This allows customers to control the entire lifecycle of their content on AWS and manage their content in accordance with their own specific needs, including content classification, access control, retention, and deletion.

Supervisory expectations	Considerations
	AWS gives customers ownership and control over their content by design through tools that allow them to determine where their content will be stored, how it will be secured in transit or at rest, and how access to their AWS environment will be managed. AWS has implemented global privacy and data protection best practices in order to help customers establish, operate, and use our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the 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. Customers can use AWS Artifact, the automated compliance reporting portal available in the AWS Management Console, to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals. There are three AWS SOC Reports available to AWS customers from AWS Artifact: • AWS SOC 1 Report • AWS SOC 2 Security, Availability, Confidentiality, & Privacy Report • AWS SOC 3 Security, Availability, Confidentiality, & Privacy Report, publicly available as a whitepaper.
6. Putting in place robust contingency plans.	Customers are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS.

Supervisory expectations	Considerations
	AWS provides customers with the capability to implement a robust continuity plan, including the use of frequent server instance back-ups, 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. In the case of failure, automated processes move customer data traffic away from the affected area. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are typically physically separated within a metropolitan region and are in different flood plains. Customers use AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS Cloud supports many popular disaster recovery (DR) architectures, from *pilot light* environments that are ready to scale up at a moment's notice to *hot standby* environments that enable rapid failover. The AWS infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, Availability Zones are each fed through different grids from independent utilities to further reduce single points of failure. Availability Zones are redundantly connected to multiple tier-1 transit providers. Additionally, the AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan is designed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach helps AWS perform system recovery and reconstitution efforts in a methodical sequence, aiming to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.

Supervisory expectations	Considerations
	AWS tests the Business Continuity plan and its associated procedures at least annually to ensure effectiveness of the plan and the organization readiness to execute the plan.
7. Taking steps to guarantee audit rights and supervisory access.	As explained in the **Security and the Shared Responsibility Model** section, it's important to note that when using AWS services, customers maintain control over their data and are responsible for managing critical content security requirements. This allows customers to control the entire lifecycle of their content on AWS and manage their content in accordance with their own regulatory needs, including to address requests for access, modification, and deletion of personal data by data subjects. The AWS Security and Audit Series offers AIs options to engage directly with AWS on audit, compliance, and security matters. These options address our customers' security and compliance concerns on an ongoing basis, while providing necessary assurances to support the secure adoption, migration, and use of AWS services. **Compliance Briefings** Compliance Briefings offer customers regular opportunities to engage directly with AWS on audit, compliance, and security matters. Compliance Briefings allow customers to address their security or compliance questions or concerns to AWS Security and Compliance Specialists, who are appropriately qualified and knowledgeable AWS personnel. The content of Compliance Briefings is tailored directly to customers' needs. Discussion topics might include, but are not limited to: • The application of the AWS Shared Responsibility Model • Deep dives into AWS audit reports and certifications • Matters pertaining to the AWS control environment • Best practices for secure architecture

Supervisory expectations	Considerations
8. Keeping clear and enforceable CSP agreements.	AWS customers might have the option to enroll in an Enterprise Agreement with AWS, which gives customers the option to tailor the agreements to help enable them to meet regulatory requirements. Customers can reach out to their AWS account team for details.
9. Ensuring responsible staff have the necessary capabilities to oversee cloud operations.	Customers are responsible for defining their own internal training and development programs. Customers can use AWS training services and resources to provide their staff with the appropriate training and resources to manage the AWS services. A range of security, identity, and compliance whitepapers are available for download from AWS, and AWS Training and Certification Programs offer a range of free digital courses, classroom-based training and AWS certifications to develop and maintain an information security capability to help meet HKMA expectations. Customers can use AWS Managed Services (AMS) and AWS Security Competency Partners customers to augment internal capabilities or to fill gaps where recruiting in-house resources is cost-prohibitive or while in-house capability is being developed. AWS Managed Services can automate common activities, such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support customer infrastructure. AWS Security Competency Partners support customers in multiple areas including infrastructure security, policy management, identity management, security monitoring, vulnerability management, data protection, and consulting services.

Next steps

Each organization's cloud adoption journey is unique. In order to successfully complete 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 learn more about such workshops, 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 regulated by the HKMA, 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 don't have an AWS representative, contact us at https://aws.amazon.com/contact-us/.

- Obtain and review a copy of the latest AWS SOC 1 and 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from the AWS Artifact portal (accessible through the AWS Management Console).

- Consider the relevance and application of the CIS AWS Foundations Benchmark available at Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0, 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 based on your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the **Additional Resources** section that follows.

- Speak with your AWS representative to learn more about how AWS is helping financial services customers migrate their critical workloads to the AWS Cloud.

Additional resources

The following are additional resources to help AIs think about security, compliance, and designing a secure and resilient AWS environment.

- AWS Compliance Quick Reference Guide – AWS has many compliance-enabling features that customers can use for their regulated workloads in the AWS Cloud. These features allow them to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, simpler operations, and improved agility by providing more oversight, security control, and central automation.

- AWS Well-Architected Framework – The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures and provides guidance to help implement designs that will scale application needs over time. The Well-Architected framework consists of five pillars: Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

  AWS has produced whitepapers addressing each pillar of the Well-Architected Framework – AWS Operational Excellent Pillar Whitepaper; AWS Security Pillar Whitepaper; AWS Reliability Pillar Whitepaper; AWS Performance Efficiency Whitepaper; AWS Cost Optimization Whitepaper, AWS Operational Resilience Whitepaper (March 2019), Data Classification and Secure Cloud Adoption Whitepaper (June 2018), AWS Policy Perspectives: Data Residency (July 2018).

- Global Financial Services Regulatory Principles – AWS has identified five common principles related to financial services regulation that customers should consider when using AWS cloud services and specifically, applying the shares responsibility model to their regulatory requirements. Customers can access a whitepaper on these principles under a non-disclosure agreement at AWS Artifact.

- NIST Cybersecurity Framework (CSF) – The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (that is, security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS cloud offering's conformance to NIST CSF risk management practices (that is, security of the cloud). AIs can use NIST CSF and AWS resources to elevate their risk management frameworks.

- Using AWS in the Context of Common Privacy and Data Protection Considerations – This document provides information to assist customers who want to use AWS to store or process content containing personal data in the context of common privacy and data protection considerations. It will help customers understand the way AWS services operate, including how customers can address security and encrypt their content, the geographic locations where customers can choose to store content, and other relevant considerations such as the respective roles the customer and AWS each play in managing and securing content stored on AWS services. For details related to Hong Kong data privacy, refer to the AWS Hong Kong Data Privacy page.

For additional help visit the Security, Identity, and Compliance Whitepapers.

Document revisions

Date	Description
February 1, 2024	First publication