AWS User Guide to Financial Services Regulations & Guidelines in Hong Kong

Hong Kong Monetary Authority

November 2017

Notices

This document is provided for informational purposes only. It represents AWS' current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This document provides information to assist regulated Authorized Institutions (AIs) licensed by the Hong Kong Monetary Authority (HKMA) as they accelerate their use of Amazon Web Services (AWS) cloud services. 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, including delivering services over the internet.

Introduction

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 Key Information - Guidelines and Circulars section on the HKMA website.[1]

The Shared Responsibility Model

Before you explore the guideline requirements, it is important that you understand the AWS Shared Responsibility Model shown in Figure 1.

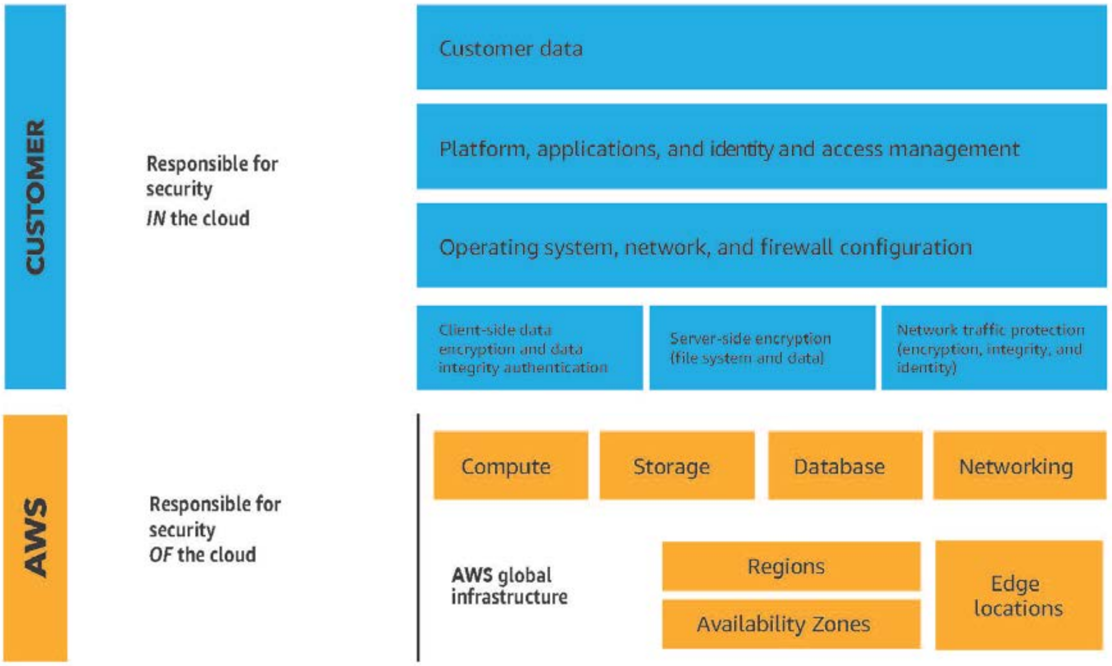
CUSTOMER
Responsible for security *IN* the cloud
Customer data
Platform, applications, and identity and access management
Operating system, network, and firewall configuration
Client-side data encryption and data integrity authentication
Server-side encryption (file system and data)
Network traffic protection (encryption, integrity, and identity)
AWS
Responsible for security *OF* the cloud
Compute
Storage
Database
Networking
AWS global infrastructure
Regions
Availability Zones
Edge locations

Figure 1: AWS Shared Security Responsibility Model

This model is fundamental to understanding the respective roles of the customer (that is, your organization) and AWS in the context of the 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 services operate. Much like a traditional data center, you are responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, in addition to the configuration of the AWS-provided security group firewall. You should carefully consider the services you choose because your responsibilities vary depending on the services you use, the integration of those services into your IT environments, and applicable laws and regulations.

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

- The data that you choose to store on AWS

- The AWS services that you use with the data
- The country where the data is stored
- The format and structure of the data and whether it is masked, anonymized, or encrypted
- How the data is encrypted and where the keys are stored
- Who has access to your data and how those access rights are granted, managed, and revoked

It is possible to enhance security or meet more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection/prevention, and encryption. AWS provides tools and information to assist you in your efforts to account for and validate that controls are operating effectively in your extended IT environment. For more information, see AWS Cloud Compliance.[2]

For more information about the Shared Responsibility Model and its implications for the storage and processing of personal data and other data using AWS, see the AWS whitepaper Using AWS in the context of Common Privacy & Data Protection Considerations.[3]

Security of the Cloud

In order to provide Security *of* the Cloud, AWS environments are continuously audited, and the infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals. You can use these 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 includes policies, processes, and control activities that leverage various aspects of the overall AWS control environment.

  The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of our 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 you can implement, and to better assist you with managing your control environment.

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

Assurance Programs

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads. The following are of particular importance to AIs:

- **ISO 27001** – This security management standard 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 which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information or to download the AWS ISO 27001 certification, see ISO 27001 Compliance.[4]
- **ISO 27017** – This code of practice 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 information security controls implementation guidance specific to cloud service providers. For more information or to download the AWS ISO 27017 certification, see ISO 27017 Compliance.[5]

- **ISO 27018** – This code of practice 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 ISO 27018 Compliance.[6]
- **ISO 9001** – This standard 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 ISO 9001 Compliance.[7]
- **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) 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 PCI DSS Compliance.[8]
- **SOC** – AWS Service Organization Control (SOC) reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. You and your auditors can use these reports to understand the AWS controls established to support operations and compliance. For more

information, see SOC Compliance.[9] There are three types of AWS SOC reports:

- **SOC 1** – Provides information about the AWS control environment that might be relevant to your internal controls over financial reporting, and information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2** – Provides you and your 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 you and your 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 to help you establish and operate in an AWS security control environment.

For more information about other AWS certifications and attestations, see AWS Cloud Compliance.[10]

For a description of general AWS security controls and service-specific security, see the AWS whitepaper Amazon Web Services: Overview of Security Processes.[11]

AWS Artifact

You can review and download reports and details about more than 2,500 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console.[12] The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (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 where AWS has multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. These Availability Zones offer you the ability to operate production applications and databases which are more highly available, fault tolerant, and scalable than would be possible from a single data center.

For current information about AWS Regions and Availability Zones, see AWS Global Infrastructure.[13]

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).

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 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. 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	AWS Response
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/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website.[14]
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.[15] 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,

Due Diligence Requirement	AWS Response
	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.[16] For a list of financial services cloud solutions provided by AWS, see Financial Services Cloud Solutions.[17] The AWS Cloud platform expands daily. For a list of the latest AWS Cloud services and news, see What's New with AWS.[18]

Outsourcing Agreements

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 expects AIs to regularly review their outsourcing agreements.

You have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give you the option to tailor agreements that best suit your 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 achieve this through a number of AWS partners that provide this capability. **Data Integrity:** For access and system monitoring, AWS Config is a service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. Config Rules enables 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 (SNS), so that you are notified of all configuration changes. AWS Config represents relationships between resources, so that you can assess how a change to one resource may impact other resources. **Data Segregation**: Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (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	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. 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 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

Requirement	Customer Considerations
service provider or destroyed	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 the AWS whitepaper AWS Cloud Security.[19] Also, see Section 7.3 of the Customer Agreement available at AWS Customer Agreement.[20] As mentioned in the Outsourcing Agreements section of this paper, Enterprise Agreements give you the option to tailor agreements that best suit your needs.

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.[21] AWS provides you with various tools you can use to monitor your services, including those already noted and from the AWS Marketplace.[22]

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 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.

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.[23]

AWS provides you with the capability to implement a robust continuity plan, including the utilization of 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.[24]

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.[25]

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. AWS also 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 according to your own requirements.

Access to Outsourced Data

The SA-2 clarifies that a 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 Common Privacy and Data Protection Considerations.[26]

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 and how these requirements may be addressed in an Enterprise Agreement with AWS, 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	AWS Response
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
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 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

ID	Guideline	Responsibility	AWS Response
			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 experience is unique. 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 workstreams that enable you to thrive in the cloud.

The AWS Cloud Adoption Framework (AWS CAF) helps organizations understand how cloud adoption transforms the way they work, and it provides structure to identify and address gaps in skills and processes. Applying the AWS CAF in your organization results in an actionable plan with defined work streams that can guide your organization's path to cloud adoption. This framework leverages our experiences and best practices in assisting organizations around the world with their cloud adoption journey.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find out more about 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.[27]

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

- Contact your AWS representative to discuss how the AWS Partner Network, AWS Solution Architects, AWS Professional Services teams, and Training instructors can assist with your cloud adoption processes. If you don't have an AWS representative, Contact Us.[28]
- Obtain and review a copy of the AWS HKMA TM-G-1 Workbook, the latest AWS Service Organization Control 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 at CIS Amazon Web Services Foundations, as appropriate for your cloud adoption and use cases.[29] 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.
- Learn more about other governance and risk management practices as necessary as part of your due diligence and risk assessment, using the

tools and resources referenced throughout this whitepaper and in the following Further Reading section.

- Speak to your AWS representative about an AWS Enterprise Agreement.

Further Reading

For additional help, see the following sources:

- AWS Best Practices for DDoS Resiliency[30]
- AWS Security Checklist[31]
- AWS Cloud Adoption Framework - Security Perspective[32]
- Introduction to AWS Security Processes[33]
- Overview of AWS Security - Storage Services[34]
- Overview of AWS Security - Database Services[35]
- Overview of AWS Security - Compute Services[36]
- Overview of AWS Security - Application Services[37]
- Overview of AWS Security - Analytics, Mobile and Application Services[38]
- Overview of AWS Security - Network Security[39]
- AWS Security Best Practices[40]
- Encrypting Data at Rest[41]
- AWS Risk and Compliance[42]
- Using AWS in the Context of Common Privacy and Data Protection Considerations[43]
- Security at Scale: Logging in AWS[44]
- Security at Scale: Governance in AWS[45]
- Secure Content Delivery with CloudFront[46]

Document Revisions

Date	Description
August 2017	First publication
November 2017	Style and Content updates

Notes

[1] http://www.hkma.gov.hk/eng/key-information/guidelines-and-circulars/

[2] http://aws.amazon.com/compliance

[3] https://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf

[4] https://aws.amazon.com/compliance/iso-27001-faqs/

[5] https://aws.amazon.com/compliance/iso-27017-faqs/

[6] https://aws.amazon.com/compliance/iso-27018-faqs/

[7] https://aws.amazon.com/compliance/iso-9001-faqs/

[8] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

[9] https://aws.amazon.com/compliance/soc-faqs/

[10] https://aws.amazon.com/compliance/

[11] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

[12] https://aws.amazon.com/artifact/

[13] https://aws.amazon.com/about-aws/global-infrastructure/

[14] http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-irhome

[15] https://aws.amazon.com/solutions/

[16] https://aws.amazon.com/financial-services/customer-stories/

[17] https://aws.amazon.com/financial-services/

[18] https://aws.amazon.com/new/

[19] http://aws.amazon.com/security

[20] https://aws.amazon.com/agreement/

[21] https://aws.amazon.com/security/security-bulletins/

[22] https://aws.amazon.com/marketplace

[23] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

[24] https://aws.amazon.com/disaster-recovery/

[25] https://aws.amazon.com/products/storage/

[26] https://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf

[27] https://aws.amazon.com/professional-services/CAF/

[28] https://aws.amazon.com/contact-us/

[29] https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

[30] https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

[31] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Checklist.pdf

[32] https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

[33] https://d0.awsstatic.com/whitepapers/Security/Intro_Security_Practices.pdf

[34] https://d0.awsstatic.com/whitepapers/Security/Security_Storage_Services_Whitepaper.pdf

[35] https://d0.awsstatic.com/whitepapers/Security/Security_Database_Services_Whitepaper.pdf

[36] https://d0.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

[37] https://d0.awsstatic.com/whitepapers/Security/Security_Application_Services_Whitepaper.pdf

[38] https://d0.awsstatic.com/whitepapers/Security/Security_Analytics_Mobile_Services_Applications_Whitepaper.pdf

[39] https://d0.awsstatic.com/whitepapers/Security/Networking_Security_Whitepaper.pdf

[40] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

[41] https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

[42] https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

[43] https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

[44] http://d0.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Logging_in_AWS_Whitepaper.pdf

[45] http://d0.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Governance_in_AWS_Whitepaper.pdf

[46] https://d0.awsstatic.com/whitepapers/Security/Secure_content_delivery_with_CloudFront_whitepaper.pdf