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

Hong Kong Insurance Authority

October 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

Introduction 1

The Shared Responsibility Model 1

Security of the Cloud 3

Assurance Programs 4

AWS Artifact 6

AWS Regions 6

Hong Kong Insurance Authority Guideline on Outsourcing (GL14) 7

- Prior Notification of Material Outsourcing 7
- Outsourcing Policy 8
- Outsourcing Agreements 9
- Information Confidentiality 10
- Monitoring and Control 12
- Contingency Planning 12

Hong Kong Insurance Authority Guideline on the Use of Internet for Insurance Activities (GL8) 14

Next Steps 17

Further Reading 18

Document Revisions 19

Abstract

This document provides information to assist Authorized Insurers (AIs) licensed by the Hong Kong Insurance Authority (IA) 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 insurance services over the internet.

Introduction

The Hong Kong Insurance Authority (IA) issues guidelines to provide the Hong Kong insurance industry with practical guidance to facilitate compliance with regulatory requirements. The guidelines relevant to the use of outsourced services instruct Authorized Insurers (AIs) to perform materiality assessments, 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:

- Guideline on Outsourcing (GL14) – This guideline sets out the IA's supervisory approach to outsourcing and the major points that the IA recommends AIs to address when outsourcing their activities, including the use of cloud services.
- Guideline on the Use of Internet for Insurance Activities (GL8) – This guideline outlines the specific points that AIs (and other groups regulated by the IA) need to be aware of when engaging in internet-based insurance activities.

For a full list of the IA guidelines, see the Legislative and Regulatory Framework - Guidelines section on the IA 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.

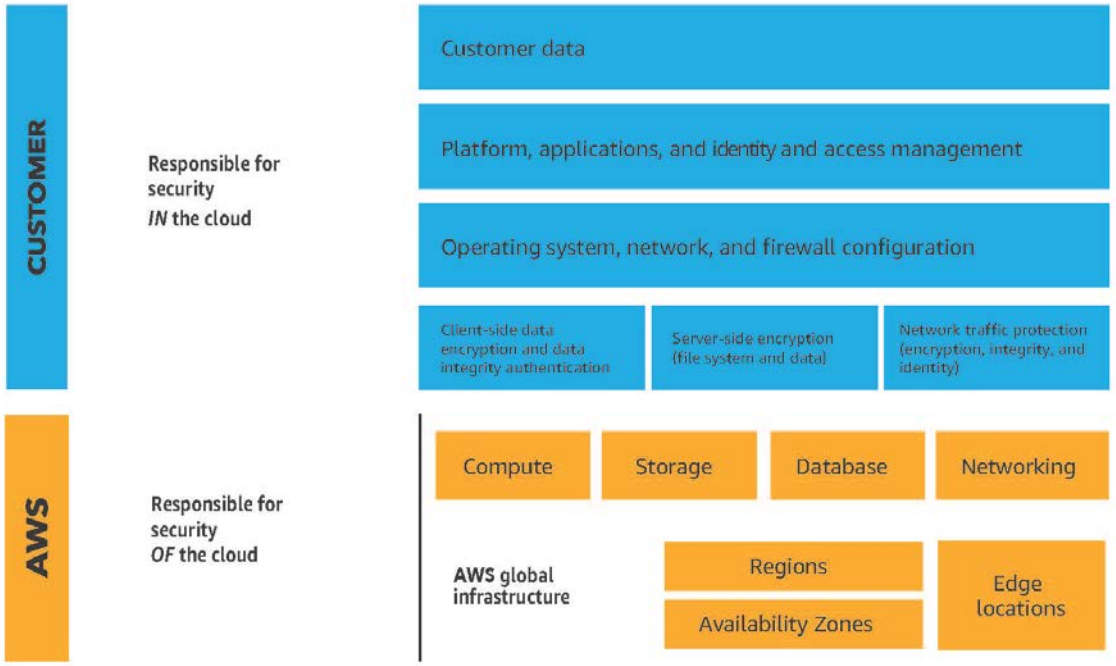

Figure 1: AWS Shared Security Responsibility Model

This shared responsibility 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 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 operates 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 that 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 ISO 9001 is establishing, maintaining, and improving your organizational structure, responsibilities, procedures, processes, and resources in a manner that ensures that AWS products and services consistently satisfy the standard's 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 (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 PCI 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 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 on 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 that 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]

Hong Kong Insurance Authority Guideline on Outsourcing (GL14)

The Hong Kong Insurance Authority Guideline on Outsourcing (GL14) 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 carry out due diligence, evaluate and address risks, and enter into appropriate outsourcing agreements. Section 5 of the GL14 states that the AI's materiality and risk assessments should include considerations such as a determination of the importance and criticality of the services to be outsourced, and the impact on the AI's risk profile (in respect to financial, operational, legal, and reputational risks, and potential losses to customers) if the outsourced service is disrupted or falls short of acceptable standards. AIs should be able to demonstrate their observance of the guidelines as required by the IA.

A full analysis of the GL14 is beyond the scope of this document. However, the following sections address the considerations in the GL14 that most frequently arise in interactions with AIs.

Prior Notification of Material Outsourcing

Under Section 6.1 of the GL14, an AI is required to notify the IA when the AI is planning to enter into a new material outsourcing arrangement or significantly vary an existing one. The notification includes the following requirements:

- Unless otherwise justifiable by the AI, the notification should be made at least 3 months before the day on which the new outsourcing

arrangement is proposed to be entered into or the existing arrangement is proposed to be varied significantly.

- A detailed description of the proposed outsourcing arrangement to be entered into or the significant proposed change.
- Sufficient information to satisfy the IA that the AI has taken into account and properly addressed all of the essential issues set out in Section 5 of the GL14.

Outsourcing Policy

Section 5.8 of the GL14 sets out a list of factors that should be evaluated in the context of service provider 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 5.8.

Due Diligence Requirement	AWS Response
(a) reputation, experience and quality of service	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.
(b) financial soundness, in particular, the ability to continue to provide the expected level of service	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]
(c) managerial skills, technical and operational expertise and competence, in particular, the ability to deal with disruptions in business continuity	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. 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, integrity, and availability of customers' systems and data. Maintaining customer trust and confidence is of the utmost importance to AWS.

Due Diligence Requirement	AWS Response
	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.
(d) any licence, registration, permission or authorization required by law to perform the outsourced service	While Hong Kong does not have specific licensing or certification requirements for operating cloud services, AWS has multiple attestations for secure and compliant operation of its services. Globally, these include certification to ISO 27017 (guidelines for information security controls applicable to the provision and use of cloud services) and ISO 27018 (code of practice for protection of personally identifiable information (PII) in public clouds). For more information about our assurance programs, see AWS Assurance Programs.[16]
(e) extent of reliance on sub-contractors and effectiveness in monitoring the work of sub-contractors	AWS creates and maintains written agreements with third parties (for example, contractors or vendors) in accordance with the work or service to be provided and implements appropriate relationship management mechanisms in line with their relationship to the business.
(f) compatibility with the insurer'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.
(g) familiarity with the insurance 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.[17] For a list of financial services cloud solutions provided by AWS, see Financial Services Cloud Solutions.[18] The AWS Cloud platform expands daily. For a list of the latest AWS Cloud services and news, see What's New with AWS.[19]

Outsourcing Agreements

An outsourcing agreement should be undertaken in the form of a legally binding written agreement. Section 5.10 of the Guideline on Outsourcing (GL14) clarifies the matters that an AI should consider when entering into an outsourcing arrangement with a service provider, including performance

standards, certain reporting or notification requirements, and contingency plans.

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

Information Confidentiality

Under Sections 5.12, 5.13, and 5.14 of the Guideline on Outsourcing (GL14), AIs need to ensure that the outsourcing arrangements comply with relevant laws and statutory requirements on customer confidentiality. The following table includes considerations for Sections 5.12, 5.13, and 5.14.

Requirement	Customer Considerations
5.12 The insurer should ensure that it and the service provider have proper safeguards in place to protect the integrity and confidentiality of the insurer's information and customer data.	**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. **Data Integrity** – For access and system monitoring, AWS Config provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. Config rules enable you to create rules that automatically check the configuration of AWS resources recorded by AWS Config. When your resources are created, updated, or deleted, AWS Config streams these configuration changes to Amazon Simple Notification Service (Amazon SNS), which notifies you of all configuration changes. AWS Config represents relationships between resources, so that you can assess how a change to one resource might impact other resources. **Data Segregation** – Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. **Access Rights** – AWS provides a number of ways for you to identify users and securely access your AWS Account. A complete list of credentials supported by AWS can be found in the AWS Management Console by choosing your user name in the navigation bar and then choosing **My Security Credentials**. AWS also provides additional security options that enable you to further protect your AWS Account and control access using the

Requirement	Customer Considerations
	following: AWS Identity and Access Management (IAM), key management and rotation, temporary security credentials, and multi-factor authentication (MFA).
5.13 An authorized insurer should take into account any legal or contractual obligation to notify customers of the outsourcing arrangement and circumstances under which their data may be disclosed or lost. In the event of the termination of the outsourcing agreement, the insurer should ensure that all customer data are 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. 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 the AWS whitepaper AWS Cloud Security.[20] Also, see the Section 7.3 of the Customer Agreement which is available at AWS Customer Agreement.[21]
5.14 An authorized insurer should notify the IA forthwith of any unauthorized access or breach of confidentiality by the service provider or its sub-contractor that affects the insurer or its customers.	AWS defines, administers, and monitors security for the underlying cloud infrastructure (i.e., the hardware, the facilities housing the hardware and the network infrastructure). Because AWS manages the infrastructure and the security controls that apply to it, AWS can: a) Identify potential incidents affecting the infrastructure; b) Determine if any access to your data resulted from that incident; and c) Determine if that access was actually unlawful or unauthorized i.e. it would be unauthorized if it was in breach of AWS Security Policies. If an incident happens within the AWS sphere of knowledge and control and this incident results in loss, disclosure, or alteration of Customer Content, AWS will promptly notify you. AWS does this regardless of whether the data is sensitive or not, because AWS does not know what the data is and protects all your data in the same way. The AWS ISO 27017 16.1.1 and 16.1.2 requirements validate that AWS maintains breach notification obligations and has processes and procedures in place to notify you in the event of a breach. If you have unique requirements, you should discuss your options with your AWS account manager. In addition to the breach notification that AWS provides, you should implement the following best practices to protect against security breaches:

Requirement	Customer Considerations
	• Use encryption to secure your data. If your data is encrypted the risk associated with a security breach is eliminated because, without the encryption key, the encrypted data is completely obscured. • Configure the AWS services to design a solution that keeps your data secure. • Manage AWS Accounts, IAM users, groups, and roles to implement least privilege permissions for access to your data. • Use monitoring tools like Amazon CloudWatch to track when and by whom your data is accessed. For more information, see the AWS whitepaper AWS Security Best Practices.[22]

Monitoring and Control

Under Section 5.15 of the Guideline on Outsourcing (GL14), AIs should ensure that they have sufficient and appropriate resources to monitor and control outsourcing arrangements at all times. Section 5.16 further sets out that once an AI implements an outsourcing arrangement, it should regularly review the effectiveness and adequacy of its controls in monitoring the performance of the service provider.

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.[23] AWS provides you with various tools you can use to monitor your services, including those already noted and others you can find on the AWS Marketplace.

Contingency Planning

Under Sections 5.17 and 5.18 of the Guideline on Outsourcing (GL14), if an AI chooses to outsource service to a service provider, they should put in place a contingency plan to ensure that the AI's business won't be disrupted as a result of undesired contingencies of the service provider, such as system failures. The AI should also ensure that the service provider has its own contingency plan that covers daily operational and systems problems. The AI should have an adequate understanding of the service provider's contingency plan and consider the implications for its own contingency planning in the event that the

outsourced service is interrupted due to undesired contingencies of the service provider.

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.[24]

AWS provides you with the capability to implement a robust continuity plan, including frequent server instance backups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic Regions as well as across multiple Availability Zones within each Region. For more information about disaster recovery approaches, see Disaster Recovery.[25]

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.[26]

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.

Hong Kong Insurance Authority Guideline on the Use of Internet for Insurance Activities (GL8)

The Hong Kong Insurance Authority Guideline on the Use of Internet for Insurance Activities (GL8) aims to draw attention to the special considerations that AIs (and other groups regulated by the IA) need to be aware of when engaging in internet-based insurance activities.

Sections 5.1, items (a)-(g) of the Guideline on the Use of Internet for Insurance Activities (GL8) sets out a series of requirements regarding information security, confidentiality, integrity, data protection, payment systems security and related concerns for AIs to address when carrying out internet insurance activities. AIs should take all practicable steps to ensure the following:

Requirement	Customer Considerations
(a) a comprehensive set of security policies and measures that keep up with the advancement in internet security technologies shall be in place	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 your systems and data. Maintaining customer trust and confidence is of the utmost importance to AWS. AWS works to comply with applicable federal, state, and local laws, statutes, ordinances, and regulations concerning security, privacy and data protection of AWS services in order to minimize the risk of accidental or unauthorized access or disclosure of customer data.
(b) mechanisms shall be in place to maintain the integrity of data stored in the system hardware, whilst in transit and as displayed on the website	AWS is designed to protect the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been altered or corrupted in transit is immediately rejected. AWS provides many methods for you to securely handle your data: AWS enables you to open a secure, encrypted channel to AWS servers using HTTPS (TLS/SSL). Amazon S3 provides a mechanism that enables you to use MD5 checksums to validate that data sent to AWS is bitwise identical to what is received, and that data sent by Amazon S3 is identical to what is received by the user. When you choose to provide your own keys for encryption and decryption of Amazon S3 objects (S3 SSE-C), Amazon S3 does not store the encryption key that you provide.

Requirement	Customer Considerations
	Amazon S3 generates and stores a one-way salted HMAC of your encryption key and that salted HMAC value is not logged. Connections between your applications and Amazon RDS MySQL DB instances can be encrypted using TLS/SSL. Amazon RDS generates a TLS/SSL certificate for each database instance, which can be used to establish an encrypted connection using the default MySQL client. When an encrypted connection is established, data transferred between the database instance and your application is encrypted during transfer. If you require data to be encrypted while at rest in the database, your application must manage the encryption and decryption of data. Additionally, you can set up controls to have your database instances only accept encrypted connections for specific user accounts. Data is encrypted with 256-bit keys when you enable AWS KMS to encrypt Amazon S3 objects, Amazon EBS volumes, Amazon RDS DB Instances, Amazon Redshift Data Blocks, AWS CloudTrail log files, Amazon SES messages, Amazon Workspaces volumes, Amazon WorkMail messages, and Amazon EMR S3 storage. AWS offers you the ability to add an additional layer of security to data at rest in the cloud, providing scalable and efficient encryption features. This includes: • Data encryption capabilities available in AWS storage and database services, such as Amazon EBS, Amazon S3, Amazon Glacier, Amazon RDS for Oracle Database, Amazon RDS for SQL Server, and Amazon Redshift. • Flexible key management options, including AWS Key Management Service (AWS KMS), that allow you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your keys. • Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, which enables you to satisfy compliance requirements. In addition, AWS provides APIs that you can use to integrate encryption and data protection with any of the services you develop or deploy in the AWS Cloud.
(c) appropriate backup procedures for the database and application software shall be implemented.	AWS maintains a retention policy applicable to AWS internal data and system components in order to continue operations of AWS business and services. Critical AWS system components, including audit evidence and logging records, are replicated across multiple Availability Zones and backups are maintained and monitored. You retain control and ownership of your data. When you store data in a specific Region, it is not replicated outside that Region. It is your responsibility to replicate data across Regions if your business needs require this capability.

Requirement	Customer Considerations
	Amazon S3 supports data replication and versioning instead of automatic backups. You can, however, back up data stored in Amazon S3 to other AWS Regions or to on-premises backup systems. Amazon S3 replicates each object across all Availability Zones within the respective Region. Replication can provide data and service availability in the case of system failure, but provides no protection against accidental deletion or data integrity compromise—it replicates changes across all Availability Zones where it stores copies. Amazon S3 offers standard redundancy and reduced redundancy options, which have different durability objectives and price points. Each Amazon EBS volume is stored as a file, and AWS creates two copies of the EBS volume for redundancy. Both copies reside in the same Availability Zone, however, so while Amazon EBS replication can survive hardware failure, it is not suitable as an availability tool for prolonged outages or disaster recovery purposes. We recommend that you replicate data at the application level or create backups. Amazon EBS provides snapshots that capture the data stored on an Amazon EBS volume at a specific point in time. If the volume is corrupt (for example, due to system failure), or data from it is deleted, you can restore the volume from snapshots. Amazon EBS snapshots are AWS objects to which IAM users, groups, and roles can be assigned permissions, so that only authorized users can access Amazon EBS backups.
(d) a client's personal information (including password, if any) shall be protected against loss; or unauthorized access, use, modification or disclosure, etc.	You control your data. With AWS, you can do the following: • Determine where your data is stored, including the type of storage and geographic Region of that storage. • Choose the secured state of your data. We offer you strong encryption for your content in transit or at rest, and we provide you with the option to manage your own encryption keys. • Manage access to your data and AWS services and resources through users, groups, permissions, and credentials that you control.
(e) a client's electronic signature, if any, shall be verified	Amazon Partner Network (APN) Technology Partners provide software solutions (including electronic signature solutions) that are either hosted on, or integrated with, the AWS Cloud platform. The AWS Partner Solutions Finder provides you with a centralized place to search, discover, and connect with trusted APN Technology and Consulting Partners, based on your business needs. For more information, see AWS Partner Solutions Finder.[27]
(f) the electronic payment system (e.g. credit card payment system) shall be secure.	AWS is a Payment Card Industry (PCI) compliant cloud service provider, having been PCI DSS Certified since 2010. The most recent assessment validated that AWS successfully completed the PCI Data Security Standards 3.2 Level 1 Service Provider assessment and was

Requirement	Customer Considerations
	found to be compliant for all the services outlined on AWS Services in Scope by Compliance Program.[28] The AWS PCI Compliance Package, which is available through AWS Artifact, includes the AWS PCI DSS 3.2 Attestation of Compliance (AOC) and AWS 2016 PCI DSS 3.2 Responsibility Summary. PCI compliance on AWS is a shared responsibility. In accordance with the shared responsibility model, all entities must manage their own PCI DSS compliance certification. While for the portion of the PCI cardholder environment deployed in AWS, your organization's QSA can rely on AWS Attestation of Compliance (AOC), you are still required to satisfy all other PCI DSS requirements. The AWS 2016 PCI DSS 3.2 Responsibility Summary provides you with guidance on what you are responsible for. For more information about AWS PCI DSS Compliance, see PCI DSS Level 1 Service Provider.[29]
(g) a valid insurance contract shall not be cancelled accidentally, maliciously or consequent upon careless computer handling.	Your data is validated for integrity, and corrupted or tampered data is not written to storage. Amazon S3 utilizes checksums internally to confirm the continued integrity of content in transit within the system and at rest. Amazon S3 provides a facility for you to send checksums along with data transmitted to the service. The service validates the checksum upon receipt of the data to determine that no corruption occurred in transit. Regardless of whether a checksum is sent with an object to Amazon S3, the service utilizes checksums internally to confirm the continued integrity of content in transit within the system and at rest. When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy. External access to content stored in Amazon S3 is logged, and the logs are retained for at least 90 days, including relevant access request information, such as the accessor IP address, object, and operation.

Next Steps

Each organization's cloud adoption experience is unique. To successfully execute your adoption, you need to understand your 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 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 can result 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.[30]

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.[31]
- Obtain and review a copy of 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.[32] 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[33]

- AWS Security Checklist[34]
- AWS Cloud Adoption Framework - Security Perspective[35]
- Introduction to AWS Security Processes[36]
- Overview of AWS Security - Storage Services[37]
- Overview of AWS Security - Database Services[38]
- Overview of AWS Security - Compute Services[39]
- Overview of AWS Security - Application Services[40]
- Overview of AWS Security - Analytics, Mobile and Application Services[41]
- Overview of AWS Security - Network Security[42]
- AWS Security Best Practices[43]
- Encrypting Data at Rest[44]
- AWS Risk and Compliance[45]
- Using AWS in the Context of Common Privacy and Data Protection Considerations[46]
- Security at Scale: Logging in AWS[47]
- Security at Scale: Governance in AWS[48]
- Secure Content Delivery with CloudFront[49]

Document Revisions

Date	Description
October 2017	First publication

Notes

[1] https://www.ia.org.hk/en/legislative_framework/guidelines.html

[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/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/

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

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

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

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

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

[22] https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf

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

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

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

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

[27] https://aws.amazon.com/partners/find/

[28] https://aws.amazon.com/compliance/services-in-scope/

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

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

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

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

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

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

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

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

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

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

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

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

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

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

43 https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

44 https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

45 https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

46 https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

47 http://d0.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Logging_in_AWS_Whitepaper.pdf

48 http://d0.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Governance_in_AWS_Whitepaper.pdf

49 https://d0.awsstatic.com/whitepapers/Security/Secure_content_delivery_with_CloudFront_whitepaper.pdf