Navigating Hong Kong SFC Compliance on AWS

May 17, 2021

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 Financial Institutions (FIs) in Hong Kong regulated by the Hong Kong Securities and Futures Commission (SFC) as they accelerate their use of Amazon Web Services (AWS) services.

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 financial institutions can consider when using AWS.
- Provides additional resources design and architect their AWS environment to be secure and meet regulatory expectations, including under SFC regulations.

Introduction

AWS provides financial services such as banking, payments, capital markets, and insurance institutions 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 stringent security requirements, 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.

The Hong Kong Securities and Futures Commission (SFC) is an independent statutory body set up in 1989 to regulate Hong Kong's securities and futures markets. The SFC is responsible for the regulation, inspection, and supervision of Licensed Corporations (LCs), including brokers, investment advisers, fund managers, and intermediaries. Financial services institutions regulated by the SFC, typically consider the following SFC Regulations to be relevant to their use of AWS services:

- IOSCO Principles on Outsourcing of Financial Services for Market Intermediaries (IOSCO Outsourcing Principles)
- Circular to Licensed Corporations (dated Oct 31, 2019) - Use of external electronic data storage

The SFC Regulations define, among other things, the minimum technical and operational requirements that LCs should put in place for the management, implementation, and control of risks related to information technology, information systems, and other resources when outsourcing IT services to a third-party service provider, including the use of cloud services.

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

For a full list of the SFC requirements, see the Rules and standards section on the SFC website.

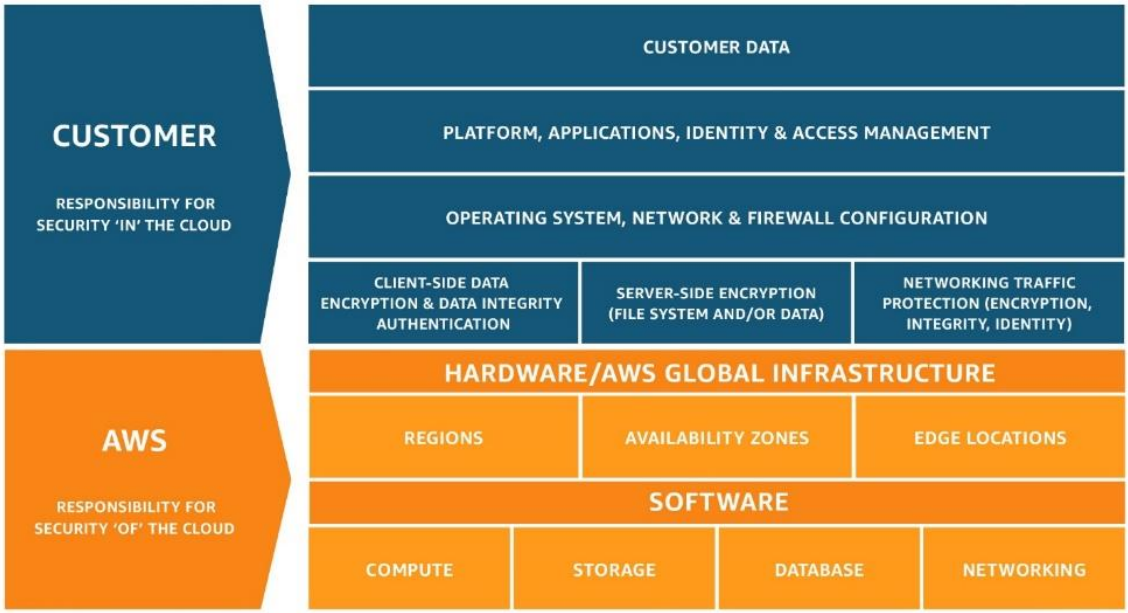
Security and the Shared Responsibility Model

It is important that LCs understand the AWS Shared Responsibility Model before exploring the specific requirements under the SFC regulations.

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.

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 Shared Responsibility Model is fundamental to understanding the respective roles of the customer 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 AWS services operate.



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 them the resources they need to perform specific tasks without having to launch and maintain virtual machines. For example, a customer can launch an Amazon Aurora database, which Amazon Relational Database Service (Amazon RDS) manages to handle tasks such as provisioning, patching, backup, recovery, failure detection, and repair.

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

- The content that they choose to store on AWS.
- The AWS services that are used with the content.
- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their content is encrypted and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility will be 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 EC2 is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks.

Customers that deploy an Amazon 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, the operating system,

and platforms, 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 IAM tools to apply the appropriate permissions.

Security OF the Cloud

AWS's infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS's compliance certifications to validate the implementation and effectiveness of AWS's security controls, including internationally-recognized security best practices and certifications. Customers can learn more by downloading the AWS & Cybersecurity in the Financial Services Sector whitepaper.

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 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, that AWS maintains compliance 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 leverage 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 Licensed Corporations (LCs):

- **ISO 27001** – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System that defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.
- **ISO 27017** – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.
- **ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

- **ISO 9001** - ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to 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 (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.
- **SOC** – AWS System & Organization Controls (SOC) Reports are independent third-party 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 may be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
    - **SOC 2**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
    - **SOC 3**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information.

- By tying together governance-focused, audit-friendly service features with such certifications, attestations, and audit standards, AWS Compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.
- For more information about other AWS certifications and attestations, see the AWS Compliance Programs webpage. For information about general AWS security controls and service-specific security, see Best Practices for Security, Identity, & 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's 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 may apply to that country.

AWS Global Infrastructure

The AWS Global Cloud infrastructure comprises 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.

These Availability Zones offer customers the ability to operate applications and databases which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. Customers can learn more about these topics by downloading our Whitepaper on Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

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

IOSCO Principles on Outsourcing of Financial Services for Market Intermediaries (IOSCO Outsourcing Principles)

The SFC encourages its regulated institutions to refer to the IOSCO Outsourcing Principles on Outsourcing of Financial Services for Market Intermediaries as a framework to manage their outsourcing activities. LCs that use the cloud are expected to carry out due diligence, evaluate and address risks, and enter into appropriate outsourcing agreements as per the IOSCO Outsourcing Principles. Section 2 of the IOSCO Outsourcing Principles states the Principles that should be applied according to the materiality of the outsourced activity.

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

Due diligence and monitoring

Section 3 Topic 1 of the IOSCO Outsourcing Principles states that an outsourcing firm should conduct suitable due diligence processes in selecting an appropriate third-party service provider and in monitoring its ongoing performance.

Table 1- Considerations for each due diligence component of Section 3 Topic 1 of the IOSCO Outsourcing Principles.

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

Due Diligence Components	Customer Considerations
Monitor the third-party service provider's performance and compliance with its contractual obligations	AWS offers service level agreements for certain AWS services. These may be updated from time to time. See https://aws.amazon.com/legal/service-level-agreements/. The AWS Service Health Dashboard provides up-to-the-minute information on the general availability of the services. The AWS Personal Health Dashboard gives customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and provides proactive notification to help customers plan for scheduled activities. AWS customers have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. For more information about AWS Enterprise Agreements, contact your AWS representative.
Compliance with applicable laws and regulatory requirements in its jurisdiction	AWS has worked with some of the most complex financial services organizations at every stage of their respective cloud journeys and understands the importance of maintaining positive relationships with customers' financial services regulators. AWS Artifact provides an accessible means for customers to access and download AWS audit artifacts in order to share these with regulators as evidence of AWS's security and compliance controls.
Outsourcing on a cross-border basis	AWS customers choose the AWS Region(s) in which their content and servers are located. This allows customers to establish environments that meet specific geographic requirements. AWS Regions are designed and built to meet rigorous compliance standards globally, providing high levels of security for all AWS customers. All AWS Regions are compliant with applicable laws and regulations.

Outsourcing Contract

Section 3 Topic 2 of the IOSCO Outsourcing Principles states that there should be a legally binding written contract between the outsourcing firm and each third-party service provider, the nature and detail of which should be appropriate to the materiality of the outsourced activity to the ongoing business of the outsourcing firm.

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 Account Manager.

Information Security

Section 3 Topic 3a of the IOSCO Outsourcing Principles states that the outsourcing firm should take appropriate measures to determine that procedures are in place to protect the outsourcing firm's proprietary and customer-related information and software.

Customers retain ownership and control of their content when using AWS services, and do not turn over that ownership and control of their content to AWS. Customers have complete control over which services they use and whom they empower to access their content and services, including what credentials will be required.

Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them.

AWS does not change customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have 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.

Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS SOC 1, SOC 2 and SOC 3 reports, ISO 27001, ISO 27017 and ISO 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.

Business Continuity

Section 3 Topic 3b of the IOSCO Outsourcing Principles states that the outsourcing firm should take appropriate measures to determine that service providers establish and

maintain emergency procedures and a plan for disaster recovery, with periodic testing of backup facilities.

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.

Operational resilience is the ability to provide continuous service through people, processes, and technology that are aware of and adaptive to constant change. It is a real-time, execution-oriented norm embedded in the culture of AWS that is distinct from traditional approaches in Business Continuity, Disaster Recovery, and Crisis Management, which rely primarily on centralized, hierarchical programs focused on documentation development and maintenance. AWS and you share a common interest in maintaining operational resilience, i.e., the ability to provide continuous service despite disruption. Continuity of service, especially for critical economic functions, is a key prerequisite for financial stability. For more information about AWS operational resilience approaches, see the AWS whitepaper Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

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.

Information Confidentiality

Section 3 Topic 4 of the IOSCO Outsourcing Principles states that the outsourcing firm should take appropriate steps to require that service providers protect confidential information regarding the outsourcing firm's proprietary and other information, as well as the outsourcing firm's clients from intentional or inadvertent disclosure to unauthorized individuals.

Customers retain ownership and control of their content when using AWS services, and do not turn over that ownership and control of their content to AWS.

AWS treats all customer data and associated assets as Highly Confidential. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. AWS is vigilant about customers' security and has implemented sophisticated technical and physical measures against unauthorized access. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used, and protected from disclosure.

For more information, see Using AWS in the Context of Common Privacy and Data Protection Considerations.

Concentration of Outsourcing Functions

Section 3 Topic 5 of the IOSCO Outsourcing Principles states that where a regulator has identified a possible concentration risk issue, outsourcing firms should consider taking steps to ensure, to the degree practicable, that the service provider has adequate capacity to meet the needs of all outsourcing firms, both during normal operations as well as unusual circumstances.

AWS builds to guard against outages and incidents, and accounts for them in the design of AWS's services to maintain the continuity of our services. AWS's global infrastructure is geographically dispersed over five continents. It is composed of geographic Regions, which are composed of Availability Zones, which, in turn, are composed of data centers. The Availability Zones, which are physically separated and independent from each other, are built with highly redundant networking to withstand local disruptions. Regions are autonomous and isolated from each other.

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable customers to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design.

Customers are responsible for deciding where to place their content, where to run their applications, and how to achieve higher levels of availability and resiliency. For example, a customer may choose to run an application that it has designed on AWS across multiple Availability Zones. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. In addition, customers can maintain additional "cold" infrastructure and backups on AWS that can activate if necessary.

For more information about AWS's approach to operational resilience, the AWS Operational Resilience whitepaper.

Termination Procedures

Section 3 Topic 6 of the IOSCO Outsourcing Principles states that outsourcing with third party service providers should include contractual provisions relating to termination of the contract and appropriate exit strategies.

If customers decide to leave AWS, they can manage access to their content and to AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Import/Export and AWS Snowball to transfer large amounts of data into and out of AWS using physical storage appliances. For more information, see Cloud Storage on AWS.

Additionally, AWS offers AWS Database Migration Service, a web service that you can use to migrate a database from an AWS service to an on-premises database. 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

Section 3 Topic 7 of the IOSCO Outsourcing Principles states that regulators, the outsourcing firm, and its auditors should have access to the books and records of service providers relating to the outsourced activities and the regulator should be able to obtain promptly, upon request, information concerning activities that are relevant to regulatory oversight.

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.

AWS gives customers ownership and control over their content by design through tools that allow customers 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 leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

AWS 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. AWS customers can use AWS Artifact to review and download reports and details of many AWS security controls and to share these with regulators as evidence of AWS's security and compliance controls.

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

SFC Circular to Licensed Corporations - Use of External Electronic Data Storage

The SFC Circular to Licensed Corporations - Use of External Electronic Data Storage Circular (the SFC Circular) sets out the requirements when LCs keep electronic regulatory records exclusively with external data storage providers (EDSPs, including cloud service providers) or with LC's affiliates.

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

The following sections list the technical and operational requirements identified under sections C and E of the SFC Circular along with AWS considerations to assist LCs understand each requirement when using AWS.

The tables in the next sections are organized into the following columns:

- **Requirement**: This column lists the technical and operational requirements that may be applicable to each of the scenarios outlined in the SFC Circular.
- **Considerations**: This column explains the AWS considerations for addressing the requirements defined in the SFC Circular. It may refer to the security and compliance of the cloud, and how AWS implements and manages the controls and/or AWS services LCs can use to address these requirements.

Section C - Requirements for keeping Regulatory Records exclusively with an EDSP

Section C of the SFC Circular sets out SFC's expectations if LCs wish to keep regulatory records exclusively with an EDSP.

Table 2- Section C of the SFC Circular

Requirement	Considerations
C.7(a) The EDSP (i) is either a company incorporated in Hong Kong or a non-Hong Kong company registered under the Companies Ordinance (Cap 622), in each case staffed by personnel operating in Hong Kong, and (ii) provides data storage to the licensed corporation at a data center located in Hong Kong (Hong Kong EDSP). In addition, the licensed corporation's Regulatory Records which are kept exclusively with the EDSP will be kept at such data center at all times throughout the period in which the Regulatory Records are required to be kept by law or regulation.	The Amazon entity is not a company incorporated in Hong Kong nor a foreign company registered in Hong Kong.
C.7(b) As an alternative, if the EDSP is not a Hong Kong EDSP as defined in paragraph 7(a), the licensed corporation must obtain an undertaking by the EDSP, substantially in the form of the template in Appendix 1 (Undertaking) of this circular, to provide Regulatory Records and assistance as may be requested by the SFC.	Refer to C.7(a) AWS recommends the LCs to also refer to the FAQs issued by the SFC under "Use of External Electronic Data Storage". As an alternative to the Undertaking from the EDSP, the SFC will accept an undertaking from each of the two Manager-In-Charges (MICs) appointed for the purposes of the SFC Circular or, with the consent of the SFC, one MIC or one Responsible Officer (MIC/RO Undertaking).

Requirement	Considerations
C.7(c) A licensed corporation should only keep Regulatory Records with an EDSP which is suitable and reliable, having regard to the EDSP's operational capabilities, technical expertise and financial soundness.	AWS is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers - including the fastest growing startups, largest enterprises, and leading government agencies - trust AWS to power their infrastructure, become more agile, and lower costs. AWS has significantly more services, and more features within those services, than any other cloud provider. The AWS cloud platform offers over 200 fully featured services, including over 40 services that aren't available anywhere else. The financial statements of Amazon.com Inc. include AWS's sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website. 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.
C.7(d) The licensed corporation should ensure that all of its Regulatory Records which are kept exclusively with an EDSP are fully accessible upon demand by the SFC without undue delay, and can be reproduced in a legible form from premises of the licensed corporation in Hong Kong approved for this purpose by the SFC under section 130 of the SFO.	Customers have full root access or administrative control over accounts, services, and applications and have complete visibility of their cloud resources, services and applications to monitor use and log, collect metrics, set alarms, and automatically react to changes. AWS customers can also provide internal users and regulators logical access to their information and data, if necessary.

Requirement	Considerations
C.7(e) The licensed corporation should ensure that (i) it can provide detailed audit trail information in a legible form regarding any access to the Regulatory Records (including read, write and modify) stored by the licensed corporation at the EDSP, and (ii) the audit trail is a complete record of any access by the licensed corporation to Regulatory Records stored by the EDSP. The audit trail information should be kept for the period for which the licensed corporation is required to keep the Regulatory Records. The access of the licensed corporation to the audit trail information should be restricted to read-only. The licensed corporation should ensure that each user who has accessed Regulatory Records can be uniquely identified from the audit trail.	AWS offers FI customers tools for audit trails. AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config and AWS Config Rules to track, monitor, analyze, and audit events. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. With AWS CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across AWS infrastructure. AWS CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. Amazon CloudWatch is a resource monitoring and management that gives a complete visibility of cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes. AWS Config is a resource configuration management service that records and evaluates configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis.

Requirement	Considerations
C.7(f) The licensed corporation should ensure that, irrespective of which EDSP is being used, and of where the EDSP maintains its hardware for the storage of information, Regulatory Records are kept in a manner that does not impair or result in undue delays to the SFC's effective access to the Regulatory Records when it discharges its functions or exercises its powers, taking into account all pertinent political and legal issues in any relevant jurisdiction.	Customers have full root access or administrative control over accounts, services, and applications and have complete visibility of their cloud resources, services and applications to monitor use and log, collect metrics, set alarms, and automatically react to changes. AWS customers can also provide internal users and regulators logical access to their information and data, if necessary.

Requirement	Considerations
C.7(g) The licensed corporation should designate at least two individuals, being Managers-In-Charge of Core Functions (MICs) in Hong Kong, who have the knowledge, expertise and authority to access all of the Regulatory Records kept with an EDSP at any time, and who can ensure that the SFC has effective access to such records upon demand without undue delay in the exercise of its statutory powers. The MICs, or their delegates, must have in their possession all digital certificates, keys, passwords and tokens to ensure full access to all Regulatory Records kept with the EDSP. The MICs will be responsible for ensuring information security to prevent unauthorised access, tampering or destruction of Regulatory Records. The MICs, or their delegates, must provide all necessary assistance to the SFC to secure and promptly gain access to all of the Regulatory Records of the firm kept at the EDSP, and put in place all necessary policies, procedures and internal controls to ensure that the SFC has full access to all Regulatory Records upon demand without undue delay. The licensed corporation and the designated MICs should ensure that the above responsibilities of the designated MICs can and will be discharged at all times.	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. AWS gives customers ownership and control over their content by design through tools that allow customers 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 leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

Requirement	Considerations
C.7(h) The licensed corporation should seek approval for the premises used for keeping Regulatory Records under section 130 of the SFO.	The location information of our data centers can be found here: https://aws.amazon.com/about-aws/global-infrastructure/

Section E - General obligations of LCs using external data storage or processing services

Section E of the SFC Circular sets out the control measures that LCs should implement when using external data storage or processing services.

Table 3- Section E of the SFC Circular

Requirement	Customer Considerations
E.11 Licensed corporations are reminded of their obligations under the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (a) to have effective policies and procedures for the proper management of risks to which the firm and its clients are exposed with respect to client data and information relevant to the firm's business operations (Relevant Information), and (b) to implement information management controls to detect and prevent unauthorized access, insertion, alteration or deletion of Relevant Information. To properly manage cyber and other operational risks, a licensed corporation using external data storage or processing services should implement the following control measures in this section	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. AWS gives customers ownership and control over their content by design through tools that allow customers 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 leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

Requirement	Customer Considerations
E, regardless of whether Regulatory Records are kept exclusively with an EDSP.	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 five AWS SOC Reports all available to AWS customers from AWS Artifact: • AWS SOC 1 Report • AWS SOC 2 Security, Availability & Confidentiality Report • AWS SOC 2 Security, Availability & Confidentiality Report (scope includes Amazon DocumentDB only). • AWS SOC 2 Privacy Type I Report • AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper.
E.12 The licensed corporation should conduct proper initial due diligence on the EDSP and its controls relating to its	AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information

Requirement	Customer Considerations
infrastructure, personnel and processes for delivering its data storage services, as well as regular monitoring of the EDSP's service delivery, in each case commensurate with the criticality, materiality, scale and scope of the EDSP's service. Such due diligence should cover:	Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. 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. Please refer to the following AWS Audit Reports for additional details: SOC 2, PCI DSS, ISO 27001 and ISO 27017. Amazon.com Inc. has a Code of Business Conduct and Ethics, available at Amazon's Investor Relations website, which covers issues including, among other things, compliance with laws, conflicts of interest, bribery, discrimination and harassment, health and safety, recordkeeping and financial integrity.
(a) the EDSP's internal governance for the safeguard of the licensed corporation's Regulatory Records (where Regulatory Records are kept with the EDSP), and may include assessing the physical security of the storage facilities, the type of hosting (ie, whether it is dedicated or shared hardware), security over the network infrastructure, IT systems and applications, identity and access management, cyber risk management, information security, data loss and breach notifications, forensics capabilities, disaster recovery and business continuity processes; and	
(b) any subcontracting arrangement by the EDSP for the storage of the licensed corporation's Regulatory Records, especially with regard to cyber risk management and information security.	
E.13 The licensed corporation should maintain an effective governance process for (a) the acquisition, deployment and use of software applications or services which read, write or modify Relevant Information, and (b) ensuring the security, authenticity,	Customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Customers have complete control over which services they use and whom they empower to access their

Requirement	Customer Considerations
reliability, integrity, confidentiality and timely availability of its Relevant Information as appropriate.	content and services, including what credentials will be required. Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have 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 provides ways to categorize organizational data based on levels of sensitivity. By using resource tags, AWS IAM policies, AWS KMS, and AWS CloudHSM, customers can define and implement policies for data classification.
E.14 The licensed corporation should implement a comprehensive information security policy to prevent any unauthorized disclosure. This policy should include an appropriate data classification framework, descriptions of the various data classification levels, a list of roles and responsibilities for identifying the sensitivity of the data and the corresponding control measures. The licensed corporation should also take appropriate steps to ensure that the EDSP protects Relevant Information which is confidential from being intentionally or inadvertently disclosed to, or misused by,	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. AWS gives customers ownership and control over their content by design through tools that allow customers 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,

Requirement	Customer Considerations
unauthorized third parties. To protect its confidential Relevant Information, the licensed corporation should encrypt it while at rest and in transit, or establish effective procedures and mechanisms to safeguard its confidentiality and security. When it is encrypted, the licensed corporation must implement proper key management controls, maintain possession of the encryption and decryption keys and ensure that the keys are accessible to the SFC on demand without undue delay where any electronic record is required to be produced in the exercise of its statutory powers.	and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure. AWS considers the identification and classification of a LC's information assets as an action for the LC to independently complete. The following AWS services and resources may assist customers:
E.15 The licensed corporation should implement appropriate policies, procedures and controls to manage user access rights to ensure that Relevant Information can only be altered for proper purposes by authorized personnel, and is otherwise free from damage or tampering. The sharing of system authentication codes (such as passwords) among users should generally be prohibited, with a view to ensuring that each user who has accessed Regulatory Records can be uniquely identified.	AWS Config provides a detailed inventory of customers' AWS resources and configuration, and continuously records configuration changes. Amazon CloudWatch provides data and actionable insights to monitor applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. AWS Systems Manager gives visibility and control of customer infrastructure on AWS. Systems Manager provides a unified user interface to view operational data from multiple AWS services and allows automation of operational tasks across AWS resources. AWS Systems Manager Inventory provides visibility into Amazon EC2 and on-premises computing environment by collecting metadata from your managed instances. Customers can store metadata in a central Amazon Simple Storage Service (Amazon S3) bucket, and then use built-in tools to query the data and quickly determine which instances are running the software and configurations required by policy, and which instances need to be updated. Customers can configure Inventory

Requirement	Customer Considerations
	on all managed instances by using a one-click procedure, and configure and view inventory data from multiple AWS Regions and accounts.
E.16 Where a licensed corporation is keeping only part of its Relevant Information with the EDSP (whether due to data sensitivity concerns or otherwise), it should put in place controls to prevent the migration of Relevant Information to the EDSP without proper authorization.	When using AWS services, customers maintain control over their content including the content that they choose to store on AWS. Customers should define their operational model based on the AWS services and products they use. As explained in the Security and Shared Responsibility section, cloud security is a shared responsibility. AWS manages security of the cloud, ensuring AWS infrastructure complies with global regulatory requirements as well as best practices. However, security in the cloud is the responsibility of the customer. This means that customers are responsible for the security programs they want to deploy to protect their content, applications, systems, and networks in the same way as they do in a local data center.
E.17 Licensed corporations using EDSP services, especially the public cloud, need to be aware of how the operation of these services and their exposure to cyber threats may differ from a computing environment at the premises of the licensed corporation, in particular with regard to information confidentiality, integrity and recoverability, and the implementation of information and security controls. Public cloud providers and users typically share responsibility for the security and control of the technology, and this may be more complicated than a	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

Requirement	Customer Considerations
traditional outsourcing model. Regardless of how the technology is deployed, the licensed corporation should ensure that the allocation of responsibilities, such as the configuration of security settings, workload protection and credential management, between the licensed corporation and the EDSP is well-defined, clearly understood and properly managed by the licensed corporation. Additionally, the licensed corporation may consider using security automation as well as the security services and tools offered by the EDSP to maintain a consistent level of security. Should such services or tools use encryption, the licensed corporation must maintain possession of the encryption and decryption keys as specified under paragraph 14 above.	SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals. There are five AWS SOC Reports all available to AWS customers from AWS Artifact: • AWS SOC 1 Report • AWS SOC 2 Security, Availability & Confidentiality Report • AWS SOC 2 Security, Availability & Confidentiality Report (scope includes Amazon DocumentDB only). • AWS SOC 2 Privacy Type I Report • AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper. To help customers meet the regulatory requirement for their portion of shared controls, Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API. Amazon Inspector security assessments also check for unintended network accessibility of Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered as pre-defined rules packages mapped to common

Requirement	Customer Considerations
	security best practices and vulnerability definitions. Examples of built-in rules include checking for access to your EC2 instances from the internet, remote root login being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers.
E.18 A licensed corporation using other forms of virtual storage should implement control measures which are appropriate for the increased complexity and security risk as compared to a non-virtual environment.	(Not applicable)
E.19 A licensed corporation using external data storage or processing services in the conduct of its regulated activities should assess the level of its dependence on the prompt and consistent delivery of services by its service providers as well as the potential operational impact on the licensed corporation and its clients if the services are disrupted. The licensed corporation should establish appropriate contingency plans to ensure its operational resilience, and to require the EDSP to disclose data losses, security breaches, or operational failures which may have a material impact on the licensed corporation's regulated activities.	Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS provides customers with the capability to implement a robust continuity plan, including the utilization 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 utilize 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

Requirement	Customer Considerations
	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, they are each fed via 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. 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.
E.20 A licensed corporation should have in place an exit strategy to ensure that the external data storage or processing services can be terminated without material disruption to the continuity of any	AWS services allow for the export of content by customers on demand, using the AWS Management Console, APIs, and other input methods. For example, AWS Snowball provides devices designed to be secure to transfer large amounts of data into and out of the

Requirement	Customer Considerations
operations critical to the conduct of regulated activities, including in the case of the insolvency of the service provider. If Regulatory Records are stored exclusively with an EDSP, this strategy should clearly outline how a transition to an alternative storage solution (which might include another EDSP) would be executed, and how the SFC's access to Regulatory Records pursuant to the exercise of its regulatory powers will not be impaired during the transition. The exit strategy should be regularly reviewed and updated as appropriate.	AWS Cloud. For more information about migrating data in and out of the AWS Cloud, see Migration & Transfer on AWS.
E.21 The licensed corporation should have a legally binding service agreement with the EDSP, which should provide for contractual termination. This may include contractual provisions requiring the EDSP to assist in a transition to a new EDSP or allow a migration of data back to storage at the premises of the licensed corporation and, where relevant, clearly delineate the ownership of the data and intellectual property following termination of the contract.	
E.22 Concentration risk may arise where a major EDSP provides data services to a large number of financial firms, since a significant disruption in its services may have an impact on the market. Depending on the scale of a licensed corporation's operations and the extent of its use of data storage or processing by an EDSP, the licensed corporation should consider	

Requirement	Customer Considerations
whether it is appropriate to use more than one EDSP, or put in place alternative arrangements to ensure operational resilience.	

Next Steps

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

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

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

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

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the AWS Artifact portal (accessible via the AWS Management Console).
- Consider the relevance and application of the CIS AWS Foundations Benchmark available here and here, as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the Further Reading section of this guide.

- 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
- AWS Security Checklist
- Securing Data at Rest with Encryption
- Cloud Adoption Framework - Security Perspective
- Introduction to AWS Security Processes
- AWS Security Best Practices
- Encrypting Data at Rest
- AWS Risk & Compliance
- Using AWS in the Context of Common Privacy and Data Protection Considerations
- Using AWS in the Context of Hong Kong Privacy Considerations
- Security at Scale: Logging in AWS
- Security at Scale: Governance in AWS
- Secure Content Delivery with CloudFront

Document Revisions

Date	Description
May 17, 2021	First publication