Alibaba Cloud User Guide

Rules and Standards of Securities and Futures Commission of Hong Kong

August 2020

Alibaba Cloud

Notices

Contents

1. Introduction

The Securities and Futures Commission (SFC) is an independent statutory body to regulate Hong Kong's securities and futures markets. As a financial regulator in Hong Kong, the SFC derives its investigative, remedial, and disciplinary powers from the Securities and Futures Ordinance (SFO), including its subsidiary legislation.

To strengthen and protect the integrity and stability of Hong Kong's securities and futures markets for the benefit of investors and the industry in general, sets of rigorous requirements are defined under SFO for the regulated entities to follow, such as Securities and Futures (Keeping of Records) Rules under Cap. 571O, section 151.

Recently, as an increasingly prevalent trend of use of external electronic data storage, including public and private cloud storage, the SFC issued a circular with the subject of Use of Electronic Data Storage on 31 October 2019 (the “EDSP Circular”) to define explicit requirements for the Licensed Corporations (LCs) to ensure the preservation and integrity of the records or documents that LCs are required to keep under Cap. 571 and 615 (Regulatory Records) when utilizing an external electronic data storage provider (EDSP).

As an international cloud service provider, Alibaba Cloud acts as an EDSP in Hong Kong and provides data and document storage services for our LCs customers. Alibaba Cloud is committed to assuring our LCs customers conform to the financial industry-specific regulatory requirements and help them to migrate from on-premises infrastructure to the cloud smoothly. Specifically, Alibaba Cloud’s OSS retention policy provides the LCs customers the capability to meet the stringent requirements under EDSP Circular for recording, storage, and retention of the Regulatory Records. In this document, Alibaba Cloud responds and clarifies its responsibilities and capabilities provided to LCs to help our customers and partners in their digital innovation journey.

2. Alibaba Cloud Security Compliance and Privacy

Alibaba Cloud adheres to domestic and international information security standards, as well as industry requirements. We integrate compliance requirements and standards into our internal control framework and implement such requirements and standards into our cloud platform and products in the beginning of design. Alibaba Cloud is involved in the development of multiple standards for the cloud industry and contributes to industry best practices. We also engage with independent third parties to verify the compliance of Alibaba Cloud according to various requirements. Certified by more than twenty standards across the globe, Alibaba Cloud is a cloud service provider with one of the most extensive ranges of certifications globally.

2.1 Security and Compliance

Given the compliance requirements are different in contexts, industries, and regions, Alibaba Cloud's overall compliance framework is divided as follows:

1) *Management system compliance*. To demonstrate Alibaba Cloud's mature management mechanism and industry's best practices, it complies with:

- **ISO 27001**: Information Security Management System
- **ISO 27017**: Code of Practice for Cloud-specific Information Security Controls
- **ISO 20000**: IT Service Management System
- **ISO 22301**: Business Continuity Management System
- **ISO 9001**: Quality Management Systems Standard
- **CSA STAR**: Maturity Model of Cloud Service Security

2) *Country specific attestations*. As the regulatory requirements vary from country to country, Alibaba Cloud is compliant with country-specific regulatory requirements:

- **MTCS:** Multi-Tier Cloud Security is the cloud security standard proposed by the Info-communications Development Authority of Singapore and released by Singapore Standards, Productivity and Innovation Board. MTCS security certification has three levels. Alibaba Cloud obtained Level-3 certification - the highest security level.

- **German Cloud Computing Compliance Controls Catalog (C5):** The cloud requirements catalog in Germany for assessing the information security of cloud services, which defines a baseline for cloud security.
- **Trusted Cloud label:** Issued by the Trusted Cloud Competence Network, it is awarded to trustworthy cloud services which meet the minimum requirements with regard to transparency, security, quality, and legal compliance.
- The **Multi-Level Protection Scheme (MLPS)** tiered protection system, by DJCP, is a basic information security system in China. The goal of this system is to develop a unified national information security protection management system and standards. Alibaba Cloud has obtained Level III certification for public cloud services and level IV for finance cloud services, which means our systems ensure the security and recovery capabilities of level three and four information in response to security threats.
- **China National Accreditation Service for Conformity Assessment (CNAS)** is the national accreditation body of China responsible for the accreditation of certification bodies, laboratories, and inspection bodies. China's State Information Center Software Testing Center (Testing Center), a CNAS accredited body, performs regular and stringent evaluations on Alibaba Cloud's products and solutions. Alibaba Cloud's robust architecture is fully recognized by CNAS and Testing Center.

3) *Industry-specific authentication.* Alibaba Cloud has been compliant with various banking and financial industries specific security standards.

- **PCI-DSS:** Payment Card Industry Data Security Standard defines operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions. Alibaba Cloud is dedicated to payment security and is strictly compliant with PCI Data Security Standards v3.2.
- **SEC Rule-17a:** Alibaba Cloud completed the assessment related to the ability of our Object Storage Service (OSS) solution to comply with the broker-dealer media requirements promulgated by the Securities and Exchange Commission (SEC) Rule 17a-4(f) and Financial Industry Regulatory Authority (FINRA) Rule 4511. Through this assessment, Alibaba Cloud can serve more customers in the global financial industry, as these regulatory requirements have been widely adopted by many other countries outside of the US as part of the function and feature measurement of a product.
- **HKMA SPMs and Circulars:** To facilitate the Authorised Institutions (AI) to meet the HKMA's regulatory requirements, Alibaba Cloud clarifies its responsibilities and controls in critical areas for which the AIs have to focus under Alibaba Cloud User Guide – Banking Regulations & Guidelines in Hong Kong. In addition, Alibaba Cloud has retained independent auditors to conduct an independent assessment as per the HKMA SPM and circulars. The independent evaluation has confirmed full compliance

by Alibaba Cloud. A workbook of how Alibaba Cloud's controls address the HKMA requirements is available for the customer's reference.

4) *Client-specific authentication.* Alibaba Cloud, as a service provider, has provided an attestation report over the internal controls related to services provided to the customers to address the risks associated with the outsourced services.

- **SOC 1&2 TYPE II and SOC3 Reports:** The Service Organization Control (SOC) reports are a series of audit reports from independent third-party auditors to indicate the effectiveness of Alibaba Cloud's control objectives and activities. These reports are designed to help customers and their auditors to get a picture of the control measures behind operation and compliance. Alibaba Cloud SOC reports are categorized into three types:

  - SOC 1 TYPE II: Internal control report on financial reporting
  - SOC 2 TYPE II: Report on trust service criteria including security, availability, and confidentiality
  - SOC 3: Report on security, availability, and confidentiality for general use purpose

Further information of certifications and compliance credentials can be found at the Alibaba Cloud Security & Compliance Center (*See Useful Resources 1*).

2.2 Privacy

Alibaba Cloud is committed to protecting customers' personal information and guarantees that such information is only used for the purposes agreed by customers. Alibaba Cloud's privacy policy is completely transparent to the public and can be found on our official website. At the same time, Alibaba Cloud takes various technical measures to ensure that the customers' personal information is well protected.

- **ISO 27018:** This establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
- **ISO 27701:** The standard is published in August 2019 to specify a Privacy Information Management System based on ISO/IEC 27001 (ISMS), 27002 (Security Controls), and 29100 (Privacy Framework). Alibaba Cloud has been certified in 2019 with ISO

27701.

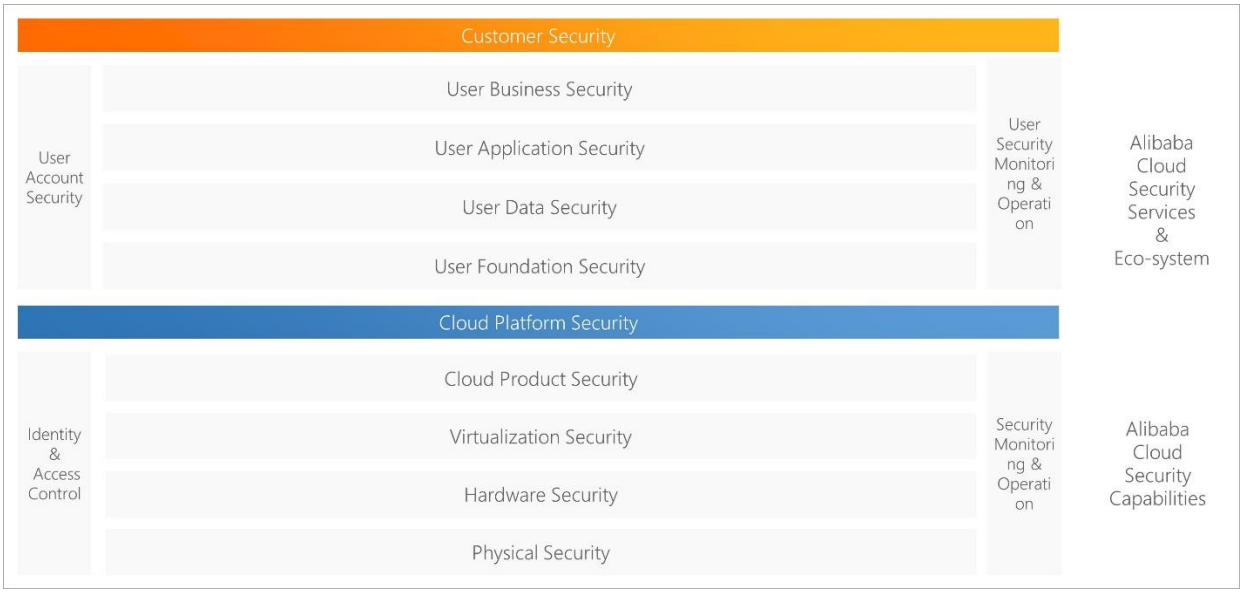
- **GDPR:** GDPR is a mandatory law requiring compliance with provisions that apply throughout the European Union to the business usage of personal data. Alibaba Cloud complies with the GDPR requirements. We also provide research papers and partner solutions to help our customers on their journey to GDPR compliance.
- **PDPA:** Personal data in Singapore is protected under the Personal Data Protection Act 2012 (PDPA). The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure, and care of personal data. Alibaba Cloud complies with the PDPA requirements.
- **EU Cloud Code of Conduct:** As a founding member and a member of the General Assembly, Alibaba Cloud is actively engaged in creating the EU Cloud Code of Conduct under GDPR Article 40 and supports the role of the cloud computing industry in improving transparency and helping cloud customers to understand how data protection issues are addressed by cloud service providers.
- **TRUSTe Enterprise Privacy Certification Standards** incorporate principles from privacy frameworks established by Asia-Pacific Economic Cooperation (APEC), Organization for Economic Co-operation and Development (OECD), and Federal Trade Commission (FTC), and also reflect input from consumers, clients, advocates, and regulators. Alibaba Cloud demonstrated compliance with TRUSTe certification standards and commitment to privacy protection.

To improve Alibaba and the broader industry's understanding of data portability, Alibaba Cloud works with Carnegie Mellon University on a privacy program where their master's degree students helped us to deliver a technical research report on data portability. Download our research paper on Supporting Data Portability in the Cloud under *Useful Resources 2* – GDPR Trust Center.

3. Shared Security Responsibilities

Shared security responsibility model is fundamental and critical for the customers to understand the concept of cloud services. Under the shared security responsibility model, Alibaba Cloud and its customers are jointly responsible for the security of customers' applications built on Alibaba Cloud. Alibaba Cloud is responsible for the safety of the underlying cloud service platform and infrastructure, and customers are responsible for the security of applications built on top of or connected to the cloud. This shared security responsibility model; however, improves upon the typical security model a customer would see in an on-premises data center. Customers can leverage the

underlying security assurance and capabilities that Alibaba Cloud provides, thus getting an overall better security return by using Alibaba Cloud.



Alibaba Cloud ensures a securely managed and operated infrastructure (including but not limited to data centers deployed across regions and zones, and Alibaba backbone networks), physical devices (including computing, storage, and network devices), distributed cloud OS named Apsara, and various cloud services and products running on top of the Apsara OS.

By leveraging its years of expertise in attack prevention technologies, Alibaba Cloud offers various security features and services to help protect customers' applications and systems. In turn, customers shall, in a secure manner, configure and use cloud products (such as the Elastic Compute Service (ECS), Object Storage Service (OSS) instances, and more), and build applications based on such securely configured cloud products. Customers can choose to use the Alibaba Cloud security services or any third-party security products in the Alibaba Cloud security ecosystem to protect their applications and assets.

With security responsibilities shared between Alibaba Cloud and its customers, Alibaba Cloud provides a secure infrastructure to help mitigate the security needs of customers, thus relieving much of the underlying security burdens while allowing customers to focus more on their core business needs. Combined with the right IT governance and controls

within the customer, these should understandably help alleviate regulatory concerns relating to the adoption of cloud services.

For more information about the shared security responsibility model, please refer to *Useful Resources 3 – Alibaba Cloud Security Whitepaper, Version 1.0.* The whitepaper covers the following aspects, such as security policies, organizational security, compliance, data security, access control, personnel security, physical security, infrastructure security, systems and software development and maintenance, disaster recovery, and business continuity.

4. Alibaba Cloud's Presence in Hong Kong

Alibaba Cloud provides a comprehensive suite of global cloud computing services to help power and grow customers' business worldwide. Hong Kong, being one of the international financial centers, is strengthening its competitive advantages through promoting FinTech investments. Alibaba Cloud serves the customers from financial industries in Hong Kong to support their rising demands in digital transformation.

We have worked with financial institutions in Hong Kong to integrate cloud computing technologies into their IT governance and business operations; this has helped them to become more flexible, improve operational efficiency and achieve their strategic objectives. Alibaba Cloud offers integrated cloud solutions to the financial services customers in Hong Kong. See *Useful Resources 4* – Alibaba Cloud Financial Service Solutions.

By setting up cloud data centers across multiple regions and zones, Alibaba Cloud offers the customers secure and reliable cloud computing infrastructure. Currently, Alibaba Cloud has two zones in Hong Kong and multiple data centers globally. Customer's businesses can be deployed across two zones in Hong Kong to implement a high availability architecture, such as same-city active-active architecture, remote data recovery, remote multi-active architecture, and also utilize data centers across regions for a geo-redundant disaster recovery architecture with features of same-city recovery and additional remote recovery.

5. Solution to Compliance with Use of External Electronic Data Storage Circular

5.1 Compliance Requirements and Alibaba Cloud's Capabilities

In the SFO (Cap. 571) and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615), it stipulates recordkeeping requirements, including retention periods for the securities and futures broker-dealer industry. Under SFO section 130, LCs are required to obtain SFC's prior written approval for utilizing any premises for keeping records or documents relating to the carrying on the regulated activities for which it is licensed. To provide LCs with greater flexibility in keeping Regulatory Records, as well as to clarify LCs' general obligations in relation to electronic data, SFC issued the EDSP circular with below principle-based requirements on LCs for using EDSP:

a. LCs should ensure the SFC's access to Regulatory Records, in a legible form, pursuant to the exercise of its regulatory powers is not restricted or otherwise undermined, and that these Regulatory Records have not been deleted or tampered with.
b. The authenticity, integrity, and reliability of Regulatory Records, as well as the ability to access them promptly, are paramount if such records are required to be produced in legal proceedings initiated by the SFC or the Department of Justice.

In other words, the Regulatory Records itself as well as the SFC's right to access such records shall not be affected by utilizing EDSPs and the controls over which shall be as effective as when such records were kept on-premises.

Besides defining the external providers of public and private cloud services as EDSPs, SFC also defined two situations that the requirements in EDSP circular do not apply to:

a. a LC which keeps Regulatory Records with an EDSP if the LC contemporaneously also keeps a full set of identical Regulatory Records at premises used by licensed corporations in Hong Kong approved under section 130 of the SFO, for example when cloud storage is only used for the purposes of data backup or ensuring data availability; or
b. a LC which uses computing services without keeping any Regulatory Records

with an EDSP, for example where cloud computing services are only used for computations and analytics while Regulatory Records are kept at the premises of the licensed corporation.

To demonstrate our commitment to our customers in complying with relevant regulatory requirements, Alibaba Cloud summarized the compliance capabilities of Alibaba Cloud Object Storage Service (OSS), with the OSS retention policy feature, in responding to the relevant storage-specific requirements set forth in EDSP Circular as below.

OSS is an Alibaba Cloud service that provides highly scalable and secure storage and archiving capabilities for objects such as unstructured data, documents, images, audio, and video files. An Alibaba Cloud account could store record objects in buckets, within one or more designated OSS regions. On top of the storage service provided, the OSS retention policy feature was designed to store record objects that are locked in a bucket, integrated controls are applied which prevent the modification, overwrite, and premature deletion of the bucket's record objects for the designated retention period. This OSS retention policy feature has been assessed and verified by an independent assessor in compliance with SEC Rule 17a-4(f) and other similar regulatory requirements. For more information about the shared security responsibility model, please refer to *Useful Resources 5* – Alibaba Cloud Compliance Certificates SEC Rule-17a.

Requirements	Alibaba Cloud's Responses
7(a) and 7(b) **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**	Alibaba Cloud is a secure cloud service platform that provides computing, storage, database, content delivery, and other functionalities to help businesses scale and grow globally. We operate 61 zones in 20 regions around the world, within which two local data centers have been operating in Hong Kong since 2014. We offer a comprehensive set of cloud services in Hong Kong to provide our LC customers to store and process their data locally.

Requirements	Alibaba Cloud's Responses
SFC.	
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.**	Alibaba Cloud strives to provide customers with consistent, reliable, secure, and regulation-compliant cloud services. We conduct self-evaluation as well as third party assessment, certification, and attestation to confirm the effectiveness of the controls and mechanisms in place. In section 5.2 below, we provide a detailed consideration factors to justify Alibaba Cloud's capabilities with reference to the Outsourcing Guidelines issued by other financial regulators.
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 ownership over the content they stored in the cloud environment. Alibaba Cloud will not have access to their content without customers' authorisation. It's the customer's responsibilities to ensure their content kept in a legible form as well as the data integrity. To provide our customer the capability to comply with the relevant requirements, LCs could consider to store the Regulatory Records in Alibaba Cloud OSS. The OSS provides an ability to store unlimited amounts of data, such as documents, images, audio, or video objects in the cloud, within one or more designated OSS regions. Three classes of storage are available within each OSS region to store data according to its lifecycle status (hot data to cold data): • Standard: highly available, high-performance storage used for data and objects requiring frequent access. • Infrequent Access: lower cost storage for data and objects requiring less frequent real-time access, such as longer-term backups. • Archive: lowest cost, highest latency storage that is best suited to long-term archival of cold objects.

Requirements	Alibaba Cloud's Responses
	Alibaba Cloud OSS also supports objects download and export from a bucket through OSS user console or API calls by authorised users and the file's URL can be shared with other authorised users so that they can view and download the files. The requested records can be retrieved and assigned to the user or regulator where may be viewed and reproduced or transferred to an acceptable medium under authorised rule. By leveraging the capabilities of OSS, LCs can fulfil this requirement by either granting access to authorised officer or exporting documents from cloud platform. The platform can log the access and operation activities performed against the objects stored in OSS.
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**	Alibaba Cloud OSS automatically records the access logs for the bucket on an hourly basis once our customers enable the logging function for the bucket. The logs will be written into an object that follows the specific naming convention and stores the object in the target bucket that our customers specify. Alibaba Cloud OSS also supports our customer to enable the real-time log query function by integrating OSS and Log Service (SLS). It allows our customers to query OSS access logs in the OSS console so that the customers can monitor OSS operations including reading, writing, and deleting activities, measure OSS access statistics, trace exceptions, and locate problems with ease. The authorised user accounts' access to the bucket can be uniquely identified from the log with time stamps. To facilitate long-term log storage and archive needs, the SLS provides the capability to ship the Logstore data to OSS and configure the retention policy on OSS console according to our customers' needs. The integrity and accuracy of the log stored in OSS can be ensured by a combination of recording and post-recording verification process of OSS. To verify that no errors occur during transmission or the recording process, the OSS automatically calculates a checksum as part of the record object upload process. The checksums

Requirements	Alibaba Cloud's Responses
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.**	calculated and transmitted with the record object by the customer source application are supported. In case that any checksums cannot be matched with original, the write process fails and an error is returned to the user, the record object must be resent by the source system. In addition, the OSS periodically scans data at rest to verify that recalculated checksums match with stored values to validate continued data integrity. In the event that the checksums do not match, an accurate replica is automatically regenerated from a duplicate. To restrict the access to the OSS where the logs are stored to read-only, Alibaba Cloud OSS provides the retention policy function for our customers to specify the protection period of objects in a bucket. The retention period can be specified ranging from one day to 70 years. During the specified protection period, the objects in that bucket are forced to follow the compliant retention policy, such as Write Once Read Many (WORM). The new OSS retention policy is set to an initial *In Progress* for a period up to 24 hours. The customers must lock the associated retention period via console, SDK, or API within this period to ensure the compliance with the rule. Once the OSS retention policy is locked, existing and new record objects within the bucket are protected against modification, overwrites, and deletions during the specified protection period. You cannot remove or shorten but can extend the retention period for the bucket's OSS retention policy. By following appropriate configurations, Alibaba Cloud's customer can fully comply with the relevant regulatory requirements in EDSP circular by leveraging the logging and WORM storage retention policy.
7(f) **The licensed corporation should ensure that the Regulatory Records are**	Alibaba Cloud OSS provides our LC customers adequate capabilities to share the URL signature with the authorised personnel within a specified period or download records and associated indexes in a legible format. The URL signature is a URL that grants access rights to OSS. The regulator could be authorised by using the shared URL

Requirements	Alibaba Cloud's Responses
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.	signature by LCs. The capabilities that support our customers to download or export the record objects and metadata include: - from the OSS user console by authorised users; - via API calls with the matched API parameters and valid authentication. The connection to the storage account can be protected by denying HTTP (that is to restrict users to use HTTPS only). Any request to the storage account under HTTP will be rejected in this case. Both transmissions through user console and API access points are protected by encrypted channel and industry-standard SSL/TLS protocol with a key length of 256-bit. LCs could fulfil this requirement by submitting the downloaded record objects and index metadata to SFC as requested.

In section E of EDSP circular, the obligations of LCs using external data storage or processing services are stipulated from the governance perspective and internal controls perspective. Alibaba Cloud have implemented sufficient controls to ease your compliance work on cloud.

Key Aspects	Alibaba Cloud's responses
a. Information security and governance	As mentioned in section 2.1 above, Alibaba Cloud adheres to domestic and international information security standards and is certified by over twenty standards across the globe.
b. Physical security	Alibaba Cloud has implemented rigorous physical security measures to safeguard our data centers, utilized advanced logical security technologies to prevent unauthorized access to the physical devices as well as cloud service related applications and systems, used comprehensive security monitoring tools to detect any incoming attacks to the cloud environment. The physical security of Alibaba Cloud data centers have been confirmed in various third-party audits every year, such as ISO27001 and SOC2 Type 2.

Key Aspects	Alibaba Cloud's responses
c. Data security	Alibaba Cloud uses advanced data encryption algorithms to ensure the confidentiality and integrity of data. The data encryption is enabled in different Alibaba Cloud products, including transparent data encryption (TDE) layer for RDS database products, automatic encryption for block storage devices used inside the virtual machines, and object data encryption for OSS. The OSS supports both server-side and client-side encryption. Server-side encryption is used to protect static data on the server side. OSS allows our customer to implement server-side encryption in any of the following methods: - OSS-managed keys: In this method, OSS generates and manages the keys used for data encryption, which adopts AES-256 encryption algorithm. - Customer master keys (CMKs) hosted by OSS: In this method, OSS generates an individual key to encrypt each object by using the default managed CMK, and automatically decrypts the object when it is downloaded. - KMS bring your own key (BYOK): In this method, OSS allows our customer to use the specified CMK to generate different keys to encrypt different objects, and records the CMK ID of the encrypted objects to their metadata. When a user with proper decryption permissions is downloading an object, OSS automatically decrypts the object. Client-side encryption supports our customers to encrypt files on the client side before the files are uploaded to OSS. Our customers can use either CMKs hosted on KMS or manually managed data keys by using the custom tools. Alibaba Cloud KMS supports secure key creation and key management. With KMS, our customers can focus on developing services such as data encryption, data decryption, and digital signature verification. In addition, to

Key Aspects	Alibaba Cloud's responses
	provide the highly-regulated industry customers extra comfort, Alibaba Cloud also provides managed hardware security modules (HSMs) feature of KMS. Managed HSM can help our customers meet stringent regulatory requirements, this feature enables easy access to certified HSMs provided by Alibaba Cloud. The managed HSM conforms to the recommendations in (NIST) 800-57 and runs under (FIPS) 140-2 level 3 standard operation model. For the data in transit, Alibaba Cloud enables HTTPS encryption to ensure data transmission security. The Alibaba Cloud console uses HTTPS encryption for data transmission. Alibaba Cloud services provide customers with API access points with HTTPS encryption enabled, allowing customers to use Access Keys to call Alibaba Cloud Service API securely. Alibaba Cloud uses industry-standard SSL/TLS protocol with a key length of 256-bit to address the need for encrypted transmission of sensitive data.
d. Authentication and access control	Alibaba Cloud has established a formal access control management policy through which logical access management for network, cloud user accounts, operating systems, applications, and source code are based on roles and job functions. Multi-factor authentications are enabled with strong password policies for logical access management. Alibaba Cloud also provides capabilities for customers to utilize Resource Access Management (RAM) to manage their accounts and resources, set password rules, including password length, history, complexity, and maximum validity period. Customers can also choose to enable multi-factor authentication via RAM console. Alibaba Cloud's operator may have one-time service permission or service account provisioned to customer's environment for troubleshooting purpose after obtaining the customer's approval. One-time access key will be granted for the account access and such access will be

Key Aspects	Alibaba Cloud's responses
	automatically revoked once the authorization is expired. For the OSS buckets locked under retention policy, the existing and new record objects within the bucket are protected from modifications and deletions during the specified protection period. In other words, no one could change or delete the objects stored inside regardless the access rights granted to the one who tries to take such action.
e. Cyber threats management and monitoring	Alibaba Cloud deploys NIDS to monitor the malicious attacks from network and security products including Anti-DDoS and WAF at network boundary to detect and protect cloud platform from attack. A self-developed threat monitoring platform is utilized to gather security events discovered internally or externally. The platform automatically pushes alerts to the security department personnel for review and follow-up. The confirmed security events will be solved timely. Besides, Alibaba Cloud invites external experts to conduct penetration tests regularly. The identified vulnerabilities are analyzed, documented, followed up, and fixed by our security professionals. To provide our customers a secure on-cloud environment, customers can utilize Alibaba Cloud Security Center to monitor the cyber-attacks to their cloud resources.
f. System security	Configuration scanning tool has been deployed by Alibaba Cloud to scan configurations of operating systems, database management systems, network devices, and virtual images. The scanning results are analyzed and deviations from configuration baseline standards are restored to the standard by operation personnel. Alibaba Cloud is responsible for the security of hardware, software, and network of the cloud platform by means of OS- and database-patch management, while customers are responsible for the security of the operating systems, software, and applications and therefore responsible for performing security patching over their own systems.
g. Performance	Please refer to Section 6.4 above for the monitoring over

Key Aspects	Alibaba Cloud's responses
monitoring and capacity planning	the Alibaba Cloud's performance. Alibaba Cloud's services provide customers with elastic scalability which allows customers to scale up and down based on their needs, and as such, supports customers growing capacities continuously.
h. Incident and malfunction management	Alibaba Cloud has established the policies and procedures to monitor, respond, manage, and report incidents and malfunctions. For the security incidents and malfunction of the cloud platform, the response team of Alibaba Cloud would follow the standard handling procedures to resolve the incident and malfunction identified immediately. A notification will be sent to the impacted customers via the agreed channel including web console, email, message, or call right after the incidents or malfunctions have been confirmed.
i. Contingency management	Alibaba Cloud has established business continuity plans and verifies the plans regularly. Alibaba Cloud facilitates various options to enable resilient solutions that fit LCs' different contingency planning requirements. Alibaba Cloud can work with the LCs and establish a viable contingency plan for different contingency scenarios, including system failure and security breach. Alibaba Cloud will also test the contingency plan with the LCs on a regular basis. Customers retain ownership and control of their content while using the Alibaba Cloud services.

5.2 Key Consideration in Outsourcing Management and Evaluating EDSP

The outsourcing guidelines issued by the financial regulators (such as HKMA and HKIA) set out the supervisory approach of the regulators in monitoring the outsourcing arrangements of the regulated entities, and provide the guideline for the regulated entities to manage their outsourcing activities. The regulated entities are expected to identify and manage the risks associated with the outsourcing arrangement including development of a comprehensive outsourcing policy, conducting materiality and risk

assessment (with respect to the impact on financial, operational, legal, and reputation aspects and potential losses to customers), conducting due diligence to service providers, performing continuous control, and monitoring and putting in place a contingency monitoring plan. Below we summarized some key considerations in evaluating the service providers for due diligence purpose, including the use of EDSPs.

Consideration Factors	Alibaba Cloud's Responses
a. **Reputation experience and quality of service**	Founded in 2009, Alibaba Cloud is an industry leading cloud provider providing a comprehensive suite of global cloud computing services which has been officially recognized as one of the only six players in the Gartner magic quadrant for cloud IaaS, worldwide. In January 2017, Alibaba Cloud became the official Cloud Services Partner of the International Olympic Committee.
b. **Financial soundness, in particular, the ability to continue to provide the expected level of service**	As a business unit of Alibaba Group (NYSE:BABA and HKEX:9988), the financial statements of Alibaba Group include the financial performance and position of Alibaba Cloud. These financial statements are available from US Securities and Exchange Commission, Hong Kong Exchanges and Clearing Market, or at Alibaba Group's Investor Relations website (see *Useful Resources 6).*
c. **Managerial skills, technical and operational expertise and competence, in particular, the ability to deal with disruptions in business continuity**	***Managerial Skills:*** Alibaba Cloud performs a comprehensive risk assessment considering factors from financial, regulatory, customer service, and reputational perspective, at least once a year, and updates the security controls and related policies based on the assessment results. ***Technical Expertise and Competence***: Alibaba Cloud provides the technical foundation to the entire Alibaba Group, including the world renowned Taobao Marketplace. From the latest statistics generated internally by Alibaba Cloud in March 2019, the Alibaba Cloud platform is capable of protecting approximately 40% of websites in China, detecting on a daily basis over 60,000 malicious IPs and defending over 3,600 million attacks and

Consideration Factors	Alibaba Cloud's Responses
	approximately 3,000 DDoS attacks every day. ***Operational Expertise and Competence***: Alibaba Cloud has established an information security management system (ISMS) and certified the ISMS according to ISO/IEC27001:2013. Alibaba Cloud has also established ITSM policies which are based on ISO/IEC20000. On a yearly basis, Alibaba Cloud performs a management review and documents the review results. If weaknesses are discovered, follow-up action must be taken to ensure continuous improvement on the management system. We also regularly engaged independent auditor to conduct SOC 2 audit over the controls we employ to protect the confidentiality, security, and availability of user data. ***Business Continuity Capability:*** Alibaba Cloud has established business continuity plans and the plans are reviewed on an annual basis. Business continuity management team performs business impact analysis and risk assessment every year, including identification of critical business processes, maximum tolerable downtime, recovery time objective, minimum service level and time needed to resume service. Alibaba Cloud, along with data center service providers, conducts data center business continuity drills every year and issues a data center business continuity report for each exercise. Alibaba Cloud is willing to jointly participate in the process of establishing the customer's business continuity plan and conduct the training together with the customer.
d. **Extent of reliance on sub-contractors and effectiveness in monitoring the work**	Alibaba Cloud creates and maintains written agreements with third parties (for example, contractors or vendors) with rights and obligations, the scope of services, compliance requirements, and services levels stated in the service

Consideration Factors	Alibaba Cloud's Responses
of sub-contractors	agreement. Vendors and contractors are required to sign the service agreement and confidentiality agreement. A periodic assessment over the vendor's performance is performed by Alibaba Cloud in accordance with the service level specified in the service agreement. In addition, Alibaba Cloud has also established Alibaba Cloud Vendor Information Security Management Policy and Vendor Management Policy to regulate the management over vendors prior to, in the progress of, and after the onsite work.
e. **Compatibility with the securities firm's corporate culture and future development strategies**	Alibaba Cloud, as a business unit of Alibaba Group, follows the Corporate Governance Guidelines as well as Code of Ethics established by Alibaba Group, which are available at the Alibaba Group's Investor Relations website (see *Useful Resources 6*). The guidelines set out the principles and practices that the Board will follow in carrying out its responsibilities, and the codes cover the aspects including compliance with laws and ethical conduct, conflicts of interests, equal opportunity and non-discrimination, safety in the workplace, bribery, related party transactions, recordkeeping and insider trading. Alibaba Cloud keeps improving the technologies and services we provide and delivers the on-demand computing resources (including servers, databases, storage, platforms, infrastructure, and applications) to fit customer's future development needs.
f. **Familiarity with the securities industry and capacity to keep pace with innovation in the market**	***Industry Familiarity:*** Alibaba Cloud has successfully helped many customers in insurance industry to move to cloud. Alibaba Cloud has been compliant with PCI-DSS for the customers in payment card industry.

Consideration Factors	Alibaba Cloud's Responses
	Market Innovation: Alibaba Cloud is continuously recognized by different industry analysts as one of the leading global cloud service providers. Alibaba Cloud obviously has the financial, operational, and managerial capacity to continue leading innovation in the market. Our Press Room (see *Useful Resources 7*) provides a wealth of our latest innovation and progress that would be of interests to the AIs.

Clause 21 under Section E of EDSP Circular sets out that the using of EDSP should be undertaken in the form of a legally binding written agreement and lists the matters that should be considered in negotiating the contract with the service provider. Alibaba Cloud has set out terms and conditions as well as Service Level Agreement (SLA) for our products. For details, please refer to the Alibaba Cloud legal document center *(*see *Useful Resource 8)*.

Alibaba Cloud provides a template of an offline Cloud Services Purchase Agreement or Enterprise Agreement where the contract terms and conditions have been set out against the HKIA's requirements in the guidelines. Alibaba Cloud customers have the option to enter into an offline Cloud Services Purchase Agreement or Enterprise Agreement with Alibaba Cloud. The offline agreements can be tailored to better meet the customers' needs. For more information, please contact Alibaba Cloud sales representative at *Useful Resources 9*.

6. Overview of Relevant Regulatory Requirements

Alibaba Cloud empowers customers to deploy on a trusted and high-performance cloud architecture worldwide. As a globally recognized industry-leading cloud service provider, we have been partners with many brokers and intermediaries in their cloud strategy, governance, and adoption process.

The SFC sets out baseline requirements expected for licensed or registered persons including technology risk management and management over the third-party service providers in the circulars and guidelines such as:

- Circular to all Licensed Corporations on Internet Trading
- Circular to All Licensed Corporations on Information Technology Management
- Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading

The relevant requirements on infrastructure and cloud service provider are of the necessary standards and do not go beyond the areas mentioned above in Section 5.1 and 5.2.

To ensure on-going regulatory compliance and fulfill their risk management duty of care, LCs must make changes to the existing strategy, governance, policies, operating model, and processes when adopting cloud services. The level of necessary change though will be on a sliding scale relative to the architectures deployed and the criticality of workloads hosted in the cloud environment. We provide professional services to assist the planning, design, execution, and evaluation process (see *Useful Resources 10*).

While the Alibaba Cloud official website and this user guide facilitate a wealth of information relevant to your considerations, our sales representative should undoubtedly be able to assist you in addressing your concerns. In case we are not already in touch, please reach us at https://www.alibabacloud.com/contact-sales. We look forward to partnering with your organization to enable your digital transformation and IT modernization journey.

7. Useful Resources

1. Alibaba Cloud Security & Compliance Center
2. Alibaba Cloud GDPR Trust Center
3. Alibaba Cloud Security Whitepaper, Version 1.0
4. Alibaba Cloud Financial Service Solutions
5. Alibaba Cloud Compliance Certificate SEC Rule 17-a
6. Alibaba Group’s Investor Relations

7. Press Room
8. Legal Document Center
9. Contact Sales
10. Alibaba Cloud Professional Services

8. Version History

November 2019: First Edition - Version 1.0
August 2020: Second Edition – Version 2.0