

Alibaba Cloud User Guide

Insurance Regulations & Guidelines in Hong Kong

March 2019



Notices

This document is provided for informational purposes only. It represents Alibaba Cloud's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. This document does not create any warranties, representations, contractual commitments, conditions or assurances from Alibaba Cloud, its affiliates, suppliers or licensors. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss. The responsibilities and liabilities of Alibaba Cloud to its customers are controlled by Alibaba Cloud agreements, and this document is not part of, nor does it modify, any agreement between Alibaba Cloud and its customers.

Contents

1. Introduction.....	1
2. Alibaba Cloud Security Compliance and Privacy	1
2.1 Security and Compliance	2
2.2 Privacy	4
3. Shared Security Responsibilities	5
4. Alibaba Cloud's Presence in Hong Kong.....	7
5. HKIA Fast Track for Virtual Insurers	8
5.1 Guideline on the Use of Internet for Insurance Activities (GL8).....	8
6. HKIA Guideline on Outsourcing (GL14).....	11
6.1 Service Provider.....	11
6.2 Outsourcing Agreement.....	15
6.3 Information Confidentiality	15
6.4 Monitoring and Control.....	17
6.5 Contingency Planning	18
6.6 Overseas Sourcing.....	19
7. Next Steps with Alibaba Cloud.....	19
8. Useful Resources	20
9. Version History.....	20

1. Introduction

Insurance industry is facing increasing pressure to adapt to the fast changing customer behavior and new business model (e.g., new sales and distribution channels) brought by the development of financial technology (Fintech) these years. To cope with this changing pace, the Hong Kong Insurance Authority (HKIA) has set out guidelines to supervise Authorized Insurers (AIs) in managing the risks associated with use of internet for insurance activities as well as outsourcing (including IT outsourcing) and complying with the relevant regulatory requirements without hindering the efficiency and effectiveness of AIs' operations.

HKIA has also been closely monitoring the development and application of technology in the insurance industry (Insurtech) and proactively assisting market participants to tackle Insurtech-related regulatory issues. In addition to Insurtech Sandbox, HKIA has sets up Fast Track for applications for authorization of new insurers owning and operating solely digital distribution channels, i.e. virtual insurers. The use of outsourcing including cloud computing services is permitted as long as the authorized insurers can demonstrate that it fulfils the HKIA's relevant guidelines in outsourcing, and addresses the technology risks with the use of digital channels such as Internet for insurance activities.

Alibaba Cloud is committed to provide assurance to the insurers to confirm our compliance to the financial industry specific regulatory requirements and help them to smoothly transit from the on-premise infrastructure to cloud adopting infrastructure. In this artifact, Alibaba Cloud provides the responses and clarities over its responsibilities and controls related to the key considerations so as to help insurance customers partner with Alibaba Cloud 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 by 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 ten standards across the globe, Alibaba Cloud is a cloud service provider with one of the most complete ranges of certifications in Asia.

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 27018:** Code of Practice for Protecting Personal Data in the Cloud
- **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 Information 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/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 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 measurement of a product function and feature.

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.

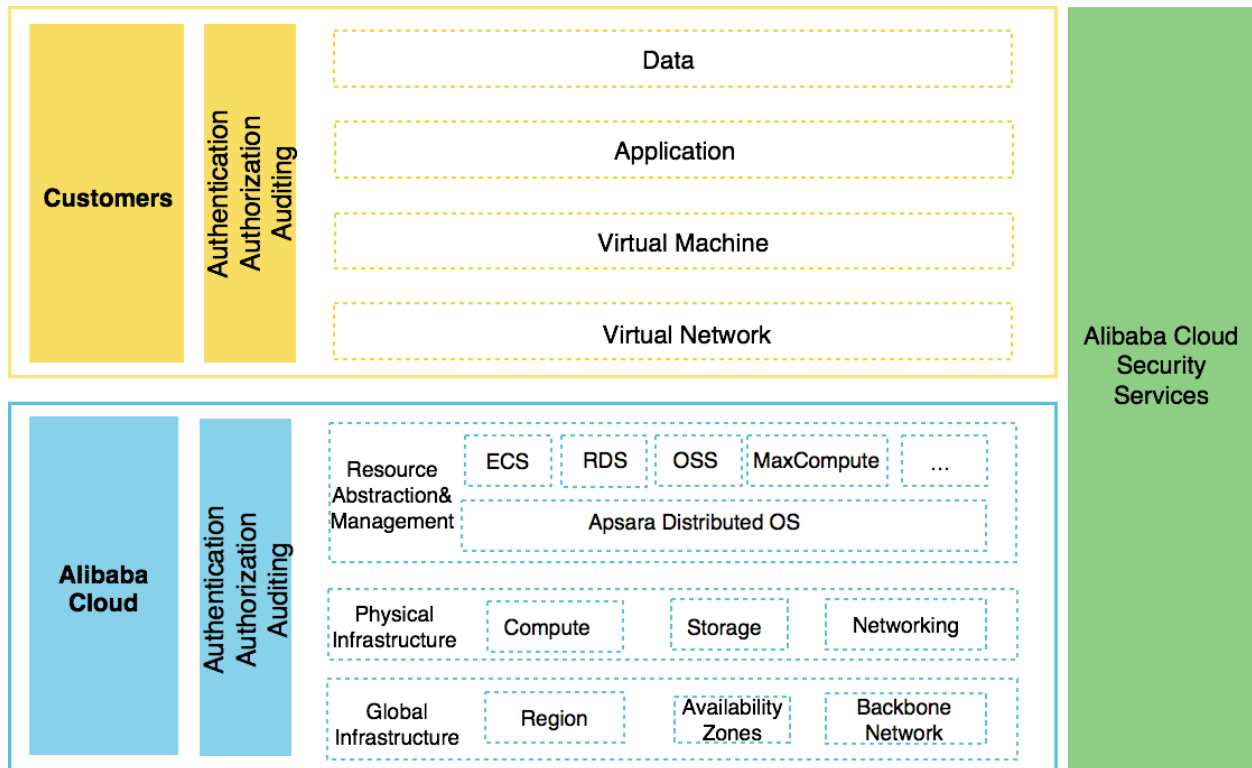
- **ISO 27018** – This establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
- **GDPR** – GDPR is a 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 paper and partner solution to help our customer 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 of the General Assembly, Alibaba Cloud is actively engaged in creating the EU Cloud Code of Conduct under GDPR Article 40, and support the role of the cloud computing industry in improving transparency and helping cloud customers understand how data protection issues are addressed by cloud service providers.
- **TRUSTe Enterprise Privacy Certification Standards** incorporate principles from privacy frameworks established by APEC, the OECD, and the 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 Resource – 3. 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 must ensure 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 must, in a secure manner, configure and use cloud products (such as the Elastic Compute Service (ECS), Relational Database Service (RDS) instances, etc.), 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 share security responsibility model, please refer to “Useful Resources – 2. 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, launching Fintech Supervisory Sandbox (FSS) 2.0, introducing new virtual bank competition, among many other initiatives. Alibaba Cloud serves the customers from financial industries in Hong Kong to support their rising demands in digital transformation.

We have worked with some financial institutions in Hong Kong to help them gain more flexibilities, improve operational efficiencies, achieve strategic objectives by integrating cloud computing technologies into their IT governance and business operations. Alibaba Cloud offers integrated cloud solutions to the financial services customers in Hong Kong. See Useful Resources – 6. 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** availability zones in Hong Kong and multiple data centers globally. Customer’s businesses can be deployed across two availability 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 featuring same-city recovery and additional remote recovery.

5. HKIA Fast Track for Virtual Insurers

HKIA launched Fast Track to promote the development and the application of new technologies in the insurance sector of Hong Kong. Fast Track will provide a dedicated queue to authorization applications using solely digital distribution channels and expedite the review of such applications. This helps stimulate innovation, enhance value proposition, improve customer experience and broaden financial inclusiveness.

Virtual insurers will be subject to the same set of codes and guidelines issued by HKIA as what are applied to conventional insurer. With adoption of new technology, it may increase the doubts of AIs to demonstrate adequacy of the control procedures to achieve the objectives of the relevant supervisory requirements of the HKIA. By leveraging Alibaba Cloud service platform and infrastructure, AIs can leverage the underlying security assurance and increase AIs confidence in compliance with the relevant requirements issued by HKIA.

5.1 Guideline on the Use of Internet for Insurance Activities (GL8)

GL8 takes into consideration the special features of the Internet which distinguish it from the conventional distribution channels to guide AIs when engaging in internet-based insurance activities. Alibaba Cloud, as a cloud service provider, understands a series of requirements regarding information security, confidentiality, integrity, data protection, payment systems security and related concerns that AIs should address when carrying out internet insurance activities under section 5.1 in GL8. We summarized the relevant considerations that AIs should be taken together with Alibaba Cloud's response in below table.

Requirements	Alibaba Cloud's Responses
a. a comprehensive set of security policies and measures that	Alibaba Cloud has maintained a comprehensive set of policies and procedures for governing and managing information security and IT operation risks. It provides guidance to all Alibaba Cloud departments and personnel for their daily work

Requirements	Alibaba Cloud's Responses
<p>keep up with the advancement in internet security technologies shall be in place</p>	<p>and management procedures to protect the security of system, data and physical environment.</p> <p>Under shared responsibility model, 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 their systems by using the security features of Alibaba Cloud products and security services. To provide a secured cloud environment to our customers, Alibaba Cloud also invites external experts to conduct penetration tests every half year. Discovered vulnerabilities are analysed, documented and followed up.</p> <p>It is customer's responsibilities to promote a secured end-to-end environment by establishing a comprehensive set of security policies and measures to govern the internet security technologies and perform the penetration tests over the internet-facing systems regularly.</p>
<p>b. mechanisms shall be in place to maintain the integrity of data stored in the system hardware, whilst in transit and as displayed on the website</p>	<p>Alibaba Cloud takes strict security measures protect the customer's data in rest and transmission. Each customer instance is segregated from other tenant's in a public cloud computing environment via virtualization technology.</p> <p>Customer should manage and take full ownership of their own data especially maintain the integrity and confidentiality of the data in rest and transit. With Alibaba Cloud, customer can leverage the underlying security assurance and capabilities that Alibaba Cloud provides.</p>
<p>c. appropriate backup procedures for the database and application software shall be implemented</p>	<p>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 customer's responsibilities to make sure their content has been backed up properly and to ensure data integrity and security.</p> <p>Alibaba Cloud facilitates different data storage, backup and protection facilities to help the customer achieve the data availability and information timely retrieval capability. Alibaba</p>

Requirements	Alibaba Cloud's Responses
	Cloud also provides security services to help customer detect any unauthorised access and modification of information.
<p>d. a client's personal information (including password, if any) shall be protected against loss; or unauthorized access, use, modification or disclosure, etc.</p>	<p>Alibaba Cloud maintains a strict access controls and grants the minimum resource access permissions to each employee based on his/her position while ensuring the segregation of duties. The requested permission is only limited to people who need to access to such data for their work upon approvals of supervisor, data and system owner, security administrator, relevant departments and based on the least privilege principle. In addition, Alibaba Cloud uses advanced data encryption algorithms to ensure the confidentiality and integrity of data, including sensitive data encryption in applications, transparent data encryption in the database, block storage data encryption, object storage system encryption and hardware security modules. Alibaba Cloud provides Key Management Service (KMS) for key management and data encryption capabilities for the encrypted storage of sensitive data on the cloud platform. Such sensitive data include authorization credentials, passwords, and encryption keys. 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 256-bit key length to address the need for encrypted transmission of sensitive data.</p>
<p>f. the electronic payment system (e.g. credit card payment system) shall be secure</p>	<p>Alibaba Cloud is a Payment Card Industry (PCI) compliant cloud service provider, as per section 2 Alibaba Cloud Security Compliance and Privacy. The customer's QSA can rely on Alibaba Cloud Attestation of Compliance (AOC) for the portion of the PCI cardholder environment deployed in Alibaba Cloud. The customer however must still manage their own PCI DSS compliance certification, and satisfy all other PCI DSS requirements.</p>

6. HKIA Guideline on Outsourcing (GL14)

The Guideline on Outsourcing (GL14) issued by HKIA sets out the supervisory approach of HKIA in monitoring the outsourcing arrangements of AIs and provides the guideline for AIs to manage their outsourcing activities. The AIs 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 of the impact on financial, operational, legal and reputation aspects and potential losses to customers), conducting due diligence to service provider, performing continuous control and monitoring and putting in place a contingency monitoring plan. AIs should be able to demonstrate their observance to the outsourcing guidelines before entering into a new material outsourcing arrangement or significant change to an existing one, by giving the prior notification of material outsourcing arrangement with checklist in Annex 3 or 4 in GL14 and relevant supporting documents, at least 3 months before the commencement day unless otherwise justifiable by AIs.

The guideline is applicable to all outsourcing arrangements of an AI which is incorporated or based in Hong Kong, or any outsourcing arrangements of non-Hong Kong incorporated or based insurers relating to that insurer's operation in Hong Kong, including the use of cloud services. In the below sections, Alibaba Cloud responds to the relevant requirements issued by HKIA in this guideline.

6.1 Service Provider

Section 5.8 of the Guidelines on Outsourcing sets out a non-exhaustive evaluation aspects over service providers for due diligence purpose, including the use of cloud services. The following table list our response to the relevant considerations.

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.

Consideration Factors	Alibaba Cloud's Responses
<p>b. Financial soundness, in particular, the ability to continue to provide the expected level of service</p>	<p>As a business unit of Alibaba Group (NYSE:BABA), 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 or at Alibaba Group's Investor Relations website (see <i>Useful Resources 10</i>).</p>
<p>c. Managerial skills, technical and operational expertise and competence, in particular, the ability to deal with disruptions in business continuity</p>	<p>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.</p> <p>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 by 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 approximately 3,000 DDoS attacks every day.</p> <p>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 users'</p>

Consideration Factors	Alibaba Cloud's Responses
	<p>data.</p> <p>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 centre service providers, conducts data centre business continuity drills every year and issues a data centre business continuity report for each drill. Alibaba Cloud is willing to jointly participate in the process of establishing customer's business continuity plan and conduct the drill together with customer.</p>
<p>d. Any licence, registration, permission or authorization required by law to perform the outsourced service</p>	<p>Alibaba Cloud has obtained multiple attestations for secure and compliant operation of our services. Globally, these include certification to ISO 27017 (guidelines for information security controls applicable to the provision and use of cloud services), ISO 27001 (Code of Practice for Cloud-specific Information Security), ISO 20000 (Information Technology Services Management Standard), ISO22301 (Business Continuity Management Standard), ISO 9001 (Quality Management Systems Standard) and ISO 27018 (Code of Practice for Protecting Personal Data in Cloud). For more information about our assurance programs, see <i>Useful Resources 1</i>.</p>
<p>e. Extent of reliance on sub-contractors and effectiveness in monitoring the work of sub-contractors</p>	<p>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 agreement. Vendors and contractors are required to sign the service agreement and confidentiality</p>

Consideration Factors	Alibaba Cloud's Responses
	<p>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 and post the onsite work.</p>
<p>f. Compatibility with the insurer's corporate culture and future development strategies</p>	<p>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 <i>Useful Resources 10</i>).</p> <p>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.</p> <p>Alibaba Cloud keeps improving the technology and services we provide and delivers the on-demand computing resources (including servers, databases, storage, platforms, infrastructure, applications, etc.) to fit customer's future development needs.</p>
<p>g. Familiarity with the insurance industry and capacity to keep pace with innovation in the market</p>	<p>Industry Familiarity: Alibaba Cloud has successfully helped with many customers in insurance industry to move to cloud. Alibaba Cloud has been compliant with PCI-DSS for the customers in payment card industry.</p> <p>Market Innovation: Alibaba Cloud is continuously recognized by different industry analysts as one of</p>

Consideration Factors	Alibaba Cloud's Responses
	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 <i>Useful Resources 4</i>) provides a wealth of our latest innovation and progress that would be of interests to the AIs.

6.2 Outsourcing Agreement

Section 5.10 of the guidelines clarifies that an outsourcing arrangement 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 5*).

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 to the customers' needs. For more information, please contact Alibaba Cloud sales representative at *Useful Resources 9*.

6.3 Information Confidentiality

Sections 5.12 to 5.14 of the guidelines emphasizes the responsibility for AIs to protect the integrity and confidentiality of the customer information by complying with the relevant statutory requirements such as Personal Data Privacy Ordinance (PDPO). Alibaba Cloud assures customers that Alibaba Cloud is committed to protecting the personal information of customers worldwide, and to complying with applicable laws of countries where our business is operated.

Key Aspects	Alibaba Cloud's responses
<p>5.12 To ensure proper safeguards are in place to protect the integrity and confidentiality of the insurer's information and customer data</p>	<p>Alibaba is compliant to ISO 27018 (Code of Practice for Protecting Personal Data in Cloud).</p> <p>Alibaba Cloud's privacy policy is completely transparent to the public where security measures are adopted to protect the customer's personal data from authorized access. The access to customer's personal data will only be limited to people who need to access to such data for their work.</p> <p>Customer's content is segregated from other tenant's data in a public cloud computing environment via virtualization technology.</p>
<p>5.13 To notify customers of the outsourcing arrangement and circumstances under which their data may be disclosed or lost; In the event of the termination, to ensure that all customer data are either retrieved from the service provider or destroyed</p>	<p>Customer Notification: It is the Als' responsibilities to notify their customers of the data outsourcing.</p> <p>Alibaba Cloud will not have access to or use the customer data unless with customer's authorization. Alibaba Cloud will not disclose customer content to any government or third party, or move customer content from the regions selected by customer, except in each case as necessary to comply with the laws or is subjected to court orders.</p> <p>Termination: Upon the contract termination, the storage service instances will be released, the original disk space and memory space will be reliably scrubbed to ensure customer data security.</p> <p>Customers have the rights to delete their accounts by having their records and information deleted online via Alibaba Cloud's international web</p>

Key Aspects	Alibaba Cloud's responses
	<p>console.</p> <p>Again, customers retain ownership and control of their content when using Alibaba Cloud services and they should be responsible for determining the data retention period and performing back up their own content.</p>
<p>5.14 To notify the IA forthwith of any unauthorized access or breach of confidentiality by the service provider or its sub-contractor that affects the insurer or its customers</p>	<p>Alibaba Cloud protects the confidentiality of customer data by preventing unauthorized access and advanced encryption technology. Alibaba Cloud also provides security services to help customer detect any unauthorized access and modification of information.</p> <p>Alibaba Cloud utilizes a threat monitoring platform to gather security events discovered internally or externally and automatically pushes alerts to the security department personnel. For the security incidents with Alibaba Cloud's platform and infrastructure, the security incident response team would follow the incident handling procedures to resolve the incidents identified. A notification will be sent to the impacted customers of the security issue via web console, email and text channel right after the incidents have been identified and resolved.</p>

6.4 Monitoring and Control

Section 5.15(c) and 5.16 of the guidelines require that effective procedures are established to monitor the performance of the service provider, and there should be an effective reporting procedure on the problems and issues relating to outsourced services. Alibaba Cloud assigns a technical account manager who is responsible for providing expertise, accelerated support and strategic advice tailored to the customer. This includes both continuous hands-on assistance and immediate escalation of urgent issues to speed resolution and keep mission-critical systems functioning.

Key Aspects	Alibaba Cloud's responses
5.15(c) To monitor each outsourcing arrangement to ensure the service is being delivered in the manner expected, and to ensure the provisions included in the outsourcing agreement are properly effected	<p>Alibaba Cloud will invite independent third party auditors to conduct auditing over the underlying cloud platform and submit the assurance reports to AIs regularly. AIs also can find Alibaba Cloud's most recent certificates and assurance reports via the Security and Compliance Center (<i>see Useful Resources 1</i>).</p> <p>For the security incidents with Alibaba Cloud's platform and infrastructure, please refer to 5.14 under section 6.3 above.</p>
5.16 To have reporting procedures that can promptly escalate problems relating to the outsourced service to the attention of the management of the insurer and the service provider	<p>Alibaba Cloud has established security vulnerability and incident reporting procedures. A vulnerability and incident reporting platform is used by Alibaba Cloud for external personnel to report incidents. The customer may raise a ticket to Alibaba Cloud via web console or contact the technical account manager directly for any incidents or problems with their environments. The after sales support team in Alibaba Cloud will follow up with the customer in accordance to the service level guaranteed in SLA.</p>

6.5 Contingency Planning

Sections 5.17 and 5.18 of the guideline indicates that AIs should maintain and test the contingency plan on a regular basis together with service providers to ensure the business continuity. AIs are expected to ensure service providers have satisfactory business continuity plans, regularly test the business continuity plans, and provide data resolvability and data recovery measures upon closure or failure of service providers.

Alibaba Cloud has established our own business continuity plans and the plans have been regularly tested. Alibaba Cloud facilitates various options to enable resilient solutions that fit AIs' different contingency planning requirements. Alibaba Cloud can work with the AIs to establish a robust continuity plan for different contingency scenarios, including system failure, security breach and etc. Alibaba Cloud can also facilitate the contingency plan test with the AIs on a regular basis.

Customers retain ownership and control of their content while using the Alibaba Cloud services. Under the circumstances that AIs would like to move their data back to on-premises or to other cloud service providers, AIs can retrieve their transaction data and account information from the web console or via the ticketing services.

6.6 Overseas Sourcing

Section 5.19(d) of the guidelines clarifies that the outsourcing services should not forbid both HKIA and AIs from accessing such data on a timely basis or inspecting the controls over operations as if the services were not outsourced by AI. Alibaba Cloud assures the customers that they have complete ownership and control over its data stored in the cloud environment.

Key Aspects	Alibaba Cloud's responses
<p>5.19(d) To ensure arrangement would not, in any case, impede the ability of the Insurance Authority to access in Hong Kong the books and records and other information of the insurer as necessary for the Insurance Authority to carry out its statutory responsibilities</p>	<p>Alibaba Cloud facilitates different data storage, backup and protection facilities to help the customer achieve the data availability and information timely retrieval capability. Alibaba Cloud also provides security services to help customer detect any unauthorised access and modification of information.</p> <p>Upon request from HKIA, independent assessment can be performed over Alibaba Cloud's data center facilities in Hong Kong. AI can also engage an external auditor to perform the independent assessment over the data center facilities.</p>

7. Next Steps with Alibaba Cloud

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 insurers and insurance intermediaries in their cloud strategy, governance and adoption process.

To ensure on-going regulatory compliance and to fulfill their own risk management duty of care, AIs must make changes to the existing strategy, governance, policies, operating model, 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, design, execution and evaluation process (see Useful Resources 8).

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 to address 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.

8. Useful Resources

1. Alibaba Cloud Security & Compliance Center
2. Alibaba Cloud Security Whitepaper, Version 1.0
3. Alibaba Cloud GDPR Trust Center
4. Press Room
5. Legal Document Center
6. Alibaba Cloud Financial Service Solutions
7. Dedicated Host
8. Alibaba Cloud Professional Services
9. Contact Sales
10. Alibaba Group's Investor Relations

9. Version History

March 2019: First Edition - Version 1.0