Alibaba Cloud User Guide

Financial Services Regulations & Guidelines in Macau

Alibaba Cloud

Legal Notices

Alibaba Cloud reminds you to carefully read through and completely understand all of the content in this section before you read or use this document. If you read or use this document, it is considered that you have identified and accepted all contents declared in this section.

1. You shall download this document from the official website of Alibaba Cloud or other channels authorized by Alibaba Cloud. This document is only intended for legal and compliant business activities. The contents in this document are confidential, so you shall have the liability of confidentiality. You shall not use or disclose all or part of the contents of this document to any third party without written permission from Alibaba Cloud.
2. Any sector, company, or individual shall not extract, translate, reproduce, spread, or publicize, in any method or any channel, all or part of the contents in this document without written permission from Alibaba Cloud
3. This document may be subject to change without notice due to product upgrades, adjustment, and other reasons. Alibaba Cloud reserves the right to modify the contents in this document without notice and to publish the document in an authorized channel as and when required. You shall focus on the version changes of this document, downloading and acquiring the updated version from channels authorized by Alibaba Cloud.
4. This document is only intended for product and service reference. Alibaba Cloud provides this document for current products and services with current functions, which may be subject to change. Alibaba Cloud makes the best effort to provide an appropriate introduction and operation guide on the basis of current technology, but Alibaba Cloud does not explicitly or implicitly guarantee the accuracy, completeness, suitability, and reliability of this document. Alibaba Cloud does not take any legal liability for any error or loss caused by downloading, using, or putting trust in this document by any sector, company, or individual. In any case, Alibaba Cloud does not take any legal liability for any indirect, consequential, punitive, occasional, incidental, or penalized damage, including profit loss due to the use of or trust placed into this document (even if Alibaba Cloud has notified you, it is possible to cause this kind of damage).
5. All content including, but not limited to, images, architecture design, page layout, description text, and its intellectual property (including, but not limited to, trademarks, patents, copyrights, and business secrets) used in this document are owned by Alibaba Cloud and/or its affiliates. You shall not use, modify, copy, publicize, change, spread, release, or publish the content from the official website, products, or programs of Alibaba Cloud without the written permission from

Alibaba Cloud and/or its affiliates. Nobody shall use, publicize, or reproduce the name of Alibaba Cloud for any marketing, advertisement, promotion, or other purpose (including, but not limited to, a separate or combined form to use the name, brand, logo, pattern, title, product or service name, domain name, illustrated label, symbol, sign, or similar description that may mislead readers and let them identify that it comes from Alibaba Cloud and/or its affiliates, of or from Alibaba Cloud, Aliyun, Wanwang, and/or its affiliates) without the written permission from Alibaba Cloud.

6. If you discover any errors or mistakes within this document, please contact Alibaba Cloud directly to raise this issue.

Contents

1. Introduction

Alibaba Cloud provides a comprehensive suite of global cloud computing services to help power and grow customers' business worldwide. We strive to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers ensure the confidentiality, integrity, and availability of their systems and data. We have worked with financial institutions in Macau to help them gain more flexibilities, improve operational efficiencies, achieve strategic objectives by integrating 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 institutions in Macau. This whitepaper is developed to illustrate how Alibaba Cloud services can help financial institutions to meet those legislations and regulatory requirements listed in **Section 2 — Regulatory Landscape of Macau**, as well as the information that Alibaba Cloud compiles internally for its compliance which customers can use, to evaluate, meet, and demonstrate compliance with legislations and applicable regulatory requirements. In addition, the whitepaper also provide guidance of how the customers shall develop their own controls framework to comply with the Legislations, Regulations and Guidelines in Macau under the shared responsibility model.

2. Regulatory Landscape of Macau

Monetary Authority of Macao ("AMCM")

The AMCM is responsible for the supervision of the monetary, financial, foreign exchange and insurance markets. It ensures their smooth operation and guides their operations according to the terms formulated in the regulatory statutes. It is obligated to monitor the stability of internal monetary and financial system and perform the functions of a central monetary depository including management of Macau's currency reserves and other foreign assets. Furthermore, it advises on policies which facilitate the sustainability of the long-term growth of the financial sector and achieve the purpose of long-term financial stability and development.

What Legislations, Regulations and Guidelines are relevant?

This user guide outlines the key consideration areas that should be aware in cloud migration from the below relevant Legislations, Regulations and Guidelines.

Regulations and Guidelines issued by the AMCM:

- Guideline on Outsourcing
- Guideline on Business Continuity Management
- Incident Reporting Measures for Major Emergencies
- Guideline on Cyber Resilience
- Guidelines on the Use of Internet for Insurance Activities
- Critical Incidents Reporting Mechanism for Insurance Sector
- Guideline on Cyber Resilience for Insurance Sector

What do the above Regulations and Guidelines cover?

Regulations and Guidelines	Applicability	Coverage
Regulations and Guidelines issued by the AMCM		
Guideline on Outsourcing	Banking Sector, i.e., Banks incorporated in Macau, Branches of banks incorporated overseas, Macao Postal Savings	The Guideline on Outsourcing was issued on 14 August, 2009. This Guideline outlines the AMCM's supervisory approach on outsourcing arrangements of credit institutions and the major prudential issues to be considered by credit institutions when entering into outsourcing arrangements.
Guideline on Business Continuity Management		The Guideline on Business Continuity Management was issued on 14 August, 2009. This Guideline sets forth the essential principles and key processes of Business Continuity Management and the supervisory approach that the AMCM will take in assessing the adequacy of credit institutions' Business Continuity Management.
Incident Reporting Measures for Major Emergencies		The Incident Reporting Measures for Major Emergencies was issued on 17 February, 2016. In this guideline, AMCM determines supervisory measures to strengthen the incident reporting measures for major emergencies and to provide better protection for the interests of the institutions and their customers as well as to safeguard the stability of the financial system.
Guideline on Cyber Resilience		The Guideline on Cyber Resilience was issued on 18 December, 2019. This Guideline sets forth the key principles in managing the risks associated with cybersecurity.
Guidelines on	Insurance Sector,	The Guidelines on the Use of Internet for Insurance

the Use of Internet for Insurance Activities	i.e., Authorized insurers, Reinsurers, Pension fund management companies, Insurance brokers and Corporate intermediaries	Activities was issued on 14 February, 2008. In this guideline, AMCM recommends the adoption of some precautions, including but not limited to internet security, data integrity, and backup procedures to safeguard the interests involved.
Critical Incidents Reporting Mechanism for Insurance Sector		The Critical Incidents Reporting Mechanism for Insurance Sector was issued on 29 December, 2017. In this mechanism, AMCM establishes requirements for insurance institutions, insurance brokers and private pension fund management companies to report critical incidents that may include system being hacked and system failure which cause significant customer data loss.
Guideline on Cyber Resilience for Insurance Sector		The Guideline on Cyber Resilience for Insurance Sector was issued on 17 December, 2019. This Guideline is established for the authorised institutions in order to provide a set of cybersecurity controls and measures for the Macao insurance sector regarding cyber risk management and to enhance the capability in defending cyber-attacks.

Other considerations

This whitepaper covers only the above in-scope Legislation, Regulations and Guidelines listed in **Section 2 — Regulatory Landscape of Macau**.

Customers should identify and understand the requirements applicable to them. The requirement applicability may vary depending on different factors, such as the location of business, the nature of industry, the type of data etc. Customers may also seek appropriate advice from Alibaba Cloud Security Compliance Specialist when necessary.

3. Compliance User Guide

Overview

Data security and user privacy are the top priorities of Alibaba Cloud. Alibaba Cloud is committed to building a public, open, and secure cloud computing service platform. Alibaba Cloud aims to turn cloud computing into a state-of-the-art computing infrastructure by investing heavily in technical innovation to continually improve the computing capabilities and economies of scale of its services. Alibaba Cloud strives to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers ensure the confidentiality, integrity, and availability of their systems and data. For details, please refer to the *Alibaba Cloud Security Whitepaper* (See "Useful Resource – 2. Alibaba Cloud Security Whitepaper, Version 2.0").

Also, 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.

Benefits of Migrating from On-premises to the Cloud

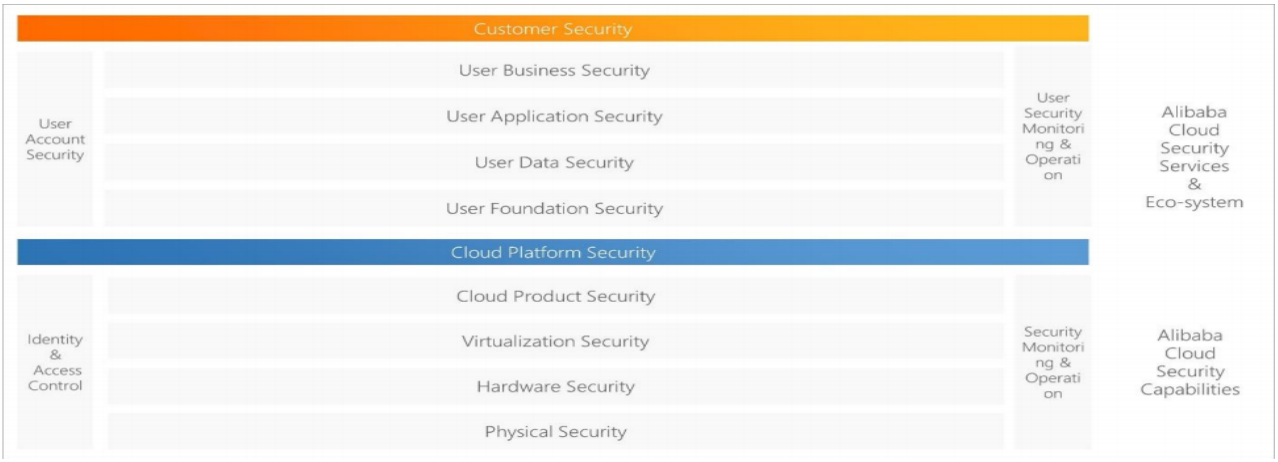
Alibaba Cloud delivers on-demand computing resources (including servers, databases, storage, platforms, infrastructure, applications, etc.) over the Internet. Alibaba Cloud can be used on a pay-as-you-go basis, which means customers can pay just for what you need. With the rapid development of cloud computing services, migrating existing server systems to Alibaba Cloud easily and quickly is of great significance for you, benefiting from cost-efficiency, data security, scalability and speed, elasticity, unlimited storage space, backup and recovery, and go global in minutes.

Besides, Alibaba Cloud provides end-to-end compliance support from Security Compliance Specialist to work with the customers on their security, risk and compliance strategies on the Alibaba Cloud platform. The professionals help the customers to understand how they

can integrate Alibaba Cloud security controls into their own control frameworks and provide recommendations in approaches on implementing their controls on Alibaba Cloud.

3.1 Alibaba Cloud Shared Responsibility Model

Alibaba Cloud employs a shared responsibility model, meaning that the security of applications built on Alibaba Cloud is the joint responsibility of Alibaba Cloud and its customers. In general, Alibaba Cloud is responsible for the security of the underlying cloud service platform and providing security services and capabilities to customers, while customers are responsible for the security of applications built based on Alibaba Cloud services. This relieves much of the underlying security burdens while allowing customers to focus more on their core business needs.



At Alibaba Cloud, we ensure the security of 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), virtualization solutions, and cloud products running on top of the Apsara distributed cloud OS. Alibaba Cloud is also responsible for identity management and access control, monitoring, and operations of the platform to provide customers with a highly available and secure cloud service platform.

Still, customers retain the responsibility for protecting their own systems by using the security features provided by Alibaba Cloud services, Alibaba Cloud Security, and third-party security products in the Alibaba Cloud security ecosystem. Alibaba Cloud offers Alibaba Cloud Security, which leverages the years of expertise in attack prevention technologies to help customers protect their applications and systems and customers should configure and use

cloud products based on security best practices, and build applications on these securely configured cloud products.

3.2 Implementation of Key Areas of Regulations and Guidelines with Alibaba Cloud

This part outlines how Alibaba Cloud can help the customers in implementing the key areas of in-scope Regulations and Guidelines listed in **Section 2 — Regulatory Landscape of Macau**.

Domain 1 - Outsourcing

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the outsourcing activities, including Policy and Procedures, Overseas Outsourcing, Due Diligence, Contract Management, Vendor Management, Confidentiality, Contingency Planning, Accountability and Audit / Review Arrangements.

- 1.1 Policy and Procedures

Key Aspects	Consideration
Policy and Procedures	Customers Customers are responsible to establish an outsourcing policy that sets out its approach to outsourcing of business activities / functions, including a detailed framework for managing all such outsourcing arrangements. The policy should be approved by the board of the credit institution, which should ensure that all relevant business units are fully aware of and comply with such outsourcing policy.

- 1.2 Overseas Outsourcing

Key Aspects	Consideration
Data Transfer to Overseas	Customers Alibaba Cloud has prepared user guide on regulations of different regions to provide an overview of the regulatory landscape of the host country and the key consideration areas that are covered in the relevant legislation,

Key Aspects	Consideration
	regulation, and guideline. The user guide is publicly available for customers in Security & Compliance Trust Center. Alibaba Cloud Alibaba Cloud understands the regulatory requirements imposed on the customers and helps the customers to fulfill such requirements by conducting regular audits following the relevant requirements. For General Control Environment of the Service Provider, please refer to Domain 1.3 — Due Diligence.
Notifications to the Authorities	Customers Customers are responsible to notify the relevant authorities listed in **Section 2 — Regulatory Landscape of Macau** for the overseas outsourcing arrangement. Alibaba Cloud provides end-to-end compliance support from Security Compliance Specialist to help customers understand how they can integrate Alibaba Cloud security controls into their own control frameworks and provide recommendations in approaches on implementing their controls on Alibaba Cloud.
Notifications to their Customers	Customers Customers are responsible to notify their customers of the jurisdiction in which the service provider is located and the right of access.
Access to Outsourced Data by Local and Overseas Authorities and Auditors	Customers Customers are responsible to ensure that access by the AMCM to the related entity would not be impeded. Alibaba Cloud Alibaba Cloud has defined respective responsibilities and obligations of customers and Alibaba Cloud and the terms and conditions in the service agreement, which includes the rights of Governmental Authorities and Auditors and clauses for overseas outsourcing.

Key Aspects	Consideration
Business Continuity Management	Customers Alibaba Cloud has defined service terms and clauses in the service agreements template, for example, condition for contingency planning where Alibaba Cloud acknowledges and agrees that Alibaba Cloud shall maintain and regularly test the contingency plans to ensure business continuity. Alibaba Cloud agrees that customers may rely on the monitoring of the service levels as set out in the service level agreement (SLA), as well as existing audit reports / certificates covering the relevant policy, procedures, controls, tests and mechanisms of Alibaba Cloud (e.g., International Organization for Standardization (ISO) 22301, Service Organization Control (SOC) 2, etc.). Customers should integrate the provider's business continuity plan (BCP) into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications. Alibaba Cloud Alibaba Cloud maintains an effective BCP in accordance with ISO 22301 with independent audit by third party conducted at least on an annual basis. The certificate of ISO 22301 is available to customer to download publicly from Security & Compliance Centre of Alibaba Cloud. For details about business continuity management, please refer to **Domain 6 – Business Continuity Management** .

- 1.3 Due Diligence

Key Aspects	Consideration

Risk Management	Customers Customers are responsible to perform risk assessment prior to the outsourcing arrangement. Alibaba Cloud has prepared user guide with the information of Alibaba Cloud's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, etc. to facilitate customers' due diligence process. Customers can find the user guide in Security & Compliance Trust Centre. *Financial soundness* Alibaba Cloud is a fully owned subsidiary of Alibaba Group Holding Limited (NYSE: BABA). Alibaba Cloud's revenue grows very fast, primarily driven by increased spending from enterprise customers. Alibaba Cloud has been keeping launching new products and features including those related to core cloud offerings, data intelligence, AI applications, security and enterprise solutions. *Reputation* Alibaba Cloud is an industry leading cloud provider in China and it has been officially recognized as one of the only six players in the Gartner magic quadrant for cloud IaaS, worldwide. *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 Capabilities* 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 distributed denial-of-service (DDoS) attacks every day. Operational Capability and Capacity Alibaba Cloud has established an information security management system (ISMS) and certified the ISMS according to ISO/IEC27001:2013. Alibaba Cloud has also established IT Service Management System (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.

- 1.4 Contract Management

Key Aspects	Consideration
Outsourcing Agreement	Customers It's the customers' responsibility to identify any relevant terms and clauses and communicate with outsourcing service providers when preparing the SLA. Alibaba Cloud Alibaba Cloud has defined respective rights and obligations of customers and Alibaba Cloud in the Service Purchase Agreement, which includes the type and level of services provided by Alibaba Cloud, as well as terms on confidentiality, data disclosure and inspection right of regulatory authorities. Customers need to confirm and agree on Service Purchase Agreement before using relevant product services. It is stipulated in Alibaba Cloud's Membership Agreement that Alibaba Cloud will not access or use customer's content except as necessary to maintain or provide the Alibaba Cloud Services or as necessary to comply with applicable laws or regulations, which is publicly available on Alibaba Cloud official website. Customers retain the right to decide where their system and data stored. In case of any relocation of customer content

	conducted by Alibaba Cloud due to data centre relocation, Alibaba Cloud shall notify the affected customers and obtain their consent as stipulated in the Service Purchase Agreement with Financial Institution customers.
Contract Management	Customers Alibaba Cloud has set out terms and conditions as well as SLAs for each product. Alibaba Cloud also provides a template of an offline Cloud Services Purchase Agreement or Enterprise Agreement. Alibaba Cloud customers have the option to enter into an offline Cloud Services Purchase Agreement or Enterprise Agreement with Alibaba Cloud. The terms and conditions in the offline agreements can be tailored to better meet the customers' needs. Alibaba Cloud Alibaba Cloud, vendors involved in the delivered services are mainly data center service providers. A service agreement is signed between Alibaba Cloud and each data center service provider to define their responsibilities and obligations. In addition, a Service Quality Warranty Letter is attached to the agreement to specify requirements on data center service availability level, business relationship and service scope etc. Alibaba Cloud continuously monitors service level of data center service providers to ensure secure and stable operation of data centers. A monthly service level report must be submitted by service providers to Alibaba Cloud for review, covering services provided during the past month, major incidents, summary of maintenance performed, and any feedback, to ensure all Alibaba Cloud's requirements are appropriately met.
Subcontracting	Customers Customers are responsible to ensure the clause associated with subcontracting arrangement is explicitly stated in the SLA. Alibaba Cloud provides customers option to further tailor terms and clauses in the Cloud Service Purchase Agreement or Enterprise Agreement for complying with relevant regulatory requirements.

- 1.5 Vendor Management

Key aspects	Consideration
Performance Monitoring	Customers Alibaba Cloud acknowledges the customers are required by government authorities to continuously review the effectiveness and adequacy of customers' controls in monitoring the performance of customers' service providers. Alibaba Cloud therefore supports the Audit by the following ways: - Customers providing a questionnaire for Alibaba Cloud to complete; or - A report provided by Alibaba Cloud to customers, addressing any queries that customers may have from time to time; or - A qualified independent third-party audit report; or - An audit to be carried out by the Government Authorities or any agent appointed by the Government Authorities, or an outside firm as mutually agreed by the Parties. Alibaba Cloud Alibaba Cloud evaluates vendors' performance monthly in accordance with the compliance requirements and service levels specified in the contracts. Data center service providers submit monthly service level reports to Alibaba Cloud, covering services provided during the past month and any feedbacks to Alibaba Cloud. Alibaba Cloud's data center managers review the reports in the monthly meetings and record exceptions into the meeting minutes.

- 1.6 Confidentiality

Key Aspects	Consideration
Customer Information	Customers It's the customers' responsibility to implement controls to ensure that the requirements of customer data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of customer information.

- 1.7 Contingency planning

Key aspects	Consideration
Termination	Customers It's the customers' responsibility to formulate a contingency plan that outlines the procedures to be followed in the event that the outsourcing arrangement is suddenly terminated or the service provider is unable to fulfill its obligations for any reason. Customers should consider the availability of alternative service providers or the possibility of bringing the outsourced activity / function back in-house in an emergency or due to substandard performance of the service provider, and the costs, time and resources that would be involved.
Daily Operational and Systems	Customers It's the customers' responsibility to ensure that they have adequate understanding of the service provider's contingency plan. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Business Continuity Management Policy to govern business continuity management. The policy defines roles and responsibilities for relevant parties, business continuity management operation model, business continuity management policies, risk tolerance level, business continuity management objectives, business continuity management evaluation and improvement, and management's responsibilities in resource management and personnel training. BCPs have been established to document the roles and responsibilities of staff in BCP which covering the scenario of products related and after-sales incident and defined the corresponding recovery time/points objectives. Besides, Alibaba Cloud has established incident response procedures to detail the roles and responsibilities and process workflow in the event of Internet Data Centre (IDC) incidents. Contingency plans have been developed to address different scenarios of interruption to IDC, including fire, network interruption, emergency power outage, and natural disasters. Alibaba Cloud conducts testing of the BCPs established for Alibaba Cloud critical services and operations at least once a year. If there is any

	discrepancy identified between the plan and the drill test result, responsible parties will assess the test result and re-perform the drill until the result is successful. Alibaba Cloud also conducts testing of data center BCPs for the continued operations of critical processes and required resources in the event of a disruption at least once a year.

- 1.8 Accountability

Key Aspects	Consideration
Accountability	Customers Customers should recognize that outsourcing a business activity does not transfer all of the risks associated to the service provider. Therefore, customers are responsible to ensure their Board of Directors and management retain ultimate accountability for the outsourced activities. Besides, customers should also ensure that the additional risks (e.g., operational, legal and reputation risks) arising from outsourcing are adequately assessed and managed appropriately.

- 1.9 Audit / review arrangements

Key Aspects	Consideration
Internal Audit	Customers Customers are responsible to ensure the internal audit function will review the outsourcing arrangement and the outsourcing process by referring to the requirements.
External Audit	Customers Customers is responsible for arranging independent assessment for assessing the risks associated with outsourcing arrangement and the risk management process. Alibaba Cloud Independent audit is conducted by external auditor over Alibaba Cloud's

	controls in accordance with applicable auditing standard on at least an annual basis to ensure Alibaba Cloud is providing secure, capable and reliable services to customers.

Domain 2 - Data Security

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the data security, including Data Protection, Data Retention and Right of Access.

- 2.1 Data Protection

Key Aspects	Consideration
Data Protection Program	<u>Customers</u> It's the customers' responsibility to establish a data protection program to protect sensitive data at rest, in transit and at use. Customers are responsible to establish own data security management framework, deploy different protection solutions in the lifecycle of data management and formulate governance policies which may cover: - Classify business data based on the importance levels and separately store data of different levels; - Implement sensitive data management for storage services that store core data, including sensitive data detection and sensitive data de-identification; - Enable static data encryption for data storage services; - Enable backup policies for storage services and specify the recovery time objective (RTO) and recovery point objective (RPO); - Prohibit anonymous data access; - Prohibit data reads and writes over the Internet; - Follow the principle of least privilege in the management of data read

	and write permissions. Regularly check for redundant authorization; - Make sure that data read and write logs are completely collected; - Monitor data access behavior in real time, and periodically review and analyze data access logs to detect suspicious data access at the earliest opportunity; and - Review governance policies on a regular basis to ensure that the governance requirements of the business for data leak risks are met. Customers should review and enhance the framework based on the development of business on a regular basis. Alibaba Cloud Alibaba Group has established Data Security Guidelines to define different data types, data owners, data classification standards, data security levels, and protection measures. The policy also governs data security management lifecycle, including data generation, data storage, data usage, data transmission, data dissemination and data disposal.
Data Classification	Customers It's the customers' responsibility to develop a formal policy on how to handle data based on the classification. Appropriate personnel such as the operation and compliance team should review the classification regularly. Customers can make use of Alibaba Cloud Sensitive Data Discovery and Protection (SDDP) which can automatically detect sensitive data stored in data sources. It supports content-based sensitive data detection for files and uses optical character recognition (OCR) technology to extract and detect sensitive information stored in pictures. SDDP also automatically classifies sensitive data that are detected in structured and unstructured data sources and displays the statistics of sensitive data.
Data Inventories and data flows	Customers Data inventories should include structured and unstructured repositories. It's the customers' responsibility to maintain data architecture and sensitive data flows, and use to ensure that data protection program provides

	adequate coverage across the corporation and third parties.
Data Encryption in Storage	Customers *Key Management Service (KMS)* Alibaba Cloud provides KMS for key management and data encryption capabilities for encrypting storage of sensitive data on the cloud platform using Advanced Encryption Standard with 256-bit key length (AES256). Such sensitive data include authorization credentials, passwords, and encryption keys. Customers can also import keys to KMS and manage service keys or user-managed keys (Bring Your Own Key ("BYOK") i.e., keys imported from key management infrastructure) as the customer managed keys ("CMK") for data encryption. *Data Encryption Service* Alibaba Cloud provides Data Encryption Service to allow management of keys including creation, destruction, import and export. It performs sensitive data encryption and re-encryption at application level using secure encryption algorithms. Alibaba Cloud Alibaba Cloud uses data encryption to ensure data security, including sensitive data encryption in applications, transparent data encryption in the database, block storage data encryption, object storage system encryption and hardware security modules.
Data Encryption in Transit	Customers Customers should apply end-to-end encryption for data in transit, especially for confidential data such as passwords and personal information. The means of protection vary with the network channels used in the data transmission process. For internal communication i.e., data transmission between enterprise sites, VPNs or dedicated lines (Express Connect) should be used to reinforce

	communication channels. Alibaba Cloud provides VPN Gateway services to help customers build end-to-end data encryption channels to ensure communication security during data transmission between on-premises data centers and Alibaba Cloud Virtual Private Clouds (VPCs). VPN Gateway establishes IPsec-VPN connection to connect an on-premises data center to a VPC or SSL-VPN connection to connect a remote client to a VPC. Customers should use Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) certificates to encrypt transmission channels for requests sent by clients through the Internet. This prevents data from being intercepted by man-in-the-middle attacks during transmission. Alibaba Cloud SSL Certificates Service can issue SSL certificates from well-known third-party certificate authorities (Cas) in the cloud. It helps customers switch from Hypertext Transfer Protocol Secure (HTTP) to HTTPS, improve the trustworthiness of their websites, and prevent their websites from being hijacked, tampered with, or spied on. Certificates Service simplifies certificate deployment and allows enterprises to perform unified lifecycle management of their certificates in the cloud, and distribute the certificates to other Alibaba Cloud services with a few clicks. <u>Alibaba Cloud</u> Alibaba Cloud console uses HTTPS encryption for data transmission. Apart from console, Alibaba Cloud products use TLS protocol to ensure data transmission security while users read and upload data. HTTPS is also used to encrypt application programming interface (API) payload data to address the need for protecting transmission of sensitive data via API.
Data Protection Tools	<u>Customers</u> Customers should consider tools (such as Data Loss Prevention solution) to detect and block unauthorized transmission of sensitive data. User data loss prevention on cloud involves the complete control over permissions on data and the monitoring and detection of data in use. To prevent data loss, customers can implement effective control over the permissions on storage and transmission products on the cloud.

	Data Management Service (DMS) Alibaba Cloud provides DMS which can provide permission management, the configuration of security rules and operation audit. For permission management, database users should apply for the permissions to extract, modify and export data in a database, table, or column. Only after the corresponding owner approves the application, database users can perform the applied operation. *Sensitive Data Discovery and Protection (SDDP)* Apart from DMS, SDDP supports instant querying of data, users, and permissions, and provides centralized query capabilities against all applicable data permissions, SDDP can also resolve the mappings between Alibaba Cloud account permissions and relevant roles. SDDP can generate alerts for data permission configuration and usage exceptions that do not comply with the security best practices in the cloud environment. Customers possess the comprehensive monitoring and detection capabilities during data transmission and processing, and to discover possible abnormal behaviors during data use in a timely manner with the adoption of SDDP. SDDP can effectively monitor exceptions that occur during the data transmission process, display the data flow lifecycle dynamically, and ensure compliant and orderly export and transmission of data. Based on log analysis, SDDP can effectively identify manual operations and API calls. Based on machine learning and big data analysis capabilities, SDDP can monitor and generate alerts for abnormal behaviors that arise during various data flows and operations. Plus, after data loss is discovered and alerts are sent, SDDP analyzes suspicious events for subsequent data loss handling processes. The event analysis feature centrally collects various types of alert events, and uses time series analysis to restore the behavior baseline of responsible parties and display the historical baseline trajectory in real time, effectively improving analysis efficiency. SDDP can handle tenant events in isolation and feedback the handling results to the machine learning model, which makes anomaly detection increasingly accurate.

	At network level, Alibaba Cloud provides Cloud Firewall (CFW) which can detect host intrusion events such as the presence of worms that stealing information compress data on infected servers and send the compressed data back to attackers. Customers can enable Basic Protection, Threat Intelligence and Virtual Patch function under advanced setting of Intrusion Prevention feature provided by CFW in order to prevent sensitive information leakage due to the presence of worms.

- 2.2 Data Retention

Key Aspects	Consideration
Data Retention	Customers Customers should keep personal data in a form which permits identification of their subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed. Prior to termination of a contract, Alibaba Cloud provides customer technical measures to download their data and delete it afterwards from Alibaba Cloud, to ensure no data will be retained in Alibaba Cloud. Elastic Compute Service (ECS), Object Storage Service (OSS) and Apsara RDS solutions (RDS) related user product documentation have been published on the Alibaba Cloud official website to define relevant customer data retention policies. When the service agreement between Alibaba Cloud and customers expires, customers' ECS and RDS instances are automatically released once beyond the data retention period and customer data is erased according to relevant agreements. Alibaba Cloud Alibaba Cloud has established a security management system for the full lifecycle of devices, including reception, storage, placement, maintenance, transfer, and reuse or decommissioning. Access control and operation monitoring of devices are managed strictly, and maintenance and stocktaking of devices are conducted on a regular basis. When any device

	is recycled or decommissioned, Alibaba Cloud takes data erasure measures for the storage media. Prior to disposal of data assets, it is necessary to check whether the media containing sensitive data and genuine licensed software has been overwritten, degaussed, or physically bended and destroyed to make sure that the data cannot be restored. When certain hard copy materials are no longer needed due to business or legal reasons, Alibaba Cloud physically destroys them or obtains proof of destruction from any third-party data processors, to ensure that the data cannot be reconstructed. On terminating services to cloud service customers, Alibaba Cloud deletes the data assets of the customers in a timely manner or returns the data assets according to relevant agreements. Alibaba Cloud uses data erasure techniques that meet industry standards. The erasure operations are logged to prevent unauthorized access to customer data.

- 2.3 Right of Access

Key Aspects	Consideration
Right of Access	Customers Customers should allow their customers to obtain personal data at reasonable intervals and without excessive delay expense. Customers are also responsible to notify their customers of the jurisdiction in which the service provider is located and the right of access.

Domain 3 - Access Control

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Access Control.

- 3.1 Access Control

Key Aspects	Consideration
Policies for Access Control	Customers Customers should establish access control management framework to govern the provisioning, modification and termination of employee access to systems and confidential data. The principle of least privilege and separation of duties should be adopted to restrict employee access to systems and confidential data. Alibaba Cloud Alibaba Cloud assigns permissions based on business needs, and centrally manages permissions by role, user group, department, and user. Each internal user can apply for and use permissions through the permission management system, and the permissions can also be revoked through the system. To strengthen permission management and reduce the risk of using incorrect permissions, Alibaba Cloud sets different levels of permissions and roles according to risks, and implements different approval processes accordingly at different permission levels. The system automatically freezes permissions that have not been used for a certain period of time. For users who leave Alibaba Cloud, the system automatically freezes their accounts and reclaims their permissions. For users who move to new positions, the system automatically revokes their permission.
User Account Management	Customers Alibaba Cloud provides customers with user identity management and resource access control capabilities. Resource Access Management (RAM) is a centralized user identity management and resource access control service provided by Alibaba Cloud which enables customers to securely authorize access to their resources and ensure access to customers'

	environments is properly restricted. RAM supports user account management in the following ways: - RAM enables an Alibaba Cloud account to have multiple independent RAM users. Within RAM, an Alibaba Cloud account owner can create independent RAM user accounts for employees, systems or applications. In order to eliminates security risks arising from sharing of Alibaba Cloud account credentials, a different password or API Access Key can be assigned to each RAM user. Besides, customers can create custom password strength policies for RAM accounts: customers can configure minimum password length, password complexity, and limits to password retries and reuse based on own business need. - Each RAM user can log on to the Alibaba Cloud console or call service APIs to perform operations on cloud resources. By default, a newly created RAM user account does not have any permissions on resources. Customers can assign minimum operation and access permissions to different RAM users following the principle of least privilege to ensure employee access to systems and confidential data is restricted by their granted access. - Further, RAM user can obtain a Security Token Service (STS) token to assume the RAM role and access the defined Alibaba Cloud resources. The AssumeRole approach provides customers the flexibility to grant temporary access to any RAM users. - Customers can implement identification and authentication mechanism based on business requirement. Multi-factor authentication (MFA) and single sign-on (SSO) services could be enabled for RAM users. Further, administrators are authenticated using AccessKey (AK) pair when accessing the Alibaba Cloud resources through APIs. - Changes to logical user access, including those that result from voluntary and involuntary terminations, should trigger automated notices, - RAM operation events i.e., access provisioning, termination and modification performed by Alibaba Cloud accounts (administrators) will

	be logged and allow tracking. Still, adequate internal controls should be implemented by Customers, including but not limited to: - Grant employee access to systems and confidential data based on job responsibilities and the principles of least privilege. The principle of separation of duties should be put in place to restrict employee access to systems and confidential data. - Although customers can use RAM to manage user identities and access permissions to resources. When an employee leaves the enterprise, any organizational structure changes resulting change in permissions of RAM users, Customers should establish a set of processes to amend and revoke access to the cloud environment and resources hosted in the environment. Customers are responsible to ensure proper accesses and permissions are granted to authorized personnel, and to accurately manage the identities and permissions of the user groups to which the RAM users belong to. In particular, customers are responsible to ensure logical access is removed immediately upon notification of the involuntary or voluntary departure of an employee. - User information such as active users and roles are available on RAM platform. However, it is Customers' responsibility to perform users access reviews periodically for all access to systems and resources using risk-based approach. - Establish proper procedure to ensure the creation, amendment and termination of accesses are submitted and approved by the appropriate personnel. - Change all default passwords and unnecessary default accounts before system implementation and thereafter on a regular basis. Last but not least, Customers should create multiple isolated accounts and set up the organizational structure, with segregation of production and non-production environments to prevent unauthorized access or changes to information assets.

	Alibaba Cloud Alibaba Cloud deployed Identify and Access Management (IAM) measures to ensure access to resources and systems within Alibaba Cloud's environment is properly managed and restricted, following the principle of least privilege and segregation of duties set forth in the Access Control Management Policy, to protect information assets from unauthorized access. Alibaba Cloud uses a centralized identity authentication system for the systems and resources within the Alibaba Cloud's environment with SSO enabled. Each employee's Active Directory (AD) account is unique and identifiable to an individual user and cannot be shared. The Human Resource System is synchronized with the identity authentication system and the permission management system, with employee data from the Human Resource System used to facilitate the creation, change, and removal of employees' AD accounts. Alibaba Cloud has established procedures to automatically create new AD accounts for new joiners. For employees who change roles or transfer to different departments, automatic notifications are sent out to the employees' supervisors to review their user access permissions and to return any unnecessary access permissions based on their current job responsibilities. For employee's termination, the employees' AD accounts are disabled within the same day of their last working day based on automated feeds from the Human Resource System. Alibaba Cloud assigns access permissions of minimum resource to employees based on their positions and roles and business needs. A centralized permission management system is used for access application, access approval, and automatic access provisioning or access removal. An employee can log onto such system to apply for access permissions as needed. Permissions are categorized into different levels based on associated level of risks, and approval mechanisms are implemented with reference to the level of access. Requested permissions are automatically granted to the employee once approvals are provided by authorized personnel. All access requests are required to be approved at least by the user's supervisor, who cannot be the same person as the requestor to

	ensure segregation of duties. Access to network devices and servers is classified into three types by Alibaba Cloud according to the risk levels, namely normal users, application administrators and system administrators. Approval workflow is pre-set within the permission management system according to the type of access. Approvers in the workflow is determined based on system owner information and application owner information stored in the respective systems.
Privileged Account Management	Customers It is Customers' responsibility to limit and tightly control elevated privileges of their employees. Customers should ensure administrators should either have two accounts: one for administrative use and one for general purpose, non-administrative tasks, or if they only have one account, then their administrative privileges are granted on a needs-basis. Customers are capable to grant diverse and privileged permissions to a single identity or a group of identities using RAM. Customers can grant the least privilege to prevent execution of privileged commands by non-privileged users such as disable, circumvent, or alter implemented security safeguards or countermeasures implemented on cloud. By using Bastionhost, Customers are capable to configure control policies such as command control, command approval, protocol control, and access control policies so as to manage the access of users to hosts. Customers can ensure commands are executed with valid reasons and required administrators' prior approvals. In order to restrict privileged account activities, in particular, to prevent unauthorized downloading or transmission of confidential data from database administrators, Customers can manage the permissions granted to those accounts using Alibaba Cloud DMS hence to revoke and reset the database access permission if needed. Stringent authentication controls should be enabled for privileged accounts, such as MFA activated for RAM accounts with privileged/administrative permissions, and privileged access to high-risk systems as identified in the

	cyber risk assessment(s) via Bastionhost. To ensure accountability, the operation events performed by RAM users that have the administrator permissions can be tracked and recorded by ActionTrail, such as a creation or deletion of a user group by a RAM user. Customers can also audit the video session recorded by Bastionhost for the purpose of review on execution of privileged functions. Alibaba Cloud Privileged access is strictly controlled by Alibaba Cloud. Root privileges are restricted to authorized personnel only. Password for root accounts is automatically rotated on a monthly basis via a scheduled job. Privileged sudo to root activities are logged and monitored.
Access Reviews	Customers RAM Alibaba Cloud offers RAM service, which customers can generate and download a RAM user credential report that contains the credential details such as user creation time, user last logon time of the Alibaba Cloud account and RAM users under the Alibaba Cloud account. By reviewing the credential reports, users can detect for the presence of unauthorised users. Alibaba Cloud Audit and monitoring rules have been defined within the access monitoring system to analyze usage of accounts and access permissions, detect potential misuse of access privileges, and generate automated alerts to notify the Security Team of any deviations or exceptions. The Security Team is responsible for following up on the alerts and take appropriate actions. In addition, a schedule job is run to identify access permissions that have not been used by users for a consecutive 90 days and send out automated emails for the associated users to confirm whether the captured access permissions are still required. Access permissions will be automatically revoked if the access permissions are confirmed to be not needed, or if no confirmation is received within one week.

Physical Access Management	Alibaba Cloud Alibaba Cloud is responsible for the physical security of all its data center facilities. Data centers are configured with strict access control such as access card and fingerprint requirements, equipped with surveillance systems covering all the areas and passages, and staffed with security guards for 24x7 patrol. Alibaba Cloud has established policies and procedures around Physical and Environmental Security Management, to regulate access security management and environmental controls. An access card system is used for access management in each data center. Only authorized Alibaba Cloud employees and entitled data center service providers personnel are granted access to the access card system. At each Alibaba Cloud data center, long-term access permissions are assigned only to corresponding maintenance personnel. If there is a need for any other person to enter the data center, the person must submit application in advance, and is granted temporary permission only upon the approval of the corresponding data center managers. Data center managers are required to notify the data center service providers' personnel of the person's identity. For each entry to or exit from the data center, such person must display his or her ID and be escorted by the data center's maintenance personnel for the entire duration of the visit. On a monthly basis, data center managers perform access reviews to ensure that user access rights in the access card system are appropriate.

Domain 4 - Network Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the IT Network Management.

- 4.1 IT Network management

Key Aspects	Consideration
Policies and Processes	Customers Customers are responsible to establish network security management policies and processes covering areas including network access, network protection, configuration and vulnerability.

	Alibaba Cloud In terms of network access management, Alibaba Cloud has established Alibaba Cloud Network Security Management Policy, which requires the production and non-production environments to be segregated and fallen into different network security domains. For configuration management, Security team has established configuration baseline standards which specify baseline requirements for operating systems (OSs), database management systems, authorized personnel, prior to execution of the audit work. And for vulnerability management, Alibaba Cloud has established Emergency Response Standard of Security Incidents to regulate security vulnerability management, including classification of security vulnerabilities and response mechanism.
Network Access Management	Customers It's the customers' responsibility to implement proper network access control (NAC) and adopt strong authentication for critical network asset. Customers can make use of the network access control list (NACL) and CFW to implement NAC. Customers can configure outbound and inbound access control policies for the internet firewall and monitoring the network flow through CFW. Moreover, a VPC firewall can be deployed to manage the traffic between VPCs. Customers can configure access control in the internet firewall, VPC firewall and internal firewall and monitor the real-time traffic of cloud assets between the internet, VPC and internal network. Customers should implement technical controls to prevent unauthorised devices from connecting to internal networks, as well as unauthorised addition of new external connections and removal of existing connections. Tools should be installed to block access attempts by unregistered devices to internal networks. Tools and processes should be in place to block attempted access from unpatched employee-owned devices and

	unauthorised devices. Authorized personnel of customers must pass two-factor authentication based on domain account name, password, and dynamic digital token received on registered devices to access different services on Alibaba Cloud. Alibaba Cloud allows customers to extend the NAC measure tool to multiple network security devices and network management tools. NAC can enhance access control by preventing unauthorized devices from connecting to internal networks and block access attempts by unregistered devices. It also prevents unauthorized actions such as adding or removing external connections. Security controls should be implemented for remote access to all administrative consoles, including restricted virtual systems. Wireless network environments should be protected with perimeter firewalls that are configured to restrict unauthorised traffic, while encryption should be adopted with encryption keys frequently changed. VPN Gateway allows IPSec-VPN connection between customers and an authorized customer gateway to form an IPSec tunnel so that only authorized parties/devices are allowed to access to VPC. For customers deploying SSL-VPN, they can establish a ClassicLink connection between VPN Gateway and VPC and configure security group rule by entering the private IP address that is allowed to access. By integrating VPN Gateway with Identity as a Service (IDaaS), customers can enable the two-factor authentication (2FA) to ensure only authorized personnel can access to VPC remotely. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Network Security Management Policy, which requires the production and non-production environments to be segregated and fallen into different network security domains.
Network Protection	Customers Customers are responsible to perform network planning include cloud-based network architecture design, configure network connection between on premises and cloud networks, network interconnection and isolation between branches, and private network access between enterprises in the

	cloud. Customers should ensure own network should be segmented in multiple, separate trust or security zones with defense-in-depth strategies to mitigate the risk of cyber attacks. VPC Alibaba Cloud offers different cloud-based network solutions, for example, customers can create an independent VPC for each network partition. In each VPC, different vSwitches are created to handle different business requirements. VPC instances are logically isolated from another VPC instance. Customers can create a VPC for the production network and another VPC for the non-production network so that they are isolated from each other to achieve logical network segmentation. Different business systems, or different VPCs, can communicate with each other by using Cloud Enterprise Network (CEN). To meet the dedicated requirements of customers, customers can configure custom settings such as route table isolation, route filtering, and routing policies as needed. The following network partitions are commonly used: - Production and testing: The resources in the production environment and test environment are deployed in two partitions. - Internet facing: This partition is similar to the DMZ in a data center. Internet egress resources, such as elastic IP addresses (EIPs), network address translation (NAT) gateways, Server Load Balancer (SLB) instances, and CFW, are deployed in this partition. - Business-to-business: The external firewall or other protection devices in the intrusion detection system (IDS) or intrusion prevention system (IPS) in the cloud are deployed in this partition. - Internal Operating and Maintenance (O&M): The resources that enterprise employees use to connect to Alibaba Cloud are deployed in this partition. These resources can be jump servers and bastion hosts. - Internet access: The resources that are used to connect to external environments, such as third-party data centers, are deployed in this

	partition. ECS A security group is a virtual firewall provided by Alibaba Cloud for ECS instances. It provides Stateful Packet Inspection (SPI) and packet filtering functions, and can be used to isolate security domains between ECS instances (or container clusters in Container Service) on the cloud. Security groups are logically isolated groups of instances that are located within the same region and share the same security requirements while also being mutually accessible. Security groups are used for NAC over one or more ECS instances. As an important means of security isolation, security groups logically isolate security domains on the cloud. CFW Alibaba Cloud CFW is the industry's first firewall as a service (FWaaS) solution targeted for public clouds. It centrally manages control policies for the access traffic from the Internet to ECS instances (Internet traffic), and provides micro-isolation policies for the access traffic between ECS instances (intranet traffic). This is because in a cloud environment, users not only need to manage boundaries between the Internet and the intranet, but also need to manage network boundaries between cloud products, between VPCs, and even between ECS instances. With CFW, users can analyze Internet and intranet traffic, gain full visibility into network-wide traffic such as traffic between security groups and Internet access traffic, and analyze and block external connections. Based on traffic analysis, CFW provides isolation and control at all levels of the entire network, including centralized control over public IP addresses, domain name-based access control, VPC-based isolation, and isolation of leased lines between Alibaba Cloud and on-premises data centers. CFW also integrates IPS and threat intelligence capabilities for intrusion detection and analysis. By default, CFW can also store network traffic and security event logs and firewall operation logs for six months. Anti-DDoS

	Alibaba Cloud provides an Anti-DDoS solution that can mitigate transport layer DDoS attacks which detects attacks using forged source IP addresses to enter to Customers' internal network continuously and block the attack. Alibaba Cloud secures all data centers with a self-developed Anti-DDoS service that provides protection against all types of DDoS attacks. It uses an AI protection engine to accurately identify attack behaviors and automatically load protection rules, ensuring network stability. Alibaba Cloud Anti-DDoS allows users to monitor risks and protection status in real time through security reports. Alibaba Cloud Anti-DDoS not only supports mitigating DDoS threats for users' business on Alibaba Cloud, but also allows them to use Alibaba Cloud's globally distributed scrubbing centers and AI protection engine for on premise businesses, in order to mitigate high-volume DDoS attacks and provide fine-grained protection against resource exhaustion attacks at the web application layer. Web Application Firewall (WAF) WAF filters out a large number of malicious access attempts by defending against common security threats reported by OWASP, such as SQL injection, XSS, common vulnerabilities in Web server plug-ins, Webshell uploads, and unauthorized access to core resources. This prevents website asset leakage, thus safeguarding website security and availability. Alibaba Cloud The network area on Alibaba Cloud is generally divided into three layers from the outside to the inside in a hierarchical manner: - Layer 1: Region and zone - Layer 2: VPC - Layer 3: Subnet and resource perimeter Alibaba Cloud isolates production networks from non-production networks. Direct access from a non-production network to any servers and network devices in a production network is not allowed. Alibaba Cloud isolates the cloud service network that provides services to external users from the physical networks that supports the underlying cloud service functionalities.

	Network ACLs are configured to prohibit access from cloud service network to physical network. Alibaba Cloud also takes network control measures to prevent unauthorized devices from connecting to the internal network of the cloud platform and prevent the physical servers of the cloud platform from initiating external connections. Alibaba Cloud deploys Bastion Host on production network boundaries. The O&M personnel in the office network can access the production network for O&M only through Bastion Host. When logging on to Bastion Host, O&M personnel must perform MFA, namely a one-time password is required apart from the regular domain account name and password. Bastion Host uses advanced encryption algorithms to ensure the confidentiality and integrity of data transmitted through O&M channels. To provide network connections for ECS instances, Alibaba Cloud connects the instances to the Alibaba cloud virtual network, which is a logical structure built on top of the physical network structure. All the logical virtual networks are isolated from each other to prevent the network traffic data from being snooped or intercepted by other malicious instances. Alibaba Cloud provides security groups to control access for ECS instances. ECS instances in different security groups cannot communicate with each other by default, while security group rules can be configured to control network access over ECS instances.

Domain 5 - IT Asset Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the IT asset management.

- 5.1 IT asset management

Key Aspects	Consideration
IT Asset Management Process	Customers Customers are responsible to maintain an inventory of the IT assets to facilitate assessment of whether appropriate cybersecurity safeguards based on their data classification and business value and are at the level of

	granularity deemed necessary are in place. Customers should assign accountability and implement tools and processes to enable tracking, updating, asset prioritizing, and custom reporting of the IT asset inventory. Customers can use SDDP to perform sensitive data detection to facilitate data classification by scanning, classification, and grading on structured and unstructured data. Customers can control the security risks and optimize relevant security policies based on the information displayed in the SDDP console to implement cybersecurity safeguards on IT assets. For example, the SDDP console displays the storage objects that contain sensitive data, visitors that access data, and anomalous data flows and activities. Customers should implement tools and processes to detect and block unauthorized changes to software and hardware, with alerts generated on malicious activities for follow-up. Cloud Config can be used to monitor and continuously evaluate the Alibaba Cloud resources. Customers can retrieve the configurations of resources and hence track the changes and compliance of configuration to supported cloud services. Controls should be implemented to detect shadow IT or IT applications that are acquired and used without having undergone proper governance and approval procedures. In this case, customers can configure an application whitelist in Security Center, which only allows authorized software to run to prevent unauthorized and malicious applications (shadow IT) to realize Endpoint Detection and Response (EDR). Customers should create a documented asset life-cycle process to limit cybersecurity risks. Such process should include the cybersecurity safeguards implemented on assets to be acquired and management of end-of-life (EOL) systems. The IT asset inventory and the identification of critical IT assets should be reviewed at least annually to address new, relocated, re-purposed, and sunset IT assets. Moreover, the supply chain risk should be reviewed before the acquisition of mission-critical information systems. Alibaba Cloud identifies, inventories, classifies, and manages information assets to ensure an appropriate level of protection over the information assets in the Alibaba Cloud environment that are used to render cloud

	services. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Information Assets Security Management Policy to regulate the identification, classification and management of information assets. *Resource Management* Users can access to Resource Management for an overview for all resources purchased under the Alibaba Cloud accounts owned by the enterprise. *DMS* DMS offers centralized platform for customers to manage their database and information assets. Data classification services offered in DMS for customers' data assets can help to identify the security level of data (confidential, sensitive and internal) according to the rule configured by security administrator in DMS.
IT Asset Inventory Checking	Customers Customers are responsible to conduct regular IT asset checking to certify the integrity of inventory records based on the information provided by cloud products. Customers should implement tools and processes to detect and block unauthorised changes to software and hardware, with alerts generated on malicious activities for follow-up. Cloud Config can be used to monitor and continuously evaluate the Alibaba Cloud resources. Customers can retrieve the configurations of resources by calling API operations by sending HTTP GET requests to the Cloud Config endpoint and hence track the changes and compliance of configuration to supported cloud services. Customers can make use of Alibaba Cloud's Resource Management to have an overview for all resources purchased under the Alibaba Cloud accounts owned by the enterprise. Besides, Alibaba Cloud offers DMS. DMS offers centralized platform for

	customers to manage their database and information assets. Customers can view the complete list of databases owned in the Database List tab. Alibaba Cloud Alibaba Cloud has established a configuration management database (CMDB) for maintaining information assets related to cloud services. Each inventoried information asset is assigned to an asset owner. Changes to the information asset inventory are also tracked in the database in real-time basis. Besides, Alibaba Cloud has also established a data security platform to maintain data, including information on retention period, classification, and security level. Approvals are triggered when changes to data classifications are attempted.
Information Asset Inventory	Customers Customers are responsible to maintain an inventory of information assets with proper classification based on the information provided by the cloud products. Customers can make use of Alibaba Cloud's Security Center to gain an overview for IT assets such as servers, containers, cloud resources, websites and software Alibaba Cloud Alibaba Cloud has established a CMDB for managing the assets related to cloud services. All inventoried assets are assigned to an asset owner, and the assignment of assets to each asset owner is documented in CMDB. In this CMDB, all the history of the changes to the entries in the inventory will be maintained. Alibaba Cloud also establishes Procurement Guideline to regulate equipment acquisition and deployment procedures. The following policies has been established by Alibaba Cloud to govern the procedure of new product development and change management: - Alibaba Cloud System Acquisition, Development, and Maintenance

	Management Provision; - Alibaba Cloud New Service and Major Service Change Management Provision; - Alibaba Cloud Information Service Change Management Provision; - Public Cloud Change Management Guidelines; and - Alibaba Cloud Management Policy of Information Service Configurations and Assets.

Domain 6 - Business Continuity Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Business Continuity Management, including Business Continuity Management and Disaster Recovery.

- 6.1 Business Continuity Management

Key Aspects	Consideration
Policy and Procedure	Customers Customers are responsible to establish an effective business continuity management framework. The Board of Directors and senior management of customers are responsible to hold ultimate responsibility for business continuity planning and the effectiveness of their BCP. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Business Continuity Management Policy and Alibaba Cloud Information Technology Management System Manual to govern business continuity management. The policy defines roles and responsibilities for relevant parties, business continuity management operation model, business continuity management policies, risk tolerance level, business continuity management objectives, business continuity management evaluation and improvement, and management's responsibilities in resource management and personnel

	training.
Business Impact Analysis (BIA) and Risk Assessment	Customers Customers are responsible for own risk identification by conducting business impact, analysis and risk assessment to identify possible scenario of disruption, assess the impact and likelihood and determine the recovery objectives based on own scenario. Alibaba Cloud Alibaba Cloud initiates the BIA process by sending out questionnaires to departments that support critical business processes. The questionnaire covers information such as relevant laws and regulations, BIA factors, impacts to business operations due to disruption of services, maximum tolerable period of disruption, recovery time objectives, minimum service level, and resources requirements. Alibaba Cloud also sends out the Alibaba Cloud Risk Assessment Questionnaire to departments that support critical business processes to initiate the Risk Assessment process. As part of the risk assessment, threats that may cause disruption to Alibaba Cloud's critical business operations are identified based on 4 defined categories of threat, including Personnel and management, physical environment, technology and natural environment. Alibaba Cloud's business continuity management team performs BIA and risk assessment on an annual basis, including identification of critical business processes, maximum tolerable period of disruption, recovery time objectives, minimum service levels and time needed to resume services. Results of the BIA and risk assessment are documented in the Alibaba Cloud business continuity management - BIA, Risk Assessment, and Strategy Report. Threats that may cause disruption to Alibaba Cloud's critical business operations are identified and documented, and corresponding strategies are developed for different scenarios of disruptions.
Communication	Customers

	Customers are responsible for communicating with affected and concerned parties in the event of a major operational disruption based on the information provided by Alibaba Cloud. Customers should identify relevant parties in the event of a major operational disruption and establish own communication protocol and communication channel to communicate with the identified parties. Alibaba Cloud Alibaba Cloud has documented the procedures for internal communications and for communicating with relevant external parties in the event of a major operational disruption in the BCPs and Incident response procedures. Alibaba Cloud has established the communication with customers via management console, email and text message, to notify customers of any event that may have an impact on them.
Testing	Customers Customers are responsible to ensure regular testing on BCP will be conducted and establish a procedure for continuous improvement of BCPs. Alibaba Cloud Alibaba Cloud conducts testing of the BCPs established for Alibaba Cloud critical services and operations at least once a year. If there is any discrepancy identified between the plan and the drill test result, responsible parties will assess the test result and re-perform the drill until the result is successful. Alibaba Cloud also conducts testing of data center BCPs with data center service providers at least once a year.
Training and Awareness	Customers It is the customers' responsibility to provide annual cybersecurity training includes cyber incident response, current cyber threats, and emerging issues. Alibaba Cloud

	Alibaba Cloud establishes Alibaba Cloud Security Management Policy of Human Resources to regulate the requirement of information security awareness training for new employees and third-party personnel. Information and data security online training and assessments are required to be completed by all existing employees on an annual basis. Professional training includes skill sharing across teams via an online learning platform; offline training and communication meetings held by internal and external senior experts are available to employees.
Crisis Management	Customers Customers are responsible for own crisis management, including setup a crisis management team, deploy a detection mechanism and establish recovery strategies for managing crisis. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Emergency Response Plan (ERP) to define classification of emergencies, roles and responsibilities, process workflow and resource management for emergency response. Incident response procedures have been established under Alibaba Cloud ERP to detail the roles and responsibilities, process workflow, recovery time objectives and escalation and notification process in the event of incidents as related to critical operations and services, network, and IDC infrastructure. Alibaba Cloud has also established incident response procedures to detail the roles and responsibilities and process workflow in the event of IDC incidents. Contingency plans have been developed to address different scenarios of interruption to IDC, including fire, network interruption, emergency power outage, and natural disasters.
Updating BCP	Customers Customers are responsible to ensure their BCPs are reviewed on a regular basis.

Audit and Independent Reviews	Customers Customers are responsible for engaging qualified and independent parties to conduct independent assessment on the business continuity process. Customers should ensure the assessment is effective, including inviting the assessor to observe testing and reviewing the assessment result by management. Alibaba Cloud Independent audit is conducted by external auditor over Alibaba Cloud's controls in accordance with applicable auditing standard on at least an annual basis to ensure Alibaba Cloud is providing secure, capable and reliable services to customers. Alibaba Cloud maintains an effective BCP in accordance with ISO 22301 with independent audit by third party conducted at least on an annual basis. The certificate of ISO 22301 is available to customer to download from Security & Compliance Trust Center on Alibaba Cloud official website.
Insurance Consideration	Customers It is the customers' responsibility to purchase insurance to cover the potential loss during the service interruption.

- 6.2 Disaster Recovery

Key Aspects	Consideration
Alternate recovery site	Customers Customers are responsible to ensure operation can be switched over to available site during disruption by implementing appropriate measures, for example, through multi-zone deployment or setup alternative site arrangement. Where alternative site arrangement is decided, customers are responsible to manage and monitoring own alternative site arrangement. Alibaba Cloud

	Alibaba Cloud offers high available cloud computing infrastructure by setting up cloud data centers across multiple regions and zones globally to ensure cloud products and services are highly available and provide multi-replica data redundancy. Besides, Alibaba Cloud provides different solution to customers to complement their business continuity and disaster recovery planning. Customer can deploy cloud systems across regions and zones to implement a high availability architecture, such as zone active-active architecture, geo-disaster recovery architecture, active geo-redundancy architecture, and disaster recovery architecture that spans three data centers across two regions. In case of failure in the primary zone, the system immediately switches the workloads to another zone.
System Backup	<u>Customers</u> Customers are responsible to utilize the highly available and multi-replica data redundancy features offered by Alibaba Cloud's products to ensure vital records are available and accessible in the event of disruption. SLB is a load balancing service that distributes traffic among multiple ECS instances. It improves the service capabilities of applications. Customers can use SLB to prevent single points of failure (SPOFs) and improve the availability of their applications. SLB is designed with full redundancy to avoid SPOFs, and supports zone-disaster recovery. By integrating with Alibaba Cloud DNS, SLB can achieve geo-disaster recovery with an availability of up to 99.95%. SLB supports auto scaling based on application workloads and provides continuous services even when traffic fluctuates. SLB is available in multiple zones in most regions to achieve zone-disaster recovery objectives. If the primary zone becomes unavailable, SLB can switch its service to a secondary zone in as little as 30 seconds and resume provisioning services. After the primary zone recovers, SLB would automatically switch back to the primary zone. The SLB service inspects the health status of your ECS instances. If an

	ECS instance is found in an abnormal state, the service will isolate the instance by not forwarding traffics to it until it recovers. In this way, SLB eliminates SPOFs and improves the service capabilities of applications. Alibaba Cloud provides the layer-4 and layer-7 load balancing services. Layer 4 service uses an optimized and customized version of the open source software Linux Virtual Server (LVS) and Keepalived to achieve load balancing. Layer 7 service uses Tengine, a web server project based on Nginx, to achieve load balancing. When combined with Alibaba Cloud Security, SLB can defend against DDoS attacks in near real time. Additionally, the Layer 7 load balancing service provides the ability to defend against HTTP/S Flood attacks. Alibaba Cloud Alibaba Cloud offers ECS which allows customers to back up system disk or data disk with snapshot manually or automatically so that customers can roll back a disk to a previous state with a corresponding snapshot when incident happen. Else, customers can also back up image that contains all the data from one or more disk (a system disk or both system and data disk) so that the image can be used to create an ECS instance with the same operating system and data environment when incident happens. ECS Images can be copied across different regions for remote backup through the image copy function of ECS.
Data Backup	Customers Customers are responsible to ensure the communication and processing capability of alternative site for operation recovery by setting up adequate telecommunication facilities and pre-installed network connections. Alibaba Cloud Alibaba Cloud employs distributed storage. Files are split into multiple data segments and stored on different devices. Each data segment is stored in multiple replicas. Distributed storage improves data reliability and security. Based on product types/tiers and business needs, Alibaba Cloud products also provide multiple protection capabilities such as multi-copy redundancy,

	system backup, live migration, load balancing, and anti-DDoS to ensure high data availability. Critical Alibaba Cloud system components are backed up at full at least twice a week and are replicated across multiple Availability Zones. Backup restoration procedures are in place. Critical Alibaba Cloud system components are restored on a monthly basis and reconciliation is performed automatically for data integrity check. Backups of critical Alibaba Cloud system components are monitored by the system. In cases of backup errors or failures, a full backup is automatically triggered until the backup is completed successfully. ECS ECS supports full and incremental system disk or data disk backup with snapshot manually or automatically so that users can roll back a disk to a previous state with a corresponding snapshot. ECS also allows to backup image that contains all the data from one or more disk (a system disk or both system and data disk) so that the image can be used to create an ECS instance with the same operating system and data environment when incident happens. Apsara DB for RDS RDS supports data and log backup to ensure users can restore their database when incident or disaster happens. RDS supports automatic and manual backup. When users specify automatic backup, RDS will perform full physical backup automatically. RDS also supports manual backup, so that users can specify the following policies: full physical backups, full logical backups, and single-database logical backups. Alibaba Cloud offers Apsara DB for RDS that allows cross-region disaster recovery backup service is supported by RDS instances for designated High-availability Editions. Besides, Alibaba Cloud offers OSS that allows remote backup for data stored in OSS through the purchase of cross-region data duplication

	services. Data Backup Service (DBS) Also, DBS supports full and incremental for logical and physical backup method. Logical backup is performed by backing up database objects such as tables, indexes, and stored procedures while physical backup is performed by backing up database files on the operating system.

Domain 7 - Incident Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Incident Management.

- 7.1 Incident Management

Key Aspects	Consideration
Policy and Procedure	Customers Customers are responsible to maintain an incident management program covering incident identification, reporting, classification, handling, notification and recording. Alibaba Cloud Alibaba Cloud has established Emergency Response Standard of Security Incidents to regulate incident management, classification of incidents and response mechanism including requirements on response time and corresponding solutions according to incident levels. The following policies are established to govern the incident management: - Emergency Response Standard of Security Incidents; - Malfunction Management Standard; - Incident response procedures Alibaba Cloud security team is responsible to initiate the incident response process and follow the standard protocols.

Incident Communication and Reporting	Customers It's the customers' responsibilities to identify, document and communicate the incident communication and reporting requirements to relevant parties. Customers are responsible to establish procedures to comply with the communication and reporting requirements. Alibaba Cloud Alibaba Cloud will respond to security incidents and vulnerabilities as soon as they are discovered. The incident response team will first verify the authenticity of the reported vulnerabilities and security incidents. Once the vulnerabilities and security incidents are confirmed, Alibaba Cloud security team will initiate the incident response process and follow the standard protocols to confirm the security severity level and impact scope of a vulnerability. The response team will ensure resources are properly allocated so that the vulnerability can be fixed, and the affected Alibaba Cloud product can be brought online within the corresponding SLA time. The incident response team will also promptly notify users of security issues through online announcements. Alibaba Cloud has established multi-channel communication to announce malfunctions that could impact customers, including Alibaba Cloud official website, station letters, SMS, e-mails and DingTalk messages. Short Message Service SMS, as a communication channels, supports users to deliver their designated messages when incident happens to designated parties by pushing notification through SMS. Direct Mail Direct Mail also allows users to inform the relevant parties of the key facts relating to the incidents through batch emails.
Testing of Incident	Customers Customers should be involved in the design and execution of

Response Plan	comprehensive test cases so as to obtain assurance that recovered systems function accordingly. Customers should also participate in disaster recovery tests of systems hosted overseas. Periodic testing and validation of the recovery capability of backup media should be carried out and assessed for adequacy and effectiveness. Alibaba Cloud Alibaba Cloud conducts testing of data center BCPs with data center service providers at least once a year to verify the effectiveness of IDC contingency plan.

Domain 8 - Vulnerability Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Vulnerability Management.

- 8.1 Vulnerability Management

Key Aspects	Consideration
Vulnerability Assessment	Customers Customers are responsible to utilise the vulnerability scanning features supported by Alibaba Cloud's products to identify and prioritise security vulnerabilities in the systems regularly. Alibaba Cloud offers Security Center Service that allow the customers to perform vulnerability scanning and fixing. Security Center then generates alerts for vulnerabilities, baseline risks, security event, and AK pair leakage. Security Center also allows users to add applications that run on their servers to an application whitelist. Security Center identifies applications as trusted, suspicious, or malicious based on the application whitelist to prevent unauthorized applications from running. Customers may also use Cloud Security Scanner (CSS) provided by Alibaba Cloud to schedule automatic task or create a manual task to perform vulnerability scanning on web applications before the applications

	are launched or undergo significant change. Moreover, Alibaba Cloud provides Container Registry which allows customers to perform security scanning on all Linux-based images to identify vulnerabilities in four levels: high, medium, low and unknown. Customers can manually scan the images or configure an automatic scanning task that permits Container Registry to perform periodic vulnerabilities assessment. By doing so, users will receive recommendations, including specific remediation guidance, from Container Registry to discover, remediate hidden vulnerabilities and escalate to relevant parties. Alibaba Cloud In Alibaba Cloud, vulnerability scanning systems are utilized internally to perform daily scans for security vulnerabilities in the cloud environment. The scanning results are submitted automatically to the security vulnerability management platform. Security incidents, vulnerabilities and threat are reported and detected via multiple channels, including internal reporting, externally reporting, subscription from external threat intelligence sources, and internal detection via scanning. Security incidents, vulnerabilities and threats are gathered into the security incident and vulnerability management platform. Security team reviews the incidents and vulnerabilities on a daily basis and appoints appropriate personnel for resolution.
Penetration Testing / Red Team Testing / Scenario-based Testing	Customers Customers are responsible to conduct testing, by creating testing tasks, on assets to identify vulnerabilities in business processes and technical controls. Customers are also responsible to ensure testing will be performed before asset changes are applied in production. Nevertheless, customers are responsible to determine the coverage of testing scope and use the testing results to enhance their secure coding practice and cybersecurity management. Alibaba Cloud security team can perform comprehensive blackbox tests on

	users' systems. The Alibaba Cloud security team will customize test plans and use cases for target test systems based on the penetration testing experiences and standards of Alibaba Cloud to help customers detect security flaws and vulnerabilities. This protects enterprises against cybersecurity threats. The penetration testing service targets business systems, web applications, mobile apps, and network/IoT/smart devices. Additionally, penetration testing professional edition provides customers with tailored test plans that exploit techniques such as social engineering, Web 2.0 vulnerabilities, and zero-day vulnerabilities in open-source software. Alibaba Cloud To ensure the effectiveness of the incident response process, Alibaba Cloud has set up a dedicated team to conduct attack drills from time to time. Alibaba Cloud also regularly invites third-party teams to conduct penetration testing on the Alibaba Cloud platform to verify the effectiveness of the Alibaba Cloud security protection system and the reliability of the incident response process.

Domain 9 - System Development Life Cycle (SDLC)

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the SDLC.

- 9.1 SDLC

Key Aspects	Consideration
SDLC	Customers Customers are responsible to establish a formal and appropriate SDLC process including checkpoints to assess security risks and identify mitigation strategies in different phrases of the SDLC. Using DevOps, customers can customize a process flow to standardize the change process. Code scanning tasks and testing can be

	created and added to a flow so that the development process will strictly follow the created flow. Following risk-based approach, vulnerabilities should be identified through code reviews and/or static code analyses for internally developed or vendor-provided custom applications to ensure that there are no security gaps before deploying into production. Apsara DevOps provides (1) scanning on sensitive codes such as API keys, in which the sensitive codes detected are classified into different criticalities to avoid sensitive codes. Besides, (2) Customers can customize scanning rules based on industry-standard or business or compliance needs and import them as code scanning tasks to help identifying and mitigating vulnerabilities. Further (3), DevOps provides a code hub to serve as a custodian for code hosting, review and scanning to protect corporate code assets. Bugs in codes would be auto-detected. Change controls and release management processes should be implemented for critical functions. DevOps (4) brings along with changes tracking, version control and quality inspection for achieving secure development. Security testing occurs in all post-design phases or activities of the SDLC for applications should be performed, and the security of both applications that connected to the internet and internal applications should be tested based on a risk-based approach against known types of cyber attacks before implementation or following significant changes. (4) Testing management is available in Apsara DevOps as well for executing tests through automation. It is achievable by establishing the test environment. Customers should identify scenarios and test cases, choose an appropriate automation tool. They are then capable to run test cases in the test environment and ultimately analyze results. In addition to code hosting, the pipeline feature provides flexible and continuous integration, verification, and release functions. Customers must make reference to the documented security criteria of the previous phase throughout the SDLC. The interdependencies between applications and services could then been identified and reviewed using pipeline release

	management. Some enterprises have a large network of application systems where the applications are closely coupled with each other and the systems are managed by different departments. In this case, manual investigation may cause omissions and it is difficult to completely review all application systems and identify the complex dependencies between systems. We recommend that these enterprises use Alibaba Cloud Application Discovery Service in cloud migration requirement assessment, cloud migration planning, and cloud-based environment construction. Application Discovery Service uses a non-intrusive data acquisition technology to build the architecture topology from the dimensions of host and process without affecting the performance of online services. It automatically analyzes and identifies hosts, processes, resource usage, and the dependencies between applications and components. Alibaba Cloud **Policies and Procedures** Alibaba Cloud establishes security development standards, including a variety of code development standards, which cover the process of design, development, testing and deployment of applications. **System Acquisition** Alibaba Cloud has established Alibaba Cloud System Acquisition, Development, and Maintenance Management Provision Policy to govern the procedure of system acquisition. **System Availability** Application Real-Time Monitoring Service (ARMS) is an end-to-end Alibaba Cloud monitoring service for Application Performance Management (APM) used to quickly develop real-time business monitoring capabilities using the frontend monitoring, application monitoring, and custom monitoring features provided by ARMS. Users can view the 3D topology graphs generated by ARMS agent. Health status of the applications and hosts will be displayed on the 3D topology graphs so that users can quickly locate incident indicator e.g., abnormal

	services, affected applications, and associated hosts to detect cyber incident. **Systems Development** Alibaba Cloud adopts Secure Product Lifecycle (SPLC) procedure, which is a solution tailored for cloud products, designed to integrate security into the entire product development lifecycle. With SPLC, a complete security development mechanism is put into place at each stage, from product architecture review, development, validation, all the way up to incident response, to ensure that the products meet the rigorous security requirements for cloud computing. **Systems Documentation** In Alibaba Cloud, application submission of configuration change, documentation and approval, are managed and logged in the change management platform. **Systems Testing** In the security validation stage of SPLC, the security team implements comprehensive security reviews on the architecture, design, and server environment of the product according to the security requirements, and also performs code review and penetration testing on the product. Any product with security problems found in this stage must be amended. Product team develops the product in accordance with the security requirements, and implement the relevant security features and requirements of the product. The product team also carries out self-testing at this stage to confirm that the security requirements have been implemented, and provides corresponding test information such as code implementations and test reports. **Systems Migration** Alibaba Cloud reviews security controls of internally developed software code before migrating to production.
Secure Coding Practice	<u>Customers</u> It's the customers' responsibility to establish secure coding practices with

	reference to industry standard. Vulnerabilities identified from vendor, security tools, penetration testing and vulnerability scanning should be considered when developing and updating such practices. Alibaba Cloud Alibaba Cloud has established security development standards, including a variety of code development standards, which cover the process of design, development, testing and deployment of applications. Alibaba Cloud has developed an internal source code repository to control changes made to the source code to ensure a high level of code security for Alibaba Cloud products. Alibaba Cloud's source code repositories are used to store source code and track changes in source code during development for version control. With the authorization management function, access permissions to the source code are properly managed based on the principle of least privilege. In addition, in the SPLC of cloud products, Alibaba Cloud security experts strictly review and validate the source code security. Alibaba Cloud also constantly performs code security scanning for software in Alibaba Cloud Marketplace to effectively manage security risks.
Secure Development Environment	Customers Customers are responsible to consider setting up development environments which have similar security controls implemented in production environment. Alibaba Cloud Apsara DevOps solution provides Git repositories for storing source code, and provides strict authorization control mechanisms. With the authorization management function, users can view their permissions on a specific Git repository or group. When users have authorization on a specific Git repository or group as a master or owner role, they can also view and modify the permissions of other members on the Git repository or group, and manage the permissions of other members based on the principle of least privilege. Alibaba Cloud

	Alibaba Cloud has segregated development, testing and production environments. Alibaba Cloud establishes a functional requirement document (FRD) and a detailed architecture diagram based on business requirements and technical frameworks and extract the security baseline requirements applicable to a product. In the secure development stage of SPLC, the product team must develop the product in accordance with the security requirements, and implement the relevant security features and requirements of the product. The product team also carries out self-testing at this stage to confirm that the security requirements have been implemented, and provides corresponding test information such as code implementations and test reports. In the SPLC of cloud products, Alibaba Cloud security experts strictly review and validate source code security to ensure a high level of code security for Alibaba Cloud products. Alibaba Cloud also constantly performs code security scanning for software in Alibaba Cloud Marketplace to effectively reduce security risks.
System Developed by Third Parties	Customers For system developed by third parties, customers should perform review on their security impact similar to the requirement for developing in-house. Authorized institutions should also maintain a list of the third parties service provider and consider implementing relevant security controls as recommended in the Third Party Management. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Information Service Availability Management Provision to ensure the availability and continuous effectiveness of information technology services meet customers' quality of service requirements. The policy defines roles and responsibilities of relevant parties and standards for availability management operations.

Domain 10 - Configuration Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Configuration Management.

- 10.1 Configuration Management

Key Aspects	Consideration
Baseline Configuration	Customers Customers are responsible to establish and enforce baseline system configuration and perform review regularly with respect to industry standard. Customers may make use of Cloud Config to track the configuration of supported cloud services such as ECS and WAF instances thus allowing customers to monitor the configuration of cloud resources continuously. Customers can configure rules to determine whether a resource configuration is compliant. A rule can be activated periodically or whenever there is configuration change. Therefore, once a rule is triggered, Cloud Config re-evaluates the resource and checks whether the configurations are compliant. If the resources to which the rule is applied are evaluated as non-compliant, remediation can be performed automatically by Cloud Config or triggered by users, in either way, the configuration of resources will change to the pre-set value according to the remediation template. Alibaba Cloud Security team has established configuration baseline standards which specify baseline requirements for OSs, database management systems, network devices and VM images. Configuration baseline standards are reviewed and updated at least once a year by the security team.
Configuration Change	Customers Customers are responsible to ensure any change to the configuration should follow change management process and utilising configuration monitoring features offered by cloud products to prevent unauthorized change of configuration on critical systems.

	Customers can make use of Security Center's configuration assessment feature to perform assessment on some specific configurations of cloud resources using pre-defined rules, for example, authentication and permissions, NAC, data security, log auditing, monitoring and alerting settings. Customers can then identify any configuration setting fails to meet the security baseline and detect if there is unauthorized change. Customers can also perform compliance evaluation on the configuration changes using predefined or customized rule(s). A rule can be activated periodically or whenever there is configuration change. Customers can also view the recent configuration change record via Cloud Config to detect any unauthorized configuration change of cloud resources. Application Configuration Management (ACM) supports querying and rolling back configurations that customers can view the configuration content of a specific version and detect authorized change to application configuration. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Management Policy of Information Service Configurations and Assets to govern the configuration management process. All configuration changes must be well planned, assessed, tested and authorized before deployment by following the Alibaba Cloud Information Service Change Management Provision. The change process is standardized and is supported by automatic systems and tools. Any changes need to go through a series of phases from application, evaluation, approval, test and implementation. Application submission of configuration change, documentation and approval, are managed and logged in the change management platform. All the changes are tested before being implemented. Nevertheless, Alibaba Cloud deploys an automatic configuration check tool to verify the configurations of infrastructure and information systems after a change in order to detect unauthorized configuration change.

Domain 11 - Change Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Change Management.

- 11.1 Change Management

Key Aspects	Consideration
Policies and Procedures	Customers It's the customers' responsibility to ensure that the change management procedures are formalized, enforced and adequately documented. Authorization and approval are required for all changes and the personnel responsible for program migration should be identified. For the purpose of accountability, proper sign-off should be adequately implemented where formal acknowledgement is obtained from all related parties. Tools to detect and block any unauthorized changes to software and hardware should be deployed. Hence, customers can make use of Cloud Config, which monitors and continuously evaluates the Alibaba Cloud resources. It retrieves the configurations of all resources by calling API operations of the corresponding cloud services and hence tracks the changes and compliance of configuration to supported cloud services. Further, Apsara DevOps allows customers to automate and streamline the change management process. Alibaba Cloud Alibaba Cloud has established a standardized change management process to ensure that all changes made to the cloud platform are recorded, evaluated, tested, approved, and where necessary, communicated prior to implementation into production following formal policies and procedures. An independent team has been set up to oversee the change management process, monitor compliance with the change management policies and procedures, and investigate on security incidents or malfunctions caused by uncontrolled changes. All changes that would affect the cloud operation, including changes to data,

	software and configuration, supporting infrastructure, hardware and network, need to go through a series of phases from application, testing, evaluation, approval, and implementation and finally to verification. Alibaba Cloud adopts a DevOps model to automate and streamline the change management process in order to deliver continuous services at higher velocity. Each of the stages of the change process is tracked via the change management system, with status of each stage recorded and supporting documentation retained. Changes are classified based on the degree of emergency as well as impact of potential system malfunctions. Changes are also managed by category based on their sources and targets, that based on the migration time, changes are categorized into normal changes and emergency changes. Normal changes are scheduled to be deployed during the pre-defined routine migration window, whereas emergency changes are deployed outside of the routine migration window or during the network block period. The following policies has been established by Alibaba Cloud to govern the procedure of new product development and change management: - Alibaba Cloud System Acquisition, Development, and Maintenance Management Provision; - Alibaba Cloud New Service and Major Service Change Management Provision; - Alibaba Cloud Information Service Change Management Provision; - Public Cloud Change Management Guidelines; and - Alibaba Cloud Management Policy of Information Service Configurations and Assets.

Domain 12 - Patch Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Patch Management.

- 12.1 Patch Management

Key Aspects	Consideration
Patch Management Process	High level responsibilities over patch management between Alibaba Cloud and customer have been defined in the Alibaba Cloud Security Whitepaper, which is publicly available for user entities on Alibaba Cloud official website. Alibaba Cloud secures its cloud platform from several aspects, including but not limited to: • protecting the security of hardware, software, and network of the cloud platform by means of OS and database patch management; and • identifying and fixing security vulnerabilities of the cloud platform in a timely manner without affecting customers' service availability. Meanwhile, customers who build cloud applications on Alibaba Cloud are responsible for protecting their systems by using the security features provided by Alibaba Cloud services and third-party security products in the Alibaba Cloud security ecosystems. Customers should harden the OS on their ECS instances and install security patches in a timely manner, while they do not need to maintain the underlying computing instances such as keeping the OS updated, hardened, or patched. Customers are responsible to establish a patch management programme in order to ensure software and firmware patches are applied promptly. <u>Customers</u> Customers are responsible to establish a patch management programme in order to ensure software and firmware patches are applied promptly. Customers should establish a formal patching process to acquire, test, and deploy software patches based on criticality and a follow-up process to classify and track actions based on priority to ensure timely closure. Systems maintained by customers should be configured to retrieve patches from the official sources in a pre-defined patch window with patch management reports reviewed to ensure the operational impact is evaluated, and such patches are tested and implemented within aggressive

	patch frames. Customers can enable the Virtual Patch function under advanced setting of intrusion prevention feature provided by CFW to receive hot patches at the network layer and automatically deploy the patches to protect cloud assets against high-risk vulnerabilities and emergency vulnerabilities that can be remotely exploited. Besides, customers can also view the latest information about the updates of security intelligence, virtual patches, and basic IPS policies that posted on CFW console to gain an overview for patch management. CFW uses an customer engine under the Virtual Patch function to automatically receive hot patches at the network layer and deploy the patches to protect cloud assets against high-risk vulnerabilities and emergency vulnerabilities that can be remotely exploited. Customizations for virtual patch policies are allowed, for example, to manually enable or disable certain patches based on criticality. Moreover, Container Service for Kubernetes (ACK) also offers customers with higher reliability and security clusters in large-scale production environments and thus allowing to deploy patches to simulated environments in advance of official deployment. Alibaba Cloud Alibaba Cloud ensures the security of hardware, software, and network of the cloud platform by means of OS and database patch management, etc. Alibaba Cloud will identify and fix security vulnerabilities through hotfix dynamical patching technology in a timely manner without affecting customers' service availability. Patches and security updates are assessed and tested before deploying to the production environment.
Patch Checking	Customers Customers are responsible to identify exceptions on configuration and patch handling of their cloud resources by utilising the scanning features and information provided by cloud products. Customers are then responsible to

	mitigate the exceptions in a timely manner or within the defined timeframe. Based on the self-developed cross-platform vulnerability scanning and repair engine of Alibaba Cloud, Security Center allows customers to scan multiple systems and applications, for example, Windows systems, third-party Linux versions for Alibaba Cloud, and mainstream CMS systems, and detect emergency vulnerabilities in systems or applications without relevant patches. Moreover, customers can add a custom software repository or software repository provided by Alibaba Cloud to Linux instances so that customers can search for and install software packages and update software applications in the repository manually. Alibaba Cloud Alibaba Cloud has deployed configuration scanning tool to scan configurations of operating systems, database management systems, network devices and virtual machine images. The scanning results are analyzed by the scanning tool and the analysis results are submitted automatically to the security incident and vulnerability management platform. Deviations from configuration baseline standards are detected and restored to the standard by operation personnel. The detection and restoration results are summarized into a weekly report for rectification. Besides, vulnerability scanning systems are utilized to perform a wide range of scanning tasks for security vulnerabilities in the cloud environment at least on a daily basis. The scanning results are submitted automatically to the security vulnerability management platform.
Remediation	Customers It's the customers' responsibilities to maintain the requirements and set timeframe for patch management. Customers are responsible to follow-up the non-compliant cloud resources when exception is identified. Alibaba Cloud Alibaba Cloud has established Emergency Response Standard of Security Incidents to regulate security vulnerability management, including

	classification of security vulnerabilities and response mechanism.

Domain 13 - Physical and Environmental Protection

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Physical and Environmental Protection.

- 13.1 Physical and Environmental Protection

Key Aspects	Consideration
Physical and Environmental Protection	Alibaba Cloud Alibaba Cloud implements environmental controls at data centers including heating, ventilation, and air conditioning (HVAC), lightning protection systems, fire detection and suppression systems, and power management systems. **Fire detection and response** For fire detection and response, Alibaba Cloud data centers are equipped with fire detection systems that utilize thermal and smoke sensors. The sensors are fitted to the ceiling and floor and give audible and visual alarms when triggered. Each data center is equipped with an integrated gas extinguishing system and fire extinguishers. Data center personnel also undergo fire detection and response training on a regular basis. **Power** For power supply, to achieve a 24/7 uninterrupted service, Alibaba Cloud data centers are powered by dual main supplies and redundant power systems. The primary and secondary power supplies and systems have the same power supply capabilities. In case of a power failure, redundant battery packs and diesel generators are enabled to power data center devices, thus allowing the data center to run continuously for a certain period of time. **Temperature and humidity** For temperature and humidity, Alibaba Cloud data centers are fitted with

	precision air conditioners to ensure constant temperature and humidity levels, which are electronically monitored. In case of any fluctuation in temperature or humidity outside of the normal range, an alarm is triggered and corrective actions are immediately taken. All air conditioning units work in hot standby mode. **Equipment Monitoring System** Nevertheless, an equipment monitoring system is utilized to monitor the environment of data centers and performance of servers. In case of any exception, an alert is triggered automatically by the system and Alibaba Cloud on-site operators will follow up with the data center service providers to resolve the issue. Alibaba Cloud adopts industry standards and best practices to safeguard customer data. Alibaba Cloud has received multiple industry standard certifications, including ISO27001, Service Organization Control (SOC) 1/2/3 and etc. and regularly complete third-party audits.

Domain 14 - Detection and Monitoring

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Detection and Monitoring.

- 14.1 Detection and Monitoring

Key Aspects	Consideration
Security Monitoring Processes	Customers It's important for customers to formally define and document, and consistently follow security monitoring processes and procedures. Documentation should be reviewed and updated to reflect changes in processes or procedures. Alibaba Cloud Alibaba Cloud has established Emergency Response Standard of Security Incidents to regulate incident management, classification of incidents and response mechanism including requirements on response time and

	corresponding solutions according to incident levels. Security monitoring in Alibaba Cloud mainly consists of three parts: log collection, anomaly analysis and detection, and alerting. Log collection aims to collect logs of hosts, networks, applications, and cloud products on the cloud platform, and import them into online real-time (such as Blink) and offline (such as MaxCompute) computing platforms. Anomaly analysis and detection aims to process and analyze the logs through security monitoring algorithms in each computing platform to monitor and identify risks. As such, all activities performed in production systems through bastion hosts are logged in real time. Monitoring rules are defined in various monitoring platform to perform automatic review of user activities and detect security events. Automated alerts are generated based on the review results and sent to security team for investigation.
Logging	Customers Customers are responsible for log management. For example, customers should ensure devices and logs are synchronized with a centralized and secured time source. In relation to this, Alibaba Cloud provides a Network Time Protocol (NTP) server to achieve synchronization local time of ECS instances thus making timestamp reliable. Customers should configure properly. Further, customers should also ensure audit log records and other security event logs are retained securely. Audit logs should be backed up to a centralized log server or media to prevent unauthorized changes and security logs for key systems and endpoints should be readily available for review with adequate retention period for incident response investigation. In view of this, logs collected by Alibaba Cloud's Log Service could be shipped to OSS for backup purposes. Customers can configure appropriate bucket policy to achieve the following: - By enabling Write Once Read Many (WORM) setting, no modification can be done to the concerned bucket thus prevent changes to

	security logs - Define retention period so that critical logs will be retained within the defined retention period to allow future investigation. Alibaba Cloud In Alibaba Cloud, all activities performed in production systems through bastion hosts are logged in real time and transferred to a central log management platform. The logs are retained for at least half a year and protected from modification or deletion. *Log Service* Alibaba Cloud provides Log Service as an observation and analysis platform that processes multiple types of data such as logs, metrics, and traces. Customers should review logs of physical and/or logical access following events. Log Service is able to perform manual and automated correlation analysis with SLS enabled. Logging practices and thresholds for security logging should be reviewed periodically to ensure that appropriate log management is in place. This could be done by using Log Service along with using ActionTrail. *ActionTrail* Alibaba Cloud ActionTrail provides centralized log management for cloud resource operations. The logon and resource access operations performed under each account are recorded. An ActionTrail record includes information such as the operator, operation time, source IP address, resource object, operation name, and operation status. The operation records stored by ActionTrail can be used for security analysis, intrusion detection, resource change tracking, and compliance audit. In a compliance audit, users may need to provide detailed operation records for Alibaba Cloud accounts and RAM users. The operation events recorded by ActionTrail can meet these compliance audit requirements. *OSS* Alibaba Cloud offers OSS that provides a secure and high-durability cloud

	storage service. Logs collected by Log Service could ship to OSS for backup.
Monitoring	Customers Customers are responsible to set-up their security monitoring mechanism by utilising the features offered by cloud products and ensure timely notification of potential security events will be delivered and reviewed by responsible personnel. Customers are also responsible to provide security monitoring reporting to their management and other audiences on a regular basis. Customers can make use of ActionTrail to monitor and record the actions performed by Alibaba Cloud and RAM account, including the access to and use of cloud products and services. Customers can either view the event records directly on the console of ActionTrail or monitored resource. Customers can also view access and activity logs that shipped from different sources e.g., ActionTrail, Security Center (network activity logs) and applications that are not deployed on Alibaba Cloud and perform analysis in SLS. With Realtime Compute, log records can be transformed so that customers can export the restructured log records from Log Services (SLS) to the security information and event management (SIEM) maintained by users or export logs to Elasticsearch (for real-time analysis) and Maxcompute (for offline analysis) that allow users to design scenario and create use cases to analyse and correlates logs from different sources for monitoring across the environment. Moreover, customers can use Dbaudit to deploy built-in or customised security rules to detect potential threat to database instances, for example, there are built-in rules to detect SQL injection, account security, data leakage and unauthorised operations. Once the security rule is violated, an alert will be generated to users thus customers can conduct investigation by reviewing logs (including operation logs). Besides, dbaudit also allows customers to review access and operation logs and there is regular system generated report which summarizing the security status of database instances (analysis based on SOX criteria) for customers' routine monitoring purpose.

	Alibaba Cloud Alibaba Cloud has installed intrusion detection software on servers to detect potential intrusion behavior. A network monitoring system is utilized to monitor network traffic and user operations in real-time and identify abnormal operations. The security team personnel will follow up on any abnormal operations identified by the network monitoring system and take necessary actions. In terms of security events and incidents, Alibaba Cloud's security incident management ensures secure operations and system protection through monitoring and detection of security events, as well as timely execution of proper responses to those events. Alibaba Cloud has established security incident response standards and guidance to regulate classification, escalation, and notification processes for security incidents. Alibaba Cloud conducts security monitoring on the cloud platform to detect security incidents where platform resources are attacked, and the security incident response process will be triggered to properly handle the incidents. Activities performed on the cloud platform are logged and imported into real-time and offline computing platforms. Logs are processed and analyzed through security monitoring algorithms in each computing platform for anomaly analysis and detection. The Alibaba Cloud security team is established for analyzing, tracking, and coordinating responses to incidents. The team reviews the results on the security incident monitoring platform to verify whether any of the events should be classified as security incidents. Confirmed security incidents will be notified and escalated to the appropriate teams for timely response based on criticality and severity levels of the incident. For security incidents that could impact customers, Alibaba Cloud would establish announcements on the Alibaba Cloud official website.
Security Information and Event Management	Customers Customers are responsible to establish security monitoring process and utilise the security detection, monitoring and alert features provided by cloud products to facilitate security monitoring. Customers are then responsible to

	decide and configure the monitoring mechanism supported by cloud products e.g., SLS through shipping and consolidating logs from other cloud resources to gain the capability to detect simultaneous attacks. Alibaba Cloud All activities performed in production systems through bastion hosts are logged in real time and transferred to a central log management platform. Monitoring rules are defined to perform automatic review of activities within the central log management platform. Automated alerts are generated based on the review results and sent to security team for investigation. Besides, Alibaba Cloud also monitors and responds to security incidents and vulnerabilities as soon as they are discovered through the external reporting channels include Alibaba Security Response Center (ASRC), Alibaba Cloud Crowdsourced Security Testing Platform, externally reported Common Vulnerabilities and Exposures (CVE) vulnerabilities of open source third-party components, and threat intelligence information from third parties. Security incidents, vulnerabilities and threat are reported and detected via multiple channels, including internal reporting, externally reporting, subscription from external threat intelligence sources, and internal detection via scanning. Security incidents, vulnerabilities and threats are gathered into the security incident and vulnerability management platform. Security team reviews the incidents and vulnerabilities on a daily basis and appoints appropriate personnel for resolution.
Security Monitoring Team	Customers It's the customers' responsibility to establish a qualified team for security monitoring, with roles and responsibilities clearly assigned in documents. Alibaba Cloud In Alibaba Cloud, the security team is responsible for analysing, tracking and coordinating responses to incidents. It reviews the results on the security incident monitoring platform to verify whether any of the events should be classified as security incidents. Security incident discovered are then notified and escalated to the appropriate teams for timely actions based on security

	incident's criticality and severity levels.

Domain 15 - Situational Awareness

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Situational Awareness.

- 15.1 Situational Awareness

Key Aspects	Consideration
Threat Intelligence	Customers It's the customers' responsibility to implement procedures to identify cyber threats of potential impact on business process or services. Such analysis should be performed regularly and the results should be applied into the cybersecurity posture. Customers can use Security Center that incorporates threat intelligence library developed by Alibaba Cloud to perform correlation analysis on access traffic and logs. Security Center is a unified security management system that identifies, analyzes, and produces alerts based on security threats in real time. With security capabilities such as anti-ransomware, anti-virus, tamper-proofing, and compliance assessment, users can automate security operations, response, and threat tracing to safeguard cloud and local servers and meet regulatory compliance requirements. Security Center provides threat detection capabilities based on threat intelligence. Based on the huge amount of network infrastructure data and threat intelligence gathered by Alibaba Cloud, Security Center performs protocol feature analysis, detects abnormal network and server behaviors based on machine learning, detects malicious domain names by domain generation algorithms (DGAs), and produces indicator of compromise (IOC) for use in the detection model. Based on the threat intelligence data, the service also integrates a server abnormal behavior detection model to

	detect suspicious processes and malicious activities from various perspectives. Customers can also leverage CFW with the built-in IPS that receives simultaneous updates of networkwide threat intelligence and detects and blocks threats from the Internet in real time. Alibaba Cloud Alibaba Cloud receives threat intelligence from various sources, including internal and external channels. Internally, Alibaba Cloud discovers possible security incidents through log collection, anomaly analysis and detection, and alert generation. The external reporting channels include ASRC, Alibaba Cloud Crowdsourced Security Testing Platform, externally reported CVE vulnerabilities of open source third-party components, and threat intelligence information from third parties. A self-developed threat monitoring platform is utilized to gather threat discovered internally or externally. The platform automatically pushes alerts to the security department personnel for review and follow-up.
Security Awareness Program	Customers It's the customers' responsibility to develop a security awareness program to enhance the security awareness of staff members. The program should be designed with different focus for different target groups covering new and existing staff. Apart from the traditional security subject matters, customers should continuously enhance the program, taking into consideration the subject matters such as newly developed technology and recent cyber-attacks. Customers may also consider requiring third parties which handle and/or process personal information or other sensitive data to complete such program. Alibaba Cloud Alibaba Cloud has established a training system as follows: – Internal product and industry training provided in the region to develop

	and equip personnel with relevant knowledge to work; – Professional cloud exams and relevant training are available to internal technical staff to maintain the technical competency; – Internal employees must participate in online training for information security awareness and take tests for code of business conduct and data security after on-board date; – Vendor employees must attend online training for information security awareness and pass online tests for code of business conduct and data security after on-board date; and – The security department communicates security awareness with employees on a monthly basis.

Domain 16 - Risk Management of e-banking

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Risk Management of e-banking.

- 16.1 Risk Management of e-banking

Key Aspects	Consideration
Security Controls	Customers It is the customers' responsibility to provide adequate assurances that transactions performed and information flowed through the electronic delivery channels are properly protected. Hence, a strong and comprehensive electronic banking security control system should be maintained to meet objectives such as authentication, non-repudiation, data and transaction integrity, segregation of duties, authorization controls, maintenance of audit trails, and confidentiality of sensitive information. Alibaba Cloud provides Alibaba Cloud Information Transmission Security Management Policy, which specifies security management requirements and measures for data transmission. All activities performed in production systems through bastion hosts are logged and transferred to a central log

	platform in real time. The logs are retained for at least half a year and cannot be modified. For logical access management, Alibaba Cloud launches Alibaba Cloud Access Control Management Policy. The policy requires that access be granted following least privilege principle, and be granted only upon business needs. The policy defines basic rules of segregation of duties by roles and functions at both managerial level and operational level according to company structure and product teams. Alibaba Cloud also establishes Alibaba Cloud Password and Key Management Policy to manage key generation, storage and usage, distribution, backup, replacement and revocation during the life cycle of cryptographic keys. Moreover, customers should ensure an appropriate level of application security and the security controls may involve the use of hardware and software tools and other security measures to deter unauthorized access to all critical electronic banking systems, servers, networks, databases and applications. The relevant control considerations may include: – Ongoing awareness of attack sources, scenarios, and techniques – Up-to-date equipment inventories and network maps – Rapid identification and mitigation of vulnerabilities – NACs over external connections – Use of intrusion detection tools and intrusion response procedures – Physical security of all electronic banking computer equipment and media. The security control system should be evaluated periodically to ensure continued effectiveness. Ongoing training at different levels of staff should also be provided in order to help them to have the necessary skills to comply with the security control system and to keep abreast of the technological and industrial advancements.

	In view of this, Alibaba Cloud offers the following controls to help customers in compliance with the guidelines: - Establishes Alibaba Group Endpoint Security Management Policy to regulate the installation of antivirus software, installation of authorized software only and patches update on user endpoint devices - Establishes a topology map for the production network and office networks showing the network architectures - Deploys configuration scanning tool to scan configurations of operating systems, database management systems, network devices and virtual images. The scanning results are analyzed by the scanning tool and the analysis results are submitted automatically to the security incident and vulnerability management platform. Deviations from configuration baseline standards are detected and restored to the standard by operation personnel. The detection and restoration results are summarized into a weekly report for rectification. - Requires authentication to external and temporary access to customer's Alibaba Cloud resources and is restricted based on customer configured authorization settings - Installs intrusion detection software on physical servers to detect potential intrusion behavior - Grants access rights to physical servers, network devices, and virtual machines to employees upon approvals by authorized personnel - Grants only authorized personnel with physical access rights to data center. On a monthly basis, Data center managers perform an access review for the access card system in data center. Customers can also provide easy-to-understand advice to their customers on electronic banking security precautions and oblige them of their responsibilities to take reasonable measures. <u>Alibaba Cloud</u> Alibaba Cloud has implemented an Information Security Strategy for information security management including the process and systems. The

	overall strategy for information security covers areas such as risk management, security strategy, information security organization, asset management, human resource management, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, etc. Alibaba Cloud also performs a comprehensive risk assessment considering factors regarding information security at least once a year and updates the security controls and related policies based on the assessment results.
Outsourcing	Customers It is the customers' responsibility to provide effective oversight of the service providers' activities to identify and control the resulting risks and to ensure that their outsourcing arrangements are in compliance with relevant statutory requirements. Customers should require service providers to implement security policies, procedures and controls that are at least as stringent as the authorized institutions would expect for their own operations. They should also require service providers to develop and implement viable contingency and BCPs to ensure the continuity of their service and performance. Such plans should be reviewed, updated and tested regularly by the service providers in accordance with changing technological conditions and operational requirements. Throughout the course of outsourcing, customers should have in place contingency plans to prepare for the possibility that the current service providers might not be able to continue operations or render the services required. Alibaba Cloud has prepared user guide with the information of Alibaba Cloud's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, etc. to facilitate customers' due diligence process. The user guide is publicly available for customers in Security & Compliance Trust Centre. Alibaba Cloud has set out terms and conditions as well as SLAs for each

	product. The information is available on Alibaba Cloud Legal Document Center (See “Useful Resource – 3. Alibaba Cloud Legal Document Center”). Besides, Alibaba Cloud provides a template of an offline Cloud Services Purchase Agreement or Enterprise Agreement where the contract terms. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Vendor Information Security Management Policy and Vendor Management Policy to regulate management over vendors and third-party employees before, during and after their onsite work.

Domain 17 - Cyber Risk Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Cyber Risk Management, Cyber Resilience Framework and Audit.

- 17.1 Cyber Risk Management

Key Aspects	Consideration
Board and Senior Management	Customers Customers are responsible to set the tone from the top and cultivates a strong culture of cyber risk management and awareness among all levels of staff and establishes oversight of cyber risks and tracking of actions to minimize cyber risk exposure.
Cybersecurity strategy	Customers Customers are responsible to establish a top-down action plan to improve the cybersecurity posture and cyber resilience of the institution’s systems, processes, and services, and regularly update policies to manage cyber risk and cyber resilience and reflect latest practices across the institution.
Cyber risk	Customers

management	Customers can establish a top-down plan of action to improve the cybersecurity posture of the entity, allocates adequate resources and expertise to implement and enforce the cyber strategy and implements appropriate governance controls to manage cyber risks consistently and systemically. Customers can build dedicated teams or designate employees to govern risks and the following steps are commonly used for cyber risk governance: - Identify and evaluate risks: Identify potential risks that may encounter at each stage, evaluate risk levels by quantifying losses, and make decisions to govern different risk levels. - Formulate governance policies: Transform governance decisions into governance policies. Governance policies are rules that are systematically implemented to restrict specific management operations on IT systems or generate alerts. - Continuously supervise governance: Take technical measures to implement management decisions. Alibaba Cloud is able to provide technical support that helps enterprises reaching their objectives. Systematic governance in the cloud can be divided into two parts: 1. Prevention: Enterprises can use the security services of Alibaba Cloud to actively defend against malicious attacks and use control policies to restrict specific management operations and changes. 2. Detection: Alibaba Cloud's cloud services supplement AI's detection capabilities in detecting insider and external threats.
Cyber risk tolerance	Customers Customers are responsible to define the cyber risk tolerance with endorsement from board and senior management and perform regular review on the cyber risk tolerance.

- 17.2 Cyber Resilience Framework

Key Aspects	Consideration
Cyber resilience framework	Customers Customers can establish own cyber resilience framework which is commensurate with its cyber risk and complexity and aligns with its organization-wide risk management framework, and ensure that the framework has been endorsed by the board.
Regular risk assessment	Customers Customers are responsible to conduct regular assessment in Guideline on Cyber Resilience and the other relevant industry standards and practices to ensure that the cyber risk management are sufficient and consistent with the nature and scale of the business.
Accountability	Customers Customers are responsible to establish clear roles and responsibilities of cyber risk management to ensure the accountability of cybersecurity and consider the independence requirement of the reporting line in the management model, such as three lines of defence model.
Budget and Resources Allocation	Customers Customers are responsible to establish a budgeting process to ensure the budget and resources allocation supporting the execution of cybersecurity management.
Staffing	Customers Customers should establish policies and procedures to govern human resourcing in supporting cybersecurity management. In particular, customers should ensure cybersecurity staff have the requisite knowledge and skills to effectively perform their duties and discharge their responsibilities. Customers should also provide tailored training programme to ensure certain areas of higher risk or priority receive greater attention and investment.

- 17.3 Audit

Key Aspects	Consideration
Audit	Customers Customers are responsible to appoint an independent audit function with adequate qualification to perform the review and report the finding to the board and senior management to ensure the adequacy and effectiveness of the cyber resilience framework. Customers are also responsible to regularly assess the audit approach in accordance with the inherent risk profile and cyber threat landscape.

Domain 18 - Software Security

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Software Management.

- 18.1 Software Management

Key Aspects	Consideration
Software Acquisition	Customers Customers are responsible to evaluate the security risk before software acquisition and perform relevant security testing prior to implementation. Alibaba Cloud *Penetration testing* Alibaba Cloud offers penetration testing services that simulate full-scale, in-depth attacks to test AI's system security and identify risks in the business process such as security defects and vulnerabilities. The service process covers from test scope determination, planning of test level with different scenarios, implementation of testing on business systems, web applications, networks, and operating systems, to delivery of test reports that include test process, risk status, vulnerability details, and fix

	suggestions.
Continuous Monitoring and Improvement	Customers Customers should deploy tools and implement processes to detect and block unauthorized changes to software, with alerts generated on malicious activities for follow-up. Customers should also formulate an asset life-cycle process to limit cybersecurity risks associated with IT assets, such as end-of-life (EOL) systems. Alibaba Cloud Cloud Config can be used to monitor and continuously evaluate the configuration of Alibaba Cloud resources. Customers can retrieve the configurations of resources and hence track the changes and compliance status of configuration of cloud services.

Domain 19 - Mobile Device Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the Policies and Procedures, Mobile Device Management and Handling of Loss Mobile Devices.

- 19.1 Policies and Procedures

Key Aspects	Consideration
Policies and procedures	Customers Customers are responsible to establish policies and procedures to govern the usage of mobile devices for staff and intermediaries and ensure they understand the related security controls and potential disciplinary actions for non-compliance.

- 19.2 Mobile Device Management

Key Aspects	Consideration

Security controls on mobile devices	Customers Authorized institutions should establish relevant security controls to protect the use of mobile device (for both corporate and personal device), especially if sensitive data is able to be accessed from mobile device. Checking should be conducted regularly for compliance.

- 19.3 Handling of Loss Mobile Devices

Key Aspects	Consideration
Missing or Stolen Mobile Devices	Customers Customers are responsible to establish the handling procedures when the mobile devices which can access to the corporate network remotely and store sensitive data are missing or stolen.
Wiping of Mobile Devices	Customers Customers are responsible to implement controls to allow them to wiping mobile devices remotely when the mobile devices are missing or stolen.

4. 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 banking institutes in their cloud strategy, governance, and adoption processes.

To ensure on-going regulatory compliance and to fulfill their own risk management duty of care, financial institutions 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, execution and evaluation processes. (See “Useful Resource – 4. Alibaba Cloud Professional Services”).

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.

5. Useful Resource

1. Alibaba Cloud Security & Compliance Center
2. Alibaba Cloud Security Whitepaper, Version 2.0
3. Alibaba Cloud Legal Document Center
4. Alibaba Cloud Professional Services

6. Version History

January 2022: First Edition – Version 1.0