Alibaba Cloud

System and Organization Controls 3 Report
Report on Alibaba Cloud's
Cloud Services System
Relevant to Security, Availability, and Confidentiality
For the Period November 1, 2018 - December 31, 2019

Report of Independent Service Auditors

To the Management of Alibaba Cloud Computing Ltd.:

Scope

We have examined Alibaba Cloud's accompanying assertion titled "Management of Alibaba Cloud's Assertion Regarding the Cloud Services System" ("assertion") that the controls within Alibaba Cloud's Cloud Services System ("system") were effective throughout the period November 1, 2018, to December 31, 2019, to provide reasonable assurance that Alibaba Cloud's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Alibaba Cloud is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Alibaba Cloud's service commitments and system requirements were achieved. Alibaba Cloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Alibaba Cloud is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Alibaba Cloud's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Alibaba Cloud's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Alibaba Cloud's Cloud Services system were effective throughout the period November 1, 2018, to December 31, 2019, to provide reasonable assurance that Alibaba Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PricewaterhouseCoopers.

PricewaterhouseCoopers

Hong Kong, China

February 14, 2020

Management of Alibaba Cloud’s Assertion Regarding the Cloud Services System Throughout the Period November 1, 2018 to December 31, 2019

We are responsible for designing, implementing, operating and maintaining effective controls over Alibaba Cloud Computing Ltd.’s and its affiliates’ (including but not limited to Alibaba Cloud (Singapore) Private Limited, Alibaba.com (Europe) Limited and Alibaba Cloud US LLC, Alibaba Cloud (India) LLP, and Alibaba Cloud (Malaysia) Sdn. Bhd., Alibaba Cloud Computing Ltd. and its affiliates are collectively referred to as the “Service Organization” or “Alibaba Cloud”) Cloud Services System (the “System”) throughout the period November 1, 2018 to December 31, 2019, to provide reasonable assurance that Alibaba Cloud’s service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our attached description of the system identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2018 to December 31, 2019 to provide reasonable assurance that Alibaba Cloud’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Alibaba Cloud’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are as follows:

- the system was protected against unauthorized access, use, or modification to meet the entity’s commitments and system requirements;
- information designated as confidential was protected by the system as committed or agreed; and
- the system was available for operation and use as committed or agreed.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a Service Organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2018 to December 31, 2019 to provide reasonable assurance that Alibaba Cloud’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Alibaba Cloud Computing Ltd.

February 14, 2020

Alibaba Cloud’s Description of the Cloud Services System Throughout the Period November 1, 2018 to December 31, 2019

I. Overview

Business Description

Alibaba Cloud, a business unit of Alibaba Group (NYSE:BABA) (“Alibaba” or the “Group”), provides a comprehensive suite of global cloud computing services to our global customers and partners as well as Alibaba Cloud’s own e-commerce ecosystem. The cloud services provided by Alibaba Cloud are powered by self-developed cloud services platform and technologies. 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. The cloud services are widely used by a variety of industries, including finance, government, games, e-business, mobile services, medical services, or multimedia. Besides the cloud services, Alibaba Cloud also provides Internet of Things (IoT) platform for a wide range of fields including intelligent life, intelligent city, intelligent manufacturing and intelligent agriculture, etc. Alibaba Cloud is dedicated to being a builder of IoT infrastructure. It is critical to the users of Alibaba Cloud's IoT Platform that the data storage and processing of the IoT platform allows the integration with APIs and other Alibaba Cloud services to enjoy a comprehensive suite of services. It features a rule engine for rapid data collection, storage, and application development. Through the efforts to build an industry-wide and integrated development platform of cloud and device terminals, set up an entire industrial chain of the IoT, and establish global wide IoT standards, Alibaba Cloud continues building an IoT ecosystem, platform and infrastructure, to speed up the integration of the physical world and digital world, and to promote the development from IoT to Internet of Intelligences (IoI).

Cloud Services covered by this Report

Alibaba Cloud is committed to building a public, open, and secure cloud computing service platform. The following services are in scope for this report:

1. Elastic Compute Service (ECS)
2. Container Service for Kubernetes
3. Container Registry
4. Object Storage Service (OSS)
5. Alibaba Cloud Content Delivery Network (CDN)
6. Network Attached Storage (NAS)
7. Virtual Private Cloud (VPC)
8. Express Connect
9. NAT Gateway
10. Server Load Balancer (SLB)
11. Elastic IP
12. VPN Gateway
13. ApsaraDB RDS for MySQL
14. ApsaraDB RDS for SQL Server
15. ApsaraDB RDS for PostgreSQL
16. ApsaraDB RDS for PPAS
17. ApsaraDB for POLARDB
18. Anti-DDoS Basic
19. Anti-DDoS Pro
20. Anti-DDoS Premium

21. Web Application Firewall (WAF)
22. Security Center
23. Resource Access Management (RAM)
24. Key Management Service (KMS)
25. ActionTrail
26. MaxCompute
27. Log Service
28. IoT Platform

Location of Data Centers covered by this Report

Alibaba Cloud is dedicated to provide stable and reliable computing and data processing capabilities and enable an interconnected world. Alibaba Cloud has 61 availability zones in 20 regions across the globe from the west to east.

The scope of locations covered in this report includes the data centres in the China (Qingdao, Beijing, Zhangjiakou, Hohhot, Hangzhou, Shanghai, Shenzhen, Chengdu), China (Hong Kong), Singapore (Singapore), India (Mumbai), Indonesia (Jakarta), Germany (Frankfurt), Japan (Tokyo), Australia (Sydney), United Kingdom (London), United States (Silicon Valley, Virginia), Malaysia (Kuala Lumpur), and United Arab Emirates (Dubai) regions.

Data center and Functions assigned or outsourced to Subservice Organizations

Alibaba Cloud uses subservice organizations ("Subservice Organizations") to provide Heating, Ventilation & Air-conditioning (HVAC) for data centers. Alibaba Cloud requires these Subservice Organizations to keep the premise safe by implementing access controls and environmental safeguards, such as fire extinguishers or closed circuit television (CCTV). Furthermore, Alibaba Cloud requires all Subservice Organizations to follow certain requirements with regard to information security and business continuity.

Alibaba Cloud is responsible for reviewing the capability and the performance of these Subservice Organizations. Contracts were signed between Alibaba Cloud and subservice organizations to define the responsibilities and obligations of both parties and specify the scope of services and service availability level of the data center. Alibaba Cloud conducts performance reviews based on Service Level Agreement (hereafter "SLA") reports, which the Subservice Organization provides monthly, in order to maintain a high service quality. These Subservice Organizations shall provide SLA reports, monthly, including major incidents, indicators, and a maintenance summary. Alibaba Cloud conducts the assessment on data center providers' service level and issues assessment reports quarterly to ensure all Alibaba Cloud's requirements are appropriately met by subservice organizations.

Complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Alibaba Cloud, to achieve Alibaba Cloud's service commitments and system requirements based on the applicable trust services criteria. Users of this report should acknowledge that the examination of service auditors did not extend to actual the controls of the subservice organizations.

II. Principal Service Commitments and System Requirements

Alibaba Cloud strives to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers ensure the security, confidentiality and availability of their systems and data. Alibaba Cloud is responsible for designing, implementing and operating effective controls over the systems and services to provide reasonable assurance that Alibaba Cloud's service commitments and system requirements are achieved. The services commitments to Alibaba Cloud's customers (User Entity) are communicated in the form of online Product Service Level Agreement ("Product SLA"), Membership Agreements, Privacy Policy, online description of the service offering of Alibaba Cloud and contracts. The details of Product SLA, Membership Agreement and other legal documents can be found at Alibaba Cloud Legal Document Centre. Alibaba Cloud has also established various communication channels for customer support including but not limited to live chat, ticket, email, suggestion posting, etc. Any potential issues that could impact the customers are also communicated with customers by global customer support team through established mechanisms. Moreover, Alibaba Cloud adheres to international standards and best practices. The details related to security and compliance are communicated with customers at Security and Compliance Centres.

The security of applications built on Alibaba Cloud is the joint responsibility of Alibaba Cloud and the User Entities. 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. Alibaba Cloud's customers should assess their objectives in choosing the services and designing the on-cloud architecture with consideration of both Alibaba Cloud's controls in place and the configurations and operational controls required as part of their security responsibilities. When designing and providing the services, to achieve the service commitments to its customers and comply with the relevant laws and regulatory requirements, Alibaba Cloud has established system and operational requirements in the form of policies, standards, manuals and procedures which are documented and communicated in organisational wide approaches.

III. Overview of Control Environment, Information and Communication, Risk Assessment, Control Activities and Monitoring Activities

Internal control is established and maintained by the Board of Directors, the management and executing staff of Alibaba Cloud. Alibaba Cloud's internal control consists of the five elements defined by the American Institute of Certified Public Accountants as following:

- **Control Environment** - is the foundation to implement internal controls, providing standard requirements and system structure and influencing the employee's internal control awareness;
- **Information and Communication** - ensures that employees obtain and communicate information about internal controls that need to be implemented through an information and communication system, and manages the operation of information communication activities;
- **Risk Assessment** - identifies and systematically analyzes relevant risks which may threaten the achievement of internal control objectives in operational activities, forming a reasonable strategy to respond to risks;
- **Monitoring Activities-** monitors the entire internal control procedure and implements remediation when necessary; if conditions permit it, adjust the corresponding control procedures to ensure a timely response of the internal control system.
- **Control Activities** – establishes and implements policies, procedures, standards and working instructions to ensure that the controls designed by management are effective to address risks to achieve the entity's control objectives and are operated effectively.

These five elements are briefly described as following.

1. **Control Environment**

Alibaba Cloud, as a business unit of Alibaba Group, organizationally aligns with the overall control environment of Alibaba Group ("Alibaba" or the "Group"). The management of Alibaba sets the core values and tone of the organization and consciousness of Alibaba people. The overall control environment reflects Alibaba Cloud's management and employees' attitudes and awareness of internal control and the activities to support effectiveness of the controls. It sets the importance of control activities to the organization and how much attention employees pay on the organization's policies, procedures and standards. Alibaba Cloud defines and implements the internal controls by setting the core values and code of conducts aligning with the Group, making the organizational structure, the roles and responsibilities of each division clearly defined and the policies, procedures and standards documented and communicated within the organization.

Alibaba Cloud organizational structure and its divisions are defined. The roles and responsibilities of each division is assigned to divisions at organizational level.

Alibaba Cloud follows Group's hiring, on-boarding and training program for its people. The formal mechanism has been established according to the policy and procedures to achieve the human resources management requirements.

2. **Information and Communication**

Alibaba Cloud has established communication channels internally and externally as per established policies and procedures, to ensure effective communication between Alibaba Cloud and its employees, as well as Alibaba Cloud and its customers.

3. **Risk Assessment**

Alibaba Cloud has established a risk management framework to identify, analyse and manage risks within the company and related to the services provided. The risk management framework involves the management and execution level personnel, covering strategic and operational risks including security, availability, and confidentiality risks.

Alibaba Cloud has established a comprehensive information security management system in accordance with the ISO/IEC 27001:2013 and relevant industry standards. It is required that an information security risk assessment to be carried out once a year, covering risk identification, classification, threat monitoring and analysis, control measures evaluation, and risk disposal, etc.

Alibaba Cloud's Information Data Center Team maintains the risk inventory of each data center, and communicates the risk inventory to the corresponding risk managers.

4. **Monitoring Activities**

Alibaba Cloud carries out a comprehensive and systematic inspection and assessment of the information security management every year, evaluating the enforcement of information security policies, standards and requirements, as well as the appropriateness of security controls. Furthermore, Alibaba Cloud's information security management is subject to regular internal audits. These validate the compliance to information security policies and the operating effectiveness of controls. Audit results are reported directly to the management.

IV. Control Activities

Alibaba Cloud establishes policies, procedures, standards and working instructions to formulate control activities. These are implemented to effectively achieve the applicable trust services criteria. Alibaba Cloud's internal control elements include controls that have a broad impact on the organization or to specific procedures and applications.

1. Information Security Governance & Risk Management

Alibaba Cloud has established policies and procedures for governing and managing information security and IT operation risks in order to provide guidance to all departments and personnel for their daily work and management procedures. All policies are available on Alibaba Cloud's internal platforms for employees' reference.

2. Human Resources

Alibaba Cloud has established the policies and code of conduct for human resources management. New employees are required to sign the labor contract, confidentiality agreement and declaration letter, in which employees' responsibilities and obligations with respect to information security are clearly defined.

Alibaba Cloud has documented and maintained the information concerning the roles and responsibilities of its employees as well as their reporting lines on internal portal which is available to all employees. The performance evaluation is conducted periodically. Any employee violation of information security and code of conduct requirements are announced on internal portal with corresponding penalty decisions.

Alibaba Cloud has established a training scheme in line with Group's requirements on code of conduct, information and data security.

3. Data Security Management

Alibaba Cloud has established Data Security Lifecycle Management process to ensure that the data security is managed and controlled throughout the data lifecycle that covers data gathering, transmission, processing, exchange, storage, and destruction. The security measures and control mechanism has been designed and implemented in line with the relevant requirements defined in Data Security Guidelines. The controls pertaining to data backup and redundancy are also established and implemented. The monitoring process is in place to ensure the effectiveness of the corresponding control design and implementation.

4. Infrastructure and Virtualization Security

Alibaba Cloud's infrastructure security measures and virtualization technology ensure the internal network and physical servers are securely protected. It prevents the cloud resources of tenants from unauthorized access and ensures the segregation among multiple tenants in a cloud computing environment by means of virtualized computing, storage, and network isolation.

Alibaba Cloud has established the hardening standards for operating system and image hardening. The operating system and image adopted for Alibaba Cloud's hosting servers are required to be configured in line with the standards.

5. Identity & Access Management

Alibaba Cloud's Identify and Access Management ensures that access to resources and systems within Alibaba Cloud's environment is properly managed and restricted, following the rules of least privileges and segregation of duties set forth in the Access Control Management Policy, to protect information assets from unauthorized access.

The policies and procedures over account and access management are in place to manage the account creation, modification and deletion. The periodic access review is in place to ensure the appropriateness of the access of employees. The password policies are embedded in account management platform to prevent simple password setting by employees.

6. Asset Management

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. The policies and procedures has been established to regulate the identification, classification and management of information assets. Besides, the guidelines governing the procedures for acquiring, deploying and disposing information assets have been established. Acquisition of new assets must be authorized by appropriate personnel. Before any new asset is deployed to the production environment, testing should be conducted with testing results documented. Requests for transferring assets out of the data centers require proper approval and transferred assets should be properly destroyed upon approval.

7. Customer Authentication and Access Management

Alibaba Cloud provides customers with user identity management and resource access control capabilities to enable customers securely authorize access to their resources and ensure that access to customers' environment is properly restricted.

Alibaba Cloud has established Website Service Agreement on its official website, which defines respective responsibilities and obligations of Customers and Alibaba Cloud related to customer access management, including level of services provided by Alibaba Cloud, as well as terms of confidentiality and data disclosure. During Alibaba Cloud account registration process, customers must agree to and confirm acceptance of the service agreement. Upon successful registration on Alibaba Cloud's website, customers are assigned with a unique Alibaba Cloud account. When a customer performs self-service password reset, the customer's identity is validated via SMS verification code on a verified mobile phone.

Resource Access Management (RAM) is a centralized user identify management and resource access control service provided by Alibaba Cloud. 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. With RAM, a different password or API Access Key can be assigned to each RAM user, which eliminates security risks arising from sharing of Alibaba Cloud account credentials. Each RAM user can log on to the Alibaba Cloud console or call service APIs by using an independent logon password or Access Key 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 permissions to different RAM users following the principle of least privilege.

Any access to customers' resources by Alibaba Cloud O&M personnel who require temporary access to customer's Alibaba Cloud resources are required to be authenticated and authorized by customers.

8. Cryptography & Key Management

Alibaba Cloud's Cryptography and Key Management ensures the confidentiality, authenticity and integrity of sensitive data through the effective use of state of the art cryptography. The policies and guidelines have been established regarding protective measures including encryption be in place for sensitive data.

Key Management Service (KMS) is a secure management service provided by Alibaba Cloud that provides basic functions such as secure hosting of keys and cryptographic operations, and integrates security practice such as key rotation. KMS can be integrated into other cloud services to encrypt user data managed by the cloud services.

Alibaba Cloud uses end-to-end encryption to ensure data security, including encryption in transit, encryption at rest and hardware-based memory encryption. Alibaba Cloud also provided HSM-based Data Encryption Service and SSL Certificates Service as part of a complete set of data encryption solutions.

9. Physical and Environmental Security

Alibaba Cloud has established policies and procedures around Physical and Environmental Security Management, to regulate access security management and environmental controls. The access authorization follows the rule of least privilege.

Alibaba Cloud data centers are equipped with necessary environmental protection and monitoring controls and mechanisms to ensure the security of physical environment. The performance of data center service providers are monitored and evaluated periodically.

10. Endpoint Security

Alibaba Cloud has established policies and procedures to regulate the management of software installation, anti-virus software, data leakage protection, as well as network admission as related to mobile devices to protect the production system from security incidents and vulnerabilities as a result of inappropriate management or misuse of mobile device. Besides, the controls and technical measures have been established to manage and monitor the Bring-Your-Own-Device (BYOD) device, anti-virus software installation to ensure the security of endpoint. The Data Leakage Prevention ("DLP") solution is also established to monitor the endpoint's data security.

11. Threat & Vulnerability Management

Alibaba Cloud's threat and vulnerability management ensures the security of Alibaba Cloud and its customers' environments by detecting system flaws and unauthorized actions and taking remediation or mitigating actions on a timely basis. Alibaba Cloud has established policies and guidelines to regulate security vulnerability management, including classification of security vulnerabilities and response mechanism. The treat and vulnerability management processed is operated in line with the requirements in the relevant policies and guidelines. Any abnormal operations were followed up by security department with necessary actions taken. The cloud platform was scanned daily, the results were gathered and monitored on a vulnerability management platform.

12. Security Incident Management

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. Security on the cloud platform is monitored to discover security incidents where platform resources are attacked and trigger the security incident response process to properly handle the incidents. Logs of activities performed on the cloud platform collected through the central logging platform are imported into real-time and offline computing platforms. Logs are processed and analysed through security monitoring algorithms in each computing platform for anomaly analysis and detection. The security team is responsible for analysing, tracking and coordinating responses to incidents on a timely basis. The confirmed security incident, if any, would be notified to the affected customers via multi-communication channels.

13. Problem Management

Alibaba Cloud has established malfunction management standards and procedures to regulate classification of malfunctions, requirements for timely response to malfunctions, as well as escalation and resolution of malfunctions according to risk level, to ensure that problems or malfunctions are identified, evaluated, escalated and resolved in a timely manner. A malfunction management platform has been developed and utilized to identify, consolidate, track and monitor malfunctions discovered via different channels. The malfunctions would be followed up by the responsible personnel on a timely basis. The affected customers would be notified via multi-communication channels.

14. Change Management

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. The access controls around the change management process have been established and implemented to ensure that access to productive systems follow the rules of least privilege and segregation of duties. Segregated environments for development, testing and production have been implemented and access the different environments is controlled and restricted to authorized personnel.

Alibaba Cloud has implemented a SPLC solution tailored for cloud products to integrate security into each stage of the product development lifecycle in order to help improve the security capabilities and reduce the security risks of cloud products. To ensure that the products meet the rigorous requirements for cloud computing, a complete security development mechanism is put into place at six different stages, from product initiation, security architecture review, secure development, security validation, product release, to incident response:

15. **Business Continuity Management**

Alibaba Cloud has established Alibaba Cloud policies and guidelines around business continuity management to ensure critical business operations could be recovered in a time manner in the event of a disruption. The business continuity plan has been developed and was tested on an annual basis.

Alibaba Cloud follows established procedures for capacity forecast, planning and monitoring to avoid capacity bottlenecks. Alibaba Cloud establishes a baseline for capacity management and evaluates the risk of impaired availability due to capacity constraints. Capacity is monitored on a real-time basis and follow-up actions are taken when forecasted usage exceeds capacity tolerances.

The service availability level was defined and committed in the Service Level Agreement which are publicly available on official website to customers.

16. **Vendor Management**

Alibaba Cloud has established policies and procedures to regulate management over vendors and third-party employees before, during and after their onsite work, to ensure that third-party service providers adhere to the agreed level of security and service delivery.

All vendors are required to go through Alibaba Cloud's background check before on boarding and are required to sign the contract and confidentiality agreement. The service provided are subject to periodical evaluation.

17. **Audit & Compliance**

Alibaba Cloud has established policies and procedures around audit and compliance management to continuously monitor internal controls, ensure commitment to high security standards and quality, maintain valid certifications and attestations, and comply with relevant statutory, regulatory and contractual requirements.

Internal audit is conducted at least once a year according to the audit plan reviewed and approved by management. Findings noted in the internal audits are regularly followed up on by the internal audit team, and corrective and preventive actions are introduced in the control environment and systems.

Alibaba Cloud is committed to continuously improving its internal control system to meet the new industry standards. Operated and maintained globally, Alibaba Cloud adheres to international information security standards and Alibaba Cloud also adheres to domestic information security standards in regions where cloud products and services are provided. Alibaba Cloud is committed to following international best practices is regularly and independently verified for compliance with industry standards. More information is available from the Alibaba Cloud Security & Compliance Center.

18. Complementary User Entity Controls

Under the shared responsibility model, the security of the applications and data resides in Alibaba Cloud is jointly responsible by Alibaba Cloud and its customer. In designing its system, Alibaba Cloud has contemplated that certain complementary controls would be implemented by user entities to meet the applicable trust services criteria. The applicable trust services criteria cannot be solely and effectively met by the controls of Alibaba Cloud. Therefore, each user entity's internal control must be evaluated in conjunction with the controls of Alibaba Cloud.

This section highlights the control areas that Alibaba Cloud considers to be the responsibilities of user entities (i.e., customers). These complementary controls should therefore be considered and developed by user entities. The following list of controls describes the additional policies, procedures and controls customers may need to implement to meet the applicable trust services criteria which can only be met if complementary controls are suitably designed and operated effectively. Each user entity must evaluate their own internal control set to determine whether the controls are designed appropriately and operated effectively. The table below is not and does not purport to contain a complete listing of the controls that provide a basis for user entities. In order to achieve effective management, user entities may also need to introduce other control activities where necessary per their specific cases.

Domain	**Applicable Product**	**Responsibilities of User Entity (i.e., Customer)**
Organization Security	All	• User entities should formulate a risk management process and assess the control objectives to address the risks when designing their complementary controls over the applications and data placed on Alibaba Cloud. • User entities should establish policies, procedures and standards to guide the information security management and operation within the organization. • User entities should establish the monitoring mechanism over the complementary controls in assessing the design and operating effectiveness of the complementary controls.
Application Controls	All	• User entities should implement appropriate controls to ensure the application level controls (e.g., segregation of duties, automated controls, system calculations, report generation, system interfaces) are designed and operating effectively.
Access Security	All	• User entities should implement access controls such as security group, RAM roles and Access Control List to protect their cloud instances. • User identity is verified via provided contact information (e.g. SMS verification code when user entities perform a self-service password reset for their cloud accounts). Therefore, user entities should implement relevant controls to ensure accurate registration and timely updates of contact details required by Alibaba Cloud such as mobile number and keep the verification channel (e.g., mobile and email) safe. • User entities should use multi-factor authentication methods to access their cloud resources. The password policy should be established with consideration of complexity of the password policy. • The access key should be appropriately protected and kept confidential. • User entities should implement a strengthened instance firewall policy.

		• User entities should ensure proper security configuration is in place to support the integrity of user authentication systems and to prevent unauthorized access. • User entities should implement access controls to protect their custom images from unauthorized access. • User entities should establish the network security standards and ensure their Virtual Private Network is only connected to appropriate internal network. • User entities should implement controls to ensure that the only authorized and secured updates are applied to rules of security group to protect access security for different ECS instances of its own. • User entities should establish and maintain the IP whitelist to protect user entities' instances from unauthorized access. • User entities should establish effective access controls for storage access to protect the buckets and objects from unauthorized access. • User entities should establish periodical review over the access and IPs authorized to their cloud resources. • User entities should enable and configure logging functionalities where applicable for sensitive activities, system errors, data changes, etc., to support monitoring controls and incident response processes.
	Only IoT Products	• User entities should implement appropriate access controls to ensure the security of their own IoT devices, servers and gateway terminals. • User entities should implement appropriate access controls to ensure the local security of the IoT firmware upgrade package developed by themselves.
Data Security	All	• User entities should implement appropriate controls to ensure cross-border data transmissions requirements are considered, if using data transmission services provided by Alibaba Cloud. • User entities should use encrypted (TLS/SSL) connection for all their interaction with Alibaba Cloud. For the user entities with higher requirements on data transmission security level (e.g., PCI DSS compliance required), TLS 1.2 should be adopted. User entities should design their CMK rotation required where necessary. • User entities should implement and maintain the encryption options based on their specific requirements.
	Only IoT Products	• User entities should evaluate and implement appropriate protective measures against the data transmitted among their own IoT devices, applications, servers and gateway terminals. • User entities should implement appropriate controls to ensure the security of sensitive data such as deviceSecret downloaded to local, as well as the security of other data stored locally.

Change Management	All	• User entities should implement appropriate change management controls for their own application and data which are hosted on Alibaba Cloud. • User entities should ensure the latest patches are applied to their instances where necessary. • User entities should set up segregated environments and user accounts to isolate the production system from development activities.
	Only IoT Products	• User entities should implement appropriate change management controls to ensure the security during the redevelopment of the software provided by Alibaba Cloud (including SDK, mobile application, AliOS Things, etc.), and ensure a timely security patch upgrade is made.
Problem Management	All	• User entities should notify Alibaba Cloud of any malfunctions, or security incidents specific to the products and services provided by Alibaba Cloud, and support timely incident response process with Alibaba Cloud.
Business continuity management	All	• User entities should establish appropriate backup and restoration strategy and plan according to their needs. These should be tested to ensure its effectiveness. Alibaba Cloud provides customers data backup functions and user entities can establish the corresponding mechanism to achieve timely backup and restoration objectives. • User entities should establish disaster recovery plan and business continuity plan according to their needs. The drill test should be performed periodically. • User entities should utilize multi-zone and multi-region options, and design and implement redundant systems to ensure a desired level of redundancy and a high availability architecture.
	Only IoT Products	• Alibaba Cloud offers device-monitoring function in its IoT Products & Services System. User entities should implement appropriate controls to monitor the status of their own IoT devices and gateways. • User entities should implement appropriate controls to ensure the effective backup of the data stored on their own IoT devices and gateways.