



System and Organization Controls 3 Report
Report on Alibaba Cloud Computing Ltd.'s
Cloud Services System

Relevant to Security, Availability, and Confidentiality
For the Period November 1, 2016 – October 31, 2017



Report of Independent Service Auditors

To the Management of Alibaba Cloud Computing Ltd.:

We have examined the accompanying management assertion of Alibaba Cloud Computing Ltd. (“Alibaba Cloud Computing”) that throughout the period November 1, 2016 to October 31, 2017, Alibaba Cloud Computing maintained effective controls over the Cloud Services System (the “system”) that were suitably designed and operating effectively to provide reasonable assurance that

- 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.
- the system was available for operation and use as committed or agreed.

based on the criteria for the security principle set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria, issued in April 2017) (“applicable trust services criteria”). Alibaba Cloud Computing management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

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 the examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion, which includes (1) obtaining an understanding of Alibaba Cloud Computing’s relevant controls over the security, availability, and confidentiality of the system, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become ineffective or fail.

In our opinion, management’s assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

A handwritten signature in dark ink that reads "PricewaterhouseCoopers." The signature is written in a cursive, flowing style.

PricewaterhouseCoopers
Hong Kong, China
December 8, 2017



Management of Alibaba Cloud Computing Ltd.’s Assertion Regarding the Cloud Services System Throughout the Period November 1, 2016 to October 31, 2017

We are responsible for maintaining effective controls within Alibaba Cloud Computing Ltd.’s (“Alibaba Cloud Computing”) cloud services system (the system) that were suitably designed and operating effectively throughout the period November 1, 2016 to October 31, 2017 to provide reasonable assurance that

- 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
- the system was available for operation and use as committed or agreed

based on the criteria to meet the security principle set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria, issued 2017) (“applicable trust services criteria”). Our attached description of the system identifies the aspects of the system covered by our assertion.

We have evaluated whether our controls were suitably designed and operating effectively throughout the period November 1, 2016 to October 31, 2017, to protect the system 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, the system was available for operation and use as committed or agreed based on the applicable trust services criteria. Based on our evaluation, we assert that throughout the period November 1, 2016 to October 31, 2017, Alibaba Cloud Computing maintained effective security, availability, and confidentiality controls that were suitably designed and operating effectively to provide reasonable assurance that 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, the system was available for operation and use as committed or agreed based on the applicable trust services criteria.

Alibaba Cloud Computing Ltd.

December 8, 2017

Alibaba Cloud Computing Ltd.'s Description of the Cloud Services System Throughout the Period November 1, 2016 to October 31, 2017

I. Introduction

Established in September 2009, Alibaba Cloud Computing Ltd. (hereafter “Alibaba Cloud Computing”) is a leading cloud computing service provider in the People’s Republic of China (hereafter “China”). Alibaba Cloud Computing provides services to a variety of customers including corporations, innovative enterprises and government authorities.

Alibaba Cloud (Singapore) Private Ltd. (hereafter “Alibaba Cloud International”) is a wholly-owned subsidiary of Alibaba Cloud Computing and responsible for the marketing, sales, media, cloud marketplace and compliance of the products on the markets outside of China.

The cloud services as described in this Description are rendered by Alibaba Cloud Computing Ltd. and Alibaba Cloud (Singapore) Private Ltd. (hereafter jointly referred to as “Alibaba Cloud”) jointly.

II. Data Centers and Services covered by the description

Location of data centers

Alibaba Cloud is dedicated to provide stable and reliable computing and data processing capabilities and enable an interconnected world. Therefore, Alibaba Cloud provides the Cloud services out of different data centers. The location(s) of the data center(s) out of which the Cloud service is provided depends on the customer’s business location.

Alibaba Cloud has established data centers in the following regions: China (North China, East China, South China and Hong Kong), Malaysia, Indonesia, United States East, United States West, Australia, the Middle East as well as Japan.



Figure: Distribution of Alibaba Cloud Data Centers

The scope of locations covered in this report includes the data centers in the China (Beijing, Hangzhou, Qingdao, Shanghai, Zhangjiakou), China Hong Kong, Singapore (Singapore), Germany (Frankfurt), Australia (Sydney), United States (Ashburn, Silicon Valley), Malaysia (Kuala Lumpur), and Dubai (Dubai) regions.

III. Cloud Services covered by this System Description

Alibaba Cloud provides its self-developed Public Cloud services. These Cloud services are offered to small and medium-sized enterprises as well as developers. They are used by a variety of industries, including finance, government, games, e-business, mobile services, medical services, or multimedia. The architectural principle of designing the services is to establish a comprehensive software/hardware system, combining thousands of servers, sharing storage, and computing resources with users and/or applications through the Internet.

The following seven Alibaba Cloud Services are subject to this description.

1. Elastic Compute Service (“ECS”)
2. Relational Database Service (“RDS”)
3. Object Storage Service (“OSS”)
4. Content Delivery Network (“CDN”)
5. Server Load Balancer (“SLB”)
6. Virtual Private Cloud (“VPC”)
7. Alibaba Cloud Security

In the following the aforementioned Cloud Services are described briefly.

1. Elastic Compute Service (“ECS”)

ECS is a computing service with scalable processing capability. ECS can be used in a variety of scenarios, such as enterprise websites, simple web applications, websites with a large number or volume of pictures/videos, applications such as self-developed databases with high input/output demands, and applications or mobile games which have highly fluctuated user traffic.

2. Relational Database Service (“RDS”)

RDS is an online database service compatible with MySQL and SQL Server protocols. It offers database online capacity expansion, database backup and rollback, as well as performance monitoring and analysis. RDS, if integrated with ECS, can improve input/output processing performance.

3. Object Storage Service (“OSS”)

The Object Storage Service (OSS) is a Cloud storage service oriented towards unstructured data. The service is horizontally scalable. OSS supports API access and offers a wide array of programming language support and tool services.

4. Content Delivery Network (“CDN”)

CDN supports content distribution to more than 500 network nodes deployed by Alibaba Cloud around the world. It reduces network delay, shortens website response times and improves website availability. CDN also helps to improve the usage of limited network bandwidth and reduces website traffic peaks.

5. Server Load Balancer (“SLB”)

SLB is a server load balancing service that is used to distribute incoming traffics among several cloud servers. SLB extends the external service capability of application systems by traffic distribution. It improves the availability of application systems by eliminating a single point of failure.

6. Virtual Private Cloud (“VPC”)

VPC helps customers to build up an isolated network environment. Customers are able to control their own virtual network, selecting the IP address range, setting up different network segments, and configuring the routing table and network gateway.

7. Alibaba Cloud Security

Alibaba Cloud Security offers one-stop security service including security vulnerability detection, Trojan detection, as well as host intrusion detection and anti-DDoS services for cloud server customers. Main functions of Alibaba Cloud Security are as follows:

- **Anti-DDoS:** The anti-DDoS module of Alibaba Cloud Security is composed of a cloud network traffic monitoring system, a DDoS mitigation system and a centralized control system, responsible for DDoS attack detection, DDoS attack filtering and centralized policy management respectively. It supports dual-way protection to prevent cloud resources from being misused.
- **Aegis (host intrusion protection):** Alibaba Cloud Aegis is a reliable and secure service. For customers who subscribe Aegis service, Aegis offer real-time monitoring of your servers and databases. Around the clock monitoring of exposed vulnerabilities ensures optimal availability of their services and applications. Aegis help customer to prevent from password brute force attacks, backdoor detection and processing, and long-distance logon alert.
- **WAF (web application firewall):** WAF is a cloud firewall service that protects core website data and safeguards the security and availability of your site. With Alibaba Big Data cloud capabilities and underlying security, WAF prevents customer asset from web-based attacks, including SQL injections, XSS, Malicious BOT, command execution vulnerabilities, and other common web attacks.

IV. Data center and Functions assigned or outsourced - Subservice Organizations

Alibaba Cloud uses 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.

Alibaba Cloud is responsible for reviewing the capability and the performance of these Subservice Organizations. 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 additional data center spot visits several times a year to ensure all Alibaba Cloud's requirements are met, appropriately.

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

Internal control procedures are managed by the Board of Directors, the management and other members, of both Alibaba Cloud Computing and Alibaba Cloud International, and shall contain the following elements:

- **Control Environment** - is the foundation to implement internal controls, providing standard requirements and system structure and influencing 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.

Alibaba Cloud establishes the following key elements in order to ensure the internal control evaluation and implementation.

1. Control Environment

The control environment reflects Alibaba Cloud's management and employees' attitudes and awareness of internal control activities. It has an impact on the importance of control activities to the organization and how much attention employees pay on the organization's policies, procedures and internal control activities. Alibaba Cloud's organization defines and executes internal controls by making the organizational structure, division of responsibilities and written policies/procedures clear.

Alibaba Cloud has developed position numbers and position responsibility documents for each type of roles and responsibilities.

Alibaba Cloud has established training and learning systems for the needs of employees and management.

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, analyze and manage risks within the Company and related to 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. It is required that an information security risk assessment will be carried out once a year, covering asset identification, and classification, threat identification and analysis, control measures evaluation and analysis, risk definition and disposal, etc.

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.

VI. Control Activities

Alibaba Cloud establishes policies and procedures to formulate control activities. These are implemented to effectively achieve the control objectives and are applicable to both Alibaba Cloud Computing and Alibaba Cloud International. Alibaba Cloud's internal control elements include controls that have a broad impact to 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.

2. Human Resources

Alibaba Cloud has established 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.

3. Data Security & Information Lifecycle Management

Alibaba Cloud has established policies for data security and information lifecycle management. In addition to the security management and control mechanisms, Alibaba Cloud has designed and implemented a series of technical measures and management procedures for data security and information lifecycle management, in order to ensure customers data security.

4. Infrastructure & Virtualization Security

Alibaba Cloud has established a General Principle of Access Control Strategies to set up the requirement that the production and non-production environments must be segregated and divided into different network security domains. Cross-domain access control is enforced by the use of IP whitelists.

a) ECS

Network traffic of different ECS instances is isolated. Alibaba Cloud controls the network traffic for data exchange to ensure that an ECS instance cannot capture or sniff network traffic of other instances. An ECS instance is bound to an IP address in the network layer the host to protect the instance from IP address spoofing.

Security groups are used to implementing access control for ECS instances. Customers are able to manage network access controls for single or multiple ECS instances by using security groups. In creating an ECS instance, customers are required to select a security group; ECS instances in different security groups cannot communicate with each other by default. Customers can configure access control policies to enable access management among ECS instances in different security groups.

System images are the template of the environment where ECS instances run, generally including operating systems and pre-installed software. Customers are able to select public images provided by Alibaba Cloud (which support multiple versions of Linux and Windows) to create instances. Customers can also create custom images based on existing ECS instances and then create instances by using custom images or images shared by other customers. By default, only users who created custom images can access and use them. Users who created custom images are able to share the images with other customers. Alibaba Cloud's public images or customers' custom images are all stored in OSS. During the process of creating instances from virtual machine images, an integrity check is performed by the use of data verification algorithms to protect the image from malicious tampering.

b) RDS

Customer isolation relies on the instance isolation mechanism of the database. Security protections are deployed on database servers to prohibit customers from loading dynamic link libraries to execute commands in the host operating systems in order to prevent unauthorized access to other customers' database instances running in the same host.

c) OSS

Data files are uploaded into OSS buckets as objects. Customers can create one or more buckets for storage, and add one or more objects into each bucket. Customers can share and download objects by using a link to uploaded files. OSS provides bucket-based and object-based access controls for customers. Only authorized customers can operate buckets and objects as authorized. OSS offers three types of access controls for buckets and objects:

- Public-read-write: Everyone can execute, read and write objects;
- Public-read: Identity authentication is required before executing any write operations to objects; everyone can read objects anonymously;
- Private: All operations to objects require identity authentication.

When a customer creates a new bucket, OSS will set up the access control type as "private" for the bucket by default, if not specified otherwise. Objects in a bucket inherit the authority of its container by default. OSS supports server-side Customer data encryption.

d) CDN

Customer's data stored in servers at CDN network nodes will be sliced to strengthen the data security. In case of a local network node malfunction, CDN will direct content requests from the malfunctioned node to those adjacent nodes that function properly according to preset rules.

e) SLB

ECS resources in the same region can be virtualized as an application service pool with high performance and high availability by setting up virtual IP addresses in SLB; access requests from clients are distributed into the pool according to the configuration of applications. SLB provides virtual IP addresses in order to hide IP addresses of back-end servers in order to achieve unified load balancing and access control.

f) VPC

Only instances bound with elastic IP addresses ("EIP") can directly access the Internet. ECS instances of different customers are located in different VPCs. Different VPCs are isolated from each other and can only be accessed from one another by the use of the IP addresses mapped to the respective external IP addresses.

5. Identity & Access Management

Alibaba Cloud has established the Alibaba Cloud Access Control Management Policy for logical access management. Operation personnel manage the cloud products or services via the IT operation platform and the IT infrastructure platform. The IT operation platform includes the individual operation and maintenance system for seven in-scope products, which is for operating cloud computing system and virtualization environments, include but not limit to execution and processes of virtual servers and infrastructure; the IT infrastructure includes operating systems, database management systems and network devices. The access is granted following the rule of least privilege for the IT operation platform and the IT infrastructure. Alibaba Cloud has separated duties of different departments and positions. All access requests need to be approved at least by the user's supervisor and corresponding access owners in order to prevent mutually exclusive access assigned to the same person. This supports the segregation of duties.

6. Unified Identity Authentication

To prevent intrusion and destruction from unauthorized internal and external users, as well as to facilitate consistent management, Alibaba Cloud's IT infrastructure can only be accessed through a bastion host. Alibaba Cloud has established password policies for the IT operation platform for identity authentication.

7. Account Management Procedure

Alibaba Cloud has established a series of procedures on account creation, modification, revocation and termination to prevent unauthorised access rights. The security department organizes business departments to perform access reviews for user accounts at least once a year.

8. Log Management

A log management platform is utilized to separately record user operations in the operation systems of seven in-scope products, as well as operating systems, database management systems and network devices supporting operation systems of seven in-scope products.

9. Customer Authentication and Access Management

During the account registration process, customers need to read and confirm the acceptance of the Alibaba Cloud Website Service Agreement on Alibaba Cloud's official website, which defines responsibilities and obligations related to customer access management.

10. Encryption & Key Management

Alibaba Cloud has established policies for encryption and key management. For data transmission security, Alibaba Cloud supports secure communication channels with strong cryptographic protocols for data transmission. HTTPS is supported by the Open API gateway of Alibaba Cloud. When a Customer logs into the management console and performs operations, identity authentication information and operation commands are transmitted via HTTPS.

RDS supports Transparent Data Encryption ("TDE") enabled by SQL Server and MySQL; OSS supports Customer data encryption at the server side. Data keys are utilized to encrypt/decrypt Customer's data; master keys are utilized to encrypt/decrypt data keys. The AES256 algorithm is utilized to encryption Customer's data and Customer's data keys.

Key Management Service ("KMS") is utilized to manage master keys of RDS and OSS customers. RDS and OSS call the internal interfaces of KMS to request the master key for data key encryption/decryption. The master key identifier is assigned to a Customer by KMS. This master key identifier is utilized by KMS to call the corresponding master key when KMS is used. HTTPS protocol is adopted in all communication channels involving cryptographic key transmission using KMS.

11. Data Center Security

Alibaba Cloud has established policies and procedures to regulate access authorization of internal personnel, access management of external personnel, data center environmental management requirements and access authorization following the rule of least privilege.

12. Endpoint Security

Alibaba Cloud has established policies and deployed Data Loss Prevention ("DLP") to monitor sensitive operations for endpoint security.

13. Threat & Vulnerability Management

A network monitoring system is utilized to monitor network traffic and user operations in real time, and identify abnormal operations. The security department personnel will follow up on any abnormal operations identified by the network monitoring system and take necessary actions.

A vulnerability scanning system is utilized to perform daily scans for security vulnerabilities in the cloud environment.

14. Security Incident Management

Alibaba Cloud utilises the security management platform for internal employees to report incidents and uses a vulnerability and incident reporting platform for external personnel to report incidents.

The security department organizes monthly meetings to report to the management on security incident management of the current month.

15. Malfunction Management

Alibaba Cloud has established the policy to regulate classification standards of malfunctions, set up the requirement of timely response for malfunctions and establish corresponding solutions to malfunctions according to risk level.

Alibaba Cloud utilizes a malfunction gathering platform to gather malfunctions discovered via the ticketing system and service monitoring system. Alibaba Cloud also utilizes a malfunction management platform to support and document classification of malfunctions, task distribution, as well as restoration and review procedures.

Alibaba Cloud has established a multi-channel communication method to announce malfunctions that could impact customers. The method includes announcements via official website, station letters, SMS, e-mails and Ding Talk messages.

16. Change Control & Configuration Management

Alibaba Cloud has established policies and procedures for change control, approval of change, and configuration management. Notifications would be sent to related Alibaba Cloud internal users as well as external users if the changes to products, supporting infrastructure or the network is expected to have internal or external impacts.

17. Business Continuity Management

Alibaba Cloud has established operational availability objectives for the following cloud products. For VPC and Alibaba Cloud Security products, the objectives of the respective ECS, OSS, or RDS services would be applicable.

- ECS is designed to provide operational availability no less than 99.95%;
- SLB is designed to provide operational availability no less than 99.95%;
- OSS is designed to provide operational availability no less than 99.90%;
- RDS is designed to provide operational availability no less than 99.95%;
- CDN is designed to provide operational availability no less than 99.90%.

Alibaba Cloud is ISO/IEC 20000:2011 and ISO22301:2012 certified, which cover business continuity management. Alibaba Cloud has established policies and operation standards with business continuity management covered. Business continuity plans are established and reviewed by the business continuity management team every year; the plans are updated according to results of the review.

Alibaba Cloud conducts a business continuity drill at least once a year. Alibaba Cloud and data center service providers conduct joint data center business continuity drills every year and data center business continuity reports would be issued accordingly. Alibaba Cloud performs backups of network device configurations by using a network device configurations system in order to ensure that network device configurations can be restored when needed.

ECS and OSS are designed to offer redundant data retention mechanisms for customer data. When customers' data is stored in ECS and OSS, three copies are automatically created in the same region where the customer purchased the service.

18. Vendor Management

Alibaba Cloud has established Alibaba Cloud Vendor Information Security Management Policy and Vendor Management Policy to regulate the management over vendors prior to, in the progress and post the onsite work.

Vendors are required to sign the service agreement and confidentiality agreement. Alibaba Cloud has stated the rights and obligations, scope of services, compliance requirements, and service levels in the service agreement. Alibaba Cloud performs a periodic assessment over vendor's performance in accordance with the service level specified in the service agreement.

Vendors involved in the services Alibaba Cloud offers 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, the Service Quality Warranty Letter attached to the agreement specifies Alibaba Cloud's requirements in data center service availability level, business relationship and service scope, as well as information security requirements. Alibaba Cloud continuously monitors service level of data center service providers to ensure secure and stable operation of data centers. Data center service providers submit the service level agreement report to Alibaba Cloud on a monthly basis. The report covers services provided during the past month. Alibaba Cloud's data center managers review the monthly report and provide feedbacks via email if there is any follow-up item.

Alibaba Cloud monitors incidents that occur at data centers to evaluate the scope of impact and severity. These incidents are then assessed to determine the risk that they may impose on Alibaba Cloud's systems. Counter measures are developed in order to mitigate the identified risks. In case that an incident occurs at a data center, the relevant data center service provider must submit a report to Alibaba Cloud, covering the causes of the incident, scope of impact and resolution status.

19. Audit & Compliance

Alibaba Cloud has established policies to regulate the procedure of building an audit plan and the execution of internal audit. The reporting and resolution procedures for internal audits require that an internal audit is conducted at least once a year. Alibaba Cloud also carries out external audits by independent third-parties.

20. Complementary User Entity Controls

In designing its system, Alibaba Cloud has contemplated that certain complementary controls would be implemented by user entities to meet control objectives or the applicable trust services criteria to be solely achieved by Alibaba Cloud's controls. 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 user entity controls should therefore be developed by user entities. Each user entity must evaluate their own internal control set to determine whether the controls are designed appropriately and implemented effectively. Insofar, these controls are intended to address certain control objectives or the applicable trust services criteria which can only be met if complementary user

entity controls, which have been assumed in the design of Alibaba Cloud’s controls, are suitably designed and operating effectively along with Alibaba Cloud’s related controls. Accordingly, 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.

Domain	Applicable Product	Responsibilities of User Entity (i.e., Customer)
Application Controls	All	<ul style="list-style-type: none"> 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.
Data Security (DTS)	All	<ul style="list-style-type: none"> User entities should utilize secure transport protocols to achieve data transmission and communication with Alibaba Cloud’s services. User entities should implement appropriate controls to ensure cross-border data transmissions requirements are considered, if using data transmission services provided by Alibaba Cloud.
Access to Programs and Data (APD)& Infrastructure and Virtual Security (IVS)	All	<ul style="list-style-type: none"> User entities should implement access controls for cloud accounts to protect user entities’ cloud service and production data from unauthorized access. User identity is verified via SMS verification code when user entities perform self-service password reset for their cloud accounts. Therefore, user entities should implement controls to ensure accurate registration and timely updates of mobile phone information, and keep their mobile phones safe. User entities should ensure proper security configuration is in place to support the integrity of user authentication systems and to prevent unauthorized access.
	Only ECS	<ul style="list-style-type: none"> User entities should implement access controls to protect their custom images from unauthorized access. If default rules of ECS security groups need to be changed, user entities should implement controls to ensure that the updated rules will protect access security for different ECS instances of its own.
	Only RDS	<ul style="list-style-type: none"> User entities should establish and maintain the IP whitelist to protect user entities’ instances from unauthorized access.
	Only OSS	<ul style="list-style-type: none"> User entities should establish effective access controls for OSS objects to protect these from unauthorized access.
Data Security (DTS)	RDS & OSS	<ul style="list-style-type: none"> User entities should utilize secure encryption method to protect sensitive data stored in RDS and OSS.
Program Change Management (PCM)	All	<ul style="list-style-type: none"> User entities should implement appropriate change management controls for their own application systems which are supported by Alibaba Cloud’s services.
Business continuity management (BCM)	All	<ul style="list-style-type: none"> User entities should implement appropriate controls and perform restore tests to complete backup and preservation of systems and data. During the preset retention period since the service expiration date or early termination date due to any reason; otherwise, user entities’ systems may become irrecoverable and

		<p>data may get lost, after Alibaba Cloud performs complete removal of user entities' systems and data once beyond the preset retention period.</p> <ul style="list-style-type: none">• Alibaba Cloud offers data backup function in its cloud services. User entities should establish corresponding procedures for timely backup and recovery testing procedure to ensure backup effectiveness.
--	--	---