



System and Organization Controls Report (SOC 3[®])

***Description of Shanghai Lily & Beauty Cosmetics Co., Ltd.'s
Online Sales Operation Service System Relevant to
Security and Confidentiality***

Throughout the Period August 1, 2018 to January 31, 2019

Report of Independent Accountants

To the Board of Shanghai Lily & Beauty Cosmetics Co., Ltd.

Scope

We have examined Shanghai Lily & Beauty Cosmetics Co., Ltd.'s ("LRLZ" or the "Service Organization") accompanying assertion titled *Management's Assertion Regarding the Effectiveness of Its Controls Over the Shanghai Lily & Beauty Cosmetics Co., Ltd.'s Online Sales Operation Service System Based on the Trust Services Criteria for Security and Confidentiality* (the "Management's Assertion" or the "Assertion") that the controls over the Shanghai Lily & Beauty Cosmetics Co., Ltd.'s Online Sales Operation Service System (the "System") were effective throughout the period August 1, 2018 to January 31, 2019, to provide reasonable assurance that LRLZ's service commitments and system requirements were achieved based on the trust services criteria for Security and Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (the "applicable trust services criteria"). This Assertion is the responsibility of LRLZ's management.

Service Organization's Responsibilities

LRLZ 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 LRLZ's service commitments and system requirements were achieved. LRLZ has also provided the accompanying Assertion about the effectiveness of controls within the System. When preparing its Assertion, LRLZ is responsible for selecting, and identifying in its Assertion, the applicable trust services 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 the Management's Assertion that controls within the System were effective throughout the period August 1, 2018 to January 31, 2019 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 the Management's Assertion is fairly stated, in all material respects. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating LRLZ's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Our examination included:

- Obtaining an understanding of the System and the LRLZ's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve LRLZ'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 LRLZ'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 any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its service commitments and system requirements related to Security and Confidentiality are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are 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, LRLZ's Management's Assertion that the controls within the System were effective throughout the period August 1, 2018 to January 31, 2019, to provide reasonable assurance that LRLZ's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Ernst & Young Hua Ming LLP Shanghai Branch

February 25, 2019

Shanghai, China

**Management’s Assertion Regarding the Effectiveness of Its Controls
Over the Shanghai Lily & Beauty Cosmetics Co., Ltd.’s
Online Sales Operation Service System
Based on the Trust Services Criteria for Security and Confidentiality**

February 25, 2019

We, as management of, Shanghai Lily & Beauty Cosmetics Co., Ltd. (“LRLZ” or “we” or the “Service Organization”) are responsible for designing, implementing, operating, and maintaining effective controls over the LRLZ’s Online Sales Operation Service System (the “System”) throughout the period August 1, 2018 to January 31, 2019, to provide reasonable assurance that the service commitments and system requirements relevant to Security and Confidentiality were achieved. Our description of the boundaries of the System is presented in *Description of Shanghai Lily & Beauty Cosmetics Co., Ltd.’s Online Sales Operation Service System Relevant to Security and Confidentiality Throughout the Period August 1, 2018 to January 31, 2019* (the “Description”) and identifies the aspects of the System covered by our assertion.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity’s Security controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are 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.

We have performed an evaluation of the effectiveness of the controls over the System throughout the period August 1, 2018 to January 31, 2019, to provide reasonable assurance that LRLZ’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and*

Privacy (the “applicable trust services criteria”). LRLZ’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 presented in the Description.

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

Our attached description of the boundaries of the LRLZ’s Online Sales Operation Service System throughout the period August 1, 2018 to January 31, 2019 identifies the aspects of the System covered by our assertion.

Very truly yours,

Shanghai Lily & Beauty Cosmetics Co., Ltd.



**Description of Shanghai Lily & Beauty Cosmetics Co., Ltd.’s
Online Sales Operation Service System Relevant to Security and Confidentiality
Throughout the Period August 1, 2018 to January 31, 2019**

Overview of the Organization

Company Overview

Established in 2010, Shanghai Lily & Beauty Cosmetics Co., Ltd. (“LRLZ” or the “Company”) is a leading online cosmetics distributor in China, providing online sales operation services to more than 50 cosmetics companies. By operating Tmall stores, LRLZ has established an online sales channel between cosmetics companies and customers¹. LRLZ devotes itself to enhancing customer experiences, and meanwhile helping more cosmetics companies achieve success in China’s market. LRLZ’s vision is to develop into one of the largest online cosmetics distributors across the world. LRLZ upholds the management philosophy of contribution to clients’ success, cooperation and sharing, honesty and accountability, and win-win achievement.

Services Overview

LRLZ provides online sales operation services to cosmetics companies, which mainly consist of the following types:

- **Product Management Service:** By means of its rich experience in e-commerce business, LRLZ offers integrative product service to cosmetics companies such as product positioning, product development, pricing strategy, selling point identification, product combination proposal for package suit, etc.
- **Tmall Store Design Service:** According to customer visual habits, LRLZ offers Tmall store style design, product page design, and other visual design services to cosmetic companies, making the store more attractive to customers.
- **Marketing Service:** LRLZ offers marketing, brand promotion and advertising strategy to cosmetics companies, which helps create customer loyalty and enlarge customer base.
- **Customer Service:** LRLZ offers customer service to cosmetics companies, handling inquires, requirements and complaints from customers. The service is performed by its Customer Service Department and certain outsourced customer service vendors.
- **Warehouse Logistics Service:** LRLZ offers warehouse logistics service to cosmetics companies, helping deliver goods to customers in a timely manner. The service is performed by certain outsourced warehouse vendors.

¹ Customers in the Description refer to buyers who place orders in Tmall stores, whereas cosmetic companies refer to LRLZ’s user entities.

Scope of the report

The scope covered in this report is LRLZ's online sales operation services system supported by the Tmall platform (the "System"). The physical access management and endpoint security management in this report only applies to LRLZ's Shanghai office where the System is operated.

LRLZ uses Alibaba Cloud Computing Ltd. ("Aliyun") to provide cloud computing services, including Elastic Compute Service ("ECS") and Relational Database Service ("RDS"), to host the applications supporting the System, as well as cloud security services; LRLZ uses Zhejiang Tmall Technology Co., Ltd. ("Tmall Technology") to provide Tmall Platform service, to operate online sales, and user operation and server security monitoring service (Yuchenghe); LRLZ uses certain customer service vendors to support customer services; LRLZ uses certain warehouse vendors to provide warehouse logistics services. Aliyun, Tmall Technology, customer service vendors and warehouse vendors are hereinafter collectively referred to as the "subservice organizations". The Description does not extend to controls of subservice organizations.

Principal Service Commitments and System Requirements

LRLZ designs its processes and procedures related to the IMS system, the OMS system and the Tmall platform to meet its service commitments and system requirements for its online sales operation services. They are based on the service commitments that LRLZ makes to user entities, and the operational and compliance requirements that LRLZ has established for the services.

Security and Confidentiality commitments to user entities are established which include, but are not limited to, the following:

- Use of management controls, operation controls and technological controls to protect confidential information
- Use of encryption technologies to protect customer data both in transit and during storage

LRLZ establishes operational requirements that support the achievement of Security and Confidentiality commitments and other system requirements. Such requirements are communicated in LRLZ's system policies and procedures, system design documentation, and agreements with user entities. Information security policies define an approach about how systems and data are protected. These include policies around how the internal control system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation of the IMS system, the OMS system and the Tmall platform.

Software

The online sales operation services are supported by the Tmall platform, the OMS system and the IMS system.

- The Tmall platform - is a business-to-customer retailing platform provided by Tmall Technology enabling businesses to sell directly to customers. Merchants such as cosmetics companies can set up and operate Tmall stores on the Tmall platform to sell products. LRLZ's responsibilities are to set up and operate user entities' Tmall stores on the Tmall platform. Customers can select their products and place orders in Tmall stores. LRLZ's employees, user entities' employees and outsourced customer service vendors have access to corresponding Tmall stores. Change management, physical access management and daily operation of the Tmall platform are managed by Tmall Technology. LRLZ is responsible for logical access management of user entities' Tmall stores only.
- The OMS system - is an in-house developed software for sales order management. It captures sales orders from the Tmall platform, processes sales order based on predefined rules, and sends processed sales orders to the IMS system. LRLZ's employees, outsourced customer service vendors and outsourced warehouse vendors have access to the OMS system. Outsourced customer service vendors have access to handle sales order cancellation, abnormal sales order and delivery order, and inquire about sales orders and delivery order. Outsourced warehouse vendors have access to inquire about sales orders and handle sales order cancellation.
- The IMS system - is an in-house developed software for inventory management, including purchase management module and inventory management module. Its main functions consist of inventory data calculation and management, and updating actual inventory data based on goods entry and delivery information. LRLZ's employees and outsourced customer service vendors have access to the IMS system. Outsourced customer service vendors have access to inquire about inventory to provide customer service.

Tmall Technology provides user operation and server security monitoring service (Yuchenghe) to monitor users' operations in the OMS system and the IMS system.

Infrastructure

LRLZ uses Aliyun's cloud computing services, including ECS and RDS to host the applications supporting the System, as well as cloud security services. Aliyun is responsible for physical environment management, physical machine management and virtualization relevant to the cloud computing service and cloud security service provided to the Company. LRLZ also uses Tmall Technology's user operation and server security monitoring service (Yuchenghe) to perform real-time scans for security vulnerabilities in the servers.

The Company obtains and reviews Aliyun's System and Organization Controls Report annually, in order to assess if all the Security and Confidentiality requirements related to the cloud service used by the Company are met.

People

LRLZ has established a comprehensive organizational structure and clearly defined employees' job responsibilities. In the meantime, reporting line has been clearly defined in an internal platform.

LRLZ has established a structured onboarding process to help new employees understand their responsibilities in information security and code of conduct. Potential candidates who apply for positions of manager level or above need to undergo background check by Human Resources specialist, and the results are documented in the internal form. Employees are required to sign agreements that include non-disclosure provisions upon hire. New hires are required to attend orientation training that covers company history, culture, policies and business system operation.

For current employees, LRLZ has established a training mechanism including quarterly on-job training and knowledge sharing and annual exam about internal policies.

To regulate employees' behaviors, the Company has established a management procedure for handling with breach of Code of Conduct.

Procedures

LRLZ has designed and implemented a series of procedures in its routine operation and management in terms of security and confidentiality, including:

- Security and Confidentiality Awareness
- Risk Assessment
- Monitoring
- Change Management
- Identity and Access Management
- Data Security Management
- Endpoint Security Management
- Security Vulnerability and Security Incidents Management
- Third Party Management

Data and Confidentiality

LRLZ has established formal policies to regulate data security management procedures. In the meantime, LRLZ has established a series of controls to ensure the security and confidentiality of data transmission, data storage, data access, data change, data extraction and data destruction.

LRLZ has segregated the data accessibility for different users by access settings, and deployed the Hyper Text Transfer Protocol over Secure Socket Layer ("HTTPS") to encrypt and protect data transmission. LRLZ has set the sanitization rules to sanitize sensitive data according to its business needs and to fulfill the service commitment on data and confidentiality.

Complementary User Entities Controls

The Description does not extend to controls of user entities. Below are the controls expected to be performed at user entities that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

Identity and Access Management:

- User entities are responsible for implementing corresponding controls to ensure usernames and passwords of their sub-accounts in the Tmall stores are kept properly; and
- User entities are responsible for implementing corresponding access controls to provide change requests to LRLZ regarding their sub-accounts creation, modification and termination in the Tmall stores in a timely manner.

Data Security Management:

- User entities are responsible for using secure transport protocols to achieve data transmission and communication with LRLZ.

Complementary Subservice Organization Controls

The Description does not extend to controls of subservice organizations. Below are the types of controls expected to be performed at the subservice organizations that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

Customer Service Vendors:

- Data loss prevention controls and information security incident management controls relevant to the security and confidentiality of customer's information processed on behalf of the Company.
- Controls relevant to timely notification of updating IMS accounts, OMS accounts and Tmall sub-accounts held by customer service vendors, and proper securing of these accounts.

Warehouse Vendors:

- Controls relevant to timely notification of updating OMS accounts held by warehouse vendors, proper securing of the accounts, and access management of their own warehousing systems.
- Data security controls, end point security controls and other controls relevant to the security and confidentiality of customer's information processed on behalf of the Company.

Tmall Technology:

- Manage change controls, manage IT operations controls, server management controls and other general IT controls relevant to the processing performed for the Company.
- Data security controls, end point security controls and other controls relevant to the security and confidentiality of customer's information processed on behalf of the Company.

Aliyun:

- Physical access controls, infrastructure and virtualization security controls relevant to the cloud computing service and cloud security service provided to the Company.