Ningxia Western Cloud Data Technology Co., Ltd.

System and Organization Controls 3 (SOC 3) Report
Report on NWCD's Cloud Services System Relevant to Security, Availability, and Confidentiality
For the Period January 25, 2019 to July 25, 2019

pwc

普华永道

Independent Service Auditor's Report

2019/ SH-0398

To the Management of Ningxia Western Cloud Data Technology Co., Ltd.:

Scope

We have examined Ningxia Western Cloud Data Technology Co., Ltd.'s (the "NWCD") accompanying assertion titled "Management of Ningxia Western Cloud Data Technology Co., Ltd.'s Assertion " (the "assertion") that the controls within NWCD's Cloud Services System (the "system") were effective throughout the period January 25, 2019, to July 25, 2019, to provide reasonable assurance that NWCD'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

NWCD 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 NWCD's service commitments and system requirements were achieved. NWCD has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, NWCD 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 NWCD'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 NWCD'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 NWCD's Cloud Services System were effective throughout the period January 25, 2019, to July 25, 2019, to provide reasonable assurance that NWCD's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PricewaterhouseCoopers Zhong Tian LLP

PricewaterhouseCoopers Zhong Tian LLP

Shanghai, The People's Republic of China

September 6, 2019

Assertion of Ningxia Western Cloud Data Technology Co., Ltd. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Ningxia Western Cloud Data Technology Co., Ltd.'s (the "NWCD") Cloud Services System (the "system") throughout the period January 25, 2019, to July 25, 2019, to provide reasonable assurance that NWCD's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A and 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 January 25, 2019, to July 25, 2019, to provide reasonable assurance that NWCD'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*). NWCD'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 is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements;
- The system is available for operation and use as committed or agreed; and
- Information designated as confidential is protected by the system 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 January 25, 2019, to July 25, 2019, to provide reasonable assurance that NWCD's service commitments and system requirements were achieved based on the applicable trust services criteria.

Ningxia Western Cloud Data Technology Co., Ltd.
September 6, 2019

Attachment A.

Ningxia Western Cloud Data Technology Co., Ltd.'s Description of the Cloud Services System Throughout the Period January 25, 2019 to July 25, 2019

I. Introduction

Since 2017, Ningxia Western Cloud Data Technology Co., Ltd. (hereinafter referred to as "NWCD") has built technology cooperation relationship with Amazon Web Services, Inc. ("AWS"), and has been delivering cloud services within China. As the cloud services operator and provider for AWS China (Ningxia) Region based out of Ningxia, NWCD provides Chinese software developers and enterprises with secure, flexible, reliable and low-cost IT infrastructure resources.

II. Services and Data Centers covered by the Description

The scope of services covered in this report includes:

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon DynamoDB
- Amazon Relational Database Service (Amazon RDS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Identity and Access Management (IAM)
- Amazon CloudWatch
- AWS CloudTrail
- AWS Snowball

The scope of locations covered in this report includes the data centers in the China Mainland (Zhongwei, Ningxia) Region.

III. Cloud Services covered by this System Description

1. Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. Amazon EC2's web service interface allows customers to obtain and configure capacity with minimal friction. It provides customers with control of computing resources and lets customers run on Amazon's proven computing environment.

2. Amazon DynamoDB

DynamoDB is a managed NoSQL database service to store and retrieve any amount of data, and serve any level of request traffic. Its guaranteed throughput and single-digit millisecond latency make it fit for gaming, ad tech, mobile and many other applications.

3. Amazon Relational Database Service (Amazon RDS)

Amazon Relational Database Service (Amazon RDS) allows customers to set up, operate, and scale a relational database in the cloud. It provides resizable capacity while managing time-consuming database administration tasks. Amazon RDS manages backups, software patching, automatic failure detection, and recovery. Customers can have automated backups performed as necessary, or manually create backup snapshot.

4. Amazon Simple Storage Service (Amazon S3)

Amazon Simple Storage Service (S3) is object storage with a web service interface, as well as API and SDK for integration with the third-party technologies, to store and retrieve any amount of data from anywhere on the web.

S3 enables customers to analyze as a scalable bulk repository, or "data lake"; backup & recovery; disaster recovery; and serverless computing. S3 supports data transfer over secured channel and automatic protection of customers' data once it is uploaded. Customers can also configure bucket policies to manage object permissions and control access to their data using AWS Identity and Access Management (IAM).

5. AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) enables customers to control access to AWS services and resources for users. Using IAM, customers can create and manage AWS users and groups and use permissions to allow and deny their permissions to AWS resources.
IAM also enables identity federation between corporate directory and AWS services. This lets customers use existing corporate identities to grant secure access to AWS resources, such as Amazon S3 buckets, without creating new AWS identities for those users.

6. Amazon CloudWatch

Amazon CloudWatch is a monitoring service for cloud resources and the applications run on NWCD's Cloud Services. Amazon CloudWatch can be used to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in NWCD's Cloud Services as well as custom metrics generated by applications and services, and any log files applications generate. Amazon CloudWatch can be used to gain system-wide visibility into resource utilization, application performance, and operational health.

7. AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS account. With CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across AWS infrastructure. CloudTrail provides event history of AWS China region account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

8. AWS Snowball

Snowball is a petabyte-scale data transport solution that uses secure devices to transfer large amounts of data into and out of NWCD's Cloud Services.

IV. 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, and consists of five integrated components:

- **Control Environment** – Control environment is the foundation to implement internal controls, providing standard requirements and system structure and influencing the employee's internal control awareness. The resulting control environment has a pervasive impact on the overall system of internal control. NWCD has sets of standards, processes, and structures that provide the basis for carrying out internal control across the organization;

- **Information and Communication** – Ensuring 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. NWCD has established a variety of internal and external communication mechanisms to ensure the smooth communication within the company, as well as between NWCD's employees and its customers;

- **Risk Assessment** – The entity's identification and analysis of relevant risks to achievement of the internal control objectives, forming a reasonable strategy to respond to risks. NWCD maintains a formal risk management program to continually identify, assess and manage risks that may threaten the achievement of its service commitments and system requirements related to security, availability and confidentiality;

- **Monitoring** – The process must be monitored and modifications should be made as necessary. In this way, the system can react dynamically, changing as conditions warrant. NWCD employs a combination of ongoing and periodic monitoring activities to monitor that controls are functioning effectively and that risks are appropriately managed;

- **Control Activities –** NWCD has developed a variety of policies and procedures including related control activities to help ensure the entity's control objectives are carried out and risks are mitigated.

V. Control Activities

NWCD has established policies and procedures to formulate control activities, which are performed at a variety of levels throughout the organization and at various stages during the relevant business process.

1. Information Security Policy and Awareness

NWCD has an established information security department to manage the events that are associated with information security and maintain formal policies and procedures for security governance and risk management.

NWCD provides on-boarding orientation and continuing education or training programs to improve employees' security and confidentiality awareness and standardize employee behavior.

NWCD maintains a formal risk management program to continually identify, analyze and manage risks that may threaten the achievement of its service commitments and system requirements related to security, availability and confidentiality.

2. Employee User Access

NWCD has established policies and procedures to regulate the process of employee and third party user accounts being added, modified or disabled promptly and being reviewed periodically, and to clarify the password configuration settings for user authentication to NWCD systems.

3. Logical Security

Policies, procedures, and mechanisms are in place to properly limit unauthorized internal and external data access and remain the logical security of the Cloud Services Systems.

APIs enable customers to articulate cloud services and resources (if resource-level permissions are applicable to the service) that they own. NWCD prevents customers from accessing cloud resources that are not assigned to them via access permissions. User content is segregated by the service's software. Content is only returned to individuals authorized to access the specified cloud services or resources (if resource-level permissions are applicable to the service).

4. Secure Data Handling

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

The security of NWCD requires both NWCD and NWCD cloud services customers to perform security controls to ensure cloud security.

5. Physical Security and Environmental Protection

NWCD designs and manages its infrastructure including the facilities, network, hardware and related operational software which are secured appropriately.

NWCD has established policies and procedures to regulate access authorization of data centers for internal and external personnel, and management of media throughout its use life, to prevent information assets from being exposed to unauthorized individuals.

Data centers are designed to meet with the data center environment management requirements.

6. Change Management

NWCD has established Change Management Policy to regulate change management process, including authorization, design, development, testing, deployment, documentation of the changes and segregation of duties which applies to program development and changes.

7. Data Integrity, Availability, and Redundancy

Integrity

NWCD maintains data integrity through phases including transmission, storage, and processing.

Availability

NWCD has established policies and procedures to define the redundancy requirement of the system deployed. NWCD has identified critical system components and backed up those components across multiple, isolated Availability Zones to cope with the event of a system outage in order to maintain the availability of the system.

NWCD continuously monitors the current usage of the cloud services for models in available Availability Zones and maintains a capacity planning to assess infrastructure usage and demands.

NWCD has established policies to cope with the incident and enhance the business continuity and specific procedures are set to regulate classification standards of security incidents, set up the timely response for security incidents and establish corresponding solutions to security incidents according to incident level.

Redundancy

Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Customers' contents are redundantly stored in multiple, isolated Availability Zones in Amazon S3.

Amazon RDS provides two different methods for backing up and restoring customer DB Instance(s): automated backups (Turned on by default) and database snapshots (User-initiated).

Amazon DynamoDB provides the option for customers to set up automatic backups.

8. Confidentiality

NWCD's systems and services are designed to enable authenticated NWCD's customers to access and manage their content. For logical access, NWCD has deployed multiple access control mechanisms to ensure the identity of the user is legitimate.

A variety of monitoring tools and controls are deployed to prevent unauthorized access to or disclosure of user's content in the data center to protect the data center from physical intrusion, thus ensuring the confidentiality of user data.

NWCD has established mechanism to ensure the confidentiality of data from within and outside of the boundaries of our environments which store the customer's content.

Services and systems hosted by NWCD are designed to retain and protect customers' data until the contractual obligation to retain a customer's content ends, or upon a customer initiated action to remove or delete their content. Once the customer-initiated deletion acts successfully,

this action works on deleted content to render the content unreadable. NWCD has deployed a tool for erasing data to guarantee the data cannot be accessed or recovered after the completion of the deletion.

9. Incident Handling

NWCD has established policies and procedures to regulate classification standards of security incidents, set up the requirement of timely response for security incidents and establish corresponding solutions to security incidents according to incident level.

10. Complementary User Entity Controls (CUECs) relevant to the system

In designing its system, NWCD has contemplated that certain complementary controls would be implemented by user entities to meet control objectives or the applicable trust services criteria. The control objectives or the applicable trust services criteria cannot be solely and effectively achieved by the controls of NWCD. Therefore, each user entity's internal control must be evaluated in conjunction with the controls of NWCD.

This section highlights the control areas that NWCD considers to be the responsibilities of user entities (i.e., customers). These complementary 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 controls are suitably designed and operating effectively. In addition, the following list of control is solely designed to address the issues about interface and communication control between user entity and NWCD. 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)
CC1.0 Common Criteria Related to Control Environment	All	• Customers should maintain formal policies that provide guidance for information security within the organization and the supporting IT environment.
CC2.0 Common Criteria Related to Communication and Information	All	• Customers should maintain formal policies that provide guidance for information security within the organization and the supporting IT environment.
CC3.0 Common Criteria Related to Risk Assessment	All	• Customers should maintain formal policies that provide guidance for information security within the organization and the supporting IT environment.

Domain	Applicable Product	Responsibilities of User Entity(i.e., Customer)
CC4.0 Common Criteria Related to Monitoring Activities	All	• User entities should implement appropriate controls to ensure monitoring activity controls are designed and operating effectively.
CC5.0 Common Criteria Related to Control Activities	All	• Customers should maintain formal policies that provide guidance for information security within the organization and the supporting IT environment.
CC6.0 Common Criteria Related to Logical and Physical Access Controls	All	• Customers should use asymmetric key-pairs or multi-factor authentication to access their hosts and avoid simple password-based authentication. • Customers should augment the NWCD instance firewalls with a host-based firewall for redundancy and egress filtering. • Customers should set up separate development and production accounts to isolate the production system from development work. • Customers should transmit secret keys over secure channels. Customers should avoid embedding secret keys in web pages or other publicly accessible source code. Customers should encrypt sensitive data at rest as well as in transit over the network. • Customers should use encrypted (TLS/SSL) connections for all of their interactions with NWCD. Best practices include the use of TLS 1.2. Customers should opt in for annual key rotation for any CMK they would like rotated. • Customers should appropriately configure and manage usage and implementation of available encryption options to meet customer requirements.

Domain	Applicable Product	Responsibilities of User Entity(i.e., Customer)
	Only IAM	• Customers should implement access controls such as Security-Groups, IAM roles to segment and isolate like-functioning instances. • Customers should utilize multi-factor authentication for controlling access to their root account credentials and should avoid using root account credentials beyond initial account configuration of AWS Identity and Access Management (IAM), except for Services for which IAM is not available. Customers should delete access key(s) for the root account when not in use.
CC7.0 Common Criteria Related to System Operations	All	• Customers may subscribe to Premium Support offerings that include direct communication with the customer support team and proactive alerting to any issues that may impact the customer. • Customer should enable and configure service-specific logging features where available for all services and implement appropriate monitoring and incident response processes. • Customers should ensure appropriate logging for events such as administrator activity, system errors, authentication checks, data deletions etc. is in place to support monitoring, and incident response processes.
CC8.0 Common Criteria Related to Change management	All	• Customers are responsible for maintaining the application of patches to their NWCD instances.
CC9.0 Common Criteria Related to Risk Mitigation	All	• Customers should maintain formal policies that provide guidance for information security within the organization and the supporting IT environment.

Domain	Applicable Product	Responsibilities of User Entity(i.e., Customer)
A - Availability Criteria	All	• User entity should implement appropriate controls and perform restore tests to complete backup and preservation of systems and data. During the present retention period since the service expiration date or early termination date due to any reason; otherwise, user entities' systems may become irrecoverable and data may get lost, after NWCD performs a complete removal of user entities' systems and data once beyond the present retention period.
	Only EC2	• EC2-Specific – Data stored on Amazon EC2 virtual disks should be proactively copied to another storage option for redundancy.
	Only RDS	• Customers should enable backups of their data across cloud services. Examples include backups of RDS.
	Only DynamoDB	• DynamoDB-Specific – Customers should set up either full or incremental automatic backups to a table in the same region or a different region.
	Only Snowball	• Snowball-Specific – Customers should not delete any local copies of their data until they have verified that it has been copied into NWCD.
C - Confidentiality Criteria	All	• Any code customers write to call Amazon APIs should expect to receive and handle errors from the service. Specific guidance for each service can be found within the User Guide and API documentation for each service. • Customers should ensure their cloud resources such as server and database instances have the appropriate levels of redundancy and isolation. Redundancy can be achieved through utilization of the Multi-Region and Multi-AZ deployment option where available.

The list of control considerations presented above does not represent all the controls that should be employed by the customer. Other controls may be required. Customer should reference additional cloud service documentation on the NWCD website.