Snowflake China Region

Operated by DCC

GXP Compliance, Considerations, and Recommended Best Practices

White Paper

Table of Contents

1. ABSTRACT

The past few years have seen tremendous change in the life sciences and healthcare industries. As part of this change, life sciences companies have been moving significant amounts of data and workloads to the cloud. This accelerated in 2020 as organizations were forced to adopt new policies around remote work, virtual commercial engagement, remote patient engagement, and decentralized clinical research.

Digital China Cloud Technology Limited's ("DCC") Snowflake China Region Operated by DCC ("Snowflake China") is a single, integrated data platform delivered as-a-service and built for the cloud. Snowflake China delivers the performance, concurrency and simplicity needed to store and analyze an organization's data in one location. Snowflake China's technology combines the power of data warehousing, the flexibility of big data platforms and the elasticity of the cloud.

Snowflake China is different from traditional legacy data platforms, Hadoop systems, or other cloud databases because of its architecture. Snowflake China has introduced a patented, multi-cluster, shared data architecture which was born and built for the cloud to revolutionize data analysis. To the user, Snowflake China provides the functionalities of an enterprise analytic database, along with many additional features and capabilities.

Customers using Snowflake China platform for good clinical, laboratory, manufacturing, or research practice (GxP) workloads will need to adapt audit policies, IT policies, and procedures to a PaaS (platform-as-a-service) model. These models have been recognized within the industry as more agile, automated, and secure by design.

This white paper provides considerations and recommendations for using Snowflake China for GxP workloads.

Throughout this white paper we call out specific requirements in the Appendix 10 Computerized Systems to Good Manufacturing Practice for Drugs and Requirements for Drug Records and Data Management (Trial), issued by China National Medical Products Administration (NMPA), which has equivalent requirements for electronic records as 21 CFR part 11, Implementation Rules for the Management Regulations of Human Genetic Resources (the HGR Implementation Rules) issued by Ministry of Science and Technology of the People's Republic of China (MOST), U.S. Food and Drug Administration (U.S. FDA) Code of Federal Regulations (CFR) Title 21, Part 11 (Electronic Records) and the European Commission, Health and Consumers Directorate-General: EudraLex, Volume 4, Annex 11 (Computerized Systems) to relate to features and functionality within the Snowflake China platform. It is not the intention of this white paper to be an exhaustive representation of all the requirements a customer should adhere to in order to maintain GxP compliance.

2. Snowflake China OVERVIEW

2.1. About DCC

Digital China Cloud Technology Limited (DCC) is dedicated to becoming a leading partner in digital transformation. Digital China has pioneered the "Digital-Cloud Integration" strategy and technical framework, focusing on key elements of enterprise digital transformation. The company is committed to building product and service capabilities in key technologies such as cloud-native, digital-native, digital-cloud integration, and the trusted computing industry. It provides ubiquitous and agile IT capabilities and integrated data-driven abilities for customers in various industries, including fast-moving consumer goods, retail, automotive, finance, healthcare, government, education, and telecommunications, at different stages of their digital transformation. By constructing innovative digital business scenarios and new business models through cross-sector integration, Digital China helps enterprise customers establish core capabilities and competitive advantages for the future, fully promoting the digital and intelligent transformation and upgrade of society.

2.1.1. Understanding cloud computing

The list of cloud acronyms is always growing and three terms, Software as a Service, Platform as a Service, and Infrastructure as a Service (SaaS, PaaS, and IaaS) are often used in the context of DCC. These three terms form the essential foundation of business cloud computing and often take complimentary roles in a cloud environment.

- SaaS (software as a service) is the one true “household name” in this list. SaaS moves software deployment and management to third-party cloud software services. Familiar SaaS platforms include CRM, marketing automation, storage solutions, and of course cloud data warehousing. SaaS apps reduce Total Cost of Ownership (TCO)by eliminating most software maintenance resources and upgrade costs. In addition, SaaS solutions hit the OpEx (Operational Expense) budget, not the CapEx (Capital Expense) budget, making it easier for businesses to fit SaaS apps into their budget.
- PaaS (platform as a service) is a cloud-based platform service that provides a foundation for developers to build custom business apps. It bundles an operating system and server software with server hardware and network infrastructure, freeing developers to focus on building high-value custom solutions for their organizations.
- IaaS (infrastructure as a service) combines highly scalable and automated compute resources with cloud storage and networking—often available on demand. IaaS gives businesses the ability to scale up and down and create virtual data centers that do not require expensive overhead costs to run and manage.

2.1.2. Snowflake China and SaaS, PaaS, and IaaS

Snowflake China Data Cloud allows you to run all your critical data workloads on one platform, including collaboration, data lake, data warehouse, and custom development capabilities, in effect also serving as a data SaaS. DCC partners with leading IaaS data services provider Amazon Web Services (AWS) to deliver highly elastic data storage, analytics, and sharing to enterprises of all types and sizes.

2.2. Snowflake China Region operated by DCC

In China, Snowflake platform is wholly operated separately by Digital China Cloud Technology Limited ("DCC"), DCC partners with Snowflake to provide consistent and extraordinary Snowflake data cloud services for China mainland customers.

Snowflake China is a fully managed service that is simple to use, but can power a near-unlimited number of concurrent workloads. Snowflake China is our customers' solution for data warehousing, data lakes, data engineering, data science, data application development, and for securely sharing and consuming shared data. The following capabilities make Snowflake China unique:

- Multi-cluster, shared data architecture: Snowflake China's architecture logically separates yet natively integrates storage, computing, and services. You can enable virtually all your users and data workloads to access a single copy of your data without impacting performance.
- Global data solution: Snowflake China abstracts the complexity of the underlying cloud infrastructures, allowing you to run your data solution seamlessly across multiple clouds and regions for a single consistent experience.
- Secure collaboration: Snowflake China enables you to collaborate securely across business ecosystems. You can also access additional shared data sets and data services via Snowflake China's Marketplace and connect similarly with thousands of DCC's customers that make up the greater Data Cloud.

2.3. DCC attestations, certifications, compliance

DCC is continuously expanding our portfolio of security and compliance Reports as our customers request them. The following is the current list of reports available to all customers and prospects under NDA.

2.3.1. Quality management

DCC follows software industry standards for the design, development, release, maintenance, and support of the Snowflake service which aligns to quality management (QMS) principles and requirements.

2.3.2. SOC 2 Type II

The SOC2 Type 2 report is an external audit over controls relevant to security, confidentiality, and availability of the systems used to process customer data.

DCC is audited by independent auditors over the design and operating effectiveness of SOC 2 controls annually according to related guidelines issued by AICPA. The audit report will be provided to related parties, including Cloud customers, regulatory bodies, and other key shareholders to create transparency on the latest internal control activities of DCC upon request.

2.3.3. MLPS

The Multi-level Protection Scheme (MLPS) in China provides detailed requirements regarding the different levels of security obligations for network operators. The evaluation agency authorized by the Ministry of Public Security evaluates Snowflake China according to relevant requirements. The information security protection level has been assessed as level 3 and has obtained filing certification.

Please contact DCC for copies of reports as applicable to your organization or to find out if a particular certification will soon be available

3. GXP COMPATIBILITY AND COMPLIANCE

DCC does not manufacture, hold, distribute, or process pharmaceuticals, medical devices, or regulatory data; therefore, predicate rules such as those for good manufacturing practices, medical devices, good laboratory practices, or good clinical practices (commonly collectively referred to as GxP) do not apply to the DCC service. Although regulatory compliance is the customer's overall responsibility, DCC understands that there is some inherited, shared responsibility in those activities.

GxP regulations are designed to ensure products, services, and information do not adversely impact, either directly or indirectly, patient safety, product quality, and/or data integrity. These regulations cover processes from sourcing raw materials to packaging design and storing conditions. This includes both physical products as well as computer systems.

Systems in a SaaS or PaaS model require controls that are outside the control of customers. These areas include infrastructure and physical security management as well as design and development activities.

3.1. Infrastructure and physical security

The Snowflake China service is a Cloud Data Warehouse designed for IaaS platforms. Snowflake China is a fully relational SQL data warehouse built for the cloud on top of the underlying Cloud Service Provider (CSP). DCC contracts with Cloud providers, which are responsible for the infrastructure and physical security at each of their sites.

DCC is committed to providing a secure, stable, consistent and reliable physical environment, DCC has implemented the following physical security control at each office location to safeguard the physical security:

- A centralized access card system has been implemented in office areas, granting access only to authorized employees.

3.2. DCC design and development

DCC has a defined software development lifecycle (SDLC) process, which is based on Agile methodologies. The SDLC is followed for any platform development activities intended to be released to Snowflake China's production environment. The process includes the following four (4) phases:

- Exploration and planning
- Development, security, and testing
- Support enablement, communication, and release
- Post-release monitoring, bug fixing, and support

Specific details regarding the SDLC, technical design, and change management are documented in our policy and procedural controls.

Snowflake China is MLPS Level 3 certified by an authorized certification agency to achieve compliance with China Cybersecurity Law.

3.2.1. Software testing

DCC incorporates multiple levels of testing as part of the development process. Testing encompasses all aspects of the SDLC, from unit testing during development to regression testing prior to each release. DCC has established relevant policies to specify specific plans and requirements for security testing before the system goes online. It is stipulated that the data from the production system should be desensitized during the software testing.

3.3. Release management

Snowflake China strictly controls the software version. Changes, updates, and new feature releases are approved by DCC prior to deployment in the production environment and related release approvals are properly recorded. Snowflake China releases software on a weekly basis, along with planned patch releases. Behavior change releases, which are changes to existing product behavior, are performed in accordance with the release management process. Snowflake China has a defined cadence with advanced notification to customers to allow for appropriate planning.

3.3.1. Weekly releases

Snowflake China follows a weekly release schedule with behavior changes added on a monthly basis. In addition, each weekly release is staged across multiple days and consists of three waves: early, regular, and final.

For additional details, please see the Snowflake China release documentation.

3.3.2. Behavior changes

Snowflake China releases feature updates on a monthly basis as described in the Snowflake China release documentation. During the testing period and opt-out period for each behavior change release, you may enable or disable the release in your account.

4. TITLE 21 CFR PART 11 ELECTRONIC RECORDS; ELECTRONIC SIGNATURES CONSIDERATIONS

Customers who use Snowflake China to manage records in electronic form (e.g., those that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations) are required to comply with applicable requirements within 21 CFR Part 11 Electronic Records; Electronic Signatures. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations.

In general, the China National Medical Products Administration (NMPA) uses equivalent requirements for electronic records as 21 CFR part 11.

The Snowflake China service has multiple functions that can aid customers in complying with these regulatory requirements. Though it is the customer's responsibility to ensure adequate documentation and testing of these requirements, this section outlines the Snowflake China functionality that customers may wish to leverage in their compliance efforts.

At present, the responsibilities of both parties are mainly stipulated by contracts and agreements. Meanwhile, in order to ensure the management of vendors, DCC defines the responsibilities and obligations between vendors by signing contracts.

4.1. Electronic records / controls for closed systems

Many of the guiding principles outlined in CFR 21 Part 11 align with core Snowflake China product capabilities and features. The following capabilities have been outlined below for specific consideration.

4.1.1. Snowflake China auditing logging and audit trails

Auditing in Snowflake China can be performed by referencing the ACCESS_HISTORY and QUERY_HISTORY views.

ACCESS_HISTORY

Access History in Snowflake China refers to whether the user query reads column data. Snowflake China does not record write operations. More information about the user Access History feature can be found in the Access_History View (in this topic).

Each row in the ACCESS_HISTORY view contains a single record per query and describes the columns the query accessed directly (i.e., the base table) and indirectly (i.e., derived objects, such as views). These records help facilitate regulatory compliance auditing and provide insights on popular and frequently accessed tables and columns since there is a direct link between the user (i.e., query operator), the query, the table or view, the column, and the data.

Additional use cases for the ACCESS_HISTORY view include:

- Discovering unused data to determine whether to archive or delete the data
- Validating data changes to notify users prior to dropping or altering a given table or view
- Auditing data access to comply with regulatory requirements and data governance initiatives

QUERY_HISTORY

This Account Usage view can be used to query Snowflake China query history by various dimensions (time range, session, user, warehouse, etc.) within the last 365 days (1 year).

4.1.2. System access and authentication

With regard to GxP guidelines, regulatory authorities have specific requirements for system access and authorization to access electronic records.

DCC provides industry-leading features that ensure the highest levels of security for your account and users, as well as all the data you store in Snowflake China.

Snowflake China supports multiple methods of user authentication, including:

- Federated authentication & SSO
- Key pair authentication & key pair rotation
- Multi-factor authentication (MFA)
- OAuth

For personnel who access the systems and infrastructure that support the Snowflake China service, each user must have a unique username and password. All authentication requires mutual authentication as well as multi-factor authentication. Customers create and manage users of the Snowflake China service application.

Snowflake China provides granular control over access to objects—who can access what objects, what operations can be performed on those objects, and who can create or alter access control policies.

Snowflake China role-based access control (RBAC)

In the Snowflake China model, access to securable objects is allowed via privileges assigned to roles, which are in turn assigned to other roles or users. In addition, each securable object has an owner that can grant access to other roles. This model is different from a user-based access control model, in which rights and privileges are assigned to each user or group of users. The Snowflake China model is designed to provide a significant amount of both control and flexibility.

Complete documentation on Snowflake China's RBAC: Overview of Access Control.

RBAC vs. multiple accounts

Should a customer use multiple Snowflake China accounts for a single organization, they have the ability to separate validated GxP workloads from non-validated workloads (e.g. Commercial workloads). This is a common best-practice deployment strategy for Snowflake China within the industry.

Should a customer wish to leverage a single Snowflake China account for all workload types (validated and non- validated), RBAC can be used to provide effective isolation for all validated roles, users, and workloads.

4.2. Electronic signatures

Snowflake China does not have electronic signature functionality.

4.2.1. Snowflake China archiving and recovery

Zero-Copy Cloning

Cloning, also referred to as "zero-copy cloning," creates a copy of a database, schema, or table. A snapshot of data present in the source object is taken when the clone is created and is made available to the cloned object. The cloned object is writable and independent of the clone source; that is, changes made to either the source object or the clone object are not part of the other. Cloning a database will clone all the schemas and tables within that database. Cloning a schema will clone all the tables in that schema.

Time Travel

Snowflake China Time Travel enables access to historical data (i.e., data that has been changed or deleted) at any point within a defined period. It serves as a powerful tool for performing the following tasks:

- Restoring data-related objects (tables, schemas, and databases) that may have been accidentally or intentionally deleted
- Duplicating and backing up data from key points in the past

- Analyzing data usage/manipulation over specified periods of time

4.2.2. Business continuity

DCC has established a solid Business Continuity Security Management Framework, with designated roles and responsibilities, adequate training, and routine table top exercise to ensure stable service under extreme circumstances

4.2.3. Impact to customer validation

The Zero-Copy Cloning feature allows the archival of data at frequent intervals and retrieval of that data on demand. The Time Travel feature allows for the unplanned or ad hoc access to a prior state of the database.

Besides the above functionality that Snowflake China provides, DCC partners with the underlying Cloud Service Provider (CSP), to host the data local back-ups and backup recovery services.

Customers should take appropriate administrative and technical measures to ensure the availability and integrity of electronic data.

5. Compliance to China GXP requirements issued by NMPA and MOST

DCC is committed to provide globally consistent and extraordinary Data Cloud service for China Mainland customers, customers are required to comply with applicable requirements within Requirements for Drug Records and Data Management (Trial) and Appendix 10 "Computerized Systems" to Good Manufacturing Practice for Drugs issued by China National Medical Products Administration (NMPA), and also comply with applicable requirements within Implementation Rules for the Management Regulations of Human Genetic Resources (the HGR Implementation Rules) issued by the Ministry of Science and Technology of the People's Republic of China (MOST)

5.1. Data integrity and confidentiality

DCC is committed to ensuring data integrity and confidentiality.

DCC’s policies and procedures set forth standard encryption technology for transferring, receiving, and storing customer data.

DCC has developed and implemented network security control to improve the robustness of the underlying network of its platform, including:

- The transmit configuration of APIs are supported by Hypertext Transfer Protocol Secure (HTTPS) to ensure all customer data transmitted over public networks is encrypted.
- Access to the production environment requires login through the operation and maintenance endpoint, and unauthorized DCC employees are not allowed to log in to the operation and maintenance endpoint

5.2. UTC synchronization

Systems are configured to synchronize information system time docks based on International Atomic Time or Coordinated Universal Time (UTC). Access to modify time data is restricted to authorized personnel.

5.3. Operating records

DCC has implemented access control and identity verification controls to ensure the operation records are retained and operating commands such as (edit, delete, transfer) are recorded.

5.4. Electronic records

According to Article 35 of the “Implementation Rules for the Management Regulations of Human Genetic Resources (the HGR Implementation Rules)” issued by MOST, all data and data usage information during the research process should be properly recorded. Please refer to 4.1. Electronic records / controls for closed systems for detail information.

6. Vendor management

DCC has established policies and procedures to foster the security management of vendors and monitors vendor performance. Contractual agreements are implemented to monitor performance.

DCC creates and maintains written agreements with vendors in accordance with the work or service to be provided. DCC monitors the performance of vendors through the annual review using a risk-based approach, which evaluates performance against contractual obligations

7. Customer support through Corrective and Preventive Action (CAPA)

DCC takes action to eliminate the cause of nonconformities within the scope of the quality management system to resolve customer queries, in order to prevent recurrence. The following procedure is followed when taking corrective and preventive actions:

1. Identify the specific nonconformities through customer queries received.
2. Determine the causes of nonconformities.
3. Evaluate the need for actions to ensure that similar nonconformities do not recur.
4. Determine and implement the corrective action(s) needed.
5. Review the effectiveness of the corrective action(s) taken.
6. Determine and implement preventive action needed.
7. Record results of action taken, and

8. Review of preventive action.

The records of corrective actions are reviewed during regularly scheduled management meetings.

8. TRAINING

DCC's hiring process ensures employees have the necessary skills, training, and experience to perform their duties. In addition to this, DCC employs a robust training program for its IT support and management staff that encompasses various topics such as threat intelligence, secure coding, incident response, compliance, network and cloud security, phishing awareness, data protection, and continuous learning, to fortify their cybersecurity skills and uphold organizational security standards.

For customers, DCC Education Services offers instructor-led classes, on-demand courses, and self- directed learning to help you and your team excel and your data initiatives to materialize. If you're just getting started with DCC or you're driving advanced data projects, we provide the training and resources to be successful every step of the way:

- Fundamentals
- Advanced
- Persona-based
- Performance Automation and Tuning

We recommend that any staff with access to Snowflake China for GxP workloads have at minimum the SnowPro Core Certification.

9. CONCLUSION

It is important to note that life sciences and healthcare organizations are ultimately responsible for compliance with GxP guidelines. This includes any applications developed on, powered by, or data managed within the Snowflake China platform. While there is no GxP "certification" for a commercial cloud software provider such as DCC, we recommend incorporating the best practices and considerations outlined in this white paper within the context of your existing quality management and compliance framework.