

ICS 03.120.20

CCS A 00



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 22275.8-2026

**Requirements of conduct for good laboratory practice - Part 8:
The application of cloud computing in GLP laboratories**

良好实验室规范实施要求 第8部分：云计算在良好实验室规范试验机构中的应用

Issued on: May 25, 2026

Implemented on: September 1, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

2	Cloud computing deployment mode
4	Overview of Cloud Computing
4.1	Concept
5.1	Responsibilities of the Testing Organization
5.2	Requirements
5.3	Implementation of Cloud Computing Solutions in the GLP Framework
5.3.2	Risk Assessment and Selection of Cloud Computing Services
5.3.3	Cloud Service Provider Evaluation
5.3.4	Service Level Agreement (SLA)
8	The application of cloud computing used in GLP laboratory ICS

Foreword

GB/T 22275.8-2026 | Requirements of conduct for good laboratory practice - Part 8: The application of cloud computing used in GLP laboratory

GB/T 22275.8-2026 English version. Requirements of conduct for good laboratory practice - Part

2 Cloud computing deployment mode

4.4 Service Model The cloud computing service models of GLP pilot organizations are mainly divided into the following types according to the types of computing resources provided.

a) Infrastructure as a Service (IaaS). For GLP pilot sites, IaaS solutions provide hardware and network (including physical and virtual) It provides hosting and maintenance services for components and ensures the availability of storage space, computing power and resources.

b) Platform as a Service (PaaS). In GLP testing facilities, the hardware and environment are provided by the platform. The platform provides data and document management capabilities. Functionality typically integrates migration, sorting, and storage services. GLP pilot facilities are still responsible for system configuration and software management. responsibility. Example

1.Cloud service providers support the deployment and implementation of Laboratory Information Management Systems (LIMS) by providing application servers and databases.

c) Software as a Service (SaaS). Under the GLP framework, the SaaS model provides experimental organizations with data generation/analysis and document management capabilities. Applications with functions such as [list of functions] are developed, installed, maintained, and updated by cloud service providers. The hardware is typically deployed on [platform name]. Data centers (often using public cloud models to support multi-user access). These data center hosting services are typically provided by software vendors. Subcontracting implementation to third parties. All security design is guaranteed by the cloud service provider (typically through other subcontractors). GLP Testing facilities need to connect to the system via a general or shared platform with specific access permissions to use the software. Training is usually provided. As part of the service. GLP pilot facilities have limited computational intervention permissions to internally defined user access rights. This also includes root access. Configure the application according to the intended use by the testing facility (including security settings during implementation). SaaS usage includes identity verification. Verify the connection to the system and enter data. Example 2.A laboratory electronic recording system can be hosted in a public cloud and can collect raw data via electronic devices. This data is transmitted directly from [the cloud] through a secure network. The device is transferred to a private (secure) zone also hosted in the public cloud for storage. Depending on the selected cloud computing service model, the management responsibility for the main components of the cloud computing solution lies between the testing organization and the cloud service provider. The overall framework for dividing the space is shown in Figure 3. Figure

3.Division of Management Responsibilities for Key Components of Cloud Computing Services between GLP Pilot Organizations and Cloud Service Providers. Cloud computing in a 5GLP environment

4.1 Concept

4.1.1 Cloud computing can be defined as a network model that supports on-demand access to shared, configurable pools of computing resources. For example, cloud computing can be defined as "a..." This enables ubiquitous, convenient, and on-demand access to shared configurable computing resources (such as networks, servers, storage, applications, and services) via a network. This model allows for rapid deployment and release of resources by minimizing management input or service interactions. (Related terms. network, server, etc.) See Appendix A for details.

4.1.2 Cloud computing has five basic characteristics, four deployment modes and three service modes, as shown in Figure 1.

4.2 Basic Features The basic characteristics of cloud computing include the following.

a) On-demand self-service allows users to access computing resources independently without needing to interact manually with service providers;

- b) Network access. Computing resources can be accessed via the network and support various heterogeneous client platforms (such as mobile devices and workstations);
- c) Resource pooling. The supplier's computing resources are centrally managed through a single-tenant or multi-tenant model to provide services to multiple users. Physical and virtual resources (such as storage, processing power, memory, and network bandwidth) can be dynamically allocated and reallocated according to user needs;
- d) Rapid elasticity (scalability). Resources can be rapidly expanded or contracted according to demand, and can be automatically allocated and released elastically;
- e) Measurable services. Cloud systems optimize resource usage by reasonably metering capabilities based on service type (e.g., active user accounts). The system can be monitored, measured, controlled, and reported, providing transparency for both suppliers and users (pay-as-you-go).

4.3 Deployment Mode Cloud computing can be deployed in different models depending on the type of use. The main difference lies in the availability of cloud infrastructure, which includes the following four types. Deployment mode. See Figure 2 for cloud computing deployment mode.

- a) Private Cloud. In the GLP framework, a private cloud refers to computing resources deployed exclusively for the exclusive use of the contracted pilot institution or its affiliated organization. Managed services. These clouds are built on private internal networks or employ fully isolated access architectures to ensure that the infrastructure is dedicated to... Contracted trial institutions, regardless of whether the cloud service is provided by an external cloud service provider or internally.
- b) Community Cloud. In the GLP framework, a community cloud refers to a cloud consisting of multiple testbeds with similar needs (such as security and compliance requirements). This is a shared cloud infrastructure. Access is not public; it is limited to specific user groups with shared needs. The cloud environment can be operated by member organizations or third-party organizations.
- c) Public Cloud. In the GLP framework, public cloud refers to computing resources available for use by the public or large groups (such as entire industry sectors). Managed services, which are provided by the respective cloud service providers in their own facilities/data centers.
- d) Hybrid Cloud. In the GLP framework, hybrid cloud refers to a combination of public and private clouds. The experimental organization uses both public and private cloud services. It has its own private cloud and can establish a two-way connection to enable the two to work together to form a unified system. Figure

5.1 Responsibilities of the Testing Organization

5.1.1 Test Facility Management (TFM) The testing facility manager is responsible for ensuring that the GLP testing facility and the systems supporting GLP activities comply with GLP specifications. When IT operations originate from this... When migrating locally controlled servers to a cloud solution, regardless of whether an internally managed cloud platform is used (as part of a pilot facility or its affiliated organization)... Whether implemented through external cloud service providers or in separate units, the testing organization should maintain appropriate understanding, awareness, and oversight of the system and its operation. Implement effective control.

5.1.2 Cloud Service Delegated Management Due to the complexity of cloud services, administrators of experimental institutions can delegate the signing and management of such service contracts to entities responsible for supplier selection and contract fulfillment. Package and oversight by professionals or specialized internal departments. Therefore, transparency of agreements and obligations among all relevant parties is a key element, allowing for [further details regarding the implementation]. The different services offered allow for scalable hierarchical management of details. It is important to emphasize that even when outsourced, TFM should still be responsible for the testing machine. The system is responsible for GLP compliance.

5.1.3 System Administrator Access Control System administrators have access to both real-time and archived data and documents. When data is hosted by a cloud service provider, data access should be clearly defined. Inquire about the context and operational procedures. Granting administrator privileges to personnel with a potential interest in the data and/or documents is prohibited. Clear guidelines should be established and implemented. Risk mitigation strategies and controlled procedures are implemented to ensure data integrity, quality, and availability, regardless of whether the system administrator is located at the testing facility or elsewhere. Supplier's office.

5.1.4 Verification of Cloud Services The project leader should ensure that all computerized systems used in the research (including virtual components that may be hosted locally or in the cloud) are properly configured. Verified.

5.1.5 Archivist The archivist is responsible for archival management. If GLP archives are stored in a cloud solution, the archivist may need to consult with experts. To assist in handling technical issues. Nevertheless, the archivist remains responsible for ensuring.

- a) The archiving conditions ensure the integrity of the archived electronic records;
- b) Controlled management of access to archives;
- c) Establish an indexing system to achieve ordered storage and retrieval of records;
- d) The migration process of archived electronic records shall be effectively controlled and documented;
- e) Establish a process for regular readability and data integrity checks;