Organisation for Economic Co-operation and Development

ENV/CBC/MONO(2023)27

Unclassified

English - Or. English

29 June 2023

ENVIRONMENT DIRECTORATE
CHEMICALS AND BIOTECHNOLOGY COMMITTEE

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Advisory Document on GLP & Cloud Computing
Supplement 1 to Document Number 17 on Application of GLP Principles to Computerised Systems

JT03522821

OECD Environment, Health and Safety Publications

Series on Principles of Good Laboratory Practice (GLP) and Compliance Monitoring

Supplement 1 to Document Number 17 on Application of GLP Principles to Computerised Systems

Advisory Document on GLP & Cloud Computing

IOMC

INTER-ORGANIZATION PROGRAMME FOR THE SOUND MANAGEMENT OF CHEMICALS

A cooperative agreement among FAO, ILO, UNDP, UNEP, UNIDO, UNITAR, WHO, World Bank and OECD

Environment Directorate
ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT
Paris 2023

ALSO PUBLISHED IN THE SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

- *No. 1, OECD Principles of Good Laboratory Practice (as revised in 1997)*
- *No. 2, Revised Guides for Compliance Monitoring Procedures for Good Laboratory Practice (1995)*
- *No. 3, Revised Guidance for the Conduct of Laboratory Inspections and Study Audits (1995)*
- *No. 4, Quality Assurance and GLP (as revised in 1999)*
- *No. 5, Compliance of Laboratory Suppliers with GLP Principles (as revised in 1999)*
- *No. 6, The Application of the GLP Principles to Field Studies (as revised in 1999)*
- *No. 7, The Application of the GLP Principles to Short-term Studies (as revised in 1999)*
- *No. 8, The Role and Responsibilities of the Study Director in GLP Studies (as revised in 1999)*
- *No. 9, Guidance for the Preparation of GLP Inspection Reports (1995)*
- *No. 10, The Application of the Principles of GLP to Computerised Systems (1995)*
- *No. 11, The Role and Responsibilities of the Sponsor in the Application of the principles of GLP (1998)*
- *No. 12, Requesting and Carrying Out Inspections and Study Audits in Another Country (2000)*
- *No. 13, The Application of the OECD Principles of GLP to the Organisation and Management of Multi-Site Studies (2002)*
- *No. 14, The Application of the Principles of GLP to in vitro studies (2004)*
- *No. 15, Establishment and Control of Archives that Operate in Compliance with the Principles of GLP (2007)*
- *No. 16, Guidance on the GLP Requirements for Peer Review of Histopathology (2014)*
- *No. 17, The Application of GLP Principles to Computerised Systems (2016)*
- *No. 18, OECD Position Paper Regarding the Relationship between the OECD Principles of GLP and ISO/IEC 17025 (2016)*
- *No. 19, The Management, Characterisation and Use of Test Items (2018)*
- *No. 20, Guidance Document for Receiving Authorities on the Review of the GLP Status of Non-Clinical Safety Studies (2019)*

- *No. 21, OECD Position Paper Regarding Possible Influence of Sponsors on Conclusions of GLP Studies (2020)*
- *No. 22, GLP Data Integrity*
- *No. 23, Quality Assurance and GLP*
- *No. 24, OECD Position Paper on Quality Improvement Tools and GLP*

About the OECD

The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organisation in which representatives of 38 industrialised countries in North and South America, Europe and the Asia and Pacific region, as well as the European Commission, meet to co-ordinate and harmonise policies, discuss issues of mutual concern, and work together to respond to international problems. Most of the OECD's work is carried out by more than 200 specialised committees and working groups composed of member country delegates. Observers from several countries with special status at the OECD, and from interested international organisations, attend many of the OECD's workshops and other meetings. Committees and working groups are served by the OECD Secretariat, located in Paris, France, which is organised into directorates and divisions.

The Environment, Health and Safety Division publishes free-of-charge documents in eleven different series: **Testing and Assessment**; **Good Laboratory Practice and Compliance Monitoring**; **Pesticides**; **Biocides**; **Risk Management**; **Harmonisation of Regulatory Oversight in Biotechnology**; **Safety of Novel Foods and Feeds; Chemical Accidents; Pollutant Release and Transfer Registers; Emission Scenario Documents;** and **Safety of Manufactured Nanomaterials.** More information about the Environment, Health and Safety Programme and EHS publications is available on the OECD's World Wide Web site (www.oecd.org/chemicalsafety/).

This publication was developed in the IOMC context. The contents do not necessarily reflect the views or stated policies of individual IOMC Participating Organizations.

The Inter-Organisation Programme for the Sound Management of Chemicals (IOMC) was established in 1995 following recommendations made by the 1992 UN Conference on Environment and Development to strengthen co-operation and increase international co-ordination in the field of chemical safety. The Participating Organisations are FAO, ILO, UNDP, UNEP, UNIDO, UNITAR, WHO, World Bank and OECD. The purpose of the IOMC is to promote co-ordination of the policies and activities pursued by the Participating Organisations, jointly or separately, to achieve the sound management of chemicals in relation to human health and the environment.

This publication is available electronically, at no charge.

Also published in the Series on Principles of Good Laboratory Practice and Compliance Monitoring: link

For this and many other Environment, Health and Safety publications, consult the OECD's World Wide Web site (www.oecd.org/chemicalsafety/)

or contact:

OECD Environment Directorate,
Environment, Health and Safety Division
2 rue André-Pascal
75775 Paris Cedex 16
France

E-mail: ehscont@oecd.org

FOREWORD

This advisory document was developed by the OECD Working Party on Good Laboratory Practice (GLP). The development of the document was led by Belgium and France (Medical Products) and included a drafting group with representatives from Australia, Austria, Denmark (Medical Products), Israel, Japan (Medical Products), Poland, Switzerland, US-EPA and US-FDA. The document was reviewed and endorsed by the Working Party on Good Laboratory Practice.

This document is published under the responsibility of the Chemicals and Biotechnology Committee which agreed to its declassification in June 2023.

Table of contents

1. Background **10**

2. Introduction **10**

3. Scope **10**

4. Overview of cloud computing **11**

4.1. Definition 11
4.2. Characteristics 12
4.3. Deployment models 12
4.4. Service models 14

5. Cloud computing in GLP environment **16**

5.1. Responsibilities of the test facility 16
5.2. Requirements 16
5.3. Implementation of cloud-based solution in GLP 18

6. Expectations of the GLP compliance monitoring authorities when inspecting cloud –based solutions **26**

6.1. Implementation of the cloud solution 26
6.2. Life cycle of the cloud service application 27
6.3. Electronic archives in cloud solution 27

7. Conclusion **28**

8. Glossary **29**

References 31

FIGURES

Figure 1. Cloud computing characteristics, deployment and service models 11
Figure 2. Cloud computing deployment models 13
Figure 3. Shared management of the main components of a cloud computing service between the GLP test facility and the cloud service provider 15

TABLES

Table 1. GLP requirement management within different cloud service models 17

1. Background

The Good Laboratory Practice (GLP) Principles require that records and materials, including electronic records and data, necessary to reconstruct non-clinical safety studies meet the requirements for data quality, data integrity and data availability and are properly retained and archived.

An increasing number of GLP test facilities use cloud applications to accommodate these requirements. However, the potential impact on GLP compliance should be considered when using cloud solutions. GLP test facilities have the ultimate responsibility for GLP compliance to assess risks to data integrity, data quality, data availability, data retention and data archiving.

Cloud refers to delivery of on-demand network access to a shared pool of configurable computing resources to users and can include software, networks/platforms or infrastructure. Cloud-based solutions in GLP could cover the external development, maintenance and hosting, inside or outside of the premises of the test facility, of computing resources such as:

1. Hardware or servers connected by networks.
2. Software or applications that capture, generate, analyse, migrate, store, archive data.
3. Interfaces between applications.
4. Databases.

2. Introduction

This document describes the expectations that GLP Compliance Monitoring Authorities have of GLP test facilities which use cloud-based solutions.

Cloud service may be involved in GLP data capture, processing, storage and archiving.

This document focuses on the specific characteristics of cloud-based solutions, especially the co-operation between the test facility and the cloud service provider, and clarifies the requirements of the GLP Principles to be applied.

This document is considered a supplement to Document No. 17 (Application of GLP Principles to Computerised Systems) (OECD, 2016[1]) and should be read and applied in conjunction with OECD Documents No. 1 (OECD Principles on Good Laboratory Practice) (OECD, 1997[2]), No. 15 (Establishment and Control of Archives that Operate in Compliance with the Principles of GLP) (OECD, 2007[3]), No. 5 (Compliance of laboratory suppliers with GLP principles) (OECD, 2002[4]) and No. 22 (GLP Principles and Data Integrity) (OECD, 2021[5]) and applicable national regulations.

3. Scope

Cloud services can be internally provided services of the test facility or of the company the test facility belongs to, or outsourced services by contracted IT service providers. When contracted, the service can be provided directly by a cloud service provider or via a vendor. Service providers may also have sub-contractors for all or part of the service. This document is applicable to all types of services.

Note: the term "cloud service provider" will be used for all types of providers of cloud services including internal IT, external IT, hosted service provider, vendor (usually an individual or entity, who sells the services), supplier (usually the one whose work is to provide the requested services) or cloud provider in the rest of this document.

The document applies to all cloud-based solutions, including the ones already in use.

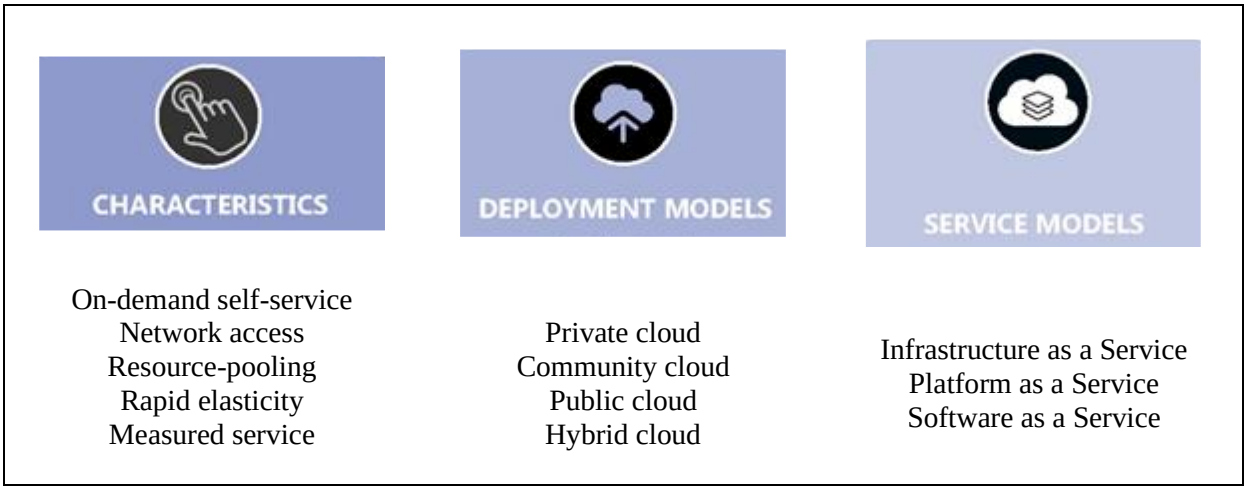
The expectations in this document for "test facilities" and "Test Facility Management (TFM)" would equally apply to "test sites" and "Test Site Management".

4. Overview of cloud computing

4.1. Definition

In general terms, cloud computing can be defined as a model that enables on demand network access to a shared pool of configurable computing resources. The US National Institute of Standards and Technology (NIST) (Peter Mell, 2011[6]) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." According to NIST, cloud computing has five essential characteristics, four deployment models and three service models as described in Figure 1.

Figure 1. Cloud computing characteristics, deployment and service models



Source: FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies (Crisanto et al., 2018[7])

These characteristics, deployment models and service models as defined by NIST are reproduced or paraphrased below. Possible GLP examples are provided in the following paragraphs (see section 4.3 and section 4.4).

4.2. Characteristics

The essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity (i.e., easily adaptable and flexible) and measured service.

1. **On-demand self-service:** Users are provided with computing resources without any human interaction with the service provider.
2. **Network access:** Computing resources are accessible over the network, supporting heterogeneous client platforms (e.g. mobile devices and workstations).
3. **Resource-pooling:** The provider's computing resources are pooled to serve multiple users under a single or multi-tenant model, with different physical and virtual resources (e.g., storage, processing, memory, and network bandwidth) dynamically assigned and reassigned according to user demand.
4. **Rapid elasticity (scalability):** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward, commensurately with demand.
5. **Measured service:** Cloud systems optimise resource use by leveraging and metering their capabilities appropriately according to the type of service (e.g., active user accounts). Resource usage can be monitored, measured, controlled and reported, providing transparency for the provider and user (pay-by-use).

4.3. Deployment models

Cloud computing can be deployed in different models according to the type of use. There are four types of deployment models: private, public, community and hybrid (Figure 2). The main differences between these deployment models relate to the availability of the cloud infrastructure:

1. **Private cloud:** The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple users (e.g. business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them. The cloud infrastructure is generally hosted out of the premises of the organisation but the data location is under the organisation control.

   In GLP, a private cloud means hosting of computing resources solely for the use of the contracting test facility or the organisation where it belongs to. This occurs within a private internal network or where the infrastructure is dedicated to the contracting test facility with completely isolated access regardless of whether it is provided by an external or internal cloud service provider.

2. **Community cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of users from organisations that have shared requirements (e.g., mission, security requirements, policy, compliance considerations for test facilities). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them. The cloud infrastructure is generally hosted off premises.

   In GLP, in a community cloud, the cloud infrastructure is shared by several test facilities that have similar interests (e.g., regarding security, compliance). Access is not public but only accessible for a defined group

of users with joint requirements. Such a cloud can be operated by one of these institutions or a third party.

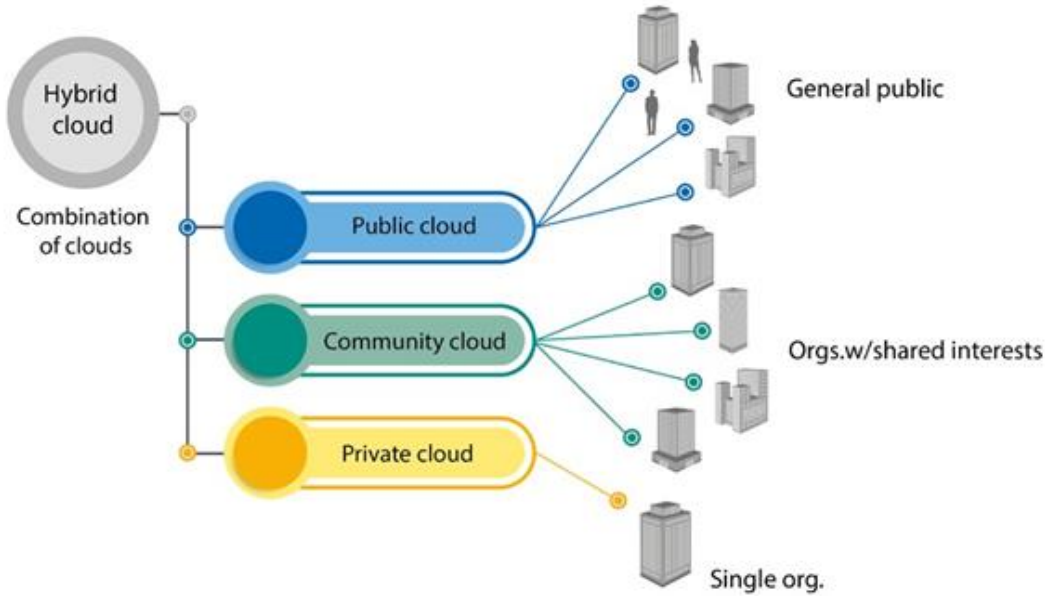
3. **Public cloud:** The cloud infrastructure is provisioned for use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider. The exact location of the physical infrastructure on which the data is stored, or the applications run, is generally unknown to the users.

   In GLP, public cloud means hosting of computing resources that can be used by the general public or a large group, such as an entire industry sector; these services are provided by the respective cloud service provider in its facilities/data centres.

4. **Hybrid cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). As examples of mixed cloud-based solutions, an application is hosted in a part of a public cloud whose accessibility and management are designed as in a private cloud by security measures and access restrictions ("private cloud in public cloud"). Or, the application is hosted in a public cloud, and the generated data are stored and saved in the servers of the test facility (mix of public cloud and traditional IT infrastructure).

   In GLP, hybrid cloud means a combination of public and private clouds. The test facility uses the public cloud but also has its own private cloud and can create a connection between the two to work as one system.

Figure 2. Cloud computing deployment models



Source: FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies (Crisanto et al., 2018[7]).

4.4. Service models

Service models refer to the type of computing resource that is offered. There are three main types of service model: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS):

1. **Infrastructure as a Service (IaaS):** The capability provided to the user is to provide processing, storage, networks, and other fundamental computing resources where the user is able to deploy and run arbitrary software, which can include operating systems and applications. The user does not manage or control the underlying cloud infrastructure (e.g. hardware) and has limited to full control over operating systems, storage, deployed applications and networking components (e.g., host firewalls)

   For GLP test facilities, the IaaS solution offers hosting and maintenance of hardware and network (both physical and virtual components) and the availability of storage and computing capacity and resources.

2. **Platform as a Service (PaaS):** The capability provided to the user is to deploy onto the cloud infrastructure user-created or acquired applications developed using programming languages, libraries, services, and tools supported by the cloud service provider. Platform as a service is where an external vendor supplies a platform for developing applications on the cloud such as an operating system, a middleware, a database, etc. in addition to the infrastructure. The provision of this service includes managing the infrastructure and basic application software. The user would be responsible for configuration of the application and its fitness for its intended use.

   In GLP test facilities, hardware and the environment are provided. The platform offers the possibility to manage data and documentation. Operations such as migration, classification, storage are also often included in such services. The GLP test facility remains responsible for the configuration of the systems and the management of software.

   - *Example: The cloud service provider provides an application server and a database to allow the implementation of a Laboratory Information Management System (LIMS).*

3. **Software as a Service (SaaS):** The capability provided to the user is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through an interface, such as a web browser or a programme interface. The user does not manage or control the underlying cloud infrastructure including applications, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

   In GLP, the SaaS model provides the test facility with applications which generate or analyse data as well as manage documentation and which are developed, installed, maintained and updated by a cloud service provider. The hardware is typically located in a data centre (mostly in public cloud to allow high amount of users). This hosting in a data centre is generally subcontracted by the vendor of the software to a third party. All the security design is ensured by the cloud service provider (usually via other subcontractors). The GLP test facility has to connect via a common or shared platform with specific access rights to use the software. Training is often part of the service provided. The level of computing intervention of

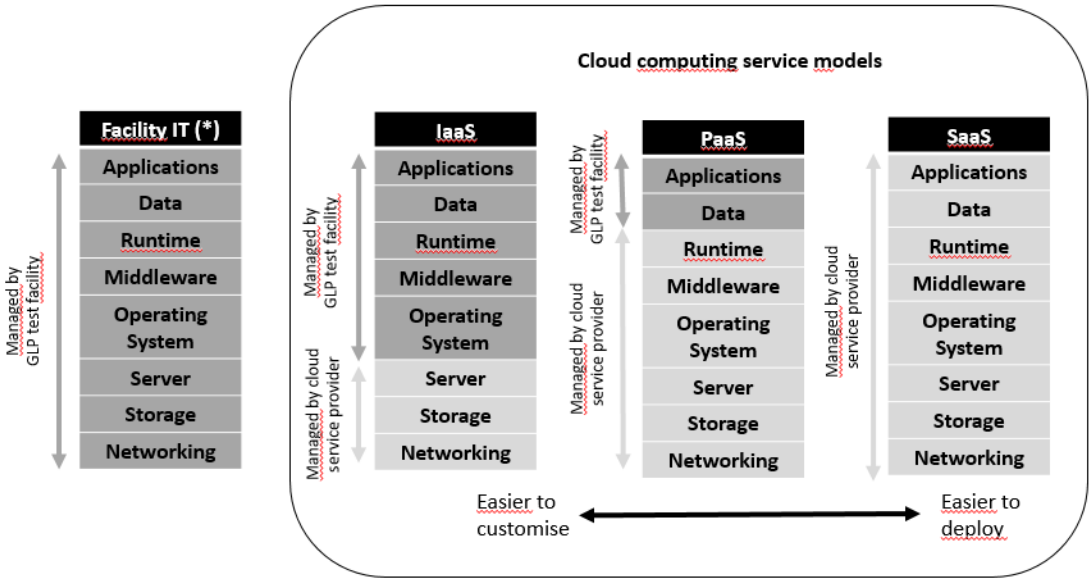
the GLP test facility is limited to internally defining user access to the system. It includes also the configuration of the application to the test facility's intended use, including security in the implementation phase. The use of SaaS consists of a connection with authentication mechanism and the entry of data.

- *Example: an electronic laboratory notebook system may be hosted in the public cloud allowing the capture of raw data on electronic devices. The data are directly transmitted from the devices via a secured network to be stored in a private (secured) area also hosted in a public cloud.*

4. **Desktop as a Service (DaaS):** compared to the SaaS model, this technology supplies also the desktop environment. In this model, all the components of the desktop are virtualized, and only a device is necessary to access the virtual desktop.

Figure 3 provides an overview of how the management of the main components of a cloud-based solution is typically shared between the test facility and the cloud service provider depending on the selected cloud computing service models.

Figure 3. Shared management of the main components of a cloud computing service between the GLP test facility and the cloud service provider



(*) Facility IT: means test facility IT systems without any use of cloud solutions.

Legend:

Managed by GLP test facility

Managed by cloud service provider

5. Cloud computing in GLP environment

5.1. Responsibilities of the test facility

TFM is responsible for GLP compliance within the GLP test facility and the systems that support GLP activities. If IT operations are moved from locally controlled servers to a cloud-based solution, it is essential that appropriate knowledge, awareness and oversight of the systems and practices remain with the test facility and control is exercised. This is regardless of whether this is an internally managed cloud (as part of the test facility or as part of the organisation to which the test facility belongs) or outsourced via an external cloud service provider.

Due to the complexity of the offered service, it is also recognized that TFM may delegate contracting and managing such services to specialists or internal specialized departments responsible for general vendor selection, contracting and supervision. Transparency on agreements and obligations of all involved parties is therefore key elements, allowing scalable level on details depending on service provided. Nevertheless, even if the tasks are delegated, TFM is still responsible for the GLP compliance of the systems used in the test facility.

The system administrator has access to live and archived data and documents. The circumstances of access and actions taken on the data need to be defined and clarified when data are hosted by a cloud service provider. Administrator rights should not be given to persons with a potential interest in the data and/or documentation. Clear risk mitigation strategies and controlled procedures should be developed and applied to ensure data integrity, quality and availably, independently on where the system administrator is located (test facility or vendor).

The study director should ensure that computerised systems (including virtual components that might be hosted locally or in a cloud) used in studies have been validated.

The archivist is responsible for the management of archives. If GLP archives are stored in a cloud-based solution, the archivist may need to use the assistance of specialists to look at technical aspects. Nevertheless, the archivist remains responsible and should still ensure that:

1. The archiving conditions ensure the integrity of the archived electronic records.
2. Access to the archives is controlled.
3. A system of indexing allows orderly storage and retrieval of records.
4. Migrations of archived electronic records are properly controlled and documented.
5. A process is implemented for periodic readability and data integrity checks.
6. A process is implemented to ensure the readability of data after being migrated from the cloud environment to the test facility (exit strategy).

The Quality Assurance (QA) programme should ensure that GLP compliance is preserved. The use of cloud-based solutions in GLP studies should be verified for their GLP compliance by QA as any other computerised systems.

5.2. Requirements

GLP requirements for computerised systems and hosted services (or cloud services) are described mainly in OECD Documents No. 1, No. 15 and No. 17. Table 1 provides an

overview of GLP requirements as specified in OECD Document No. 1 in relation to the different cloud computing service models.

Table 1. GLP requirement management within different cloud service models

Legend of the Table:
Light Grey: under the full management and intervention of the test facility.
Dark Grey: management and interventions shared among the test facility and the cloud service provider and its subcontractors, if any.
Black: under the full management of the cloud service provider.

Note: it is the ultimate responsibility of the test facility to assess and demonstrate whether the cloud-based services can ensure data quality, data integrity and data availability and do not affect GLP compliance of the test facility

(*) Traditional IT: means test facility IT systems without any use of cloud solutions.

Computing resources	Traditional IT (*)	GLP Principles requirements	Cloud service models		
			IaaS	PaaS	SaaS
Raw Data (including metadata)		1.2.2.f, 1.4.3, 8.3.5			
Data generation					
Data classification and accountability					
Protection					
User access management					
Encryption					
Metadata, audit trail generation and management					
Migration		1.2.2.f, 1.4.3, 8.3.5			
Physical security measures for raw data		1.2.2.i			
Applications and software		1.1.2.b, 1.1.2.q, 1.2.2.g, 4.1			
Application level controls (access, rights)					
Physical security measures for hosting of applications					
Runtime (databases)		1.1.2.q			
Middleware (interface between applications)		1.1.2.q			
Operating systems (Windows, Linux, etc.)		1.1.2.b			
Virtualisation		1.1.2.b			
Servers (account, application and data servers)		1.1.2.b, 3.1.1			
Storage		1.1.2.b, 1.2.2.i, 3.1.1			

Computing resources	Traditional IT (*)	GLP Principles requirements	Cloud service models		
			IaaS	PaaS	SaaS
Backup and restore		1.1.2.b, 1.2.2.i, 3.1.1			
Data archiving		1.1.2.b, 1.1.2.l, 1.1.2.q, 3.4, 9.2.7, 10			
Host infrastructure					
Physical security measures for hosting of archives					
Networking (web browser, web server)		1.1.2.b			
VPN, firewall, and network security					
Network control					
Disaster Recovery Plan (DRP)		1.1.2.b, 3.1.1, 3.4			
Retirement		1.1.2.q, 10.4			
IT personnel		1.1.2.b,c,d, 1.4.1			
Computerised systems validation (and periodic review, change control)		1.1.2.q, 1.2.2.g			
Quality Assurance (QA)		1.1.2.f, 2.1.1, 2.1.2			

All requirements indicated in OECD Document No. 17, section on "supplier" (section 1.6, paragraphs 34 to 40) should be fulfilled by the test facility to manage the cloud service providers.

Document No. 17 states that (paragraph 39) cloud or hosted services (e.g. platform, software, data storage, archiving, backup or processes as a service) should be treated like any other supplier service and require written agreements describing the roles and responsibilities of each party.

It is the responsibility of TFM to evaluate the relevant service and to estimate risks to data quality, data integrity and data availability. TFM should be aware of potential risks resulting from the uncontrolled use of cloud services and should have the means to be made aware of these risks and its impacts on GLP compliance. Appropriate risk mitigation measures should be in place and documented.

Cloud service providers can interact directly or as a subcontractor from another supplier. TFM should appropriately control all GLP relevant suppliers and subcontractor activities should be transparent to TFM. Written agreements between the test facility and the cloud service provider should mention if parts of the service may be subcontracted (see section on "Service Level Agreement").

5.3. Implementation of cloud-based solution in GLP

Where cloud services are used to provide, install, configure, integrate, qualify, maintain, modify or retain a computerised system, the following four key elements will play a crucial role in ensuring whether a GLP test facility can demonstrate compliance to the GLP Principles.

1. Detailed risk assessment (with the description of the cloud solution as prerequisite).
2. Thorough cloud service provider assessment, including audits when relevant, prior to use and periodic review.

3. Clearly defined service level agreements directly related to the operational activities and services to be provided.
4. Validation of the computerised systems hosted in cloud-based services.

Note: the same requirements are valid for physical and virtual servers.

5.3.1. Risk assessment and selection of the cloud-based services

Risk management should be applied throughout the lifecycle of any computerised system, taking into account data quality, data integrity and data availability.

Prior to committing to a cloud-based solution, TFM should identify and describe potential failure modes, assess the associated risks for GLP compliance, including the likelihood and impact, and where applicable, come up with effective mitigating actions. Cloud-based services should be developed, released and managed to ensure data quality, data integrity and data availability without jeopardizing GLP compliance of the test facility.

A detailed description of the expectations to the use of the cloud solution and the associated impacts should be available before any choice is made. The steps of the risk assessment include (but are not limited to):

1. Expected objectives and functionalities including system requirements, user requirements and constraints for the system.
2. Infrastructure and applications: the extent to which infrastructure, network/platforms and applications are expected to be provided.
3. Impact on GLP compliance, especially regarding data migration and storage, resulting from adopting the system provided by the cloud service (non-exhaustive list):
    a. Expected new data process and changes from the current system: in particular, steps for data migration should be carefully identified and described.
    b. Associated new risks on data quality: risks linked to newly supplied applications to capture, generate or analyse data (reliability, availability of system and data, backup plans for system failure).
    c. Associated new risk on data integrity and data availability: level of control of remote access to the data, level of protection of the data, secure location for the physical storage of the data (physical infrastructure access, disaster recovery strategy, recovery time objectives and recovery point objectives, location of the data hosting servers, long term integrity of electronically archived data). For SaaS, as the test facility has generally no access to the software itself in case of release event, impacts on data integrity and data availability should be carefully considered by end user when anticipating the business continuity plan, the disaster recovery plan and the exit strategy of the GLP test facility.
    d. Impacts on systems architecture (both the test facility systems architecture and the systems architecture of the cloud service provider), organisation and operating model.
    e. Impacts on protection of data ownership.
    f. Impacts on competence of the study personnel, study directors, QA personnel and archivist, especially need for training.
4. Expected measures to mitigate the identified risks, including (non-exhaustive list):

   a. Need for adequate controls to maintain or verify data quality, data integrity and data availability and the need for data review.
   b. Existence of audit trails, where appropriate.
5. Established criteria for selection of the cloud service provider including compliance with specific quality standards and the availability of contingency plans for provider failure such as disaster recovery, security of the cloud service provider etc. (see also section on "cloud service provider assessment").
6. Service migration plan for provider end of service.
7. Archiving (when applicable).

When a cloud solution is being selected for use, a clear and complete description and implementation plan should be generated. This should include:

1. Cloud service provider(s): name(s) and address(es) of the company (if known, address(es) of the data centres) and contacts, reference to the contract(s).
2. Details of any subcontractors of the cloud service provider(s) relevant to GLP compliance: technical role, names and addresses, reference to the contracts.
3. Overview of the solution selected with detailed description, gaps between expected and provided functionalities, services/products selected, parties involved and delivery location(s).
4. Detailed specifications of activities performed by the cloud service provider (see Table 1), especially sharing of technical tasks, roles and responsibilities between the cloud service provider, its subcontractors and the test facility (see also section on "service level agreement").
5. Detailed process of validation, including tasks and means provided by the cloud service provider (including possible access when relevant to a test environment where the system can be tested before being put into production).
6. Detailed specification ensuring control of access to the data (remote access, cloud service providers' access to systems and data, cloud service providers' access to perform changes directly within database where applicable), level of protection of the data, (including IT security activities, e.g., management and review of user accesses, management of passwords, management of firewalls, backup and restore, handling of security incidents, maintenance and security patching of platforms (databases and operating systems), intrusion detection and protection).
7. Determining the type of service model to implement –IaaS, PaaS or SaaS.
8. Determining the type of deployment model – private, public, community or hybrid.
9. SOPs required to govern the routine use, administration and maintenance of the system.
10. Training of the test facility personnel if required.
11. Means of control of the solution by the test facility: these controls should be planned to verify that the system is maintained in a validated state to ensure data quality, data integrity and data availability. These controls should be implemented independently from the cloud service provider (internal or external provider), be monitored and the documentation retained. The effort of control should be linked to the functionalities ensured by the cloud-based solution. For example:

a. If the cloud-based solution is used for archiving data, periodic controls should be implemented to verify the data integrity and data availability of the archives. The frequency of such controls should be risk-based.

b. If the cloud-based solution is a SaaS, data quality, data integrity and data availability can be verified by electronic controls in each run or periodically, check-sums, review of audit trails or of the accesses, or any other solutions. The frequency of such controls should be risk-based. Periodic SaaS application reports which can be provided by the cloud service provider cannot replace independent controls.

5.3.2. Cloud service provider assessment

Note: The management of the cloud service provider plays a vital role to ensure the quality and compliance of the services. The expectations of the test facility from the cloud service provider to ensure a level of service that is fit for purpose for GLP use should be defined in the service level agreement (see section on "service level agreement").

The established criteria for the selection of cloud service providers should be documented.

The competence and reliability of a cloud service provider are key factors when selecting a product or service provider. A cloud service provider audit may be appropriate and the decision to conduct an audit or not of the cloud service provider should be based upon documented risk assessment. The audit team could also include users, QA personnel, IT experts and/or external experts.

Activities of cloud service providers may be subcontracted to other suppliers. In case of any subcontracting, it is the ultimate responsibility of the test facility to assess and demonstrate that the cloud-based services do not affect GLP compliance of the test facility.

During cloud service provider assessment, it is essential to verify which (if any) quality system is in place at cloud service provider (including systems of relevant subcontractors).

Cloud service provider (and subcontractor) may hold certified quality systems. These may be considered by the test facility, if they support GLP compliance of the test facility.

Note: some national regulations (non GLP) may require that the cloud service providers have defined certifications on the level of security they provide prior to ensure the hosting of some specific data (e.g., personal data, medical data, health data). Responsibility of TFM is limited to GLP compliance issues.

Test facility can also choose to outsource the assessment of the cloud service provider to an external expert and the appropriateness of this should be assessed by TFM, with the support of QA.

Following general items may be addressed during the assessment (non-exhaustive list):

1. Quality system of the cloud service provider if any (including subcontractor(s) and standard operating procedure management).
2. Documentation process.
3. Personnel management (including training).
4. Confidentiality and security.
5. Control of access to data.
6. Premises and used technology.

7. Qualification of equipment involved in system in scope.
8. Qualification of system in scope (to verify that the required functionalities are successfully tested).
9. Understanding and policy of data integrity.
10. Backup and restore tests.
11. Disaster recovery processes.
12. Exit strategy.
13. Technical assistance resources.

With regards to the cloud-based solution itself and the associated service, the test facility should assess if the provisions of cloud-based services meet the predefined expectations. The cloud service provider needs to have the systems and information readily in place which are commensurate to the activities they perform to support GLP compliance. The cloud service providers should have (considering the service they provide):

1. Personnel records of all employees directly involved in the services provided to the test facility including:
    a. Records describing the basic education/training and professional experience.
    b. Training records of continuing education, IT and Quality Management related, appropriate to perform their duties.
    c. Description of the current responsibilities and roles (e.g. job description, organisational chart).
2. GLP awareness training. This may be a risk mitigation strategy of TFM to ensure key personnel understands the GLP regulations and requirements applicable to the services being provided, in particular data security and storage.
3. Specific provisions in relation to cloud services including, for example:
    a. Documentation about the life cycle of the provided system.
    b. Data integrity understanding of data flows, data processing.
    c. Back-up and restoring of electronic data and records.
    d. Archiving of electronic data and records.
    e. Electronic data ownership and access rights.
    f. Change and release management.
    g. Management of the subcontractors, if applicable.
4. Documentation about all activities performed on behalf of the test facility that ensures the traceability of these activities.
5. Provided access to documents as requested for inspections or QA audits.
6. Have qualified equipment/hardware in place.

Test facility should verify that the documentation and procedures of the cloud service provider are adequate to ensure a suitable qualification and validation approach for the services provided.

5.3.3. Service Level Agreement (SLA)

> **Note:** Different terms are used to describe document(s) in which operating clauses for cloud service are described: contracts, quality (assurance) agreements, technical specifications, etc. The term Service Level Agreement (SLA) is used in this document.

Risk assessment, validation of the system, cloud service provider assessment and service level agreement should clearly indicate that the relevant aspects to data quality, data integrity and data availability are covered when cloud computing is implemented at the test facility. Formal agreements should exist between the GLP test facility and the cloud services providers. These agreements should include clear responsibilities of the cloud services providers' subcontractors, with statements of the responsibilities for the data of any third party(ies) involved in the service.

The SLA is the central document defining all aspects of collaboration between the GLP test facility and the cloud service provider. The SLA should address all relevant aspects including, but not limited to, responsibilities, the use of subcontractors, documentation, performance, archiving, training, communication, reporting lines, audits, validation.

The use of subcontractors by the cloud service provider should not affect the data quality, data integrity and data availability or overall GLP compliance of the test facility. Appropriate arrangements should be in place for the orderly transfer of the activity, data or services from the contractor to subcontractor. Subcontracting should be authorised in the service level agreement between the test facility and the cloud service provider.

Although there is no general requirement for the supplier to be GLP compliant itself, all requirements relevant to ensure data quality, data integrity and data availability should be included in the SLA. SLA should allow the cloud service provider to understand and assume its responsibilities on the data and those entrusted to its subcontractor(s). The test facility should conduct due diligence to ensure the provided service does not compromise data integrity and supports GLP compliance in general.

Roles and responsibilities

Roles and responsibilities of test facility and cloud service provider should be clearly described.

TFM has the overall responsibility for GLP compliance of the life cycle of their computerised systems and for IT supporting services, even if cloud service providers provide these services.

The cloud service provider is responsible for the delivery of cloud-based services that enables the test facility to fulfil all applicable GLP requirements, as specified in the SLA.

If activities from the cloud service provider are subcontracted to other suppliers, this should be addressed. A list of subcontractors, subcontracted activities and associated responsibilities should be present in the SLA.

It is highly recommended that draft SLAs are reviewed by QA in order to ensure all aspects of GLP compliance are met, however, final responsibility for SLA approval remains at TFM.

Modalities of periodic review of existing SLAs should be defined in the SLA. The possibility of cloud service provider audits should be defined in the SLA and scheduled in the QA programme of the test facility.

Documentation such as SOPs, personnel records, reports, change control documentation of both partners should reflect respective information from the SLA. Each party should maintain the specific documentation required by the SLA.

System life cycle

The SLA should describe the duties of the cloud service provider (and any subcontractor(s)) and the test facility during the life cycle of the supported systems. This may include installation, configuration, integration, validation, maintenance (e.g. via remote access), modification, retention or retirement of the system. As a minimum, following points should be covered:

1. Data storage.
2. Security.
3. Change control (including application/software updates) and configuration management. A period of time should be discussed with the cloud service provider and defined in the SLA to allow the test facility to conduct testing before implementing changes on the cloud services. The SLA should also state that details about the modifications of the new version and documentation about validation, when applicable, should be provided to the test facility. Access when relevant to a test environment where the new version of the system can be tested before being put into production should be available.
4. Incident management.
5. Business continuity (including back-up and recovery, especially back-up intervals, details on possible locations of mirroring, expected documented confirmations about back-up and mirroring, time for recovery, etc).
6. Qualified infrastructure.
7. Data management.
8. Data integrity maintained throughout record retention period.
9. Periodic evaluation by the test facility.

Security and Access Control

Appropriate technical and organisational measures should ensure the logical and physical security and availability of both the data and systems. Maintenance of the systems and incident management should be addressed in the SLA.

The SLA should also cover the management of access privileges, including the periodic review of accesses, and these should be restricted to authorised personnel regardless of how the system is accessed.

It should be clearly stated that data should not be accessed, migrated (manually, not by storage controller), changed, modified or deleted by the cloud service provider or its subcontractor without prior formal written authorisation by TFM.

Procedures on how to prevent cyber-attacks, including, but not limited to, access to electronic data during attacks, and how to restore data and ensure integrity of raw data once it is available again, should be defined.

Documentation of the cloud service provider on the systems

The SLA should define which records are to be retained and archived. The physical and/or logical location of archiving and the retention period should also be defined. The test facility should define documents and records of the cloud service provider that ensure the required traceability of the provided system and verify the availability of such documentation. All defined documents should be accessible by the test facility and GLP compliance monitoring authority inspectors.

Communication

The communication lines between the test facility and the cloud service provider should be described in the SLA. The means of communication such as physical or virtual meetings, phone, email, hot line should be defined. There should be an agreement as to which information is to be shared (incident management, change control, access to the data by the vendor etc.). Both parties should cooperate to ensure the compliant and valid operation of the system and to maintain the qualified and validated state of the system.

Exit strategy

The SLA should clearly describe the test facility's right to obtain all data and meta-data (including audit trails) in a readable and convertible format, in case the contract with the cloud service provider is terminated (see also OECD document No. 22 chapter 6).

Final destruction of data

The SLA should define the process of destruction of data after termination of the contract. The SLA should state that the cloud service provider shall effectively and irreversibly remove and destroy all the data belonging to the test facility after recovery. The cloud service provider should upon test facility's request provide documentation for certification of such removal and destruction.

5.3.4. Validation of the computerised systems in the cloud-based service

As a requirement of the use of computerised systems in GLP, the test facility should use validated systems only, regardless of whether they are SaaS or hosted on IaaS/PaaS.

All requirements concerning the computerised system validation should be met. Decisions on the extent of validation activities and data integrity controls, performed under the responsibility of TFM, should be based on a justified and documented risk assessment on the computerised system.

The test facility should ensure that all computerised systems are properly validated. The test facility should clearly define the user requirement specifications (even if they may originate from the cloud service provider validation documentation).

The test facility should understand what needs to be validated (the application as fit for its intended use within the process), who is responsible to ensure all requirements for computerised system validation are met.

If part of the validation documentation is supplied by the cloud service provider, it should be assessed by the test facility for its relevance in the validation process. In case validation documentation from the cloud service provider is used, this should be readably available at the test facility.

For example, in the case of a SaaS:

1. The cloud service provider can provide evidence that the successful installation and management of the application, such as application functional testing, automated testing, unit testing, application programming interface (API) testing, have been performed; even though this may have happened independently of the test facility involvement. The cloud service provider can qualify the hosting infrastructures. SOP for the lifecycle of the application are generally issued by the cloud service provider. TFM should assess the work of the cloud service provider to confirm it has been performed properly for the system in use in the test facility and to detect what is missing. TFM should document and approve this assessment.
2. The test facility should conduct any additional testing that needs to be completed, especially testing in the test facility environment, and the controls needed for the ongoing compliant use of the system (including training of the users, issuance of SOP for the use of the application in a GLP environment).

As for all computerised systems, the test facility should also make proper arrangements and have procedures in place in case the agreement with the cloud service provider ends or the system is retired, to ensure all data and metadata (including all audit trails) are archived or migrated throughout the duration of the required retention period. Provisions for exit strategy to ensure the data recovery should be tested where possible during the validation of the system.

6. Expectations of the GLP compliance monitoring authorities when inspecting cloud – based solutions

GLP systems should be validated and operated in a way which ensures the outcome and integrity of GLP data regardless of whether they are installed locally or provided as a cloud service.

6.1. Implementation of the cloud solution

The following documentation should be available to allow verification of the cloud services by GLP inspectors:

1. Records of the implemented systems, including the rationale for the selection of the systems, the risk assessment on data quality and integrity and the description of the implemented systems.
2. Documentation on the validation process:
    a. The documentation of the qualification activities performed by the cloud service provider should be available at the test facility.
    b. The evidence that the qualification activities by the cloud service provides have been assessed as complete and adequate should be provided during the inspection either by the test facility itself, or with help from the cloud service provider where the test facility relies partially on qualification documentation provided by the supplier.
    c. The documentation of additional qualification/validation activities based on a documented risk assessment that is performed by the test facility should also be available.

3. The rationale for the choice of the cloud service provider (see also section on "cloud service provider assessment"), even if internal, should be available and include documented assessment/audit of the cloud service providers quality system and qualification and validation processes. Any shortcomings identified should be mitigated by the test facility.
4. The service level agreement between the test facility and the cloud service provider, with clear descriptions of the shared activities and responsibilities on the system.

6.2. Life cycle of the cloud service application

Evidence of the measures implemented by the test facility to ensure continuous validity of the cloud-based solution should be available (by the test facility itself or enforced through the SLA with the cloud service provider). This includes provisions to ensure (list non exhaustive):

1. Availability, maintenance, updates, business continuity, disaster recovery plan and migration plan of the system.
2. Data integrity throughout the life cycle.
3. Data quality throughout the life cycle.
4. Data availability.
5. An independent plan of controls implemented and conducted by the test facility to ensure that the cloud-based system stays in a validated state through its life cycle.
6. Documentation about remote access and authentication.
7. The exit strategy, when the contract is ended, should clearly describe how the test facility will obtain all data and meta-data (including audit trails) in a readable and convertible format, in case the contract with the cloud service provider is terminated.

In addition to the documentation, demonstration of how a system works can be requested by inspectors to verify its compliance. The test facility should have available details of the functional tests of the system for the inspectors.

6.3. Electronic archives in cloud solution

Cloud service providers may act as a contract archive by providing services or components to retain and archive GLP relevant data and records.

GLP compliance monitoring authorities have different approaches concerning contract archives. Some include them in their monitoring programmes as GLP archive providers; others consider them during the inspection of a test facility. Electronic archives should comply with the applicable GLP Principles (including OECD Document No. 15) and TFM must ultimately ensure that this occurs. Cloud service providers may also be inspected for the GLP compliance by the monitoring authorities.

Inspection of the location of servers used for archiving (e.g. buildings, rooms and cabinets) to verify the physical security of the hosting facilities is not always possible, especially if the location is unknown. However, it is noted that some GLP compliance monitoring authorities require details on location of a cloud archive for physical verification, which excludes the use of servers with unknown location for the hosting of electronic archives.

The test facility should be able to provide documented evidence of GLP compliance for the archive such as the service level agreement and assessment/audit of both the cloud service provider and of the system.

Information on the computerised systems and cloud service providers that support logical and technical integrity should be available. This would include proves of full control by archivist, access control, inventory for indexed orderly storage, record retrievability, evidence of record integrity and traceability from raw data to final report.

The relevance of all measures to ensure logical, technical and physical integrity should be documented in a risk-based rationale.

Measures such as a risk-based back up policy are important. Documented evidence of relevant and efficient back-up and mirroring measures and restoration protocols and a control over those processes by the test facility should be available.

7. Conclusion

Cloud service providers can offer various solutions that allow acquisition of data for the safety of humans, animals and environment. Implementation of cloud-based solution should not jeopardize the compliance of the GLP activities so that data quality, integrity and availability are assured.

When conducting an inspection with cloud-based services involved in the test facility processes, GLP inspectors expect TFM to be able to demonstrate that GLP compliance is still ensured with the implemented cloud service and that TFM has adequate means to control it.

8. Glossary

Back-up (see document No. 17).

Change control (see document No. 17).

Computerised system (see document No. 17).

Data (see document No. 17 or 22).

Database: a database is information that is set up for easy access, management and updating. Computer database is an organised collection of data stored, maintained and accessed electronically. Small databases can be stored on a file system, while large databases are hosted on computer clusters or cloud storage.

Data centre: a data centre is a physical facility which is used to house electronic applications and data. A data centre's design is based on a network of computing and storage resources that enable the delivery of shared applications and data. The key components of a data centre's design include routers, switches, firewalls, storage systems, servers and application-delivery controllers.

Data protection: data protection is the process of safeguarding data from corruption, compromise or loss and providing the capability to restore the data to a functional state when something happens to render the data inaccessible or unusable.

Encryption: data encryption converts data from a readable, plaintext format into an unreadable, encoded format. Users and processes can only read and process encrypted data after it is decrypted. The decryption key is secret to be protected against unauthorized access.

Hardware: hardware refers to the computer's tangible components or delivery systems that store and run the written instructions provided by the software.

Qualification (see document No. 17).

Qualified/verified infrastructure: IT infrastructure qualification is the process of demonstrating that IT components are developed to be fit for their intended use, meet specified requirements and that the system's fitness state is maintained throughout each point in the system's life cycle.

Life cycle (see document No. 17 for computerised system life cycle and document No. 22 for data life cycle).

Network: a computer network is a set of computers sharing resources located on or provided by network nodes. The computers use common communication protocols over digital interconnections to communicate with each other.

Operating system (see document No. 17).

Recovery time objectives: recovery time objective is the goal an organisation sets for the maximum length of time it should take to restore normal operations following an outage or data loss.

Recovery point objectives: recovery point objectives is the goal for the maximum amount of data the organisation can tolerate losing. This parameter is measured in time: from the moment a failure occurs to the last valid data backup.

Risk (see document No. 17).

Risk assessment (see document No. 17).

Risk mitigation (see document No. 17).

Security (see document No. 17).

Server: a server is a software or hardware device that accepts and responds to requests made over a network. The device that makes the request, and receives a response from the server, is called the client.

Software (see document No. 17).

Validation (see document No. 17).

Virtual Private Network (VPN): a virtual private network, or VPN, is an encrypted connection over the internet from a device to a network or between two networks. The encrypted connection ensures that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

References

OECD (2016), *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 17: Advisory Document of the Working Group on Good Laboratory Practice : Application of GLP Principles to Computerised Systems*. [1]

OECD (1997), *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 1: OECD Principles on Good Laboratory Practice (revised in 1997)*. [2]

OECD (2007), *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 15: Advisory Document of the Working Group on Good Laboratory Practice : Establishment and Control of Archives that Operate in Compliance with the Principles of GLP*. [3]

OECD (2002), *OECD Series on Principles of GLP and Compliance Monitoring Number 5 (Revised): Consensus Document on COMPLIANCE OF LABORATORY SUPPLIERS WITH GLP PRINCIPLES*. [4]

OECD (2021), *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 22 Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity*. [5]

Peter Mell, T. (2011), *The NIST Definition of Cloud Computing*, NIST. [6]

Crisanto, J. et al. (2018), *FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies*, https://www.bis.org/fsi/publ/insights13.pdf. [7]

Stocker, E. and B. Grobauer (2011), *Understanding Cloud Computing Vulnerabilities*, Security & Privacy IEEE, https://www.infoq.com/articles/ieee-cloud-computing-vulnerabilities/. [8]