Quality Matters™

Member Newsletter of the Society of Quality Assurance

Back to *Quality Matters* Home

Published with Volume 41.1 of Quality Matters, SQA Technical Article 2025-1.

A joint position paper by the Computer Validation and Information technology Compliance (CVIC) Specialty Section and the Japan Society of Quality Assurance

Using a Cloud Environment for Regulated Data

SQA CVIC Contributors:
Richie Siconolfi, FRQA
Vince D'Angelo
Bill Drummond
Chris Meister
J. Heléne Andersson, RQAP-GLP
Joseph Franchetti
Kevyn Matijevich, RQAP-GCP
Ricardo Torres-Rivera, PMP
Santosh Tharkude, CISA, CET

JSQA Contributors:
Daisuke Sasaki
Akira Yamazaki
Wataru Matsugi
Yoshikazu Masaki
Noriaki Katanozaka, PhD
Isao Watanabe
Yoshiaki Hiraishi
Terukazu Kitahara
Ryo Okumura

Introduction

The advent of technology has impacted the regulatory environment in many ways. In one respect, it has made controlling regulatory information easier, quicker, and with better reliability. However, in another respect, technology has made compliance a challenge. This position paper represents critical thinking of risk assessment, computer software assurance, and computer system validation in relation to the use of cloud environments for the storage of regulated data. The requirements should be the same for on-premises data centers. Finally, points to consider for meeting regulatory compliance requirements when using a cloud environment are presented.

Where is it Written?

There are many laws, regulations, and guidance documents that require computerized systems to be validated. Validation is only one part of compliance. By implementing cloud computing, the regulated industry may conduct their work faster, cheaper, and better. While this represents progress, it also forces the company implementing a cloud computing system to spend more time up front to conduct risk assessments based on critical thinking, regulatory requirements, widely accepted guidance documents, and cloud computing standards. The references listed below are some of the key regulations that impact computer system validation and risk assessment. There are two regulations we should discuss to establish a baseline for points to consider.

The first document is the Supplement 1 to OECD Document Number 17 on Application of GLP Principles to Computerised Systems[1]. These are the key concepts from this guideline:

- “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.”
- “Data integrity maintained throughout record retention period.”
- “The physical and/or logical location of archiving and the retention period should also be defined.”

OECD Document Number 15 on Establishment and Control of Archives that Operate in Compliance with the Principles of GLP state the following:

- Test Facility Management is responsible for providing archive facilities.
- “If a sponsor or test facility management uses a contract archive for the storage of records and/or materials for a GLP study, the contracting parties should ensure compliance with the relevant sections of the Principles of GLP.”
- “The Study Director is responsible for ensuring that during or immediately after completion (including termination) of a study, all study related records and materials are transferred to the archive(s).”
- “The archivist is responsible for the management, operations and procedures for archiving in accordance with established Standard Operating Procedures, and the

Principles of GLP."

- "IT personnel involved in archiving operations (such as ensuring integrity of electronic records) should be adequately trained and their activities should conform to GLP requirements. Since activities pertaining to archiving are the primary responsibility of the archivist, these IT personnel ideally should work under the direction and supervision of the archivist." (It is the sponsor's responsibility for ensuring compliance with the regulations.)

The other document to consider is US FDA 21 CFR Part 11 Guidance on Scope and Application[2]. Within this guidance document, the US FDA allowed regulatory discretion for record retention, audit trails, electronic signatures, and validation. This translates to critical thinking. For example, the regulated industry can conduct and document a risk-based approach to validation providing the process has been vetted and documented. These three guidelines allow the regulated industry to assess cloud environments for regulated data and computerized systems. Addressing these regulations in a robust action plan will provide adequate mitigation.

Assessing Cloud Service Providers

The US FDA and ICH introduced the concept "Quality by Design."[3]This was originally directed toward manufacturing of regulated product. However, many quickly used the concept to assess computerized systems for 21 CFR Part 11 compliance via the Scope and Application Guidance document previously mentioned. By incorporating Quality by Design, along with critical thinking, and a documented risk-based approach to validation can be easily applied to ensure data retention in the cloud environment is safe, retrievable, and maintains its data integrity and data quality.

It has been proposed that regulators may need the physical address of the cloud service provider hosting a company's data to conduct an independent inspection, but it would suffice, as cloud users, to be satisfied with a geographical region, such as Eastern United States or Western Europe. The justification for using region is based on cloud technology, where data may be geographically controlled by identifying and configuring authorized regions as deemed appropriate by the cloud user, which provides a sufficient level of local control. Other reasons for the selection of a region might be to align with allowable locations to hold personal data under local or national data protection regulations. Controls may be assessed via means other than conducting an onsite visit to a cloud service provider.

Based on critical thinking in a risk-based assessment, a cloud data solution may be preferred to an on-premises solution for multiple reasons, such as:

- Reducing facilities expense;
- Outsourcing and transferring the risks of operating a data center to a qualified service provider
- Assessing compliance controls are in place to minimize compliance risks, including cloud service providers for their interpretation of regulatory compliance.

Once the risk-based assessment has been documented to assure continued compliance, initiate periodic reviews. The regulated company should document a plan and subsequent report to defend a risk-based approach to store regulated data with a cloud service provider. This starts with an evaluation of the cloud service providers access, safeguards, backup strategy and the shared responsibility model many cloud service providers describe on their public facing websites. Review processes for incident and problem management and processes for notifications of change control. Ensure cloud service providers maintain processes for information security and backup and restore of data when used for that purpose. Regulated companies may also institute their own backup and restore procedures.

The regulated company is responsible to assure processes for computerized system validation, data integrity, business continuity and disaster recovery, with input from the cloud service provider. A company may be able to leverage testing conducted by cloud service provider to support the computerized system validation process.

There are many approaches to developing a risk-based approach by employing the elements of critical thinking. Here are other key areas to consider:

- Record criticality (High, Medium, or Low as determined by the cloud user's procedures for a risk-based approach to validation)
- Criticality of computerized system[4]
- FDA's inspection discretion for validation, record retention, and audit trail[5]
- Regulated companies may consider using experienced third-party auditors to evaluate cloud service providers.
- Cloud provider ISO certifications, such as ISO 9001, 27001 and 13485 (See the Bibliography)

Points to Consider

- Cloud Service Provider Assessments is the responsibility of the regulated company. As stated above conduct risk-based assessment prior to use. Work with the Cloud Service Provider to identify the geographic location.

- Data Integrity is the principle combined with continuity of your business. Seek assurances and objective evidence that controls are in place to safeguard data from unauthorized changes. This may be accomplished with computerized system validation.
- Disaster Recovery is being comfortable with the cloud provider's recovery point objective (RPO) and recovery time objective (RTO).
- Audit Team: The audit team could also include users, QA personnel, IT experts and external consultants.
- Change Control: Because some Software as a Service (SaaS) vendor companies may not have control over software upgrades, based on criticality, companies may develop and implement system-specific procedures to assess release notes to determine impacts (e.g., validation documentation and existing SOPs) and define applicable action plans.
- Exit strategy: Ensure contracts specify how and when data and metadata will be returned, in what format, how long the extraction process is allowed, and assurances that copies of data held in the cloud environment are permanently removed and deleted. For example, in some instances, an exit strategy may be included as part of procurement or contractual documents, service level agreements (SLAs) or similar.
- Additional points to consider are highlighted in the appendix to this document.

Summary

Cloud service providers offer security, reliability, and data protection for regulated data. However, it is up to individual regulated companies to conduct audits and assessments of the providers to verify regulatory compliance. This requires each company to develop and demonstrate compliance by implementing a risk-based approach to assessments, audits, and validation by providing evidence based on critical thinking, partnerships with cloud service providers, and ensuring periodic reviews are conducted and documented.

References

1. 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, June 2023
2. US FDA Guidance for Industry, 21 CFR Part 11, Electronic Records; Electronic Signatures - Scope and Application, August 2003
3. Guidance for Industry, Q8(R2) Pharmaceutical Development, November 2009
4. GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems, Second Edition, 2022
5. US FDA 21 CFR Part 11 Scope and Application Guidance Document, 2004

Bibliography

- US FDA 21 CFR Part 58 Good Laboratory Practice Standards
- USFDA 21 CFR Part 11Electronic Records and Electronic Signature Rule

- MHRA ER/ES Guideline
- MHRA CSV Guideline
- Japanese GLP Regulations
- General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002
- EU GMP Chapter, Annex 11 Computerised Systems, 2011
- ISO 9001 Quality Management System
- ISO 27001 Information Security Management System
- ISO 13485 Medical Device Quality Management System
- ISO 27017 Cloud Security Control
- Certificates of Operation
- SOC 2 Report and Certified Auditor

Appendix

This appendix (PDF) is intended as an aid in meeting OECD 17 Supplement 1 (OECD 1 S1) requirements. Refer to the actual regulation for specifics to ensure compliance. Although specific to Good Laboratory Practices (GLP), the supplement's various guidance may be appropriate for other regulated cloud systems and services. For brevity, not all references within the supplement are identified when addressing the same topic.

Appendix

This appendix is intended as an aid in meeting OECD 17 Supplement 1 (OECD 1 S1) requirements. Refer to the actual regulation for specifics to ensure compliance. Although specific to Good Laboratory Practices (GLP), the supplement's various guidance may be appropriate for other regulated cloud systems and services. For brevity, not all references within the supplement are identified when addressing the same topic.

OECD 17 S1 Section#	OECD 17 S1 Section Name	Select OECD 17 S1 Extracts	Comment
5.1	Responsibilities of the test facility	Test Facility Management (TFM) may delegate contracting and managing such services to specialists or internal specialized departments responsible for general vendor selection, contracting and supervision…TFM is still responsible for the GLP compliance of the systems used in the test facility.	Delegation of responsibilities between TFM and specialists or specialized departments should be documented and include measures for TFM "awareness and oversight."
5.1	Responsibilities of the test facility	The circumstances of access and actions taken on the data need to be defined and clarified when a cloud service provider hosts data.	Throughout the supplement there is emphasis on SLAs documenting a clear division of responsibilities between the cloud user and the cloud provider. The section 5.1 extract regards system administrator access. See also OECD 17, section 1.6. QA should review draft SLAs for GLP compliance. Final SLA approval remains with TFM (may be delegated). TFM should have procedures in place describing how data will be accessed and retrieved. These procedures are important for daily operations to ensure data integrity.

5.1	Responsibilities of the test facility	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. The Quality Assurance (QA) programme should ensure that GLP compliance is preserved.	As with the TFM, GLP responsibilities of other staff are unchanged. Although supplier management practices may outsource specific procurement and contractual activities to external contractors, the QA unit is still responsible for managing and monitoring GLP compliance, including but not limited to supplier audits, software validation, and others.”
5.2	Requirements	It is the responsibility of TFM to evaluate the relevant service and to estimate risks to data quality, data integrity and data availability.	Conduct quality risk management appropriate to the level of risk and ensure TFM awareness, including a detailed risk assessment.
5.2	Requirements	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”).	GLP site’s audit of cloud providers (prior to use and periodic review) should include a review of SLAs for a cloud provider’s GLP relevant subcontractors (identification, responsibilities, and notification of changes).
5.3.1.3.c	Impact on GLP Compliance	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).	Specific data center locations and addresses may not be available to cloud users due to security concerns (see also section 6.3). However, SLAs should identify the regions for all data locations (e.g., production, backup, archive), as well as provide for advance notification of any location changes. The notification period should be specified.

5.3.2	Cloud Service Provider Assessment	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… 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.	Cloud providers may publish certification evidence on their websites. Certification results may be considered as evidence of the vendor's quality system standing when those certifying organizations use their subject matter experts to conduct assessments. These certifications alone do not obviate the need for a well-considered, risk-based validation for GLP computerized systems (see also 5.3.4 regarding computer system validation). The extent of validation should be based on a risk-based approach that takes into consideration the evaluation of the vendor's quality system."
5.3.3	Service Level Agreement (SLA)	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).	The SLA should also indicate the means and allowed timeline for the cloud user to obtain data. The cloud service provider should provide specifics about the means and allowed timeline for obtaining data as part of the exit strategy. The SLA should allow for testing the exit strategy to ensure the means and allowed timeline are achievable and are in a usable format for the next data life cycle steps (e.g., archiving, use in a different system). When conducting (and testing) the exit strategy, the cloud consumer should use a data migration approach to ensure all data, including metadata, are moved completely and without data integrity issues.
5.3.4	Validation of the computerised systems in the cloud-based service	If the cloud service provider supplies part of the validation documentation, it should be assessed by the test facility for its relevance in the validation process. In case validation	The SLA should describe what documentation would be required from the cloud service provider, the means of access, and required

		documentation from the cloud service provider is used, this should be readably available at the test facility.	timeline for availability in support of audits and inspections.
6.1.3	Rationale for Cloud Service Providers	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.	Rationale and criteria for vendor selection may be found in documentation generated during the procurement process and be separately documented in other system records (e.g., validation plan, risk assessments). Evidence should be readily available for audit and inspection.
6.3	Electronic archives in cloud solution	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.	As appropriate, SLAs should include provisions for providing regulatory inspectors details on the location of cloud archives.