Results of the Survey
(Supplementary Information)

Status of Data Integrity (DI) Implementation at GLP Facilities in Various Countries

This document provides detailed survey results by country, supplementing the information presented in the poster.

Prepared by
International GLP Research Team
Group 1, Division 1
Japan Society of Quality Assurance (JSQA)

June 2026

1 Results of the Survey

The responses are summarized below. For the question numbering, items related to audit trails were assigned to Q3 (up to six questions), those concerning the handling of electronic data to Q4 (up to thirteen questions), questions regarding the automated capture of weighing values to Q5 (up to two questions), questions related to blank sheets to Q6 (up to three questions), and, as other topics, issues specific to Japanese GLP -namely, the retention period for TK samples and the attachment of pathology reports to the final study report- were assigned to Q7 (up to three questions). To track the number of questions in each category, sub-numbers were designated (e.g., Q3-1). When follow-up questions were added based on the respondents' answers, additional sub-numbers were appended (e.g., Q3-1-1).

A total of 63 responses were collected. The affiliations and the breakdown of GLP facilities and QA organizations were as follows:

Association	GLP Facilities	QA Organizations	Both GLP Facilities & Organizations	Total Entities
SQA (America)	14.3	0	0.5	14.8
SOFAQ (France)	12.5	1	1	14.5
KSQA (Korea)	10	0	0.5	10.5
GQMA (Germany)	9.5	0	0	9.5
RQA (United Kingdom)	6.3	0	0	6.3
SARQA (Sweden)	1	1	1	3
SPAQA (Switzerland)	0.8	0	0	0.8
CSQA (China)*	44	10	0	54
TSQA (Taiwan)	0.5	0	0	0.5
Others	2	0	0	2
Total (Unadjusted for Overlaps)	**101**	**12**	**4**	**116**

* Initially reported as a single aggregated response (n=1). Detailed data became available after the SQA Annual Meeting.

However, some entities held multiple affiliations. The overlap details were as follows:

Overlap Combination	Count
SQA & RQA	3
SQA, RQA & SPAQA	1
SQA & TSQA	1
SQA & KSQA	3
RQA & SOFAQ	1
GQMA & SPAQA	1
Total Overlaps	**10**

Free-text comments were included exactly as written by the respondents. Descriptions for which no clear answers were obtained have been omitted from this report. Additionally, when aggregating the number of responses, organizations that belonged to multiple groups were counted as 1/n.

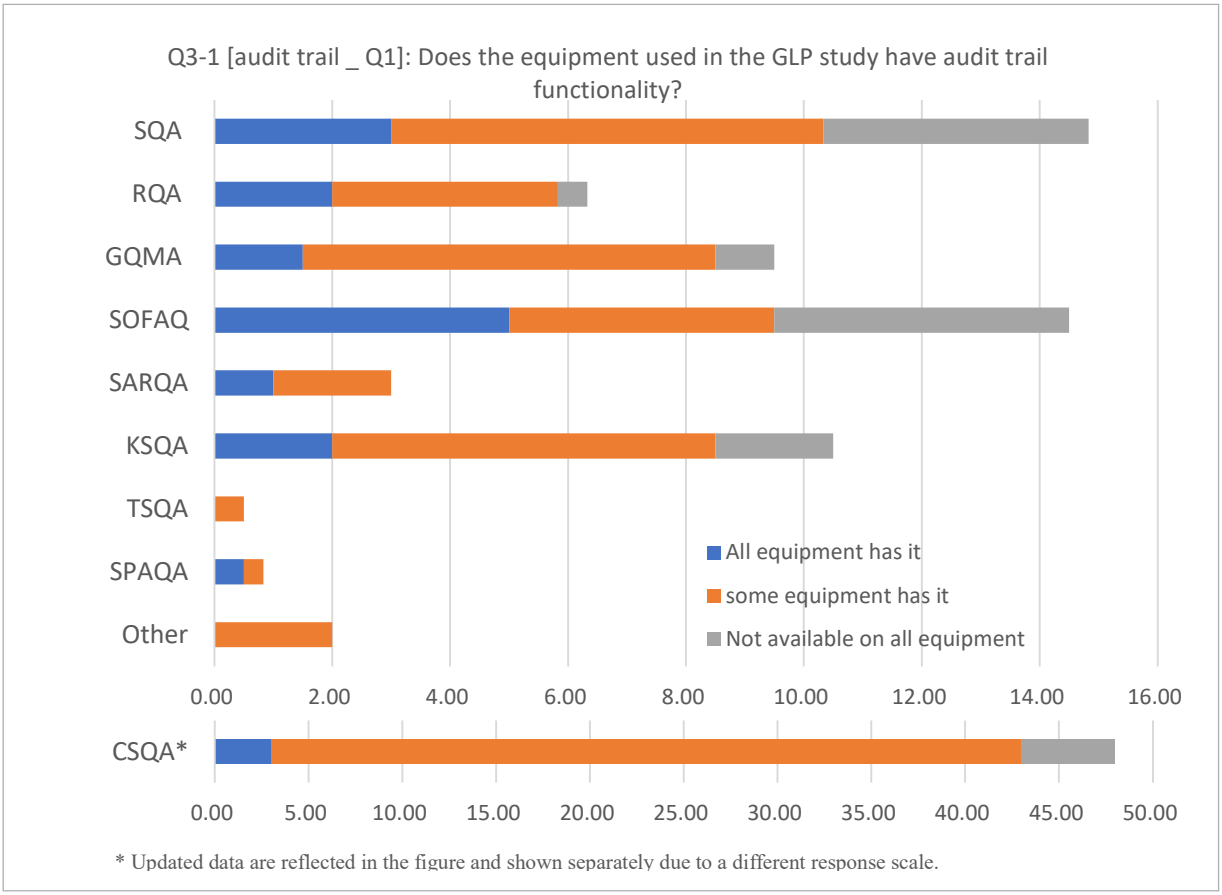
1-1 Audit trail

Q3-1 [audit trail _ Q1]: Does the equipment used in the GLP study have audit trail functionality?

All equipment has it.

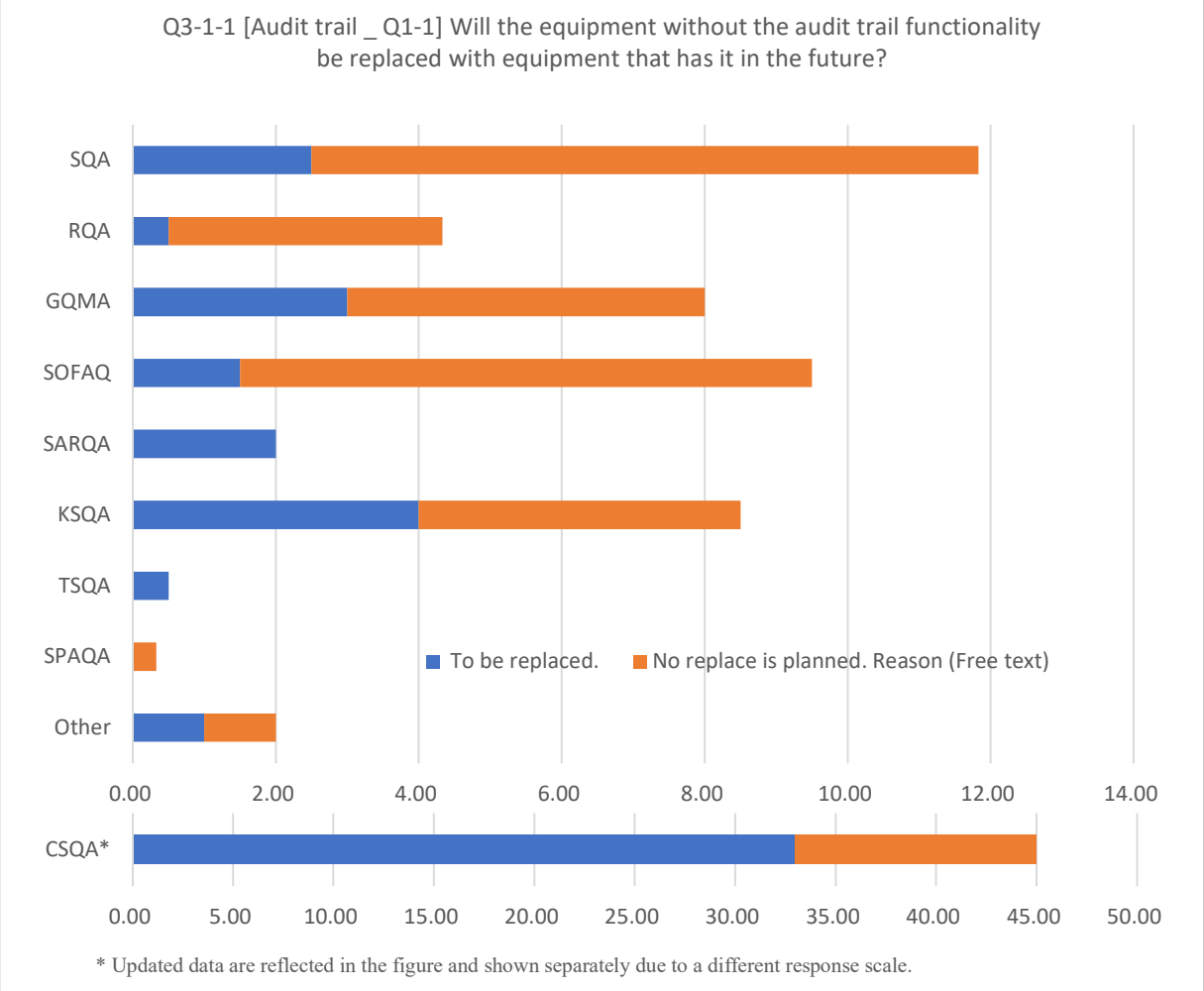
Some equipment has it. → To Q3-1-1

Not available on all equipment. → To Q3-1-1



Overall, the predominant response indicated that the audit trail function was implemented on only some instruments. Although the proportion of respondents reporting implementation on all instruments was somewhat higher among SOFAQ, SQA, RQA, GQMA and SARQA, reports of instruments lacking the audit trail function were also widespread, indicating the coexistence of both fully implemented and non-implemented instruments within these groups.

Q3-1-1 [Audit trail _ Q1-1] Will the equipment without the audit trail functionality be replaced with equipment that has it in the future? To be replaced. No replace is planned. Reason (Free text)



Among respondents who selected 'Some equipment has it' or 'Not available on all equipment' in Q3-1, we examined whether they plan to transition to equipment with audit trail functionality. The majority responded that 'No replacement is planned.' The reasons for not planning such a transition are listed below.

Q3-1-1 No replace is planned. Reason (Free text)

SQA (America)

- Equipment without complete GLP compliant audit trails use an SOP described manual process to document and remediate items
- equipment like balances, centrifuges do not require audit trails
- The pieces of equipment are built for clinical work versus preclinical and, by design, do not have an audit trail.

- Some systems have add on software that does audit trail function. Because of this software we do not plan on replacing equipment for audit trail reasons.
- No replacement available. Risk mitigation plan completed with documented process to handle data created by the equipment, corrections or updated needed, review and approval process.
- not all equipment used will use an audit trail such as centrifuge, pipette, vortexer, etc
- For a system that does not have audit trail, the files can not be edited. This is typically used for review files to place highlighting flag markers to mark points on interest. No change to the raw data can be made. If highlight flag need to be changed a new review file will be made.

RQA (United Kingdom)

- Mitigation has been applied as a paper booklet to log the most important details. This is only for simple systems (platereder). All Chemistry systems have full audit trails.
- Legacy system which has mitigation in place

GQMA (Germany)

- In general yes, but for some equipment there is no system with audit trail. We have a paperbased log file that fulfill the audit trail function
- Some will be replaced, some not because it is not available on the market or its price is too high.
- no money
- Some systems do not provide audit trail functionalities but are required to perform specific data recording and/or assessments. A system is in place to store any electronic files which provides audit trail functionality on file level.
- Maybe far future investment.

SOFAQ (France)

- specific lab equipment may not have an audit trail. for those a risk analysis and mitigation actions are defined. an SOP is written
- No always possible to replace or expensive
- Data integrity guaranteed to date with the measures put in place Not used frequently - Financial impact - Human resources unavailable
- Money
- Majority of equipment are only a value to read on a display. Otherwise, the problem could be because of investment to do.
- Mitigation actions towards risks
- To be replaced
- Because of the cost or non-existence
- audit trail not available for certain specific equipment

KSQA (Korea)

- Most instruments either support audit trails or are used in connection with software that provides this function. For some older instruments where audit trail functionality is not available, a usage log is maintained as a minimum data integrity measure. So far, regulatory authorities have not raised any issues with this approach.
- As a small organization, we do not have such an electronic operating system.
- Installation involves considerable expenses.
- Not necessary
- Financial support is not available.

SQA & RQA

- Equipment is imaging and there are limited options for audit trail capabilities
- Will have procedure work arounds where possible restricting changes to data as well as have controls to limit the data file from changes.
- MRI, CT Scanners used are the same as hospital equip. therefore not designed for use in regulatory studies

SQA, RQA & SPAQA

- Procedures are in place to adhere with ALCOA++ expectations

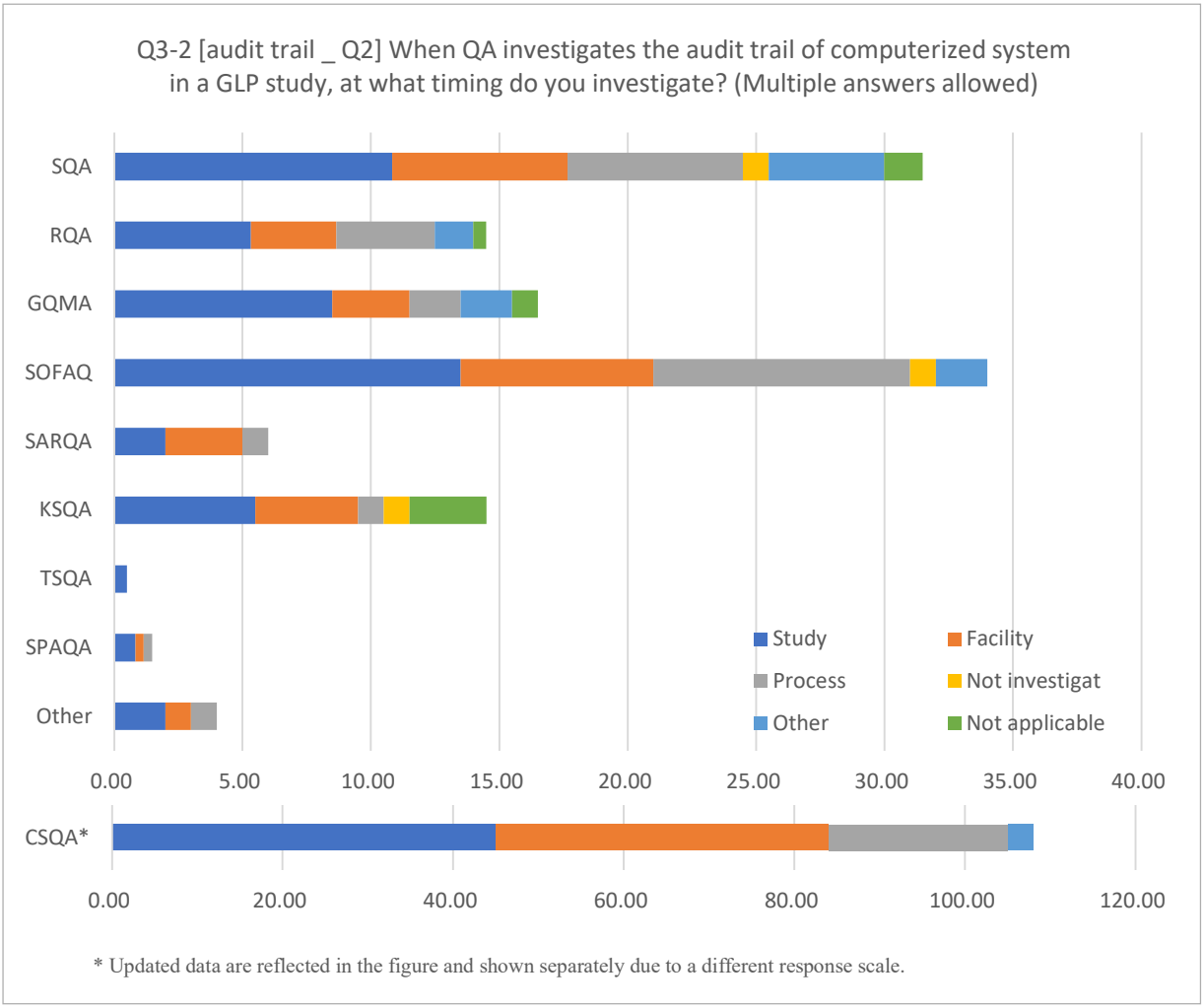
SQA & KSQA

- The installation cost is high

Other

- This is not planned

Q3-2 [audit trail _ Q2] When QA investigates the audit trail of computerized system in a GLP study, at what timing do you investigate? (Multiple answers allowed)
Study-based inspections
Facility-based inspections
Process-based inspections
Not investigated
Other (Free text)
Not applicable to the respondents to this question.



Regarding the timing at which QA reviews audit trails in GLP studies, 'study-based inspections' were the most frequently selected option, followed by 'facility-based inspections' and 'process-based inspections.' In addition, some respondents indicated that audit trails are reviewed during examinations of the final report or raw data. Details of other responses are listed below.

Q3-2 Other (Free text)

SQA (America)

- during report audit the audit trails of the associated data are reviewed/investigated
- Periodic Review for computer systems
- Verify during the review of study raw data
- during audit of the data

RQA (United Kingdom)

- final report audit

GQMA (Germany)

- audit of the final report
- risk-based

SOFAQ (France)

- At the Validation of computerized system step.
- raw data electronic audit

SQA & RQA

- study (for study data) and also facility (for access control and configuration changes)

CSQA (China)

- In a GLP study, when experimental phases involve the use of computerized systems—such as during LC-MS/MS sample loading—QA should review the system's audit trail. Following the completion of the experimental phase, and during the QA audit of data and the final report (when all data are circulated for QA review), the audit trail must be examined again to ensure data integrity and compliance.

Q3-3 [audit trail _ Q3] Please let us know the viewpoint of inspection when QA inspects the audit trail of computerized system in a GLP study. (Free text)

The summary of responses was as follows. Details of individual responses are provided below.

- Ensuring DI (ALCOA+):

Verification of the history of changes (including the person responsible, date/time of modification, content of the change, and justification), retention of original data, assessment and documentation of the appropriateness of change justifications, and confirmation that no improper modifications or deletions have occurred.

- Review of Audit Trail Records:

Confirmation that the audit trail function is continuously enabled, verification of the absence of missing entries, assessment of unauthorized shutdowns or configuration changes, and sampling-based review of audit trail entries.

- Access Control and User Permissions:

Verification of login/logout records, assignment of access rights according to user roles, confirmation of whether shared accounts are used, and review for unauthorized operations or abnormalities in logs.

- Appropriateness of Change Control:

Evaluation of the appropriateness of change approvals, consistency with change-control documentation, and reconciliation with instrument outputs, final reports, and electronic data.

Q3-3 Free text

SQA (America)

- not sure i understand the ? QA reviews the audit trail for regulatory compliance that the original entry and revised entry are present (not obscured), who made the entries including date and time, along with reason for revision. QA insures these are not late entries unless supporting rationale for such, and that

the entries make logical sense to explain the nature of the revision.

- QA reviews audit trails for each study, as well as during the periodic review for each computerized system.
- The key focus is on verifying the data integrity, traceability and compliance to GLP principles.
- QA determines which audit trails require QA review based on system, GLP-critical data, relevant parts of the audit trail. QA checks whether the audit trail function is enabled, if it is configured properly, gaps, access control, user ID and timestamps, do modifications to data have justifications, are entries chronologically consistent and support reconstruction. Compare audit trails to study protocol, SOPs, printed outputs and final report. Did anyone review the audit trails during study conduct?
- Checking Compliance to 21 CFR Part 11.
- QA typically has read only access in the system to view data including audit trail.
- Review for compliance with the established procedure. Review for anomalous entries. Review for errors in audit trail reliability.
- QA ensures audit trail is present and tracks details needed to recreate study
- QA reviews audit trails as part of the data audit. This includes a review of the associated audit trail and metadata to ensure modifications to the data are documented with the reason for the change, who performed the change and when the change was made. In conducting this review, auditors must give consideration to whether the reasons for change, and the person making the change, were appropriate, and that changes were made in an acceptable timeframe.
- QA will confirm audit trail is present and spot check entries for compliance with GLP, protocol and SOP.

RQA (United Kingdom)

- For, each system an percentage of runs are viewed including the study audit trail, and overall system audit trail where this exists.
- QA has read only access to most systems and this allows access to view the audit trail. For systems where QA access does not allow for viewing the audit trail, QA will review the audit trail with the system owner. When QA are auditing the audit trail, we are primarily looking that the audit trail meets data integrity requirements. There is a separate audit trail review by IT (e.g. for security), as well as the system owner or BSME (e.g. to evaluate that the reasons for change are technically valid)
- For study audits looking for any unusual logs, reasons for changes, timing of activities, who has access. QA sample the audit trail since some can be very long. Concentrate on either one particular run or one sample to see its journey. For facility audits look at general system logins.
- Study and system audit trails are reviewed by QA and the study director. QA sample the audit trail, the SD has to conduct a full review and sign to say this has been done.

GQMA (Germany)

- The audit trail of the LIMS system is audited study based to see the changes on a study basis. In the facility based inspections the focus is on the system audit trails
- Audit trail is considered part of the raw data and inspected as such.
- QA inspects whether any changes were made and properly justified.

- Complex and difficult, often only with help of laboratory possible as audit trails often document everything
- not checked up to now.
- not defined it yet
- plausibility, availability, completeness, alcoa,
- Traceability of all data and entries with respect to corrections and additions; correct application of user permissions within the system.
- Audit trail is mainly inspected with study row data.

SOFAQ (France)

- Study-based inspections
- inspectors expect OECD 22 to be applied. we have SOP for review of data and data audit trail by operations/study directors. audit trails are also integrated in QA audits
- Agree with that.
- Each action has to appear on the audit trail of the computerized system (login, logout, each modification, each action, process...). If the equipment has not this functionality, a logbook is implemented to list at least the login / logout, and each modification is printed and joined to the raw data of the study.
- During the inspection, the inspector asked us for the audit reports and validation of the computerised system. She first checked whether the data flows had been carried out and traced. She then focused on security breaches and verified that the audit covered these elements (breaches) in order to guarantee that there had been no breach of data integrity.
- not concerned
- We want to see the old value, new value, who did the modification, when, for what reason. The document cannot be changed. The document must be easily readable (no IT language)
- Initial data: Author, date, time
  Change: same ac above + clear justification
- Verification that there are no deletions or unjustified modifications and that all results are present and coherent.
- No problem
- Confirm that audit trail entries comply with ALCOA++ principles. Check that changes are justified, documented, and traceable to responsible individuals (Ensure QA can reconstruct the sequence of events)
  Prioritize audit trail review for critical data impacting study integrity
- The audit trail is part of the raw data. Traceability of entry is checked.
  Traceability of data corrections is checked. Presence of justification for modifications is checked
- We will check that the software administrator is not involved in the study and, if so, the justification. that persons not involved in the study intervened in the software. consistency between the series recorded in the software and the series recorded in the laboratory notebook and associated printed raw data. the presence or absence of changes made to the results of the processed series.

KSQA (Korea)

- We verify whether the events identifiable from the raw data are consistent with the audit trail records. This includes checking the operator ID, date, access records, data acquisition date, modification history, and the validity of the reasons for any changes. In the case of bioanalysis performed using LC-MS, it is also necessary to confirm whether there are any analysis execution data not attached as raw data and whether reintegration has occurred. However, there is some concern that a complete investigation may not be performed due to insufficient technical expertise with analytical instruments.
- Verify that all details related to the record, such as time, user, and purpose, are retained. Interruption during analysis Unauthorized manual manipulation Creating batches identical to printed copies Use of manual integration Appropriateness of re-integration
  Accuracy of test-related information (such as test number, substance name, and details of the study director and actual performers).

SQA & RQA

- Not applicable at my current lab. At other facilities, when we inspected audit trails, it was done in conjunction with the study or facility data review to ensure the data was collected contemporaneously. The inspection was often a deep dive into one or two records, and a high level review of the remaining audit trails.
- Looking to see that data audit trails were reviewed and that any changes have been verified. Lso look for system changes to ensure change control or other supporting documents are available.
- Study: to reconstruct the study who did what, when is it in order, also any changes i.e. re-integrations.
  Facility: who has access, their level, changes to the configuration, or software upgrades are their change controls to support changes

SQA, RQA & SPAQA

- Data Lifecycle

SQA & TSQA

- Is the audit trail reasonable? Any supporting document for the audit trail.

SQA & KSQA

- When QA inspects the audit trail of a computerized system in a GLP study, QA checks and confirms the following:
  1. that all changes to data can be associated with the persons who made those changes (e.g., by use of timed and dated electronic signatures)
  2. the comparison between the changed electronic data from the equipment and the data presented in the final report
  3. that a clear reason for all changes has been given
  4. that the reason for the change is properly stated in the final report
  5. that the computerized system design always provides for the retention of full audit trails to show all

changes to the data without obscuring the original data.

- Audit trail is recommendable but traditional system is economical. Computerized system requires more manpower and money

RQA & SOFAQ

- Existence, use as per SOP

GQMA & SPAQA

- Audit trail is considered part of the raw data and inspected as such.

Other

- Data deletion and manipulation.
- Studies that have used computerised system is usually audited by QA. This involves logging into the system and checking for entries, deletions etc.

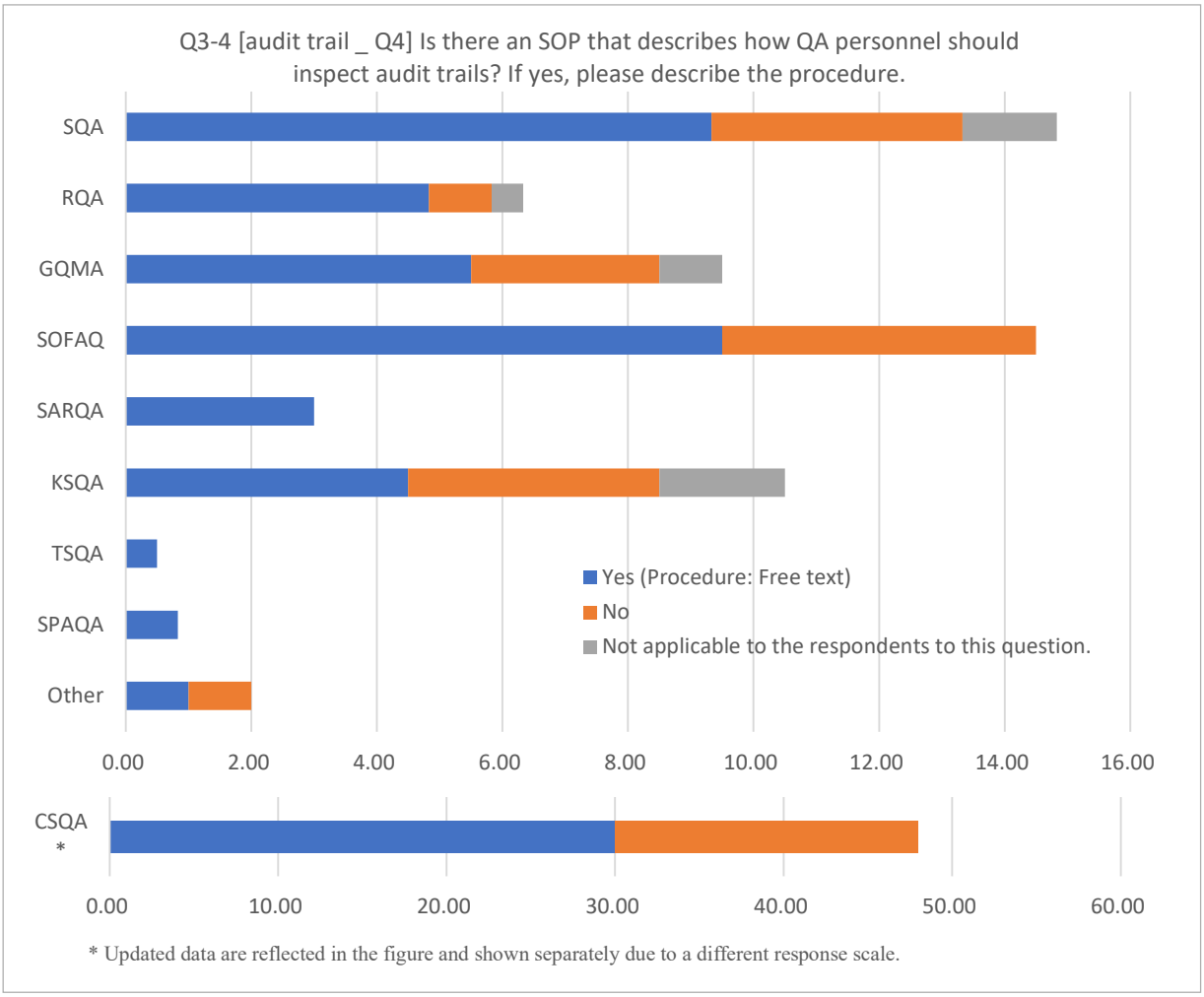
CSQA (China)

1. Fundamental Objectives: Ensure data integrity, traceability, and authenticity, and comply with GLP and relevant regulatory requirements.
2. System Validation: Verify that the system has undergone complete and adequate validation, supported by a User Requirement Specification (URS) that conforms to standard operating procedures (SOPs).
3. Continuous Audit Trail Functionality: Confirm that the audit trail function is continuously enabled throughout the study, with no unauthorized shutdown, configuration modification, or deactivation.
4. Access and Permission Management：Review that user permissions are assigned appropriately by role and aligned with job responsibilities. Ensure there is no misuse of shared accounts and that login logs show no irregularities.
5. Essential Elements of Audit Trail Records: Check that audit trail records capture all necessary details, including operator identity, timestamp, operation content, rationale for the justification, written authorization, and electronic signature
6. Coverage Across Data Lifecycle: Ensure the audit trail covers critical data activities such as creation, modification, deletion, renaming, movement, processing, calculation, reporting, and archiving
7. Review of Critical Operations and Changes: Investigate any unauthorized changes to parameter, data processing methods, file movement/deletion/overwriting; Confirm that method parameters, templates, and sample sequences are consistent with those at validation release, with no unauthorized changes. Verify that operations such as excessive peak integration, retesting are compliant and fully documented. Ensure that manual integration is either absent or, if present, is supported by fully justified and credible rationale with appropriate authorization.
8. Authorization, Traceability, and Data Protection: Ensure all operations (modification, deletion, renaming, etc.) are properly authorized and traceable; Confirm that deleted data remains fully traced; original records are not arbitrarily overwritten; and any modified data is clearly identified; The audit trail itself is unalterable, and archived records are retrievable after system changes/decommissioning.

By systematically reviewing these areas, QA helps ensure that the computerized system maintains reliable and trustworthy records in support of GLP study outcomes.

(Data from 48 Facilities)

Q3-4 [audit trail _ Q4] Is there an SOP that describes how QA personnel should inspect audit trails? If yes, please describe the procedure.
Yes (Procedure: Free text)
No
Not applicable to the respondents to this question.



More than half of the respondents answered 'Yes,' indicating that an SOP describing the procedures for reviewing audit trails had been established. However, free-text comments frequently mentioned the use of system-specific checklists, such as software-specific procedures and keyword searches (e.g., 'delete'). Details regarding the SOP procedures reported by respondents are listed below.

Q3-4 Yes (Procedure: Free text)

SQA (America)

- our inspection and report audit SOPs state to review the audit trail for GLP compliance. there is a positive documentation on each of these audit plans indicating this item was reviewed.
- There is a general SOP for study conduct which includes audit trail review (by study director as well as QA).
- We have developed the audit trail check list to verify the audit trails.
- The procedures followed by the technical team state how audit trails should be reviewed. There is a procedure that writers of these SOPs follow to determine what kind of audit trail review criteria must be reviewed. Auditors are instructed by SOP to follow instrument SOPs for audit trail review.
- Specific to each equipment. Details how and where to access the audit trail for the study and the system.
- We include how to audit trails as part of our SOP on how to audit data, reports, and report amendments

RQA (United Kingdom)

- Review of ~10% of runs. Ensuring traceability of data processing and that excessive reprocessing has not been performed.
- general SOP which gives an overview of sampling, SOPs for individual systems are being written.
- Varies depending on Facility, process or study audit

GQMA (Germany)

- The inspection SOP is defining this
- Part of the QA SOP on raw data audits. QA has read access to electronic systems incl. audit trail
- Audit trail review is describe in every system SOP as this is system specific.
- There are software specific checklists with instructions (e.g. software specific keywords to search for like "delete")
- our SOP requires the use of checklists for performing an audit trail inspections.
- No detailed instructions but audit trail review is following the same rational as applicable to any other (paper-based) documentation

SOFAQ (France)

- we have dedicated SOPs
- Read-only auditor account, global audit procedure and system-specific procedure for accessing the audit trail
- How an audit trail should be is explained in the procedure Raw data management. Audit is auditing according to what is explained in all procedure, specially this procedure for managing of raw data.
- Sometimes
- As described in Q3-3
- The SOP explain the action spectrum, the methodology and support documentation.
- Particular attention is paid in the event of delayed data entry or changes made to the data after entry.
- For regulatory assay studies, a review of electronic data and audit trails from analytical software is performed for at least one series of analyses, using working document ADM_FORM_593, which is appended to the audit report. The working document details the points that are verified. The audit trail

for analytical software is performed once all samples in the study have been assayed. For all assay studies (GLP or non-GLP) under LIMS, a review of the LIMS audit trail is performed each time a new version of an already audited results table is audited, in order to verify whether the previously audited results have been modified since the last audit.

KSQA (Korea)

- Cannot be shared due to internal procedures.
- Generate codes for audit trail search. Include a QA review checklist. Codes in English (manual integration, abort, error).
- SOP exists detailing the inspection checklist for each stage and the specific checkpoints for every step.
- QA inspection manual is available.

SQA & RQA

- Yes, it requires audit trail review on the specific system. There should be an indication in the system's transaction logs that individuals went directly to the system for review.
- varies between system, but is part of the QC checks of data specifically for changes, SD also peer reviews specifically for incidents/changes to the data on their study.

SQA, RQA & SPAQA

- SOP on review of audit trail

SQA & TSQA

- QA should output the raw data at adequate interval and review the audit trail.

SQA & KSQA

- At the stage when QA audits the final report, especially when comparing the raw data with attachments, the QA team also enters the Audit Trail module of the computer system directly, and checks that,

  1) all changes to data can be associated with the persons having made those changes (e.g., by use of timed and dated electronic signatures)

  2) the changed data among the electronic data of the equipment matches the data on the final report

  3) a reason for changes has been given

  4) the reason for the change is properly stated in the final report

  5) the computerised system design always provides for the retention of full audit trails to show all changes to the data without obscuring the original data.

RQA & SOFAQ

- Trigger events, frequency and sample size

GQMA & SPAQA

- Part of the QA SOP on raw data audits. QA has read access to electronic systems incl. audit trail

Other

- There is a broader term stated in a specific SOP used for study audits and includes a line that QA should audit trail. The scope of the audit trail is not detailed in the SOP.

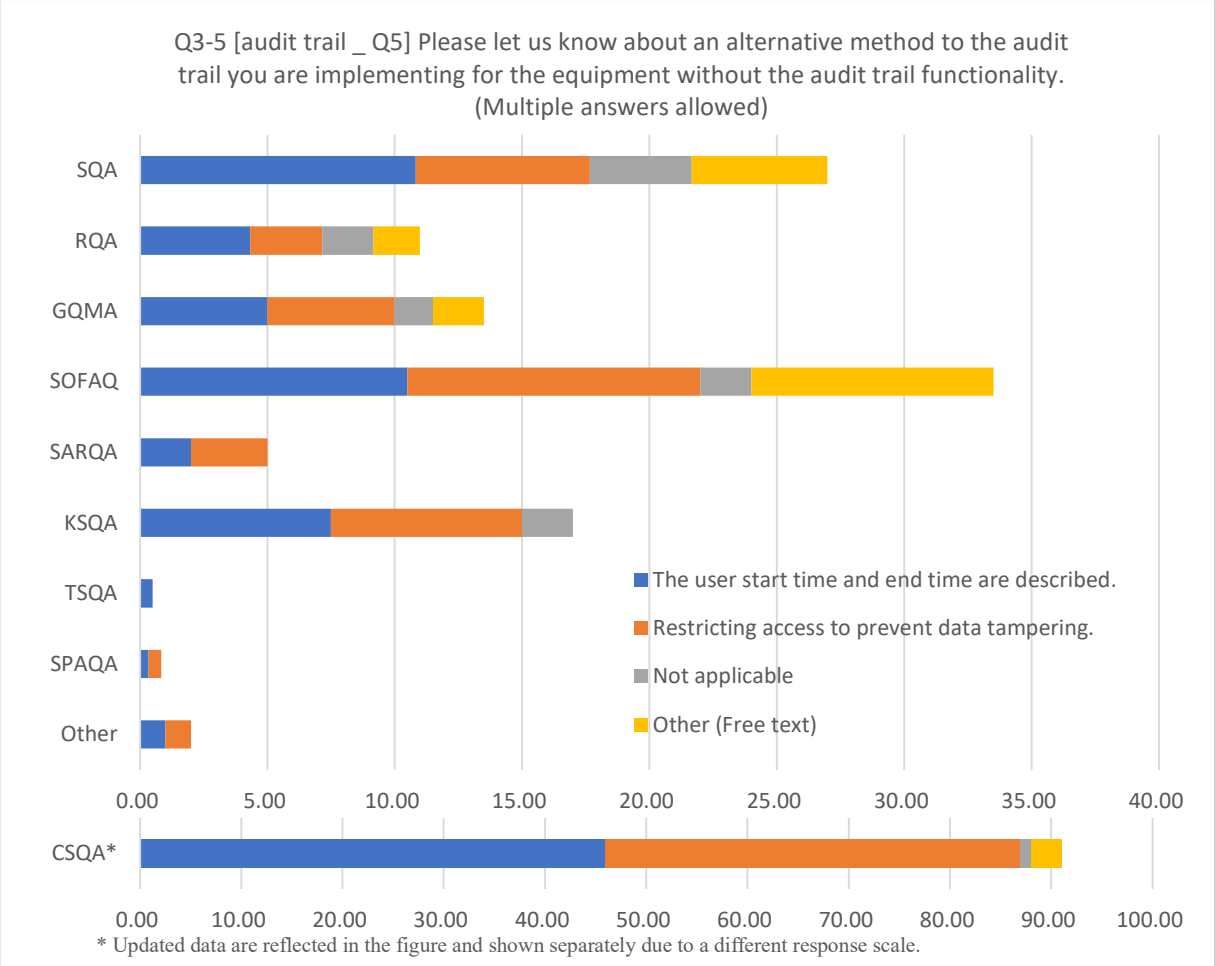
CSQA (China)

1. Key Focus of Review: The audit trail review should comprehensively cover critical data activities such as creation, modification, deletion, storage, collection, and method changes. It must ensure that original data and reasons for any modifications are retained. Verification should confirm that the audit trail function is continuously enabled and operating correctly, with complete logs of all key operations and system activities. Each record must include user ID, timestamp, action performed, and justification for changes to ensure accurate timing and clear traceability. Access permissions must align with the authorized permission list, with strict control over data access and indexing. Special attention should be given to non-routine operations, system changes or decommissioning, data interruptions, manual integrations, and re-testing activities.
2. Requirements for Data Storage and Traceability: Upon study completion, data must be promptly placed under electronic isolation and controlled access, with support for archiving functions. If the system lacks built-in archiving capability, data integrity must be ensured through verified backup procedures. Data should be convertible to standard formats, with corresponding software systems retained and compatibility maintained during upgrades. In the event of system decommissioning, data readability must be guaranteed via hardcopy output or validated migration methods. Complete and accurate archiving of audit trails is required to support long-term traceability.
3. Quality Assurance (QA) Activities: The QA department shall operate under exclusive system accounts and perform audits using differentiated account scenarios. Inspections include in-process reviews during studies, random checks after study completion, annual facility-wide audits, and quarterly targeted inspections. QA shall utilize SOPs and standardized checklists to verify consistency between raw and derived data, and cross-reference audit logs with instrument usage records. All review results must be formally documented in QA checklists and audit reports. Any anomalies detected shall be recorded in an "Audit Trail Deviation Form" for further investigation and resolution.

(Data from 24 Facilities)

Q3-5 [audit trail _ Q5] Please let us know about an alternative method to the audit trail you are implementing for the equipment without the audit trail functionality. (Multiple answers allowed)

The user, operation start time, and end time are described in the record of use.
Restricting access to prevent data tampering
Not applicable
Other (Free text)



As the primary alternative measures to audit trails, many respondents reported combining 'The user, operation start time, and end time are described in the record of use' with 'Restricting access to prevent data tampering.' Details of other responses are listed below.

Q3-5 Other (Free text)

SQA (America)

- It varies by the capabilities of each system. A log is generally used listing user/ date/ time/ study number/ and for some systems which task.
- Placing data in folders that restrict changes or deletion using Operating System controls. Using software to provide audit trail.
- Use of equipment logbooks and review/approval dated signature.

- Hand record forms are used and kept with the study data.

GQMA (Germany)

- System specific forms that have to be completed.
- SOP regulation on when files are saved and if (and how) changes to files are allowed (in some cases like digital photographs taken by digital camera or some data loggers audit trail functionalities and user management is not available).

SOFAQ (France)

- QC procedures - export of data after Qced
- See Q3-3
- Printing of the data with date and signature
- Procedure requiring the record of what is required from an audit-trail
- Register to be completed by hand
- Immediate print out
- Automatically manage the printing of data
- screenshot

SQA & RQA

- restricting access to actual data files and copying to secure share areas.
- Raw data file is transferred on completion to folder on server with limited users having write access. But all personnel have read access. This is documented and signed and dated.

SQA, RQA & SPAQA

- Log books entries in raw data

RQA & SOFAQ

- documentation "safety nets"

Other

- Paper based audit trail.

CSQA (China)

1. The technician prints out and signs the data immediately after its generation.
2. A handwritten signature, accompanied by the current date, is required.
3. Electronic data (such as e-files or e-databases) are managed through IT control measures—including access, modification, and deletion controls—and stored in controlled electronic paths with designated e-folders. When printed, the paper copy must include a handwritten signature and current date. All electronic and printed data are subject to full control, quality checks, quality assurance, and archiving.

(Data from 3 Facilities)

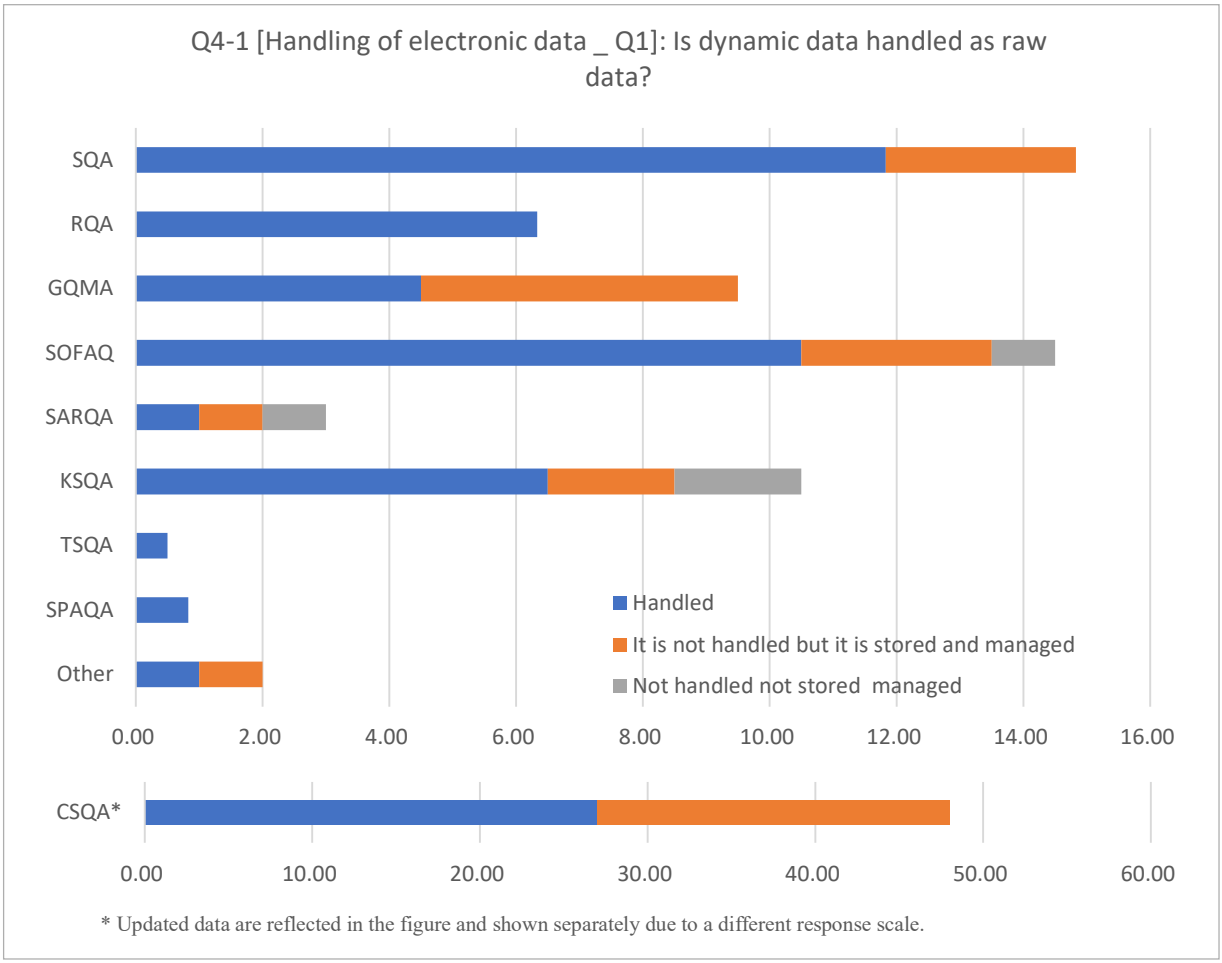
1-2 Handling of electronic data

Q4-1 [Handling of electronic data _ Q1]: Is dynamic data handled as raw data?

Handled.

It is not handled (e.g., paper or PDF that outputs dynamic data is referred to as raw data), but it is stored and managed.

Not handled, not stored / managed (e.g., paper or PDF that outputs dynamic data is regarded as raw data).



Responses indicating 'Handled' accounted for the majority. When including those who answered, 'It is not handled (e.g., paper or PDF outputs containing dynamic data are regarded as raw data), but it is stored and managed,' it can be inferred that systems for the storage and management of dynamic data are generally in place.

Q4-2 [Handling of electronic data _ Q2] Where do you store the dynamic data after the study is completed?
On a physical server located within the facility
In a cloud-based storage system
On a PC directly connected to the equipment
On removable media (e.g., USB, external hard drive)
Other (please specify):

As storage locations for dynamic data after study completion, 'on a physical server located within the facility' and 'on removable media (e.g., USB, external hard drive)' were the two most frequently reported. Details of other responses are provided below.

Q4-2 Other (please specify)

SQA (America)

- we use both a combination of data centers and cloud based storage systems
- A combination of these depending on the capabilities of the system physical server. cloud-based storage.

removable media.

- electronic archive
- Paper copies are printed out and/or burned to non-editable media such as a CD and maintained with the study file.
- It is stored locally on the system, an exact copy with signatures is moved to a server within the facility. That server is backed up and stored off site.
- Depends on the system - cloud server, on-premises server, on archive hard drive, in printed version - as applicable.

SOFAQ (France)

- the storage/archiving process of e data including dynamic data are system specific. it is considered in the validation risk assessment for each system. so we have storage of e data on a physical server but also for some system storage in the cloud or on external hard drive. all physical media is covered by a validation study that runs for 10 years
- I am sorry, I am not sure to well understand what is a dynamic data, and in consequence your question
- Hard copy

KSQA (Korea)

- Cloud-based systems, PC-connected equipment, and removable media are all used.

SQA & RQA

- Cloud-based system and limit access to data if possible.
- During study on all electronic data is transferred (if not saved directly) to a cloud-based storage system. On study completion is moved to an area which is accessible by the archivist

GQMA & SPAQA

- Server is the e-archive with respective access rights.

Other

- This needs clarifying for our business, we do have a physical server but we also utilise the cloud.

CSQA (China)

1. In this context, PDF files and printouts generated from dynamic data are classified as raw data and are archived in the facility's server room.
2. Remote backup.
3. Dynamic data are stored on a NAS backup system physically located within the facility and managed under GLP-compliant IT procedures.
4. Removable storage media.

(Data from 4 Facilities)

Q4-3 [Handling of electronic data _ Q3] Who manages the dynamic data after completion of the studies conducted in your country's GLP testing organization, and how is it managed?
Example: "The Archivist manages the dynamic data. It is stored on a secure server under his/her supervision." (Free text)

The archivist was most frequently identified as the primary administrator of dynamic data. In addition, some responses indicated that the IT department or system administrators provide technical support, and that the Study Director may hold ultimate responsibility for ensuring data handover and archiving. With respect to storage media, respondents reported the use of secure servers, as well as removable media such as USB drives and external hard drives, cloud-based storage, and paper printouts. Details of the responses are provided below.

Q4-3 Free text

SQA (America)

- data is moved to appropriate storage folder location by department data generators, and then the archivist confirms the data presence and locks/archives the data
- The archivist manages the dynamic data. It is stored either on an archive server or in a system where the archivist has sole access to the data after archiving (or physically in the archive for removable media).
- Managed by the Archivist and Item
- The Archivist manages the dynamic data. It is stored on a secure server under his/her supervision
- The data is archived and under the control of the archivist.
- IT is currently responsible but we are actively evaluating this approach and looking to change.
- The Archivist or delegate to the archivist manages the dynamic data. It is stored on a secure server under his/her supervision. It is most often viewable by those that have access but no changes are allowed without a process that goes through permission of the archivist. Study director acknowledgement is required for archivist to give permission to alter.
- The archivist locks the electronic data upon study completion. It is stored in the appropriate electronic location. The printed PDF copies are stored with the study records.
- Archived data is under control of archivist
- The SD/PI has access to our online e-archive folder in which at the completion of the study they move the data to a staging folder there. The archivist then reviews the staging folder and moves the data to a permanent folder. The e-archive folder has limited access to include only SD/PI, those with archive submittal training, and the archivist.
- Archivist manages data and its stored on a secure Archive server.

RQA (United Kingdom)

- The SD is responsible for organising archiving and then it is held under the control of the Archivists.
- The Archivist manages the dynamic data. It is stored on a secure server under his/her supervision
- The Archivist manages the dynamic data. It is stored on a secure server under his control

GQMA (Germany)

- The archivist, it will be transferred to an e-Archive
- By the archivist, physical and electronic data are handled by the same staff.
- IT manages dynamic data under the supervision of the archivist.
- The Archivist manages the dynamic data. It is stored on a secure server under his/her supervision.
- The Archivist manages the dynamic data. It is stored on a secure server under his/her supervision. IT needs to define access rights for the archive folder containing the dynamic raw data.
- data are locked and can only be accessed under the supervision of the archivist
- Electronic data are generally archived comparable to paper records, i.e. under the full supervision of the named archivist.
- Dynamic data are stored on removable media together with row data in the GLP archive.

SOFAQ (France)

- informatic service
- in all cases it is under the archivist control and according to system specific SOP
- The archivist manages the dynamic data. it is archive on a secure server under his supervision
- The Archivist manages the dynamic data. It is stored on a removable media (external hard drive)
- The Archivist manages the dynamic data. It is stored on external hard drive
- Most of dynamic data are printed and stored by the archivist as hard copy. Further, some dynamic data will be stored on a server, by the IT Manager, under supervision of the archivist.
- Study Director
- The Archivist manages the dynamic data. It is stored on a secure server under his/her supervision
- Yes, The Archivist manages the dynamic data. It is stored on a secure server (in a part of application) under his supervision

KSQA (Korea)

- Electronic data stored and transferred via portable media are managed by the Archivist, while backup data stored on the server are managed by the Computer System Manager.
- Archivist or Stores electronic records in the electronic data rack within the archive room.
- System administrator: Server management.
  Until the transfer, the study director manages the data. After the transfer, the data custodian stores and manages the media containing study-specific data (USB and external hard drive with dual backup) in the archive room.
- A separate Archivist is designated, and server management is handled by the head of the Management Information Team.
- The person responsible for data storage manages the storage room.
- External hard drive, cloud server, and archive room PC.

SQA & RQA

- The USB drive with the dynamic data is archived with the rest of the study data and materials, which

includes a lot of paper data, and the archivist then manages the data.

- Archivists.
- The Archivist manages the dynamic data. They receive an instruction from the PI/SD to move all electronic raw data to the folder on a cloud server only accessible by them.||We have one system where the data is held on the system, the data is 'locked' by an archivist to prevent changes after study completion

SQA, RQA & SPAQA

- Study director -> Archivist

SQA & TSQA

- All the dynamic data generated during the study would be stored in the study folder and be archived by the archivist to a secure server with restrict access.

SQA & KSQA

- The Archivist manages the removable media (e.g., USB, external hard drive).
- The Archivist manages the dynamic data. It is stored on a secure server under his/her supervision

RQA & SOFAQ

- Archivist

GQMA & SPAQA

- By the archivist, physical and electronic data are handled by the same staff.

Other

- The archivist.
- Currently the management of the data storage/archiving is being considered to be rolled out under archivist control in a secure folder with collaboration with IT.

CSQA (China)

1. In 73% of facilities, the Archivist is primarily responsible for managing the dynamic data. This role oversees core tasks including the daily management, archiving, and long-term preservation of dynamic data.
2. Other key personnel also contribute to data management. IT/IT Administrators, System Administrators provide technical oversight. Study Director (SD) holds ultimate responsibility for ensuring data archive upon study completion and directly manages dynamic data in specific scenarios.
3. A common workflow involves a transition of responsibilities. Unarchived data is mostly managed by the IT department; After archiving, the data is typically transferred to the Archivist’s custody. In some cases, the Archivist conducts management work with IT support.
4. Data Storage Methods and Carriers: Dynamic data is stored using a combination of secure methods:

- Primary Storage Carriers: Secure servers, which may include local secure servers, validated secure servers, NAS storage systems, disk arrays, and internal institutional servers.
- Auxiliary Storage Carriers: Removable storage devices such as Compact Discs (CDs), external hard disks, and USB flash drives.
- Special Storage Forms: Cloud storage solutions and entrusted management by contracted suppliers (often for data from dedicated equipment).

(Data from 48 Facilities)

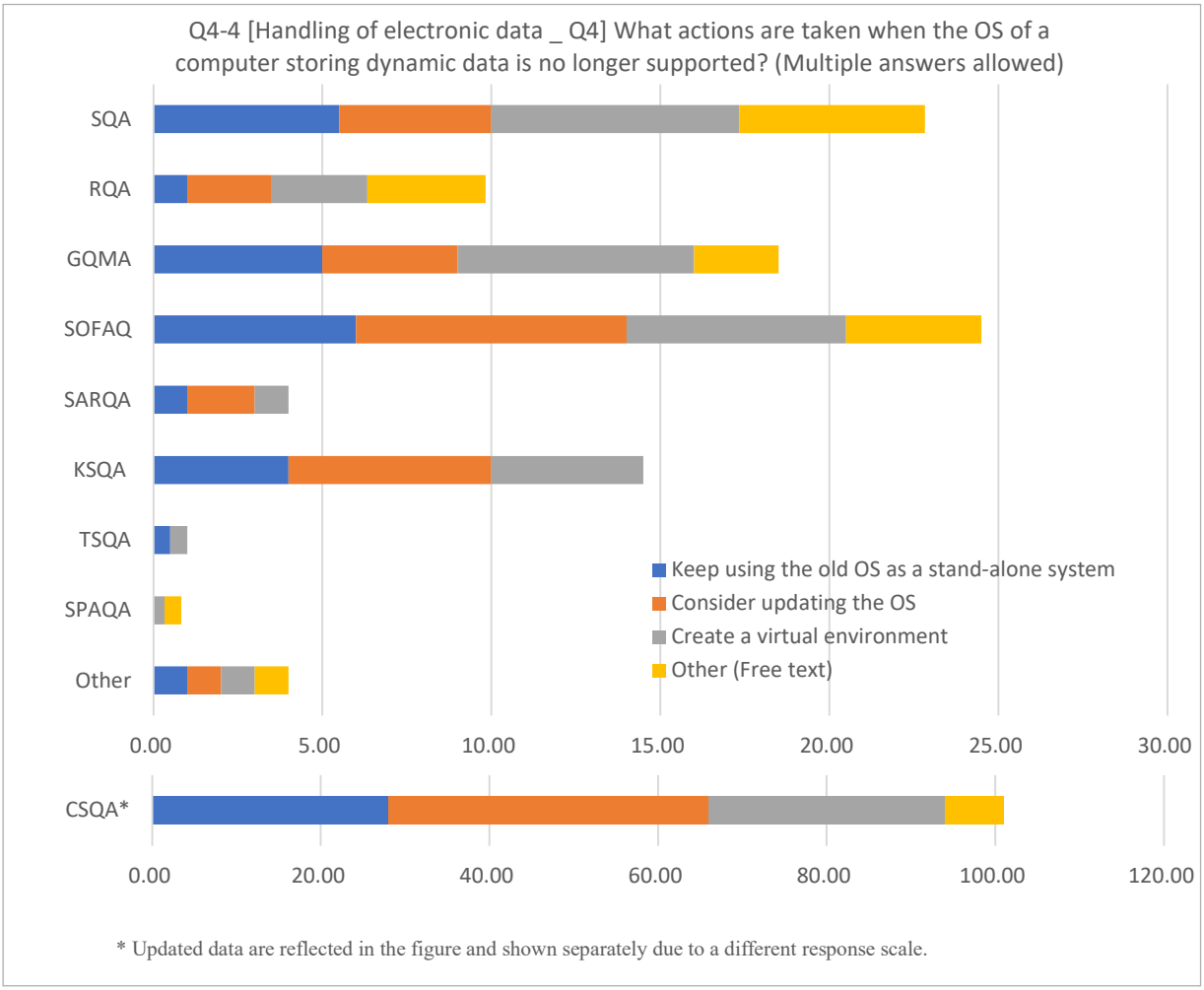
Q4-4 [Handling of electronic data _ Q4] What actions are taken when the OS of a computer storing dynamic data is no longer supported? (Multiple answers allowed)

Keep using the old OS as a stand-alone system

Consider updating the OS

Create a virtual environment, migrate the data, and maintain it

Other (Free text):



* Updated data are reflected in the figure and shown separately due to a different response scale.

There was a tendency to adopt one of three approaches -using the existing OS in a stand-alone configuration, continuing operation in a virtual environment with data migration and maintenance, or updating the OS- based on the assessed level of risk. Details of other specific responses are provided below.

Q4-4 Other (Free text)

SQA (America)

- Dynamic data is not stored on individual computers. Each system is assessed periodically to ensure data is still retrievable.
- Not applicable. Original dynamic data is on disc.
- I know we verify the data is viewable in case of inspection but I'm not sure how that is done

RQA (United Kingdom)

- system dependent. This is evaluated for each system as needed and is dependent on the limitations of each system. Archiving of the system or migration to a new system.
- Depending on the system upgrade where possible or consider other IT mitigations ongoing Microsoft support etc. or alternative OS.

GQMA (Germany)

- Data export as flat files
- Archived data might be also migrated to the new version of a software.

SOFAQ (France)

- the decision will be system dependent and it may be any of the above options. we also can decide to decommission the system and move to a long term human readable format to keep on a server. keeping a stand alone system is not the preferred option
- Consider updating the software producing dynamic data.
- Conversion of data to standardized or long-term readable formats

SQA & RQA

- Has not been an issue yet. ||At other facilities I have worked at we would retain the old OS in the archives to assist with viewing the data.
- Create an equivalency of the new OS to ensure the readability of data for applications.
- Also validate to transfer the data to updated software (if its still in use). ||If the data is 10years old the dynamic data is moved to non-dynamic data following a risk assessment.

GQMA & SPAQA

- Case by case - risk assessment to conclude on the best possible option.

Other

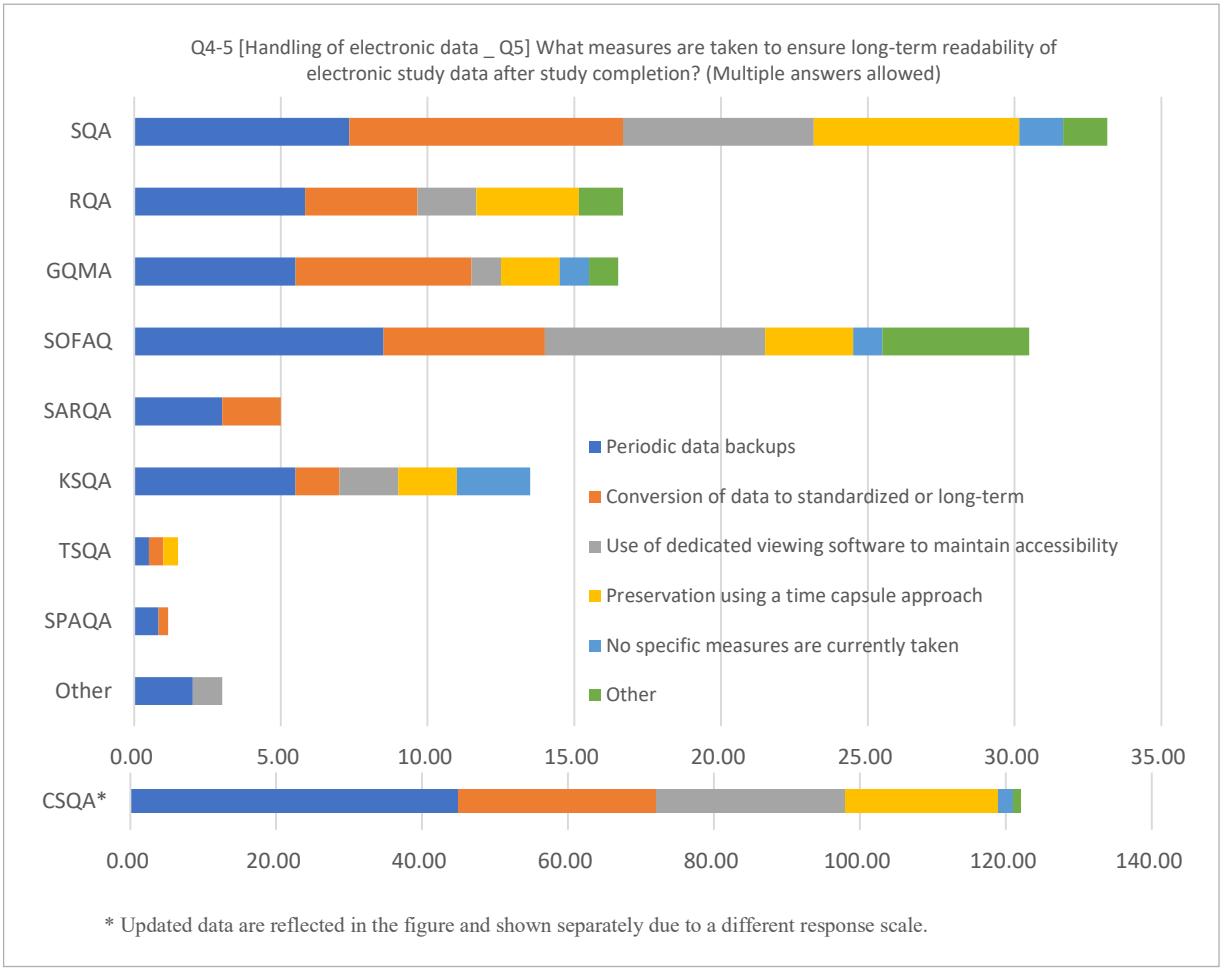
- No there yet but the requirements for legacy systems is on our radar.

CSQA (China)

1. Convert to paper records as the original record.
2. If considering updating OS, a test must be carried out to make sure it is compatible with the dynamic data generated with old OS.
3. Conduct a risk assessment on the legacy operating system, and determine control measures based on the risk assessment results to ensure data integrity requirements, such as installing antivirus software, isolating from the external Internet, and increasing the frequency of penetration testing.
4. When the OS is no longer supported, the system is converted into a stand-alone offline system. Dynamic data are also migrated to a virtual environment to maintain accessibility.
5. All records must be archived in accordance with a formally documented archiving strategy before the computerized system is decommissioned.

(Data from 7 Facilities)

Q4-5 [Handling of electronic data _ Q5] What measures are taken to ensure long-term readability of electronic study data after study completion? (Multiple answers allowed)
Periodic data backups
Conversion of data to standardized or long-term readable formats
Use of dedicated viewing software to maintain accessibility
Preservation using a time capsule approach (e.g., maintaining legacy systems or environments)
No specific measures are currently taken
Other (Free text):



The combined use of 'periodic data backups,' 'conversion of data into standardized or long-term readable formats,' 'use of dedicated viewing software to maintain accessibility,' and 'preservation using a time-capsule approach' was commonly reported. Details of other responses are provided below.

Q4-5 Other (Free text)

SQA (America)

- this is addressed via the decommissioning of the system and evaluation for what type of long term data solution is best that could be migration of data and virtualization

RQA (United Kingdom)

- Returned to Sponsor

GQMA (Germany)

- Long-term readability needs to be assessed during Computerised System validation.

SOFAQ (France)

- in addition to the above we have implemented regular verification or check of data readiness
  it is sampling based and done by the archivist
- Hard copy stored in the archives.

- Periodic tests of readability
- Periodic verification that data is legible
- Ensure that new systems can read old data

SQA & RQA

- Periodic data backups, Conversion of data to standardized or long-term, Preservation using a time capsule approach

CSQA (China)

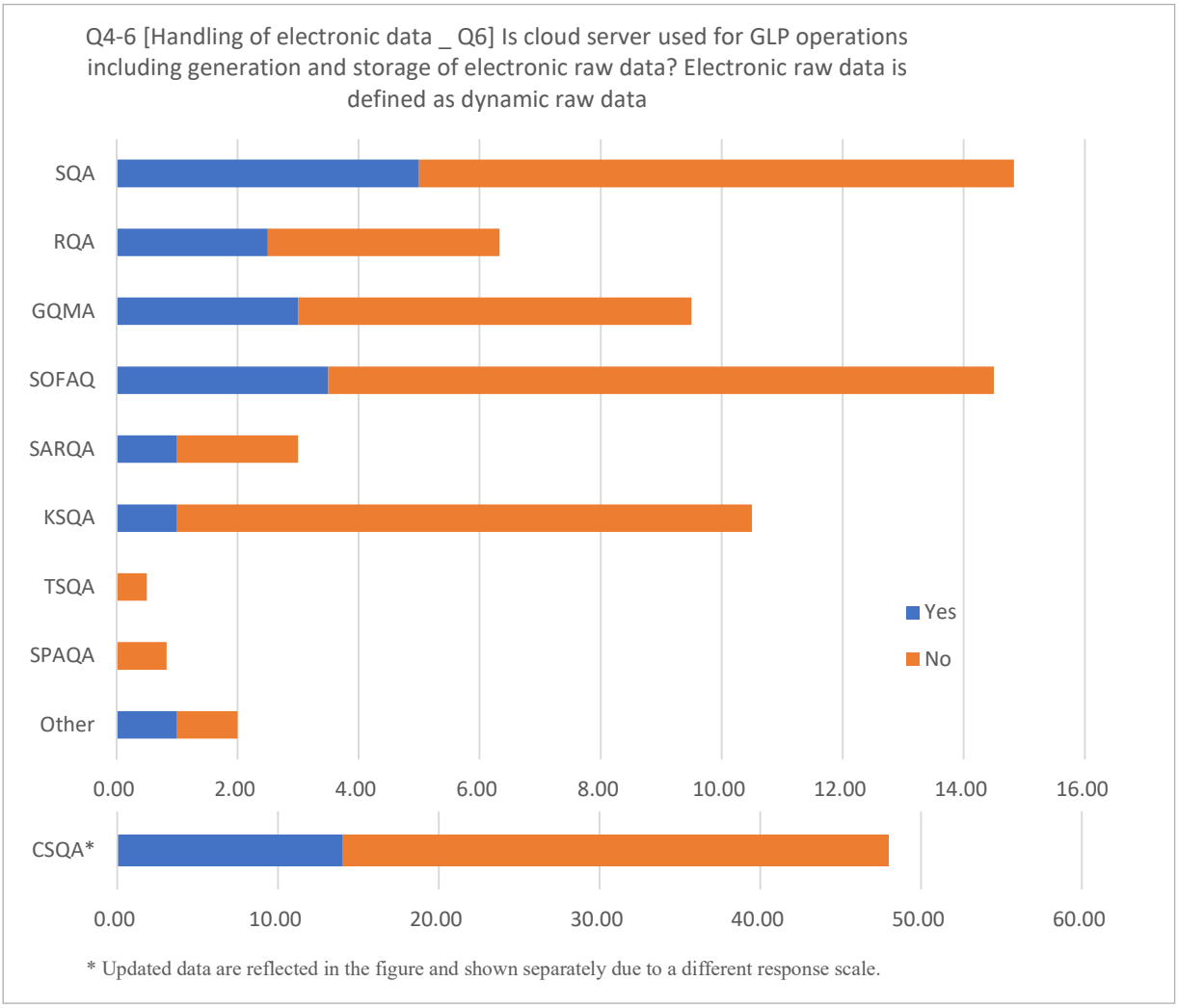
- The readability of the study electronic data is reviewed regularly with IT support.

(Data from 1 Facility)

Q4-6 [Handling of electronic data _ Q6] Is cloud server used for GLP operations including generation and storage of electronic raw data? Electronic raw data is defined as dynamic raw data collected directly during the process of an experiment (excluding values, charts, etc. that are transcribed for the first time, SOPs, and documents).

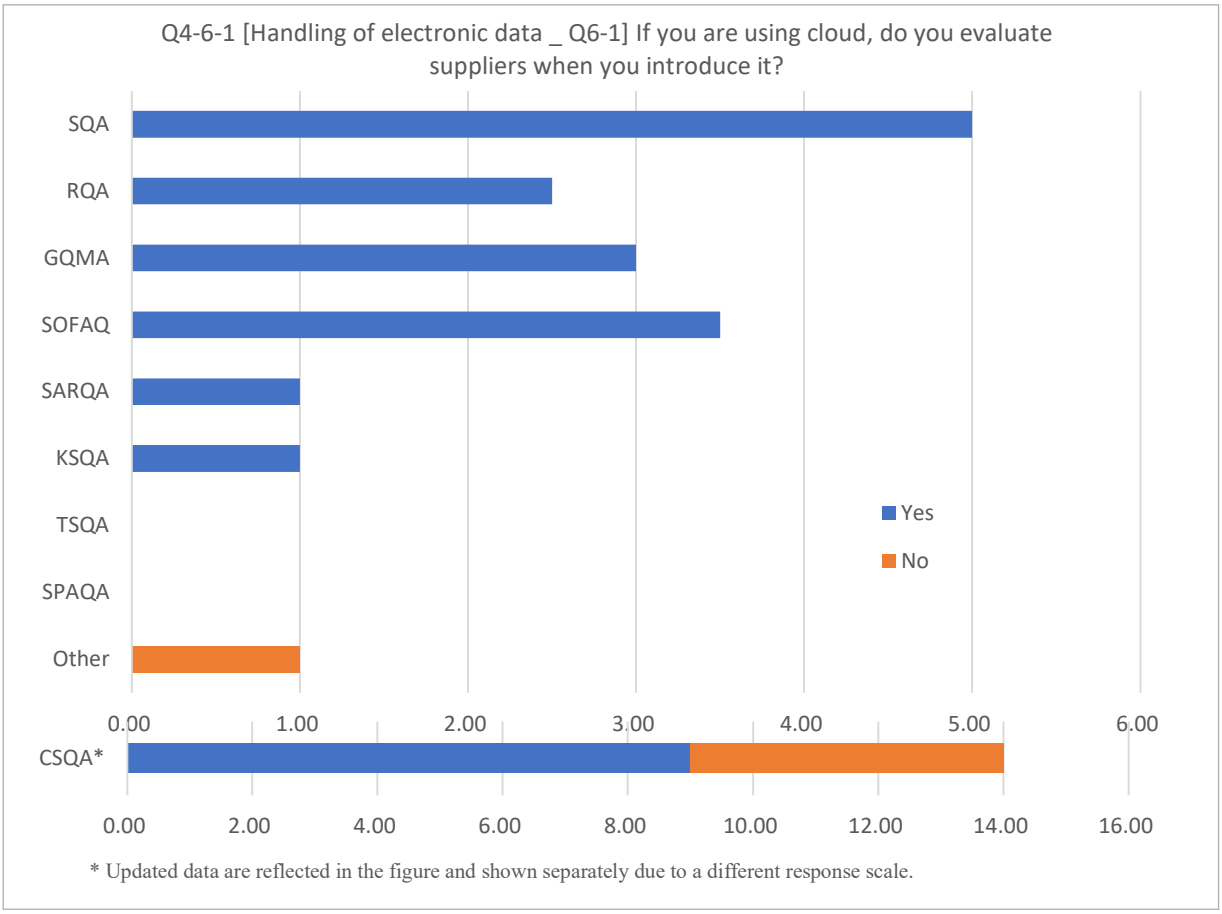
Yes (please describe the contents freely) → Q4-6-1

No



Overall, non-use of cloud storage ('No') was predominant; however, a certain level of cloud utilization was observed among RQA and SQA, GQMA, SQFAQ, SARQA and CSQA respondents.

Q4-6-1 [Handling of electronic data _ Q6-1] If you are using cloud, do you evaluate suppliers when you introduce it?
Assessed (please describe the criteria used to evaluate the supplier)
Not evaluated



Among respondents who answered 'Yes, cloud services are used' in Q4-6, most indicated that they conduct supplier evaluations for cloud utilization. The evaluation items included confirmation of compliance with the requirements of OECD GLP Document No. 17 (Application of the GLP Principles to Computerised Systems), risk-based assessments, IT security, and maintenance practices. Details of the evaluation items provided by respondents are listed below.

Q4-6-1 Assessed (please describe the criteria used to evaluate the supplier)

SQA (America)

- adheres to SDLC requirements
- Yes, using criteria established in SOP for software vendors.
- vendor audit questionnaire
- Questionnaire to understand the providers change control and security processes. Acquire certifications SOC2 required.

RQA (United Kingdom)

- Supplier/Vendor Assessment, depending on outcome of assessment, audit of supplier/vendor may be required.
- OECD guidance, SLA, TQA.

GQMA (Germany)

- vendor audit regarding ISO/OECD/FDA requirements
- Assessed by global IT QA
- Assessment of quality standards, contractual agreements etc. established at the Cloud Server provider based on risk-assessment.

SOFAQ (France)

- Qualification process, SLA with all OECD 17 S1 requirements
- Validation tests, reliability, security, maintenance, service, contract
- T security, accessibility, retention, migration

KSQA (Korea)

- We conducted a vendor qualification before introducing the cloud-based system. At that time, we created and used an evaluation checklist based on the supplement to OECD Document No. 17.

SQA & RQA

- Typical vendor audit to ensure long-term access.
- OECD 17 supplement 1. Based on security including independent checks/testing such as vulnerability scanning, penetration testing, back-ups, location i.e. EU based,

RQA & SOFAQ

- OECD guidance, SLA, TQA

Other

- Not evaluated

Q4-7 [Handling of electronic data _ Q7] What measures are taken for information security measures to prevent information leakage and hacking of electronic data? (Multiple answers is possible)

User account management

Implementation of security measures (e.g., firewall, anti-virus layer and software) to the system and verification of the functions

Procedures for handling information security incidents

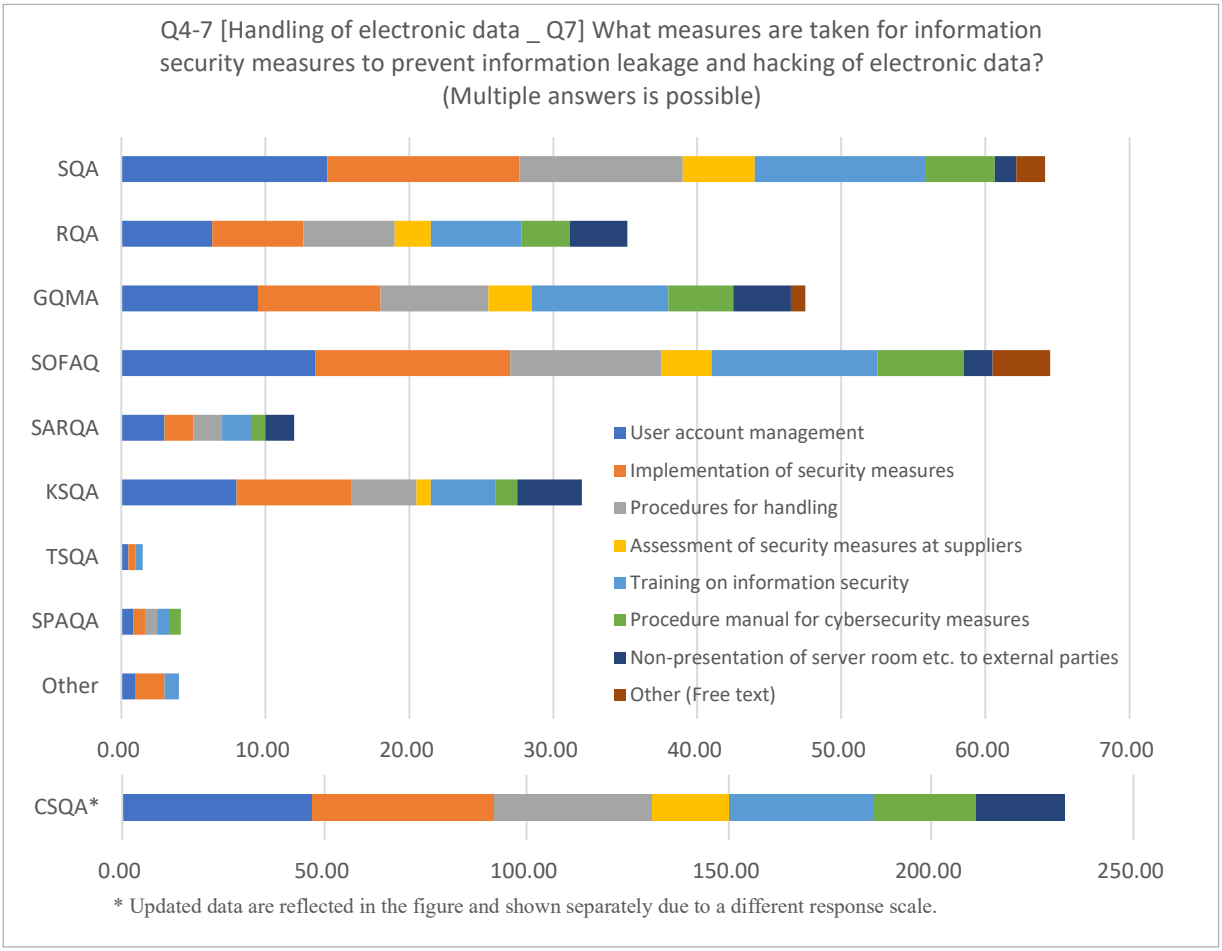
(In the case of cloud) Assessment of security measures at suppliers

Training on information security

Procedure manual for cybersecurity measures

Non-presentation of server room, etc. to external parties

Other (Free text):



The main measures reported were user account management, implementation of security measures (e.g., firewall, anti-virus layer and software) to the system and verification of the functions, training on information security, and procedures for handling information security incidents. Details of other responses are provided below.

Q4-7 Other (Free text)

SQA (America)

- inclusion in business continuity and disaster recovery plans and periodic testing and supplier auditing to confirm security
- penetration testing by external parties

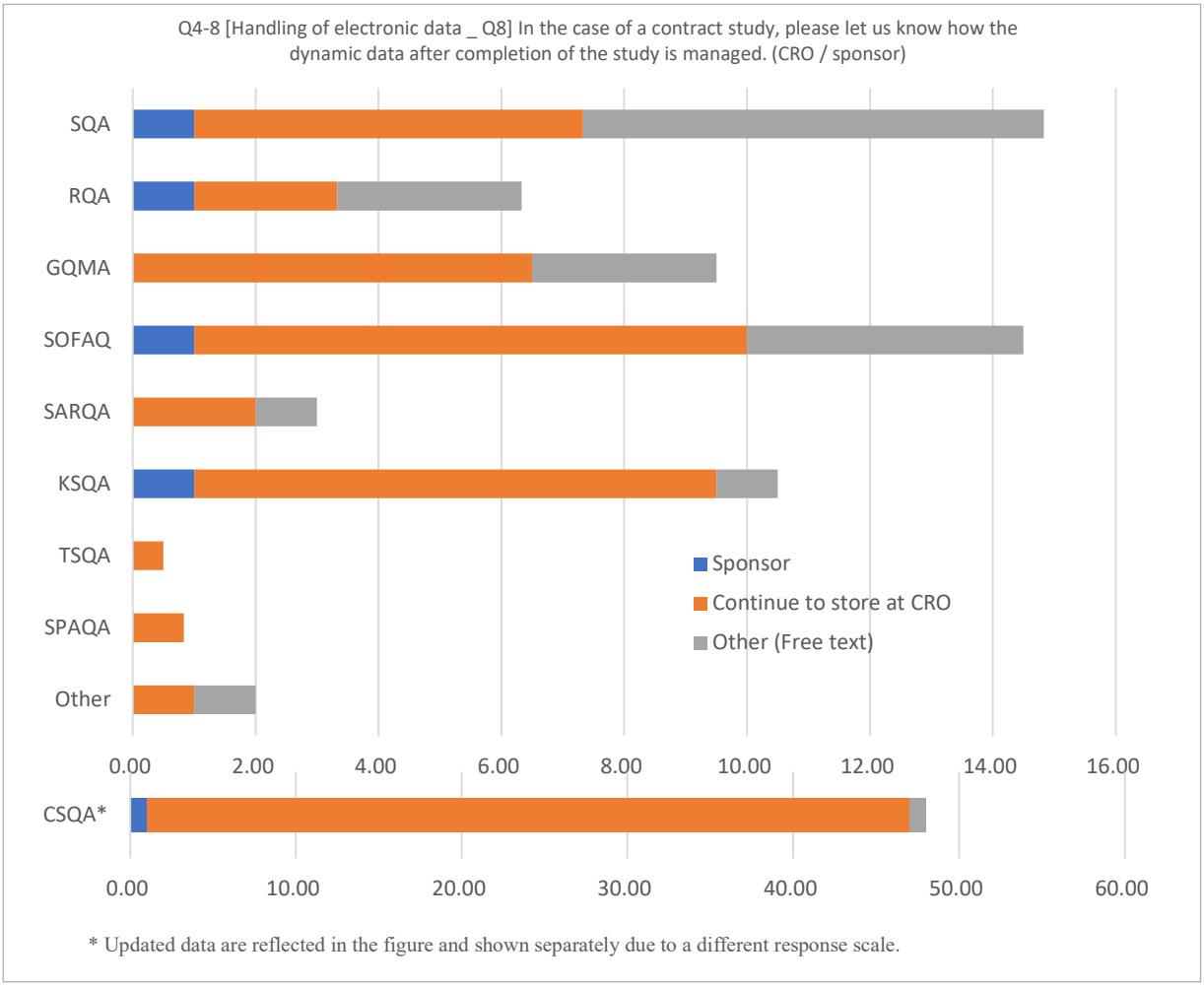
GQMA (Germany)

- Cloud providers usually have established security measures based on ISO regulations which also prevent accessibility of server rooms by visitors.

SOFAQ (France)

- use of secured and maintained portal for sharing sponsor data. Information technology security evaluate all requests for new tools
- electronic data are not available on line or on cloud server
- Back-up server not linked to the main one
- restricted access to the server room

Q4-8 [Handling of electronic data _ Q8] In the case of a contract study, please let us know how the dynamic data after completion of the study is managed. (CRO / sponsor) Transfer to the sponsor after completion of the study Continue to store at CRO after completion of the study Other (Free text):



More than half of the respondents indicated that continued storage was performed by the CRO. Details of other responses are provided below.

Q4-8 Other (Free text)

SQA (America)

- depends on the ability of the test facility/test site could be either options
- Varies by contract with each sponsor.
- It is often stored at the CRO for a time and then transferred to the sponsor or contract archive after contracted time is up.
- Depends on the contract with the CRO/sponsor. Most often, continue to store at approved archives and

pass the cost onto the sponsor after 3 years.

- Back up at CRO
- Depending on the contract with the Sponsor, after a period of time designated by protocol, it can be stored at facility or moved to the Sponsor

RQA (United Kingdom)

- Both of the above, depending on the sponsor

GQMA (Germany)

- Additional send flat copies to sponsor

SOFAQ (France)

- we have to store the data at the Test Facility for few cycles of inspection as per OECD 15
- not concerned
- Stored at CRO during 6 years and then, chose to continue or to change
- Transfer to the sponsor after the end of archiving period

KSQA (Korea)

- After a specified retention period, consult with the sponsor before returning or disposing of the materials.

SQA & RQA

- Data are archived at the CRO, then sent to off-site archives for long term storage.
- based on contract terms.
- stored for a period after completion then transferred to sponsor. The sponsor can also have the option that it is retained by the CRO

Q4-9 [Handling of electronic data-Q9] If the use of electronic signatures is permitted for GxP documents in your country, please specify the applicable laws, regulations, or guidelines. (Free text)

Details of the free-text responses are provided below.

Q4-9 Free text

SQA (America)

- 21 CFR Part 11 electronic signatures
- 21 CFR Part 11
- India does not have a GxP-specific regulation but in our test facility we are currently following the 21 CFR Part 11 or EU Annex 11 principles.
- Title: 21 CFR Part 11 — Electronic Records; Electronic Signatures
  Authority: U.S. Food and Drug Administration (FDA)

Applies to: All FDA-regulated industries, including nonclinical laboratory studies conducted under GLP (21 CFR Part 58).

Scope: Establishes the criteria under which the FDA considers electronic records and electronic signatures to be trustworthy, reliable, and equivalent to paper records and handwritten signatures.

Key Provisions: 11.10 – Controls for closed systems (security, audit trails, operational checks) 11.30 – Controls for open systems 11.50 – Signature manifestations (printed name, date/time, meaning) 11.70 – Signature/record linking 11.100–11.300 – Electronic signature requirements, including identity verification and certification to FDA.

ChatGPT said: Yes — the use of electronic signatures for GLP documents is permitted in the United States, and it's governed by a combination of federal regulations and FDA guidance, primarily under 21 CFR Part 11.

Here's the regulatory basis 🏛️ 1. 21 CFR Part 11 — Electronic Records; Electronic Signatures

Title: 21 CFR Part 11 — Electronic Records; Electronic Signatures

Authority: U.S. Food and Drug Administration (FDA)

Applies to: All FDA-regulated industries, including nonclinical laboratory studies conducted under GLP (21 CFR Part 58).

Scope: Establishes the criteria under which the FDA considers electronic records and electronic signatures to be trustworthy, reliable, and equivalent to paper records and handwritten signatures.

Key Provisions:11.10 – Controls for closed systems (security, audit trails, operational checks) 11.30 – Controls for open systems 11.50 – Signature manifestations (printed name, date/time, meaning) 11.70 – Signature/record linking 11.100–11.300 – Electronic signature requirements, including identity verification and certification to FDA.

👉GLP documents (e.g., protocols, amendments, final reports, SOP approvals, QA statements) can be signed electronically if the system and process comply with Part 11.

🧪 2. 21 CFR Part 58 — Good Laboratory Practice for Nonclinical Laboratory Studies

Relevant sections: 58.33 – Study Director responsibilities 58.185 – Reporting of nonclinical laboratory study results (requires signed final report GLP regulations do not prohibit electronic signatures. They require that the study protocol, amendments, and final report are signed and dated by the Study Director and other responsible personnel. If these signatures are electronic, they must meet the Part 11 requirements to be considered valid.

FDA Guidance: "Part 11, Electronic Records; Electronic Signatures — Scope and Application" (2003) This guidance clarifies FDA's enforcement discretion for certain aspects of Part 11 but affirms that: Electronic signatures intended to replace handwritten signatures must comply with the electronic signature provisions of Part 11 Subpart C. Part 11 applies to GLP studies because these generate data submitted to the FDA in support of research or marketing applications.

- FDA Part 11 is utilized.
- 21 CFR part 11 is required and use of closed-system as defined therein. |GDPR training and procedures.
- We follow OECD
- electronic signatures are permitted if being done under 21CFR part 11 compliance
- FDA title 21 part 11

RQA (United Kingdom)

- It is allowed by the UK GLP, however we do not use electronic signatures.
- Yes, OECD GLP.
- OECD 17

GQMA (Germany)

- There are special signature laws available in Germany. The system should also meet all OECD and FDA requirements
- Federal Law on Certification Services in the Area of Electronic Signatures and Other Applications of Digital Certificates
- REGULATION (EU) No 910/2014
- OECD 22, (EU) Nr. 910/2014 eIDAS
- it has to be a qualified electronic signature (QES)
- OECD series on Good Laboratory Practice|eIDAS; REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- EU elDAS regulations apply. In some countries (e.g. Germany, Poland) qualified electronic signatures are mandatory for GLP study documents (Study Plans, Amendments, Final Reports).
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257 28.8.2014, p. 73)

SOFAQ (France)

- FDA 21 CFR part 11, eIDAS (european regulation)
- OCDE n°1 - Principle on GLP
  OCDE n°17 - Application of GLP Principles to computerized system European Regulation N°910/2014
- level 3 of european EIDAS that is compliant with GxP
- OECD22
- 1-EU Regulation No. 910/2014 (eIDAS)
  Governs electronic identification and trust services across the EU, including France. Defines three levels of electronic signatures: Simple Electronic Signature (SES) Advanced Electronic Signature (AES) Qualified Electronic Signature (QES)
  Only QES has the same legal standing as a handwritten signature and benefits from a presumption of reliability. [docusign.com], [helpx.adobe.com] 2-French Civil Code Article 1366: An electronic document is considered written if the person can be identified and integrity is guaranteed. Article 1367: Defines electronic signature as a reliable identification process linking the signature to the act.3-Decree No. 2017-1416 of 28 September 2017
  Sets conditions for reliability of electronic signatures under French law.(docusign.com)
  4-Sector-specific GLP requirements

GLP principles in France are based on Directive 2004/10/EC, transposed into French law via Annex II to Article D523-8 of the Environmental Code. These principles require data integrity and traceability, which electronic signatures can support if compliant with eIDAS and Civil Code provisions. (COFRAC)

- OECD guidelines
- We follow the guidelines set out in OECD GLP No. 10.

KSQA (Korea)

- (1) OECD GLP No. 17. Application of GLP Principles to Computerised Systems. (2) OECD GLP No. 22. Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity
- FDA regulation
- There is no specific law issued regarding electronic signatures, and we refer to OECD documents for guidance.
- Compliant with international guidelines.
- 21cfr part 11
- Electronic signatures are not utilized.

TSQA (Taiwan)

- Electronic Signatures Act, Ministry of Digital Affairs, Taiwan.

SPAQA (Switzerland)

- Federal Law on Certification Services in the Area of Electronic Signatures and Other Applications of Digital Certificates

SQA & RQA

- US FDA: 21 CFR Part 11, following 21 CFR Part 58 requirements for signatures
- Part 11 / Annex 11
- UK GLP Regulations 1999 No. 3106|OECD|

SQA & TSQA

- Electronic Signatures Act, Ministry of Digital Affairs, Taiwan.

SQA & KSQA

- (1) OECD GLP No. 17. Application of GLP Principles to Computerised Systems.|(2) OECD GLP No. 22. Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity
- FDA regulation

RQA & SOFAQ

- 21CFR11, OECD 22, EU directive

GQMA & SPAQA

・ Federal Law on Certification Services in the Area of Electronic Signatures and Other Applications of Digital Certificates

Other

・ UK GLP Regulation, OECD
・ OECD guidelines (no.17)

CSQA (China)

1. Good Laboratory Practice for Non-clinical Laboratory Studies (Order No. 34 of the China Food and Drug Administration)
2. 21 CFR part 11;
3. OECD No. 22 Advisory Document of the Working Party on Good Laboratory Practice
4. Electronic Signature Law of the People's Republic of China
5. NMPA GMP Appendix: Computerized Systems, Validation and Verification;
6. Requirements for Drug Records and Data Management (Trial Implementation)
7. OECD No. 17 Application of GLP Principles to Computerized Systems. 2016

(Data from 48 Facilities)

Q4-10 [Handling of electronic data _ Q10] If there are any additional requirements that are not specified in laws, regulations, guidelines, etc., please let us know the contents and the requestor. (Free text)

Most respondents indicated that no additional requirements applied; however, some cited foreign regulatory requirements and ALCOA+ principles, which had been mentioned in Q4-9. Details of the responses are provided below.

Q4-10 Free text

SQA (America)

・ Annex 11 for EU clients - which aligns with 21 CFR part 11.
・ none that I know of

RQA (United Kingdom)

・ Application of GLP Principles to Computerised Systems
https://one.oecd.org/document/ENV/JM/MONO(2016)13/en/pdf

GQMA (Germany)

・ Contracts with our customers
・ Only legal regulations apply.

SOFAQ (France)

・ not applicable in France

- European Regulation on GDPR 2016/679
- content of the contract

KSQA (Korea)

- There have not yet been strict regulatory requirements regarding data integrity.
- Clarity in the definition of the original document (depending on the situation).
- Inquire about operational matters with relevant external organizations.

SQA & RQA

- Electronic records for studies include output from different computerized systems and scans of data. All electronic records are transferred to a USB, with verification of transfer, then archived at study completion for GLP studies.
- Data Integrity Principles are enforced. ALCOA++
- 21 CFR part 11

SQA & TSQA

- It covers various industries so only general rules are specified in the law. No specific requirements for GxP documents.

CSQA (China)

Based on our returned survey questionnaires,

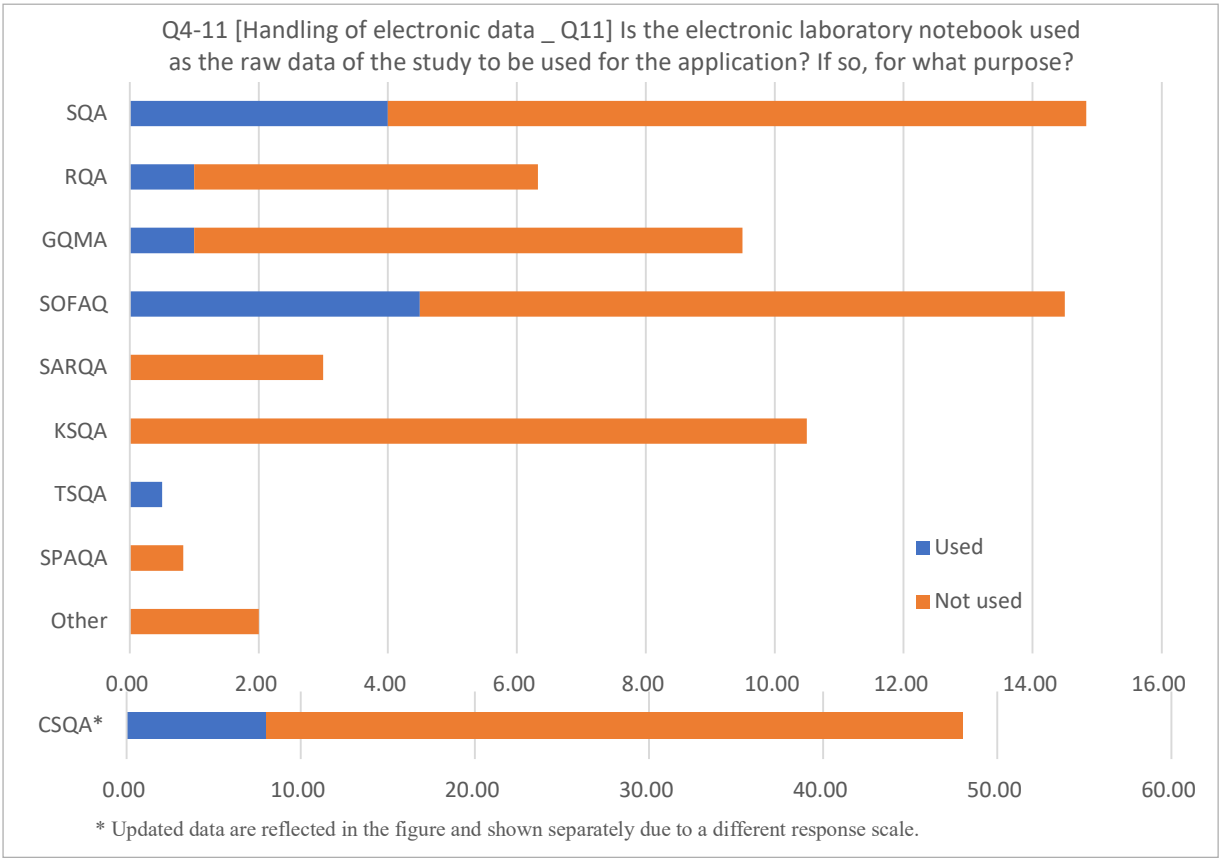
1. Clarification on whether a user account can serve as an electronic signature to attribute actions to a specific operator.
2. Electronic signatures must ensure full traceability to the individual who performed the signed action.
3. In GLP and other regulatory environments, electronic signatures must not only satisfy the "reliability" criteria outlined in the Electronic Signatures Law, but also comply with specific computerized system requirements under relevant NMPA GxP provisions—such as those governing access controls, audit trails, and system validation.
4. QA has introduced requirements for periodic long-term data integrity verification and additional IT audits of backup systems.
5. The use of personal USB flash drives for copying data is strictly prohibited.

(Data from 8 Facilities)

Q4-11 [Handling of electronic data _ Q11] Is the electronic laboratory notebook used as the raw data of the study to be used for the application? If so, for what purpose?

Used (Purpose of use: Example) Study records, equipment inspection records, free text) → Q-4-11-1

Not used



Use of electronic laboratory notebooks remains limited overall; however, their adoption, although still modest, was observed among SQA and SOFAQ respondents.

Q4-11 Other matters requiring action (Free text)

SQA (America)

- Study records (data) and equipment inspection records
- Study records
- I think it is used from study records for a specific study design however I have not audited this study design yet.

RQA (United Kingdom)

- Study data

GQMA (Germany)

- Currently developed and implemented during the next months

SOFAQ (France)

- ELN from Sapio - sample preparation and reagents tracking
- Study records
- study record as requested from the Sponsor
- Study data

SQA & RQA

- Not solely, but used for appropriate records.

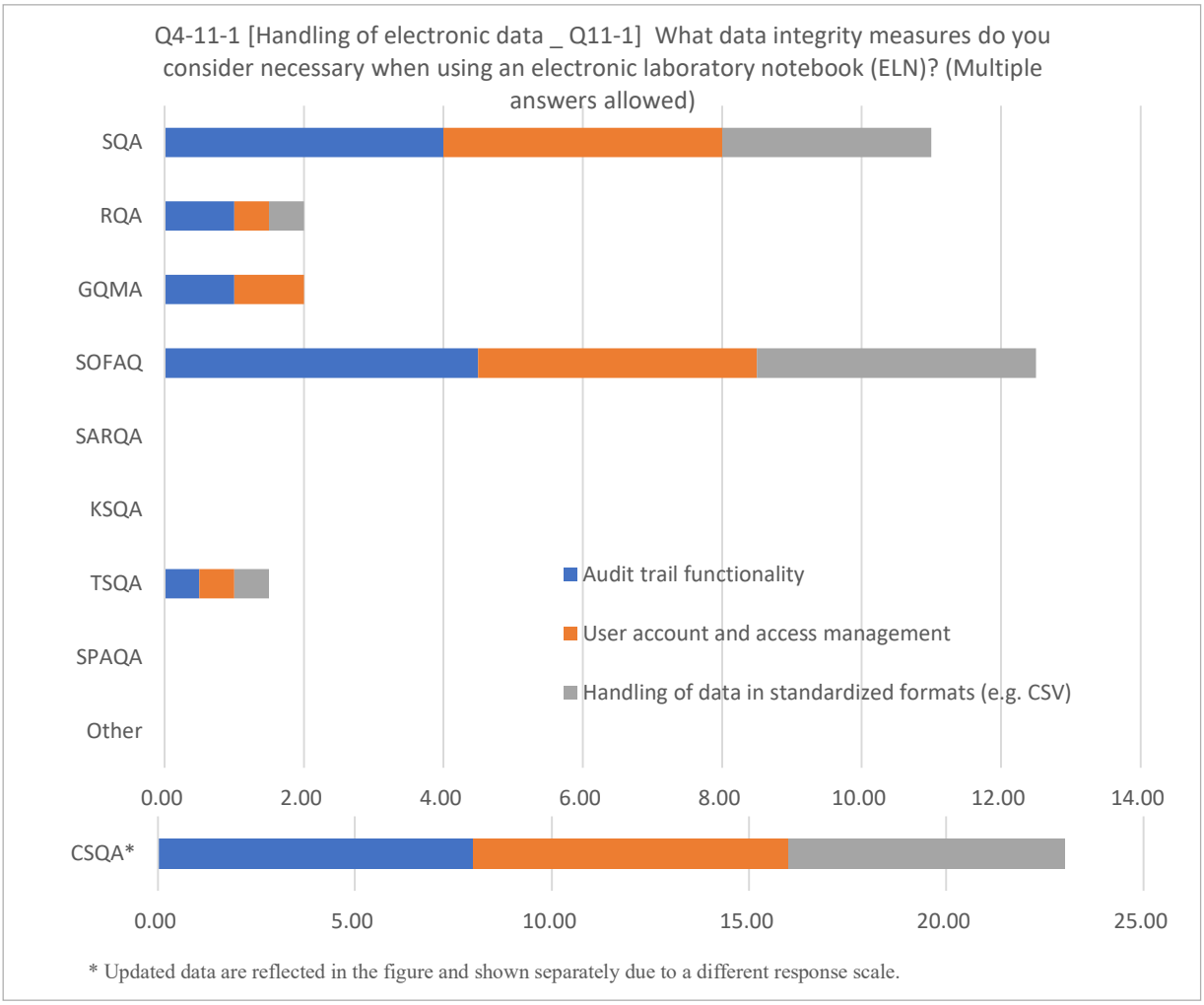
SQA & TSQA

- Data collected by the computer system (LIMS) are regarded as raw data and are submit to the regulatory authorities.

RQA & SOFAQ

- Study data

Q4-11-1 [Handling of electronic data _ Q11-1] What data integrity measures do you consider necessary when using an electronic laboratory notebook (ELN)? (Multiple answers allowed)
Audit trail functionality
User account and access management
Handling of data in standardized formats (e.g., CSV)
No specific measures are currently taken
Other matters requiring action (Free text):



Among respondents who selected 'use of electronic laboratory notebook' in Q4-11, we examined the measures required to ensure data integrity when using an electronic laboratory notebook. The most frequently identified requirements were audit trail functionality, user account and access management, and handling of data in standardized formats (e.g., CSV). Details of other necessary measures reported by respondents are provided below.

Q4-11-1 Other matters requiring action (Free text)

SQA (America)

- inventory and equipment management

RQA (United Kingdom)

- Same as any other Lab System.

GQMA (Germany)

- Export of data packages in human-readable format at study completion to be archived in an electronic archive under GLP.

SOFAQ (France)

- Validation

SQA & RQA

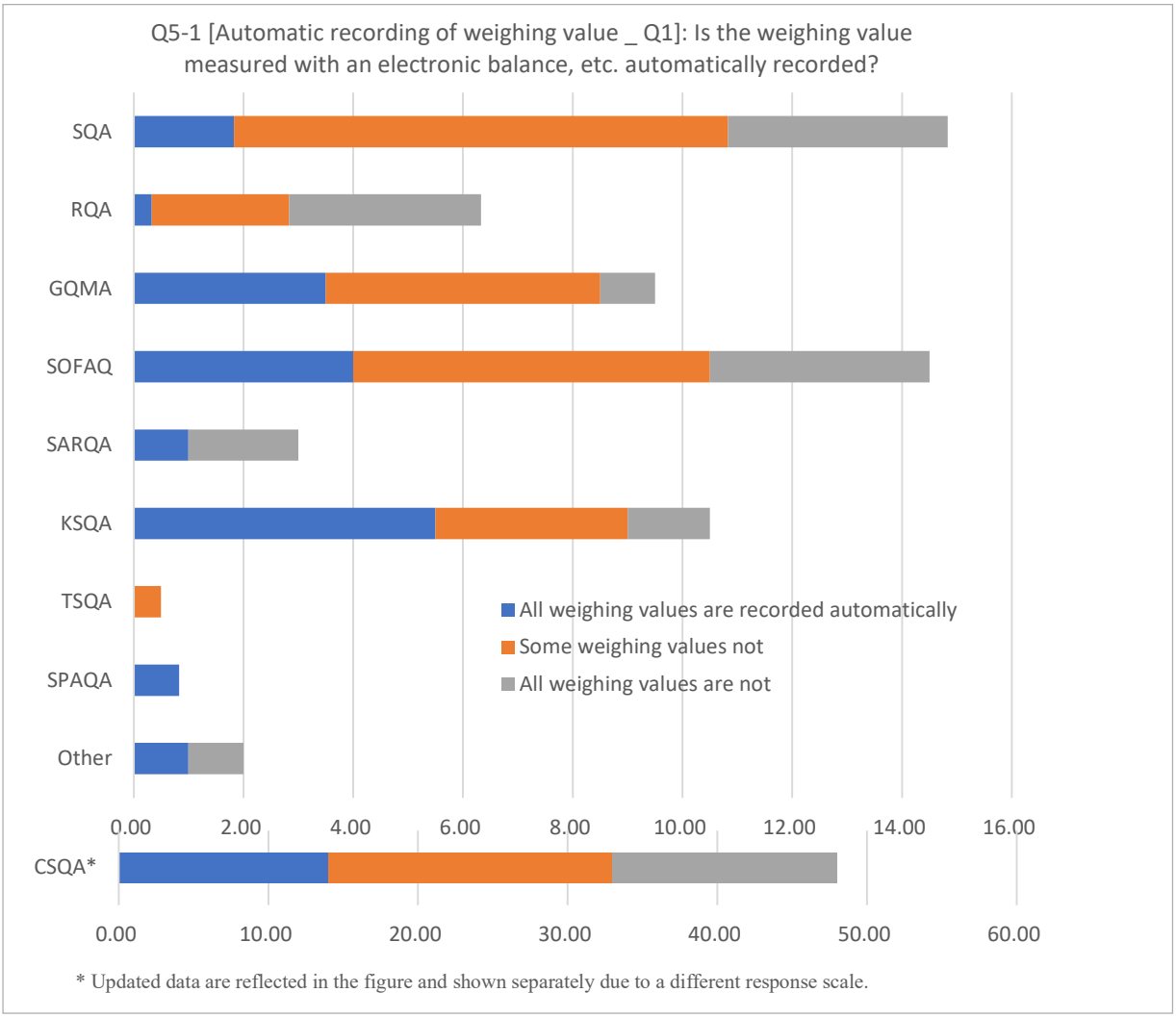
- Same as any other Lab System.

RQA & SOFAQ

- Audit trail functionality

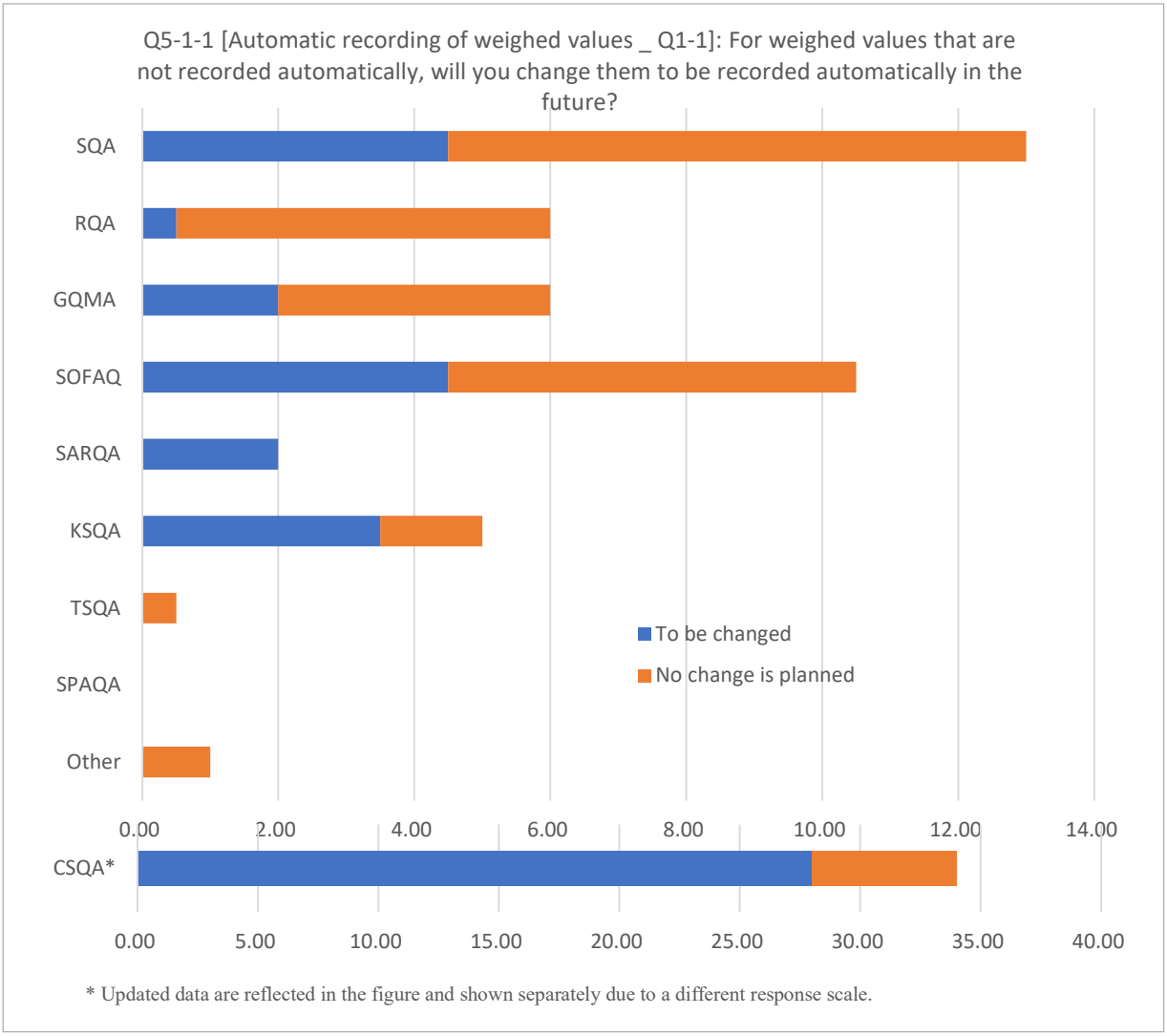
1-3 Automatic recording of weighing value

Q5-1 [Automatic recording of weighing value _ Q1]: Is the weighing value measured with an electronic balance, etc. automatically recorded? All weighing values are recorded automatically (output to computerized system, automatic printing, etc.). Some weighing values are not recorded automatically (e.g., manually recorded on blank forms*). → To Q5-1-1 All weighing values are not recorded automatically (e.g., manually recorded on blank forms*). → To Q5-1-1 *: Blank forms indicate "The use of blank paper proformas for raw data recording" as described in OECD No. 22 Section 6.2.



Responses indicating 'Some weighing values not recorded automatically' accounted for the majority. In contrast, KSQA showed relatively higher proportions of responses indicating that 'all weighing values are recorded automatically.'

Q5-1-1 [Automatic recording of weighed values _ Q1-1]: For weighed values that are not recorded automatically, will you change them to be recorded automatically in the future? To be changed. No change is planned. Reason (Free text)



* Updated data are reflected in the figure and shown separately due to a different response scale.

Among respondents who selected 'Some weighing values are not recorded automatically (e.g., manually recorded on blank forms)' or 'All weighing values are not recorded automatically (e.g., manually recorded on blank forms)' in Q5-1, we examined their plans for future implementation of automated recording. The majority responded that 'No change is planned.' Details regarding the reasons for not planning such changes are provided below.

Q5-1-1 No change is planned. Reason (Free text)

SQA (America)

- manual values are back-entered into electronic systems. Only occur is the system is down.
- not needed

- Weights are performed infrequently at our lab where automated weight recording is not cost effective.
- Budget restrictions
- Lower priority change
- a business decision to continue recording on paper at this time

RQA (United Kingdom)

- No current plans to implement this. Critical weights are confirmed by a second person or analytical measurements.
- no change is planned. Potentially in the future, but not at this time.
- A trial was done for a balance printer but this was more time consuming and did not link to records easily
- They are a small number of weights.

GQMA (Germany)

- Weighed is judged as not critical in our processes and used rarely.
- not needed
- no change planned at the moment
- Maybe far future investment.

SOFAQ (France)

- Tickets are printed and joined to the raw data
- no time to work on this subject
- No need of a new balance and this modification will change the process a lot.
- Risk based
- Cost and field environment
- Only a few weighings are recorded manually. Otherwise, most of our weighings are recorded automatically.

KSQA (Korea)

- Installation involves considerable expenses.

SQA & RQA

- Do not currently have an electronic system to receive automatic weighed values
- process does not allow automatic recording. May be transcribed to the eSystem.
- large animal (sheep, pigs, cattle) are analogue scales
-

SQA & TSQA

- It could be recorded by controlled form. Not all studies used LIMS to collect the raw data. Manual recording is still used in our facility.

SQA & KSQA

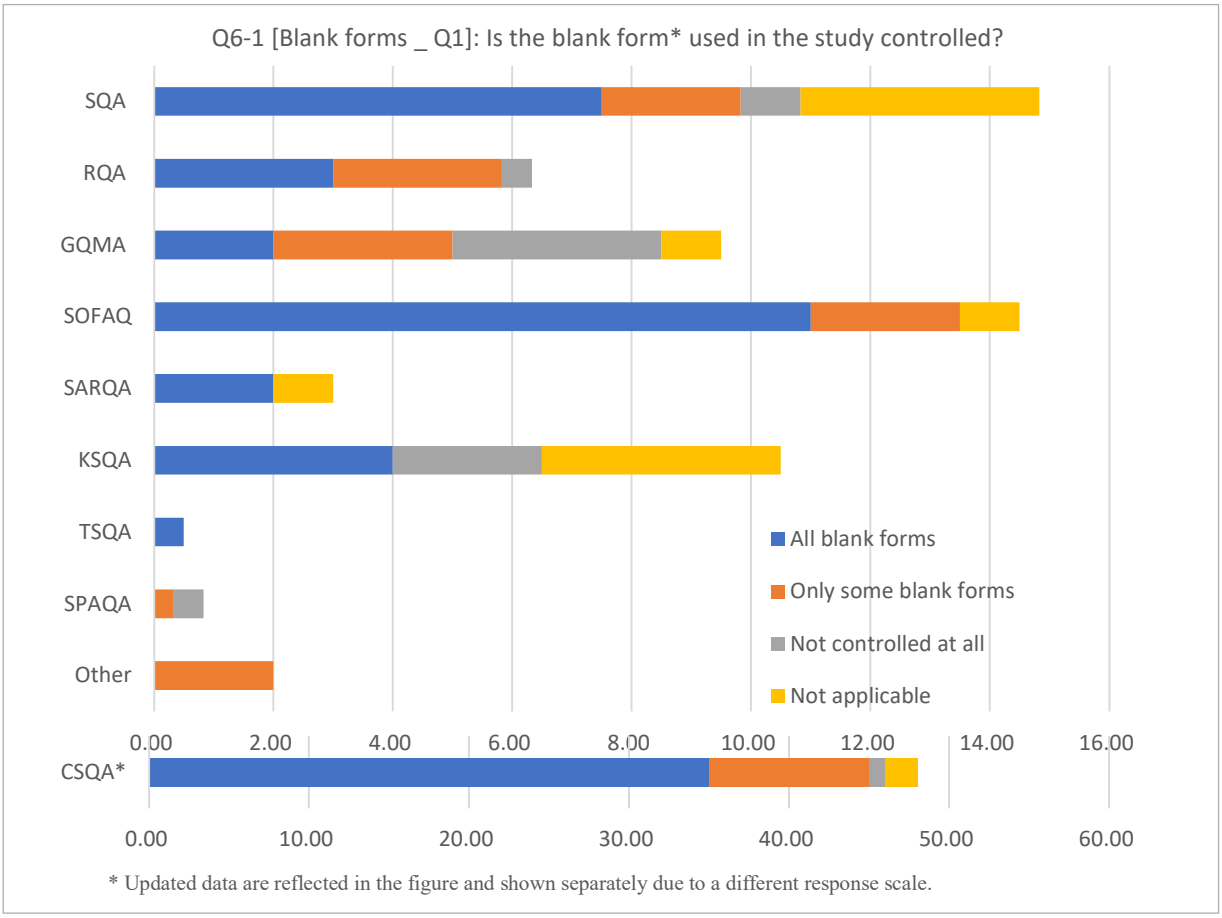
- The installation cost is high.

Other

- No change planned.

1-4 Blank forms

Q6-1 [Blank forms _ Q1]: Is the blank form* used in the study controlled? * Blank forms indicate "The use of blank paper proformas for raw data recording" as described in OECD No. 22 Section 6.2. All blank forms are controlled. → To Q6-1-1, Q6-1-2 Only some blank forms are controlled. Controlled blank form (free entry) → Q6-1-1, Q6-1-2 Not controlled at all. Not applicable



Regarding the management of blank forms used in studies, the most frequent response indicated that all such blank forms are managed. Details of other responses are provided below.

Q6-1 Other (Free text)

RQA (United Kingdom)

- Study data is recorded to controlled forms, facility data is not.
- Controlled based on risk and criticality of the record to the study.

GQMA (Germany)

- Based on a Risk Assessment
- forms are controlled, but the number of printouts used is not controlled
- The system should always allow to record any raw data at any time even if not 'controlled' form is available.

SOFAQ (France)

- Others are templates that need to be flexible. But all this is specified in procedure
- Those which are controlled are those used with automatized calculation.

SQA & RQA

- Based on criticality of data to be recorded

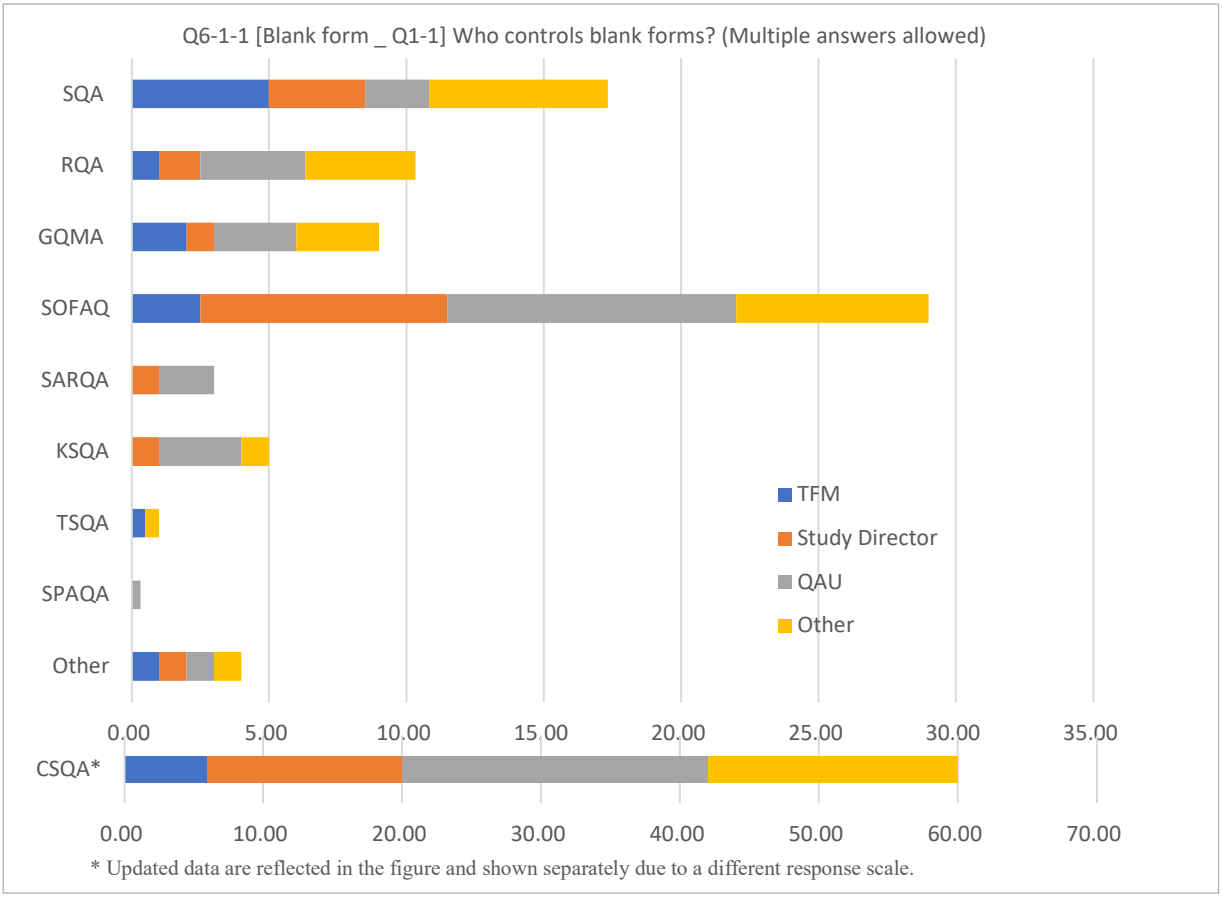
RQA & SOFAQ

- study data primary endpoint, critical site and study data

Other

- new process for us and work in is in progress

Q6-1-1 [Blank forms _ Q1-1] Who controls blank forms? (Multiple answers allowed)
TFM
Study Director
QAU
Other (Free text)



Among respondents who selected 'All blank forms are controlled' or 'Only some blank forms are controlled' in Q6-1, we examined who was responsible for the management of blank forms. The primary individuals identified were the QAU, the Study Director, and TFM. Details of other responses are provided below.

Q6-1-1 Other (Free text)

SQA (America)

- corporate compliance
- Document Controller
- Document Control
- Some blank forms are printed from quality management system.
- depends on the use study specific is under the SD and TSM; generic use that are also part of a study are under the TFM and QA

RQA (United Kingdom)

- office administrator issue template paper to SD for printing.
- uploaded to document management system
- Document controller

GQMA (Germany)

- 2nd person with training on the SOP and process
- Quality Management Department
- It is the responsibility of each member of staff to ensure blank forms are controlled so that no information never gets lost.
-

SOFAQ (France)

- study personnel responsible for data quality (OECD 1)
- Technician
- Operation manager
- Technicians
- supervisor/ study coordinator
- The Quality Control Unit checks the values entered in the form.

SQA & RQA

- document controller
- May be part of a QMS System

SQA & TSQA

- The blank controlled forms are stored in a Portal system upon approved by the TFM.

Other

- Study specific blank forms are controlled by Study Director. General reagents and equipment forms are controlled by Document Control Unit.

CSQA (China)

1. Document Management Department
2. Department Heads
3. Compliance Team / Unit
4. Designated person in each Department
5. Form owner
6. SOP Defined Forms Management (Specialized Forms Administrator)
7. Project Management
8. Facility Table Management Person

(Data from 17 Facilities)

Q6-1-2 [Blank forms _ Q1-2] Please let us know how you prepare and control the blank form to be used in the study. (Free text)

Among respondents who selected 'All blank forms are controlled' or 'Only some blank forms are controlled' in Q6-1, we examined how blank forms used in studies are created and managed. The summary of responses is as follows.

- Creation:

Most respondents indicated that blank forms are created by the Study Director. In cases where standardized formats or common templates are used, the document control department or the QAU was reported to create the templates.

- Creation methods:

Reported practices included creating forms from standardized templates, assigning control numbers, version numbers, and issuance dates, printing on watermarked paper for use, and generating electronic forms registered within QMS or document management systems.

- Management methods:

Management was most commonly performed through QMS systems, which incorporated access control, printing permissions, and template registration. Additional practices included management under SOPs and management through electronic document control systems.

Details of the responses are provided below.

Q6-1-2 Free text

SQA (America)

- Varies by department and study type
- In our Facility, we are using controlled formats for the GLP studies. These are prepared by the HOD/Senior Study Director, reviewed by QAU and approved by the TFM.
- There is only one blank form called Open Notes. This form can be used to record a lengthy conversation or event. The header requires the user to record the study ID, Animal ID and the Date. The form also requires the user to record their initials and date.
- A QMS system allows for restricted access to access and print forms.
- Blank form may be included in the protocol printable from our quality management system. Some forms are maintained in quality management system and may be printed as required. Some require a signature before use to say they are the correct revision printed from the quality management system.
- Generic use forms that also fit a study are controlled with the normal controlled document process. An assigned owner/author, review by QAU, review and approval by TSM. Reviewed periodically and updated as needed. Associated SOP identified.

  Study specific forms that only apply to that study or sponsor are controlled by the SD as the owner/author with delegated TSM review/approval. They are not part of the controlled document system and are maintained by the study team and updated as needed.

- we keep our blank forms in an electronic document system in which there are headers/footers than contain the version number, revision, history, etc.
- We have harmonized blank forms that can not be edited by the technician. For study specific forms, the Study Director has to approve the form prior to use on study and document it.

RQA (United Kingdom)

- Forms are automatically logged as printed.
- office administrator issues watermarked paper to SD. The number of pages issued is recorded. SD prints forms on watermarked paper as required. At the end of the study, the number of pages is reconciled (e.g. number printed, number watermarked paper not printed, versus number pages issued).
- excel or word document, uploaded to document management system. Study director signs off workbooks before use to check all forms needed are present
- Prepared by technical staff, stamped, signed and dated by issuing staff

GQMA (Germany)

- The forma are QCed prior to its use and approved to be used
- Electronic document management system with versioning and access control
- The examining staff are trained to print out only the forms required for specific studies. Only the latest versions of forms are available.
- via an electronic document management system.
- Blank forms should always follow Study Plan requirements. SOP regulations defined handling blank forms and completed forms are scanned as soon as possible.

SOFAQ (France)

- audits, viewer,
- we have paper form for listing the daily activities to be performed in a study room. these check lists are prepared for one week. they are daily form. after QC the blank forms are binded. at the end of each day there is a QC of completed forms to verify ALCOA++
- Checks of entered data
- The blank form is prepared based on the study plan in order to record all stages of the study. When verifying the study plan, the QAU checks that the blank forms are complete and comprehensive.
- When a new version of a guideline is available, the blank form is controlled with the GSP
- Original template are managed by a Document Management Software. The document is printed then filled in by the staff (Tech, Study Director, QAU...) and controlled by another person at a moment of the process.
- Described in a procedure
  Form number and version number, wearing the related procedure number
  Procedure review & approval also means associate Forms review & approval
- It is checked that all information to record for the experiment are asked, for example : name of operator and signature, the date, name of equipment, name of reagents and all experimental details

- Prepared by Study personnel with control access when automatization is implemented. Validated by TFM and control by QA before dispatching.
- Technicians and Study Director
  Blank forms is automatically printing with the date and hours
  Blank forms are managed by IT system to assure the effective and approve version is used
- A quality control is done before
- Our blank forms are checked beforehand by quality assurance and entered into a document management system. Only forms validated by QA should be used in studies. However, in the case where a form that has not been validated by quality assurance must be used in a study, quality assurance will audit the forms in addition to the reported values.

KSQA (Korea)

- Whenever a form registered in the SOP is revised, it is distributed in both paper and electronic formats, and the responsible personnel are notified of the changes and the effective date through training.

TSQA (Taiwan)

- The blank controlled forms are stored in a Portal system upon approved by the TFM. Study technicians would download the forms from the Portal system and fill out required information then record data int the form.

SPAQA (Switzerland)

- Forms are part of SOP and controlled by QA

SQA & RQA

- For facility records, forms can be updated and released as a new version when changes are needed, and the release of these forms is controlled by TFM, reviewed by the QAU, and the document controller completes the form change over and documents the changes. ||For GLP study specific records, the Study Director creates the forms, the QAU audits the forms for use, and these are version controlled for use on the study by the Study Director. A study specific log tracks the forms created for use on the study. The forms are almost the same from study to study, with minor changes to meet protocol requirements updated for each study.
- Print with a sequential number

SQA, RQA & SPAQA

- Forms are part of SOP and controlled by QA

SQA & TSQA

- The blank controlled forms are stored in a Portal system upon approved by the TFM.|Study technicians would download the forms from the Portal system and fill out required information then record data int the form.

RQA & SOFAQ

- As standard Forms, included in the Quality documents life cycle

Other

- We approve the form and save as a PDF on the network where it automatically prints with a time and date stamp.
- Study specific forms are prepared by study director; sometimes competent study personnel prepares the forms and is reviewed by study director. Forms are issued with version no.

CSQA (China)

"In our returned questionnaires, the management of blank forms in GLP studies is typically governed by the following comprehensive control measures to ensure data integrity and traceability:

1. Template and Version Control
   Blank forms are created from unified, fixed templates, each assigned a unique control code/number and an effective date. The Quality Assurance Unit (QAU) or document control department maintains the latest versions, and only the currently approved versions are permitted for use in studies.
2. Hierarchical Classification and Change Management
   Forms are managed under a classified system (e.g., categories for sponsor communication, central management, and experimental data). Any modifications require a formal application and approval process, with the QAU responsible for documenting the control status.
3. Application and Issuance Process
   Form requests are submitted via electronic systems or specific application forms, and are reviewed and approved by the QAU or designated personnel. Issued forms are stamped with a controlled seal, and issuance/receipt details are recorded; some forms also include security features such as watermarks and page numbers.
4. Controlled Printing
   Forms must be downloaded from controlled systems or secure cloud drives for printing. Timestamp and printer operator information are automatically recorded. Forms are printed on demand, and private storage or copying is strictly prohibited.
5. Usage and Completion Guidelines
   During form completion, any blank fields that are not applicable must be crossed out. The responsible individual must sign and date the form, and each page must bear a controlled mark (e.g., seal or code).
6. Recovery and Archiving
   Unused forms must be returned and formally voided. All used forms are counted, and complete records of issuance, recovery, and destruction are maintained. Upon study completion, the forms are audited and archived.
7. Roles and Permissions
   The QAU leads the form control process. The Study Director or department heads are responsible for approvals, while specialized personnel manage the templates. General operators are typically granted

read-only or on-demand access permissions to prevent unauthorized use.

(Data from 44 Facilities)