Altasciences, 6605 Merrill Creek Parkway, Everett, WA 98203, United States
Altasciences.com | contact@altasciences.com

Risk-Based Auditing and its Application to GLP Computerized System Validation Procedures

Cody Woodman, Shayna Halverson RQAP-GLP, Kayla Russell RQAP-GLP, and Chad Greenfield
Altasciences, Seattle, WA, United States

Click here to listen to the recorded poster presentation

ABSTRACT

In this poster, we provide a step-wise application of risk-based auditing of computerized systems for regulated use at each phase of its life cycle. Computerized systems are being used more frequently in GLP environments as new technologies become available, and, as such, must be assessed for risks to electronic record integrity and to assure continued validity of the records. Electronic records generated by these systems are utilized heavily in GLP regulated studies, thus expanding on the need for system validations. Using several case studies, we provide a framework for practical application of conducting risk-based auditing on a computerized system using Part 11 and [1]GAMP5 principals on all phases of a computerized system's life cycle from acquisition, validation, change managements, and continued maintenance. We discuss the importance of systematic monitoring of previously validated systems through science-based quality risk management, to identify risks and to remove or reduce risk to an acceptable level, as well to select the appropriate life cycle activities for specific systems. Validation efforts should be commensurate with the risk level associated with system usage. Through adequate validation efforts and proper life cycle monitoring activities, the integrity of electronic records generated by computerized systems can be assured and maintained.

METHODOLOGY

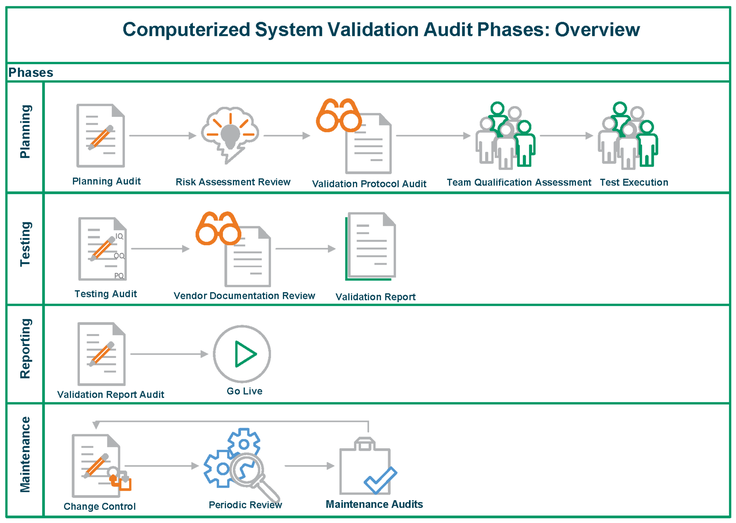

Figure 1. A brief overview of the auditing phases of a validated computerized system.

Planning

When auditing the planning phase of a computerized system validation for GLP compliance, the QA auditor plays a critical role in ensuring the process is well-defined and adheres to applicable GLP regulations. Key QA responsibilities include:

- Reviewing the Risk Assessment: Insight can be provided during the risk assessment to help identify potential areas where the system could impact data integrity, Part 58, or Part 11 compliance. This insight can help ensure that the validation protocol addresses the areas of risk identified.
- Auditing the Validation Protocol: The validation protocol should cover all essential aspects such as system identification, the proposed scope of use, the validation strategy (IQ/OQ/PQ, as applicable), system-specific SOP creation, roles and responsibilities, system release criteria, and applicable references to SOPs.
- Assessing Validation Team Qualifications: The auditor should confirm that the validation team possesses the necessary qualifications and training to conduct the validation, including GLP and Part 11 training, CSV-specific SOPs, and subject matter expertise in the field of the computerized system's proposed use.

Case Study—Auditing a Validation Protocol

A validation protocol was written for a newly acquired droplet digital PCR reader. During the planning phase audit, it was noted that the validation protocol referenced an SOP regarding system backups and recovery that was recently rendered obsolete. As this was the only driving document cited for system backups and recovery, the ability to retrieve data generated by the computerized system throughout the retention period was at risk. The auditor brought this to the attention of the validation team, who revised the validation protocol to include the updated SOP reference before execution of testing, thereby ensuring procedures were in place to back up and recover system data.

Testing

During the testing phase audit, the auditor should focus on ensuring the validation activities are executed thoroughly and adhere to the documented plan. Major aspects to confirm include:

- Test Script Execution: Pre-defined test scripts should be executed meticulously, to provide documented evidence of the system's functionalities for the proposed scope of use. Vendor testing documents should be leveraged where applicable. Test scripts should describe the scope of testing and provide details on the specific steps to be executed, data to be entered, expected results of the test step, and observed results. Test scripts should cover all critical functionalities of the system relevant to GLP studies including data acquisition, processing, storage, retrieval, and reporting functionalities, as applicable.
- Part 11 Compliance: Testing should include measures to ensure that all Part 11 and predicate rule requirements are met, including access controls, electronic signatures, and audit trail functionality.
- Data Integrity: The validation process should evaluate controls to safeguard data integrity within the system. This should include testing for measures that prevent unauthorized data alteration, deletion, or loss.
- Exceptions: Unforeseen circumstances encountered during validation testing should be documented as exceptions. Exceptions should be reported to include the root cause and impact on subsequent validation activities. If exceptions cannot be resolved, workarounds should be documented and justified.

Case Study—Leveraging Vendor Testing Documentation

A testing facility had just finished test script execution for a newly acquired real-time PCR system, leveraging vendor documentation for installation and operational qualifications. During the audit of the testing phase, it was noted that vendor operational qualifications included one test step that did not meet the vendor's pre-defined acceptance criteria, however, this step was marked as passed. As this was the only documentation of testing for this function, the reliability of the system for its intended use was at risk. Since the vendor's field service technician could not reconstruct the correct data, the technician came back onsite to retest the instrument, providing results that passed the previously pre-defined acceptance criteria.

Reporting

The validation report should accurately reflect the validation activities and their outcomes. During the reporting phase, the auditor should review the validation report to ensure it identifies any special considerations, exceptions encountered during testing, and the overall conclusion of the validation status. Traceability between validation requirements and associated testing efforts should be clear (typically in the form of a traceability matrix or other supporting document), to ensure reviewers can follow the testing procedures and understand the rationale behind the conclusions.

LIFE CYCLE ACTIVITIES

Once a computerized system has been validated and released for use in a GLP environment, it is imperative to ensure the validated state is maintained throughout the life cycle of the system. This is achieved through a robust change control process, periodic reviews performed by the validation team, and maintenance audits of computerized systems commensurate with their previously determined risk.

Change Controls

Change control procedures should be established for validated computerized systems and should clearly define the scope of changes. Procedures should be in place to request changes to a validated system (before making any changes) in a well-defined process for submitting, reviewing, and approving change requests. Change requests should be reviewed by key stakeholders and personnel with relevant expertise to determine the potential impact of the proposed changes. Original validation documentation should be reviewed to determine if updates are required due to changes being implemented. For more complex changes, a risk assessment should be performed to identify and evaluate potential risks to the system's validated state and GLP compliance. A change control summary report should be provided once testing is complete, and all exceptions are concluded. Any adverse events and remediation should be included, as applicable. Change controls should be audited per their determined risk; low-risk change controls should be reviewed during maintenance auditing of the system, with higher-risk change controls audited at the time of implementation.

Maintenance Audits

Maintenance audits are periodic evaluations designed to ensure that validated systems continue to function as intended and meet GLP principles. A risk-based approach should be utilized to optimize efficiency and effectiveness. The focus should be tailored to:

- Change Controls: Change controls should be reviewed per their previously defined risk. Changes with potentially higher risks (e.g., complex system modifications, software upgrades, cross-site validations) should receive a more in-depth examination. This will ensure a thorough evaluation of critical changes while streamlining review for low-risk modifications.
- Periodic Reviews: Systematic evaluations should be conducted at defined intervals by the Validation Team, to ensure the system remains validated and assure compliance with applicable GLP regulations. These reviews should verify that the controls implemented during validation are still adequate and effective in maintaining data integrity and the system's functionality throughout its life cycle.
- Risk-Informed System Auditing: Systems and their functionalities can be more heavily targeted based on previously assessed risk. Computerized systems that have been deemed inherently high risk (e.g., category 5), should receive more frequent maintenance audits with a rigorous examination of all controls, and a larger sample set should be reviewed. Lower-risk computerized systems (e.g., category 3), should receive maintenance audits at a lower frequency, commensurate with the previously assessed risk. Critical functionalities (e.g., audit trails, data capture and transmission, storage and retrieval, electronic records, and signatures) should be the primary focus of the audit. In addition to scheduled maintenance audits, computerized systems should be reviewed during audits of all critical phases in a GLP study. These should ensure that the system is being used as intended by the end-user, and that proper maintenance is being conducted and documented.
- Computerized System Maintenance: Maintenance of computerized systems utilized for GLP data collection should be documented and available, including routine maintenance, non-routine maintenance, and calibration records. Maintenance performed by third parties should be reviewed by system owners and applicable stakeholders and retained with the computerized system maintenance records.
- Current System Usage: User manuals, SOPs, the original validation documents, and training materials should be reviewed to obtain an understanding of the system's intended functionalities, identified workarounds, and authorized use. Targeted interviews should be conducted with personnel who utilize the system for GLP data collection to ensure conformance with the system's intended use.

Case Study—Conducting a Maintenance Audit

A maintenance audit is being conducted on a previously validated flow cytometer. The auditor implements a risk-based approach focusing on areas with the highest potential to compromise data integrity and GLP compliance in the context of system usage. Critical functionalities have been identified as user access, data acquisition, analysis settings, and reporting functionalities. Upon review of system access logs, the auditor observes that multiple users who are no longer with the testing facility still have access and that additional users have been given access without relevant GLP training. While subject matter expertise plays a role in computerized system usage, documented GLP training is imperative for all users of a computerized system. The system owner is informed that certain user accesses should be revoked and that new users should receive GLP training before system usage, thereby ensuring the computerized system remains validated.

CONCLUSION

By implementing a risk-based approach to computerized system validation audits in a GLP environment, organizations can achieve a more efficient and effective validation process. This targeted approach focuses resources on areas of greater risk, streamlining the audit process while ensuring continued data integrity and GLP compliance. This approach fosters a culture of continuous improvement, prompting organizations to proactively identify and address potential issues. Risk-based auditing contributes to the overall reliability and trustworthiness of data generated by computerized systems within GLP environments.

Reference: [1]GAMP5: A Risk-Based Approach to Compliant GxP Computerized Systems

© 2024 Altasciences. All Rights Reserved.