AUDIT TRAIL REVIEW PROCEDURE

Document ID:	SOP-DI-002
Revision:	1.0
Effective Date:	*[DD.MM.YYYY]*
Review Date:	*[DD.MM.YYYY + 2 Years]*
Owner:	Quality Assurance
Approved by:	*[Name], Head of Quality*

Revision History

Rev	Date	Author	Description
1.0	*[DD.MM.YYYY]*	*[Name]*	Initial Release

1. Purpose

This procedure defines the requirements for reviewing audit trails in GxP computerized systems. Audit trail review is a critical component of data integrity assurance and regulatory compliance.

2. Scope

This SOP applies to:

- All GxP computerized systems with audit trail functionality
- Laboratory Information Management Systems (LIMS)
- Chromatography Data Systems (CDS)
- Manufacturing Execution Systems (MES)
- Enterprise Resource Planning (ERP) systems
- Any other system capturing GxP-critical data

3. Regulatory Requirements

Regulation	Requirement
EU GMP Annex 11.9	Audit trails should be available and convertible to a generally intelligible form and regularly reviewed.
21 CFR 11.10(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions.
PIC/S PI 041-1	Audit trails should be reviewed as part of the routine data review/approval process.
WHO TRS 1033	Audit trails should be reviewed and any irregularities should be investigated.

4. Types of Audit Trail Review

Review Type	Frequency	Purpose
Batch Release Review	Every batch	Verify data integrity of batch-related records before release
Periodic Review	Monthly or Quarterly	Systematic review of system-wide audit trails for anomalies and trends
For-Cause Review	As needed	Investigation of suspected data integrity issues or deviations
Annual Assessment	Annually	Comprehensive review of audit trail configuration and effectiveness

5. What to Review in Audit Trails

5.1 Minimum Review Elements

- WHO - User identification (individual, not generic)
- WHAT - The data element that was changed
- WHEN - Date and time stamp of the action
- OLD VALUE - The previous value before change
- NEW VALUE - The new value after change
- WHY - Reason for change (where captured)

5.2 Actions to Monitor

- Data creation, modification, and deletion
- User login/logout events
- Failed login attempts
- System configuration changes
- User account management (creation, modification, deactivation)
- Method/parameter changes
- System date/time changes

6. Red Flags Checklist (12 Critical Indicators)

Based on 2024 FDA inspection findings. The following indicators require immediate investigation:

#	Red Flag	Description & Investigation Action
1	**Changes Outside Working Hours**	Data modifications at nights, weekends, or holidays. Verify legitimate business need.
2	**Changes Before Batch Release**	Multiple changes immediately before QA review or batch release. May indicate result manipulation.
3	**Missing Reason for Change**	Changes without documented justification. Required by Annex 11.9.
4	**Test Repetitions Without OOS Investigation**	Multiple test runs where only passing results are reported. Check for hidden failures.
5	**Deleted Data**	Any data deletion without documented justification and QA approval.
6	**Sequence Gaps**	Missing sequence numbers in batch records or sample IDs. May indicate removed records.
7	**Backdated Entries**	System timestamp differs from recorded activity time. Violates contemporaneous recording.
8	**Generic/Shared Logins**	Use of shared accounts (Lab, Admin, QC). Violates attributability requirement.
9	**Timestamp Anomalies**	Inconsistent timestamps, time jumps, or out-of-sequence events.
10	**Unusually Short Processing Times**	Activities completed faster than physically possible. May indicate pre-dating.
11	**Audit Trail Gaps**	Periods with no audit trail entries despite expected system activity.
12	**Excessive Failed Logins**	Multiple failed login attempts may indicate unauthorized access attempts.

7. Review Procedure

7.1 Batch Release Review

Note: This review is performed as part of the Batch Release procedure (refer to SOP-BR-001 or equivalent Batch Release SOP). Audit trail review must be completed and documented prior to QP/QA batch release approval.

1. Access the audit trail for the batch/sample being reviewed
2. Filter audit trail for the relevant time period and data elements
3. Check for any red flags from Section 6
4. Verify all changes have documented reasons
5. Confirm no deletions occurred without approval
6. Document the review in the batch record or review form
7. Escalate any findings per Section 8

7.2 Periodic Review

8. Generate audit trail report for the review period
9. Review login patterns - identify unusual access times or locations
10. Check for failed login attempts and patterns
11. Review system configuration changes
12. Analyze data modification trends
13. Document findings and trends
14. Complete the Periodic Review Form (Appendix A)

7.3 For-Cause Review

15. Document the trigger for the for-cause review
16. Expand the scope to cover all potentially affected data
17. Review all users who accessed the affected records
18. Check for patterns across multiple systems
19. Interview relevant personnel if needed
20. Document findings in deviation/investigation report

8. Escalation Path

Finding Severity	Action Required	Timeline
CRITICAL	Immediate escalation to QA Head and Site Director. Initiate formal investigation. Consider batch quarantine.	Within 4 hours
MAJOR	Report to QA Manager. Document in deviation system. Initiate investigation.	Within 24 hours
MINOR	Document finding. Include in trending. Address through CAPA if recurring.	Within 5 business days

8.1 Critical Findings Examples

- Evidence of intentional data manipulation or falsification
- Audit trail disabled without authorization

- Systematic deletion of failing test results
- Evidence of backdating batch release documentation

9. Documentation Requirements

- Batch Release: Document review in batch record - sign and date
- Periodic Review: Complete Periodic Review Form (Appendix A)
- For-Cause Review: Document in deviation/investigation system
- Retain all audit trail review documentation per retention policy

10. Training Requirements

- All reviewers SHALL be trained on this procedure before performing reviews
- Training SHALL include recognition of red flags and escalation requirements
- System-specific training SHALL be provided for each system reviewed
- Refresher training SHALL be conducted annually

Appendix A: Periodic Audit Trail Review Form

Field	Entry
System Name:	
Review Period:	From: _____ To: _____
Reviewer:	
Review Date:	

Checklist:

Item	Yes/No	Comments
1. Audit trail enabled and protected?		
2. Any changes outside working hours?		
3. Any changes missing reason for change?		
4. Any deleted records identified?		
5. Any sequence gaps identified?		
6. Any generic logins used?		
7. Any excessive failed login attempts?		
8. Any timestamp anomalies?		
9. Any unusual patterns identified?		
10. All findings escalated as required?		

Findings Summary:

_____

_____

_____

Conclusion: ☐ No findings ☐ Findings - see above

Reviewer Signature: _____ **Date:** _____

QA Approval: _____ **Date:** _____

Compliant with FDA 21 CFR Part 11, EU GMP Annex 11, PIC/S PI 041-1, and WHO TRS 1033