AI Audit Trail Review Checklist

GMP / Pharma QA Tool for AIforQA.org

Short Description

This checklist helps pharmaceutical QA, CSV, Data Integrity, and IT Quality teams evaluate whether AI can support audit trail review while maintaining data integrity, human oversight, appropriate escalation, and compliance with applicable GMP/GxP expectations.

Intended Use

- Planning audit trail review activities for GxP systems.
- Assessing AI-assisted anomaly detection for audit trails.
- Supporting periodic audit trail review activities.
- Evaluating audit trail review for systems subject to 21 CFR Part 11 or equivalent electronic record expectations.
- Reviewing LIMS, QMS, LMS, MES, ERP, CDS, electronic document systems, and other GxP systems.
- Supporting data integrity investigations where AI-generated alerts, exceptions, or patterns require human verification.

Scope

Category	Description
Included	AI-assisted audit trail review planning, exception identification, anomaly detection, periodic review support, review-by-exception assessments, data integrity triage, and human verification workflows for GxP systems.
Excluded	Unapproved autonomous AI decisions, automatic closure of audit trail exceptions, unsupervised batch release decisions, use of public AI tools with confidential/GMP data, and replacement of company procedures, validation requirements, or qualified human review.

User Instructions

1. Identify the GxP system, process owner, system owner, audit trail location, and review frequency.

2. Define whether AI will be used for advisory review, anomaly detection, prioritization, exception flagging, or investigation support.

3. Complete the System Information Table before performing the assessment.

4. Answer each checklist question as Yes, No, or N/A. Record the risk impact and evidence or justification.

5. For AI-detected exceptions, complete the AI Exception Review Table and verify the exception against the source audit trail.

6. Determine whether the AI signal is a true exception, false positive, false negative concern, system issue, data integrity concern, or no-impact observation.

7. Escalate any significant concern according to company deviation, CAPA, data integrity, cybersecurity, or validation procedures.

8. Complete the Final Review Outcome and Approval Table. Retain the completed checklist and supporting evidence as required by company procedures.

Key Definitions

Term	Definition
Audit trail	A secure, computer-generated, time-stamped record that captures activities affecting electronic records, including creation, modification, deletion, user actions, and system events.
Critical data	Data that can directly or indirectly affect product quality, patient safety, batch disposition, regulatory decisions, or GMP compliance.
AI-assisted review	Use of an AI tool to support audit trail review by identifying patterns, anomalies, exceptions, or review priorities for qualified human assessment.
Anomaly detection	Identification of audit trail events or patterns that differ from expected behavior, historical baseline, or defined rules.
Data integrity	The completeness, consistency, accuracy, trustworthiness, and reliability of data throughout its lifecycle.
ALCOA+	Data integrity principles: Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available.
Human verification	Qualified human review of AI-identified events, source records, audit trail details, and GMP significance before any conclusion or action is taken.
False positive	An AI-flagged event that is determined after human review not to be a true exception or concern.
False negative	A relevant exception or concern not detected by the AI tool.
Review by exception	A review approach that focuses human attention on predefined exceptions, anomalies, and risk-significant events while maintaining appropriate oversight of the full record context.

System Information Table

Field	Information / Response
System name	
System owner	
Vendor	
Version	
GxP process supported	
Audit trail location	
Audit trail fields available	
Review frequency	
AI tool used	
Reviewer	

Main Checklist Table

Review Area	Assessment Question	Yes	No	N/A	Risk Impact	Comments / Evidence
Audit trail completeness	Does the system generate audit trails for all required creation, modification, deletion, approval, review, and system events?	☐	☐	☐	High if incomplete	
Audit trail completeness	Are audit trail records complete, retained, readable, and available for the required retention period?	☐	☐	☐	High	
Audit trail completeness	Are audit trail records protected from unauthorized alteration or deletion?	☐	☐	☐	High	
Critical data identification	Have critical data elements been defined for this system or process?	☐	☐	☐	High	
Critical data identification	Has the audit trail review scope been prioritized based on critical data and GMP risk?	☐	☐	☐	Medium/High	
User activity review	Does the review include user activity associated with critical data creation, modification, deletion, and approval?	☐	☐	☐	High	
User activity review	Are unusual user behavior patterns reviewed, such as repeated corrections, late entries, or unusual access times?	☐	☐	☐	Medium/High	
Data creation/modification/deletion	Are changes to critical records reviewed for reason, authorization, timing, and GMP impact?	☐	☐	☐	High	
Data creation/modification/deletion	Are deleted, overwritten, voided, or canceled records reviewed and justified?	☐	☐	☐	High	
Date/time changes	Are system date/time changes, backdating, or time-zone changes captured and reviewed?	☐	☐	☐	High	
Date/time changes	Are timestamps synchronized and protected from unauthorized modification?	☐	☐	☐	Medium/High	
Failed login attempts	Are failed login attempts, locked accounts, and suspicious access patterns reviewed?	☐	☐	☐	Medium	
Privilege changes	Are changes to user roles, privileges, administrator rights, and security settings reviewed?	☐	☐	☐	High	
Electronic signatures	Are electronic signature events reviewed for user, meaning, date/time, and record association?	☐	☐	☐	High	
AI anomaly detection	Is the AI tool configured to detect relevant audit trail anomalies based on the system intended use?	☐	☐	☐	Medium/High	

Review Area	Assessment Question	Yes	No	N/A	Risk Impact	Comments / Evidence
AI anomaly detection	Are AI-detected anomalies linked back to source audit trail events and evidence?	☐	☐	☐	High	
Exception handling	Are criteria defined for what constitutes an audit trail exception?	☐	☐	☐	Medium/High	
Exception handling	Are exceptions triaged, documented, investigated, and escalated according to risk?	☐	☐	☐	High	
Human verification	Are all AI-flagged audit trail exceptions reviewed by a qualified human reviewer?	☐	☐	☐	High	
Human verification	Can reviewers accept, reject, or override AI findings with documented rationale?	☐	☐	☐	Medium/High	
False positives	Are false positive AI alerts tracked and periodically assessed for threshold or model adjustment?	☐	☐	☐	Medium	
False negatives	Is there a process to evaluate missed exceptions or AI false negatives?	☐	☐	☐	High	
Escalation criteria	Are escalation criteria defined for potential data integrity concerns, system issues, cybersecurity events, deviations, and CAPAs?	☐	☐	☐	High	
Validation requirements	Has the AI-assisted audit trail review function been assessed for validation impact?	☐	☐	☐	High	
Validation requirements	Have AI rules, models, thresholds, data mappings, reports, and dashboards been tested as applicable?	☐	☐	☐	High	
Part 11	Has the system been assessed for 21 CFR Part 11 applicability, including electronic records and electronic signatures?	☐	☐	☐	High	
Part 11	Are audit trail controls, access controls, authority checks, and record retention controls verified as applicable?	☐	☐	☐	High	
ALCOA+	Does the review support ALCOA+ expectations for critical electronic records?	☐	☐	☐	High	
ALCOA+	Are original data preserved and available for review even when AI summaries are generated?	☐	☐	☐	High	
Cybersecurity	Are AI tool access, data transfers, integrations, and hosting arrangements assessed for cybersecurity risk?	☐	☐	☐	Medium/High	
Cybersecurity	Are suspicious access, privilege escalation, or unusual system interactions escalated to IT/security?	☐	☐	☐	Medium/High	

AI Exception Review Table

Exception ID	Detected by AI	Audit Trail Event	User	Date/Time	System Impact	Reviewer Assessment	True Exception?	Investigation Required?	Comments
							☐ Yes ☐ No	☐ Yes ☐ No	
							☐ Yes ☐ No	☐ Yes ☐ No	
							☐ Yes ☐ No	☐ Yes ☐ No	
							☐ Yes ☐ No	☐ Yes ☐ No	
							☐ Yes ☐ No	☐ Yes ☐ No	
							☐ Yes ☐ No	☐ Yes ☐ No	
							☐ Yes ☐ No	☐ Yes ☐ No	
							☐ Yes ☐ No	☐ Yes ☐ No	

Final Review Outcome

Outcome	Selection / Comments
☐ No significant concerns	
☐ Minor observations	
☐ Investigation required	
☐ CAPA required	
☐ AI model/tool requires adjustment	
☐ System/data integrity concern identified	

Required Documentation

- Completed AI Audit Trail Review Checklist
- System information and audit trail review scope
- AI tool configuration, rules, model version, and validation evidence as applicable
- Source audit trail records or controlled links to source records
- AI-generated exception reports, anomaly reports, or dashboards
- Human reviewer assessments and final review outcome
- Deviation, CAPA, data integrity investigation, cybersecurity ticket, or system issue records if applicable
- Change control records for AI tool, model, threshold, data pipeline, or reporting changes
- Periodic review records and management review summaries where applicable
- Training records for users and reviewers performing AI-assisted audit trail review

Approval Table

Role	Name	Department	Signature	Date
Prepared by				
Reviewed by				
Approved by				

Disclaimer

This tool is intended as a practical quality assurance aid and does not replace company procedures, regulatory requirements, or formal validation/compliance review.

Website Integration Block

Website Field	Recommended Content
SEO title	AI Audit Trail Review Checklist for GMP and Pharma QA Teams
Meta description	Download a GMP checklist for AI-assisted audit trail review, data integrity, Part 11, ALCOA+, and human oversight.
Recommended URL slug	/tools/ai-audit-trail-review-checklist
Recommended tags	AI, Audit Trail Review, Data Integrity, 21 CFR Part 11, ALCOA+, CSV, GMP, QA, GxP Systems
Short website excerpt	A practical GMP checklist to help QA, CSV, Data Integrity, and IT Quality teams assess and document AI-assisted audit trail review controls.
Related AIforQA.org article ideas	AI for Batch Record Review by Exception; AI for GMP Document Review; AI for Pharmaceutical Risk Management Under ICH Q9; What Happens When AI Makes a GMP Mistake?
Suggested internal links	/articles/ai-batch-record-review-by-exception; /articles/ai-gmp-document-review-workflows; /articles/ai-pharmaceutical-risk-management-ich-q9; /tools/ai-validation-readiness-assessment; /tools/ai-tool-gmp-risk-assessment-checklist