PRACTICAL DATA-INTEGRITY TOOL

Audit-Trail Review Checklist & Workbook

Define the scope. Find the critical events. Understand the context. Protect the reliability of GMP decisions.

USE THIS WORKBOOK TO

01	02	03	04
Plan a risk-based review	Examine critical data and actions	Investigate exceptions in context	Document conclusions and trends

Prepared by S. BHATTI
Registered Pharmacist / Pharmaceutical Operations Leader

Version 1.0 | September 2026
pharmaopsacademy.com

DECISION GUIDE

From system log to quality evidence

An audit trail is part of the complete electronic record. Review should be risk-based, timely and performed by trained personnel who understand both the system and the underlying GMP activity.

Decision point	If yes	If no / unresolved
Could an event affect a released result or GMP decision?	Review with the record before approval or release.	Escalate before relying on the data.
Is the critical-data lifecycle covered?	Evaluate relevant data, method, access and system trails.	Expand scope and document limitations.
Is the event expected and authorised?	Link it to the approved procedure, change or business reason.	Treat it as an exception requiring impact assessment.
Is the explanation independently supported?	Record rationale and close or trend according to procedure.	Preserve evidence and open or link an investigation.
Does the event recur?	Assess governance, design, access, workload and training causes.	Document evidence supporting isolated treatment.

STOP RULE	Do not clear logs, overwrite configurations, disable accounts, reprocess data or alter the affected record until evidence is preserved and Quality authorises the response, unless immediate security containment is essential.

Suggested review gates

Gate 1: scope and records defined. Gate 2: access and system state confirmed. Gate 3: critical events evaluated in context. Gate 4: exceptions and impact resolved. Gate 5: conclusion, escalation and trends approved.

SECTION 1

System, record and review scope

System / application / instrument / equipment

System version, configuration and audit-trail source

Scope element	Selection / period	Rationale / reference
Product, batch, sample, run or record		
Users and roles		
Date and time range		
Data, method and configuration trails		
Access, privilege and security logs		
Interfaces, transfers and system events		

Critical data and GMP decision supported

Known limitations or unavailable audit-trail functions

Review role	Name / independence	Signature / date
Primary reviewer		
Technical support		
Quality approver		

SECTION 2

Review readiness and system controls

Readiness check	Yes / No / N/A	Evidence / finding
Audit trails enabled for all GMP-critical functions		
Events capture user, time, old value, new value and reason where applicable		
System date, time zone and clock synchronisation controlled		
Reviewer access appropriately restricted		
Filters, exports and reports validated or controlled		
Audit trails protected from untraceable modification		
Accounts unique; generic access prohibited or justified		
Privileges reflect responsibilities and segregation of duties		
Backup, retention and retrieval protect the complete record		

Configuration or access concerns requiring escalation

KEY POINT	A clean event list does not prove control if logging was disabled, incomplete, poorly configured or reviewed through filters that excluded relevant events.

SECTION 3

Critical record-level event review

Event / risk signal	Expected evidence	Finding / reference
Creation or acquisition	Record identity, user, time and sequence are attributable.	
Modification or overwrite	Old/new values, reason, user and approval retained.	
Deletion, invalidation or exclusion	Justification and impact documented.	
Reprocessing or reintegration	Original remains visible; approval requirements met.	
Repeat, abort or failed activity	All attempts retained and evaluated; no testing into compliance.	
Late entry or backdating signal	Chronology, source evidence and impact assessed.	
Electronic signature / approval	Signer, meaning, date and record linkage are secure.	

Records sampled and selection rationale

Record-level exceptions requiring follow-up

SECTION 4

Method, configuration and system events

Event category	Review questions	Finding / reference
Method / recipe / master data	Who changed what, why, when and under which approved change?	
Calculation / integration settings	Could the change alter results, alarms, limits or disposition?	
Configuration / logging settings	Were logging, retention, review or security functions changed?	
Date / time changes	Was chronology affected and was the change authorised?	
System errors / interruptions	Were crashes, interface failures or recovery events assessed?	
Reports and exports	Do reports faithfully represent approved source data and metadata?	
Backup, restore and archive	Are restored or migrated records complete and traceable?	

Change-control, incident, maintenance or validation references

Potential impact on records, batches or validated state

SECTION 5

User access, privilege and security

Control / event	Questions	Finding / evidence
Account lifecycle	Were creation, change, disabling and review timely and authorised?	
Privileged access	Are administrator actions independent, traceable and limited?	
Segregation of duties	Can users create, modify, test and approve the same record?	
Failed / unusual login	Do repeated failures, off-hours access or locations need review?	
Dormant / generic accounts	Are inactive, service, default and shared accounts controlled?	
Privilege changes	Were role elevations approved and later removed?	
Emergency access	Was break-glass access controlled and reviewed?	

User / role	Event and date	Authorisation / explanation	Impact / action

SECTION 6

Critical-event and exception log

Date / user / record	Event and original context	Authorisation / evidence	Impact and decision

Classification	Meaning	Required response
Expected / authorised	Fully supported approved activity.	Reference and close or trend.
Documentation weakness	Legitimate activity may lack adequate evidence.	Correct where permitted; assess systemic gap.
Unexplained critical event	Reason or authorisation unsupported.	Preserve evidence; investigate before relying on data.
Potential integrity breach	Possible deletion, concealment or unauthorised change.	Restrict risk, expand scope and notify Quality.

SECTION 7

Conclusion, escalation and trends

Summary of records, users, periods and event types reviewed

Critical exceptions and impact on data reliability / product decisions

Conclusion	Select	Evidence expectation
Acceptable	[ ]	No unresolved event affects reliability or the GMP decision.
Acceptable with follow-up	[ ]	Data reliable; corrective or monitoring action required.
Investigation required	[ ]	Critical event or limitation remains unexplained.
Data not reliable	[ ]	Record cannot support the intended quality decision.

Escalation and linked deviation / CAPA / change control

Trend signals across users, methods, systems or products

Next review period and risk-based rationale

CLOSEOUT CHECK

Before the review is approved

Confirm	Yes / No / N/A	Reference
Scope covers the critical-data lifecycle and justified period		
System and audit-trail configuration support meaningful review		
Controlled filters did not omit relevant users or events		
Original/changed values, reasons, users and timestamps assessed		
Deleted, invalidated, aborted, failed and repeated activity considered		
Method, configuration, access and administrator events included		
Exceptions assessed against independent source evidence		
Impact covers data reliability, batches, validated state and prior decisions		
Recurring events trended and linked to investigation or CAPA		

Final approval	Name / role	Signature / date
Reviewer		
System / process owner		
Quality Unit		

Primary references

EU GMP Annex 11: Computerised Systems - https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf
FDA: Data Integrity and Compliance With Drug CGMP - https://www.fda.gov/media/119267/download
WHO TRS 1033, Annex 4: Guideline on data integrity - https://www.who.int/publications/m/item/annex-4-trs-1033

EDUCATIONAL USE This workbook does not replace validated system procedures, approved review processes, Quality Unit authority or applicable regulatory requirements.