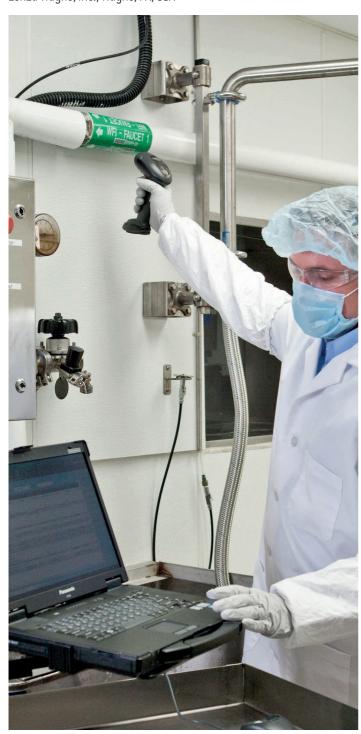# Practical Applications of Data Integrity and Audit Trail Review

Robert Lutskus
Lonza Wayne, Inc., Wayne, PA, USA

Introduction

With the prominent rise of electronic systems used in both laboratory and manufacturing processes, companies have been forced to educate staff and develop procedures on the use and management of these systems. For many years there was little guidance on the expectations from auditors on how to ensure that these systems are in compliance and remain that way. Validation is a core part of this guidance and therefore was a primary focus of the systems. As auditors became familiar with the system use and maintenance, general data integrity (DI) became the regulatory and compliance focus. Today, audit trails are a critical focus of DI, and companies must understand the expectations of the review and management of these audit trails.

Figure 1
Overview of ALCOA+ requirements.

Regulatory guidance

21 CFR Part 11 Subpart B Sec 11.10 Controls for Closed Systems

"Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying."

EudraLex Volume 4 Annex 11: Computerised Systems

"Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed."

PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments

"Where available, audit trail functionalities for electronic-based systems should be configured properly to capture general system events as well as any activities relating to the acquisition, deletion, overwriting of and changes to data for audit purposes. Audit trails should be verified during validation of the system. Companies should implement procedures that outline their policy and processes for the review of audit trails in accordance with risk management principles."

FDA Data Integrity and Compliance with CGMP

"Regarding audits, FDA recommends that audit trails that capture changes to critical data be reviewed with each record and before final approval of the record. Audit trails subject to regular review should include, but are not limited to, the following: the change history of finished product test results, changes to sample run sequences, changes to sample identification, and changes to critical process parameters. FDA recommends routine scheduled audit trail review based on the complexity of the system and its intended use."

MHRA

"An audit trail provides for secure recording of life-cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the "who, what, when and why" of the action. Routine data review should include a documented audit trail review where this is determined by a risk assessment."

Current regulatory requirements

Expectations today for audit trail entries GAMP 5 guidance

Automated – The audit trail entries must be automatically captured by the computer system whenever an electronic record is created, modified or deleted.

Secure – Audit trail data must be stored in a secure manner and must not be editable by any user.

Contemporaneous – Each audit trail entry must be time stamped according to a controlled clock which cannot be altered. The time should either be based on central server time or a local time, so long as it is clear in which time zone the entry was performed.

Traceable – Each audit trail entry must be attributable to the individual responsible for the direct data input. Updates made to data records must not obscure previous values and where required by regulation the reason for changing the data must also be recorded.

Maintained – The audit trail must be retained as long as the electronic record is required to be stored.

Available – The audit trail must be available for agency review and copying.

Identification of the user making the entry – This is needed to ensure traceability. This could be a user's unique ID, however there should be a way of correlating this ID to the person.

Date and time stamp – This is a critical element in documenting a sequence of events and vital to establishing an electronic record's trustworthiness and reliability. It can also be effective deterrent to records falsification.

Link to record – This is needed to ensure traceability. This could be the record's unique ID.

Original value - new value – This is needed in order to be able to have a complete history and to be able to reconstruct the sequence of events.

Reason for change – This is only required if stipulated by the regulations pertaining to the audit trailed record.

System audit trail vs data audit trail

System audit trail – The system audit trail is comprised of settings that are applied to the system or logs that capture activity or communication.

Figure 2
Example of system audit trail.

Data audit trail – The data audit trail is comprised of information that is applied directly to data *i.e.* electronic records/results.

Figure 3
Example of data audit trail.

Selecting a system/remediating a system

The good, the bad and the ugly

Bad – These audit trails are ones that are missing information or ones that utilize files for auditing. Especially if those files are able to be edited (Figure 4).

Ugly – These audit trails have all the necessary information, but it is poorly organized, difficult to search and/or mixed in with logs (Figure 5).

Good – These audit trails give clear visibility into change. Typically, they will clearly identify changes to the user. They will have tools for searching and facilitate a timely review (Figure 6).
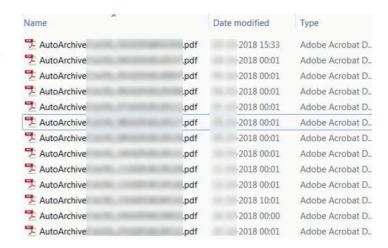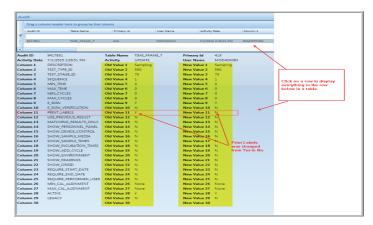

Figure 4
Bad audit trail.
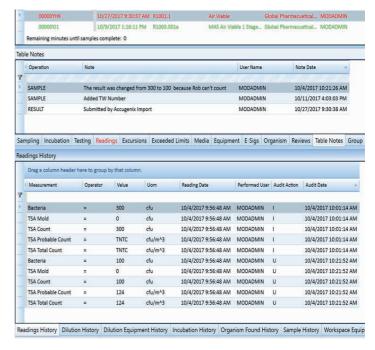

Figure 5
Ugly audit trail.

Figure 6
Good audit trail.

System review and remediation

System review is essential for identifying and remediating critical gaps in your systems. There should be a review of the system capabilities against current audit trail expectations to document any gaps in functionality. Once that review occurs an evaluation of remediation options can be executed. This could include upgrades to existing software, utilizing third party auditing tools or system replacement. System replacement allows a bottom up approach to ensuring the system has adequate audit trail controls in place. This process should start before a system is selected as part of a request for proposal (RFP) process. The finalized user requirements specification (URS) that comes out of the RFP process will allow you to define good audit trail requirements up front. Based on the URS, design documents are created that should clearly identify where the audit trail resides, necessary parameters, usability, viewability, searching and sorting information and most importantly the design controls. These will outline its ability to be turned off and its ability to capture all actions in the system.

Audit trail review

General guidelines dictate that the system must be validated first. Define which data is critical to patient safety and regulatory compliance. Analyze the path of data in the system and the business process, specifically looking at the critical data. Identify areas of high risk to patient safety and compliance. Develop risk-based approach based on criticality of data. Ultimately, the audit trail review is dictated by the type of audit trail. For the system audit trail, it should be reviewed periodically based on risk. The goal is to focus on anything with direct impact to product or release via failure mode and effects analysis (FMEA). This can be very specific for a company because it ensures changes of master data, configuration, interfaced devices/systems, infrastructure or settings. If the system lacks certain controls, making changes requires significantly more verification steps to ensure the change was made appropriately. For the data audit trail, it should be reviewed as part of regular review, prior to batch disposition. It also needs to be an integrated part of the approval process, which is clearly outlined in a procedure.

Audit trail tools

The mechanics of review are based upon a risk assessment that is generated for the system. The goal of the risk assessment is to be quantifiable, objective and actionable. It should take into account the possible measures that can be implemented to reduce the risk to data integrity. The FMEA tool is a common and standard way to assess quality control systems. It is a qualitative and systematic tool, usually created within a spreadsheet, to help practitioners anticipate what might go wrong with a product or process. In addition to identifying how a product or process might fail and the effects of that failure, FMEA also helps find the possible causes of failures and the likelihood of failures being detected before occurrence. It provides a framework to consistently assess the risk to data integrity and perform standardized reassessments as the systems and processes change and evolve.

Based upon the outcome of the assessment, procedures defining the frequency and process for audit trail review should be created. Part of this process should include how the evidence of the audit trail review should be captured. This can include the use of tools external to the system, if the system itself does not have adequate capability to do so. And allows for a clear link between the audit trail and its review. Tools to efficiently identify the required Critical Audit Trail Entries should be developed and validated. These can include: validated Excel spreadsheets, validated access data bases (Scripts), customized reports or other validated software (using a validated interface)

Periodic review

This is the scheduled review of the system audit trail. The frequency is based upon the GAMP category and the criticality of the data in the system. It should confirm traceability or documentation of data in the audit trail, for example, deletions, modifications of GxP critical data items, undocumented configuration changes and system access.

Contact information

North America

Customer Service: +1 800 638 8174 (toll free)
Fax: +1 301 845 8338
order.us@lonza.com
Scientific Support: +1 800 521 0390 (toll free)
scientific.support@lonza.com

Europe

Customer Service: +32 87 321 611
order.europe@lonza.com
Scientific Support: +32 87 321 611
scientific.support.eu@lonza.com

International

Contact your local Lonza distributor

Customer Service: +1 301 898 7025
scientific.support@lonza.com

International Offices

Australia	+61 3 9550 0883
Belgium	+32 87 321 611
Brazil	+55 11 2069 8800
China	+86 6430 3488
France	0800 91 19 81 (toll free)
Germany	0800 182 52 87 (toll free)
India	+91 22 4342 4000
Japan	+81 3 6264 0660
Luxemburg	+32 87 321 611
Singapore	+65 6521 4379
The Netherlands	0800 022 4525 (toll free)
United Kingdom	0808 234 97 88 (toll free)

Lonza Walkersville, Inc. – Walkersville, MD 21793

www.lonza.com/moda