Practical Applications of Data Integrity and Audit Trail Review
Demystifying the Audit Trail
Agenda

- Regulatory requirements
  - ALCOA+
  - Current Guidance
  - What does it look like on paper
  - Is this new?

- Today's Expectations
  - Regulatory Requirements

- Types of Audit Trails
  - Types of audit trails (Data and System)
  - Understand what is in the application audit trail
  - Examples of Good, Bad and Ugly Audit Trails
  - System Selection considerations

- How to Review
  - Critical Audit Trail Data
  - Risk Assessment
  - Periodic Review
  - Documentation
Regulatory Requirements
ALCOA + Refresher

- **Attributable**
  - Data must be recorded so that it can be linked to the unique individual who produced it. Every piece of data entered into the record must be capable of being traced back to the time it was taken and to the individual who entered it.

- **Legible**
  - Data must be traceable, permanent, readable, and understandable by anyone reviewing the record. This is expanded to include any metadata pertaining to the record.

- **Contemporaneous**
  - Data are data that are summarily entered into the record at the time they are generated.

- **Original**
  - Data, or the source data, is the record medium in which the data was first recorded. An original data record should include the first data entered and all successive data entries required to fully detail the scope of the project.

- **Accurate**
  - Data are correct, truthful, complete, valid, and reliable. Controls put in place to assure the accuracy of data should be implemented on a risk-based structure.

- **Complete**
  - Data including any repeat or reanalysis performed on the sample.

- **Consistent**
  - All elements of the analysis such as the sequence of events follow on and are date or time stamped in the expected sequence.

- **Enduring**
  - Not recorded on the back of envelopes, cigarette packets, sticky notes, or the sleeves of a coat but in notebooks or electronic media in the data systems of instruments.

- **Available**
  - Data can be accessed for review and audit or inspection over the lifetime of the record.
Core purpose for the audit trail?
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 documentation 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.”
“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.”
# Regulatory Requirements

## Paper Audit Trail

<table>
<thead>
<tr>
<th>Step</th>
<th>Test description</th>
<th>Actual Result</th>
<th>Tester Sign / Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Record Equipment number and Temperature</td>
<td>Equipment Number: 1MC01, 1NC02</td>
<td>RL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Temperature: 95°F, 35°C</td>
<td>26Feb2019</td>
</tr>
</tbody>
</table>

- 1) Wrong Measurement 26 Feb 2019 RL
- 2) Incorrect Rounding 26 Feb 2019 RL
- 3) Write over 26 Feb 2019 RL
- 4) Incorrect Equipment ID 26 Feb 2019 RL
Regulatory Requirements

- Dated requirements
  - Annex 11 – 2011

- Recent Guidance
  - PIC/S - 2016
  - FDA- 2018
  - MHRA – 2018
Regulatory Requirements

- Systems User Requirements Specification
- Previous Audit Focus
Today’s Expectations
Regulatory Requirements

Expectations today for the Audit Trail – 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.

- **Archived**
  - 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.
Regulatory Requirements
Expectations today for Audit Trail Entries - GAMP 5 Guidance

- 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 reconstruct the sequence of events

- Reason for Change
  - This is only required if stipulated by the regulations pertaining to the audit trailed record.
Types of Audit Trails
Types of Audit Trails

- **System Audit Trail**
  - Applied to system settings or actions
  - Reviewed periodically based on risk

- **Data Audit Trail**
  - Applied to data i.e. electronic records/results
  - Reviewed as part of regular review
Types of Audit Trails

Data Audit Trail

<table>
<thead>
<tr>
<th>Step</th>
<th>Test description</th>
<th>Actual Result</th>
<th>Tester Sign / Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Record Equipment number and Temperature</td>
<td>Equipment Number: Hime + West + Inc02</td>
<td>RL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Temperature: 95 °C 35 °C 35 °C</td>
<td>26 Feb 2019</td>
</tr>
</tbody>
</table>

- Wrong measurement 26 Feb 2019 RL
- Incorrect rounding 26 Feb 2019 RL
- Write over 26 Feb 2019 RL
- Incorrect equipment ID 26 Feb 2019 RL
# Types of Audit Trails

## System Audit Trail

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Process/Function</th>
<th>Event Type</th>
<th>Time</th>
<th>Event Details</th>
<th>SPN No.</th>
<th>User/Role</th>
<th>Comment/Additional Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>17/11/2019</td>
<td>Test production</td>
<td>Test</td>
<td>123456</td>
<td>9:00</td>
<td>New package was added to the system</td>
<td>None</td>
<td>Writer</td>
<td>None</td>
</tr>
<tr>
<td>21/11/2019</td>
<td>Production stop</td>
<td>Production</td>
<td>789012</td>
<td>13:30</td>
<td>Production was stopped due to maintenance</td>
<td>None</td>
<td>Editor</td>
<td>None</td>
</tr>
<tr>
<td>23/11/2019</td>
<td>Change</td>
<td>Package</td>
<td>345678</td>
<td>11:00</td>
<td>Change was made to package details</td>
<td>None</td>
<td>Reader</td>
<td>None</td>
</tr>
</tbody>
</table>

(1) P = production, C = Change, CR = change request, RP = report, ML = maintenance, CA = calendar, OC = other comment

---

Robert Lutskus | Lonza Informatics | 25 June 2019
Audit Trail Examples
Audit Trail Examples

Bad
Audit Trail Examples

Ugly
# Audit Trail Examples

Click on a row to display everything in the row below in a table.

Print Labels was changed from Yes to No.

<table>
<thead>
<tr>
<th>Column</th>
<th>Table Name</th>
<th>Old Value 1</th>
<th>Old Value 2</th>
<th>New Value 1</th>
<th>New Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DESCRIPTION</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>2</td>
<td>TEST_TYPE_ID</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>3</td>
<td>TEST_STAGE_ID</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>4</td>
<td>SEQUENCE</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>5</td>
<td>MIN_TIME</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>6</td>
<td>MAX_TIME</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>7</td>
<td>MIN_CYCLES</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>8</td>
<td>MAX_CYCLES</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>9</td>
<td>E_SIGN</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>10</td>
<td>E_SIGN_VERIFICATION</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>11</td>
<td>PRINTLABELS</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>12</td>
<td>USE_PREVIOUS_RESULT</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>13</td>
<td>MATCHING_RESULTS_ONLY</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>14</td>
<td>SHOW_PERSONNEL_PANEL</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>15</td>
<td>SHOW_DEVICE_CONTROL</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>16</td>
<td>SHOW_SAMPLE_MEDIA</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>17</td>
<td>SHOW_SAMPLE_TIMES</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>18</td>
<td>SHOW_INCUBATION_TIMES</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>19</td>
<td>SHOW_ADD_CYCLE</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>20</td>
<td>SHOW_ENVIRONMENT</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>21</td>
<td>SHOW_READINGS</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>22</td>
<td>SHOW_ORIGID</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>23</td>
<td>REQUIRE_START_DATE</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>24</td>
<td>REQUIRE_END_DATE</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>25</td>
<td>REQUIRE_PERFORMED_USER</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>26</td>
<td>MIN_CAL_ALIGNMENT</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>27</td>
<td>MAX_CAL_ALIGNMENT</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>28</td>
<td>ACTIVE</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>29</td>
<td>LEGACY</td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
<tr>
<td>30</td>
<td></td>
<td>Old Value</td>
<td>Old Value</td>
<td>New Value</td>
<td>New Value</td>
</tr>
</tbody>
</table>
# Audit Trail Examples

## Standards Results

<table>
<thead>
<tr>
<th>Standards</th>
<th>Conc./Dil.</th>
<th>Well</th>
<th>Reaction Time (sec)</th>
<th>Average Reaction Time (sec)</th>
<th>Back Prediction (Linear Regression)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank</td>
<td>Blank</td>
<td>A 5</td>
<td>***</td>
<td>***</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A 6</td>
<td>***</td>
<td>***</td>
<td>***</td>
</tr>
<tr>
<td>Std. 1</td>
<td>0.05</td>
<td>B 5</td>
<td>3236</td>
<td>3258</td>
<td>0.0318</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B 6</td>
<td>3280</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Std. 2</td>
<td>0.5</td>
<td>C 5</td>
<td>1401</td>
<td>1405</td>
<td>1.23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 6</td>
<td>1409</td>
<td></td>
<td></td>
</tr>
<tr>
<td># Std. 3</td>
<td>5</td>
<td>F 5</td>
<td>1138</td>
<td>1130</td>
<td>3.18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>H 8</td>
<td>1122</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reviewed By: ___________________________  Date/Time: ___________________________

(!! = Masked, *** = reaction time > 3300, ????? = atypical, # = Modified, >>>>> = High OD)

(In Notes: ! = Masked Point(s), * = Point(s) Did Not React, ? = Atypical Point(s), # = Modified, > = High OD, <LS = Less than the lowest standard)
Audit Trail Examples

Data Audit Trail
- Audit Trail review as part of sample review
- The system will automatically flag any sample that has had a value changed from an initial save/signature.
- Reviewer doesn’t need to go to the historical “Audit Trail” that is difficult to find information for end users.
- System displays a history of the sample information in a user-friendly, tab based design
- Reviewer can see
  - Initial Entry
  - Who Performed the action
  - When the performed the action
  - Updated Entry
  - Who performed edit/update
  - When the performed the action/update
  - The note associated with the change
Audit Trail Examples

Good
## Audit Trail Examples

### Good

<table>
<thead>
<tr>
<th>EQUIPMENT_TYPE_ID</th>
<th>DESCRIPTION</th>
<th>CREATED_USERNAME</th>
<th>CREATED_DATE</th>
<th>UPDATED_USERNAME</th>
<th>UPDATED_DATE</th>
<th>ACTIVE</th>
<th>LEGACY</th>
<th>AUDIT_ACTION</th>
<th>AUDIT_DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No equipment type</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>2</td>
<td>Incubator</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>3</td>
<td>Samples Refrigerator</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>U</td>
<td>2/3/2019 10:46 PM</td>
</tr>
<tr>
<td>4</td>
<td>Active Air Sampler</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>5</td>
<td>Particle Counter</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>6</td>
<td>Incubator 20-35</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>7</td>
<td>Incubator 20-35</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>8</td>
<td>Incubator 20-25</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>9</td>
<td>Incubator 20-25</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>10</td>
<td>Incubator 20-25</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>11</td>
<td>Incubator 20-35</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
<tr>
<td>12</td>
<td>Incubator 20-35</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>MDADMIN</td>
<td>7/31/2018 10:54 AM</td>
<td>Y</td>
<td>N</td>
<td>I</td>
<td>7/31/2018 10:54 AM</td>
</tr>
</tbody>
</table>

...
Review and Auto Approval

Concentrate on the most important samples

- Review and Approve by Exception
  - Allows reviewer to concentrate on samples with issues instead of the 95-98% that followed the defined, validated process
  - System only approves samples that meet criteria
    - No edits to information
    - No out of specification results
    - No notes from users
    - And many more...

- System Checks
  - Controls sample workflow
  - Enforces incubation/hold times
  - Ensures scheduled samples are taken
  - Ensures media is within expiration and passed qualifying testing
  - Ensures equipment is within calibration
  - Ensures all fields are filled out
  - Ability to have secondary electronic verifier signatures
  - Flags any sample with a change, note or out of specification limit
  - Displays audit trail if any changes occurred
System Selection

Current state vs Future State

- Understand how your current system is capturing data.
- Remediate?
- Replace?

- When selecting new systems:
  - RFP/URS Considerations
  - System Implementation

- Show and Prove!
How to Review
Audit Trail Review

General

- 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 defined data
- Identify areas of high risk to patient safety and compliance
- Develop risk-based approach based on criticality of data
Audit Trail Review

The type of review shall be based on the type of audit trail…

Data Audit Trail

- Reviewed as part of regular review
- Must be reviewed before e.g. a batch is dispositioned.
- Review needs to be done as an integrated part during approval process clearly outlined in a procedure
- MODA enables an easy review within the approval screen as shown before... No additional reports, windows and pain

System Audit Trail

- Applied to system settings or actions
- Reviewed periodically based on risk = focus on anything with direct impact to product or release via FMEA
- Can be very specific for a company because it ensures changes of master data, configuration, interfaced devices/systems, infrastructure or settings.
- Change management is where the pain comes in.
  - If the system lacks certain controls, making changes require significantly more verification steps to ensure the change was made appropriately.
The goal is to create a risk assessment that is:

- Quantifiable
- Objective
- Actionable

Take into account the possible measures that can be implemented to reduce the risk to data integrity.

FMEA is commonly used as a risk assessment for data integrity.

Standard way of assessing all QC systems.

This provides a framework to consistently assess the risk to data integrity and perform standardized reassessments as the systems and processes change and evolve.
Audit Trail Review

Risk Assessment

- Define data integrity failure modes for the different stages

- Where can manual steps compromise the integrity of the data?
  - Define accepted level and not acceptable level
  - Calculate score
  - Define actions for score above acceptable level
  - Recalculate score taking into account actions
  - Repeat until score below acceptable level or risk accepted
Audit Trail Review

What to look at for all types of Audit Trails

- Periodic Review – Scheduled Review of System Audit Trail
  - Deletions
  - Modifications of GxP critical data items
  - Undocumented configuration changes
  - Corrupt entries
  - Anomalies in date and time stamps
  - Changes inconsistent with adjacent data
  - Generic account access recordings (outside of system-required accounts, such as accounts required to run background jobs).
  - Addition of critical authorizations
  - Sequence of samples

- Frequency of Periodic Review
  - Based on GAMP category
  - Criticality of Data
Audit Trail Review

Documentation

- System Tools vs External Tools
- If possible, evidence of audit trial review is made in the computerized system software itself, rather than using a (hybrid) paper record.
- Allows for clearer link between the audit trail and the 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)
Summary
Summary

- **Good Audit Trails:**
  - Captures the information required by regulations
  - Separate data audit trails from system audit trails
  - Saves the audit trails compliantly within the system
  - Allow you to easily review the relevant audit entries

- **“Ugly” Audit Trails:**
  - Captures the information required by regulations
  - Mix data audit trails with system audit trails
  - Require you to have a process for searching the audit trail during review

- **Bad Audit Trails:**
  - Mix data audit trails with system audit trails
  - Saves the audit trails as files outside of the application/database, or
  - Does not fully capture the information required by regulations
- Define a process to evaluate existing systems for audit trail review
- Define a process to review existing system audit trails
- Review relevant data audit trail when approving the data
- Review relevant system audit trail periodically
- Implement the search criteria in your procedures to make the review process easier
- Evaluate the quality of the audit trail when implementing new systems
Any questions?
Thank you