Checklist for implementation and review of Audit Trail

1. **Purpose**



The purpose of this document is to serve as an inspira­ti­onal checklist for implementation of Audit trail review.

As you probably know, the purpose of the Audit Trail review is to identify:

* intentional manipulation of data
* out of compliance production
* bad alignment with the data integrity regulatives

As a benefit we avoid spreading our most valuable and secret data, without our knowledge.

When implementing Audit Trail review in the organi­zation, it is important to understand the process of the audit-trail generation. This includes under­standing which log files fulfil the requirements for being an audit trail. A log file and an audit trail is not the same. For a log file to be valid as an audit trail, the generation and contents must be qualified. Once the relevant data to combine in the audit trail review are identified, it must be identified where (and if) data is available. When the relevant log files, holding the data, are found, qualification of these must be ensured.

It may (if audit trail review is considered adequately early in the process, and yes, it must be considered as early as the basic design and requirement development phases) be required to post additional URS requirements to system vendors. This is to ensure that the individual systems will generate an appropriate and useful audit trail.

Solid “rules” for what to review for, must be defined, for example via a risk based approach. It is relatively easy to find that someone tried to log in 3 times in a row and was rejected every time, if it is well defined what to look for. It is much harder to identify “suspicious behavior” if it is not defined what that may be. “Rules” must be concrete and meaningful. In general, it is more important to know if someone who was known not to be in the building logged-in, than it is to know that someone was denied a login, because the first indicates out of compliance behavior, the second shows that the access control works as intended, or that someone forgot their password.

With qualified data available, the review procedure can be written. Methods (e.g. the main issue about using an automated method, which is cheaper in the long run, or a manual method which is easy and cheap to implement) must be decided.

Things to take into consideration: If the manual method is selected, a thorough training of the reviewers must be performed in order to secure an acceptable compliance. Audit trail reviewing is tedious and requires experienced personnel. However, if the automated approach is selected it will enforce the same compliance level over time regardless of changes in e.g. personnel and organization.

The form in section 3 can be used as a rough checklist for the implementation of audit trail reviews: The form gives some structure and path forward to the considerations and work to be performed, before easy and manageable reviews can be performed.

1. **Use of this check list**

This checklist is the current thinking of Stage One Computing A/S, and is not to be considered as the final and ultimate explanation to all audit trail review challenges. Any system will have significantly more challenges and nuances than this template can possibly cover, so use it wisely with your own data.

The checklist is free to use as you wish, but please send us a kind taught, and feel free to contact us for any questions and/or comments:

Stage One Computing A/S

Lejrvej 17, Kirke Værløse

 DK-3500 Værløse

+45 47382038

info@stageone.dk

Should you consider implementing automated audit trail review, we can also supply you with both consultancy and a technical solution.

1. **Change log**

|  |  |  |
| --- | --- | --- |
| Version | Changes | Date / Init |
| 00f | * Checklist section “Allowable frequency of review” added reference to Dec.2018 FDA Data Integrity Q&A guide.
* Added change log.
 | 2018.12.14 / CXST |

1. **Checklist**

|  | Topic | Results and notes |
| --- | --- | --- |
| 🞏 | Identify which regulatory requirements to fulfil |  |
| 🞏 | Specify requirements for audit trail system to the supplier:* Requirements for (uniform) formats
* Preferred audit trail setup (one or more pr. system)
* Data transfer/export functionality
	+ Manual or automated
	+ Real time/pr. Batch
	+ To other IT systems (formats accepted and interface method)
	+ Data identifier (tag number or similar)
* Print function required
	+ Page X of Y
	+ File name
	+ System identifier
	+ Date and time (incl. time zone)
 |  |
| 🞏 | Identify all audit log files* Manual logbooks
* Log files in equipment (beware, there may be more than one log file pr. System)
	+ Vision systems
	+ Robots
	+ PLC and SCADA systems
	+ Pick and place units
	+ Smart sensors
* Server logs
* Operating system logs in equipment
* Management system logs (LIMS, ERP, MES, SCADA etc.)
* Lab systems logs
* Production system access control system log
* Building and room access log
* HVAC system log
* BMS system log
* Remote access/jump server logs
* Outlook calendar
* Training system
* CR/CC system, CAPA system, deviation system logs
* Data transfer log
 |  |
| 🞏 | Define a list of critical events, e.g. based on a RISK analysisConsider:* Change of critical process parameters
* The process
* Access to premises
* Access to systems
* Internal and external employees
* Guests
* Attempt of unauthorized access
* Disabling of events (e.g. HVAC system event suppression)
* Connection of external devices
* Risk of Virus/malware
 |  |
| 🞏 | Identify in which logs you can find the relevant dataTry to be as specific as possible. E.g.:* Connection of an external storage device can be found in the Windows security log. Entry ID is 6416 ”A new external device was recognized by the system.”
 |  |
| 🞏 | Define review rules. E.g.:* Combine data from building access log with data from windows security log, in order to identify if someone tried to log in, while not being in the building
* Combine data from building access log with data from windows security log, in order to identify if someone tried to log in as administrator, while administrator was not in the building
* Combine data from HVAC SCADA system with batch system in order to identify if a batch was active while an alarm from the HVAC system was suppressed
* Combine data from the Windows security log, in order to identify if an external device was connected to the system, while the administrator was NOT logged on
* Combine data from the training system with data from the machine Windows log, in order to identify if people who are not trained are accessing the machine
* Combine data from the HR system with logins in security log, in order to list who should be deleted from the access to the system
* Combine the GxP disk share access log with the electronic log book data, in order to identify why data was accessed (or changed)
* Combine data from the equipment log with data from the electronic (or manual) logbooks to identify if the WHY is registered for all changes of parameters
* Combine building access log, with electronic log for printed packaging materials, in order to identify if the responsible for the printed packaging materials has left the production room, while printed packaging materials are not locked up, and the cleaning person is present (e.g. during lunch breaks)
 |  |
| 🞏 | Consider maximum allowable frequency of Audit trail review:* Immediately (e.g. if rule indicates a security breech)
* At batch review (e.g. if rule indicates something is affecting batch results)
* In a scheduled review (e.g. periodic review of who was logged in, and who should be deleted from the systems)

**Note** According to the clarifications made by FDA in the “Data Integrity and Compliance with Drug cGMP Q&A guide for industry” dated Dec. 2018, reviews must be conducted according to cGMP regulations, e.g.:* 21 CFR part 211.188 (b), which requires review after each significant step in manufacture, processing, packaging or holding
* 21 CFR Part 211.22, which requires review before batch release

Must be supported by risk assessment, related to:* Criticality of data
* Implemented control mechanisms
* Potential impact on product quality
 |  |
| 🞏 | Consider data availability:* Who can access data
* Are they electronically available via a network
 |  |
| 🞏 | Consider practical aspects:* Who will review audit trail
* Are there adequate and alternative staff resources
* Any additional technical training required
* Is there a (realistic) time consumption estimate for the review process
* Does the execution of review affect batch release
* Should (part of) the process be automated
* Are result review or additional sample test required
* Should the process be validated so that consistent results can be achieved
 |  |
| 🞏 | Establish a procedure for audit trail review. Consider:* Who
* When
* What
* Why
 |  |
| 🞏 | Define spot check method* If the company has CCTV, spot check between data logged via human intervention (where people must actively initiate the registration of a log entry), against the time stamps recorded in the CCTV
* If “Why” is not verified for all loggings where it Is relevant, spot check that registration of “Why” is present for a larger sample of log entries
* Research of what is going on between batches. Inspect during a typical maintenance period, such as Christmas or Easter. Verify that all suppressed events are logged as suppressed, and restored to validated state
 |  |