**Data Integrity Checklist**

**Introduction**

Rx 360 published (Rx-360 Supply Chain Security Checklist for Auditors\_v.2.0) on November 21st, 2011. The purpose of this audit guide was to serve as a tool for assurance of supply chain security and integrity. However the guide was not specified for the identification of Data Integrity. The dedicated checklist for Data Integrity was developed to meet the increasing needs for Asian countries especially India and China.

*The purpose of this audit guide is to serve as a tool for identify the potential data integrity issues. It is not a standard.* This audit guide is a companion tool that can be used in conjunction with the experience and expertise of the auditor. It is **NOT** a checklist and should not be used in that manner. The audit guide is not all inclusive and is meant to be used in addition to standards/guidelines that address GMP/quality assurance topics during audits of facilities supplying materials to the pharmaceutical industry. These materials include excipients, raw materials/basic chemicals, APIs and registered intermediates, packaging, and labeling. The elements of the audit guide should be used where applicable (for example, not all line items in the audit guide are relevant to a given type of supplier).

It is assumed that companies using this audit guide for audit purposes will review the results within the context of the type of facility being audited and apply risk/benefit approaches accordingly. Please note that Comments are required for any “No” responses.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Applicable to: | | | |  |  | Observation |  | COMMENTS (NOTE: comments are mandatory if response if “No”) |
| API | Excipient | BC/RW | PKG/Dist | **A** | **Documentation** |  |  |
|  |  |  |  | **Sr. No** | **Item** | **Yes/Document Number** | **No** |  |
|  |  |  |  |  | **General Part** |  |  |  |
|  |  |  |  | 1. | Entries are legible and clear. |  |  |  |
|  |  |  |  | 2. | Entries are performed on real time basis-no evidence of back dating. |  |  |  |
|  |  |  |  | 3. | Corrections are made so that original entry is not obscured and signed by the doer; corrections are dated and justified adequately. |  |  |  |
|  |  |  |  | 4. | Verify entries made by a single person for the signature (atleast 5). |  |  |  |
|  |  |  |  | 5. | Page numbering is in sequence- no evidence of replacement/missing pages. |  |  |  |
|  |  |  |  |  | **Area Specific Document** |  |  |  |
|  |  |  |  | 6. | Extra copies of pages in the BMR/Analytical Test report are issued and authorized by the Quality Assurance department and the same is reflected on the document as such. |  |  |  |
|  |  |  |  | 7. | Log books (equipments: ware house, manufacturing, quality control/others: environmental monitoring, equipment usage & equipment maintenance) are up to date, recorded on time basis and with entries corresponding to the actual actions. |  |  |  |
|  |  |  |  | 8. | The printout of the weighing balance is available for all the tests, involving weighing, conducted which directly or indirectly results into in-process material/batch release. |  |  |  |
|  |  |  |  | 9. | All the chromatograms are available along with the Analytical Report |  |  |  |
|  |  |  |  | 10. | The injection sequence timing is in line with standard/sample weighing and injection time? |  |  |  |
|  |  |  |  | 11. | Verify Soft data against hard data for any change in data, unreported data or repeat testing. |  |  |  |
|  |  |  |  |  | **Microbiology Laboratory** |  |  |  |
|  |  |  |  | 12. | Verify media preparation and reconciliation and destruction record. |  |  |  |
|  |  |  |  | 13. | Verify Incubation record, Autoclave logs and ensure if it is as per validated loads and media preparation. |  |  |  |
|  |  |  |  | 14. | Compare Procedures against actual practices with reference to testing, sample handling, recording of results. |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Applicable to: | | | |  |  | **Observation** |  | COMMENTS (NOTE: comments are mandatory if response if “No”) |
| API | Excipient | BC/RW | PKG/Dist | **B.** | **Computer System** |  |  |
|  |  |  |  | **Sr. No.** | **Item** | **Yes/Document Number** | **No** | **Remark** |
|  |  |  |  |  | **General** |  |  |  |
|  |  |  |  | 1. | PLCs used in the manufacturing, testing or maintaining the critical process parameter are protected for password for individual users |  |  |  |
|  |  |  |  | 2. | PLC has adequate control to prevent changes in process parameters eg: The display shows the parameters as per specification but actual processing time has been changed in the PLC. |  |  |  |
|  |  |  |  | 3. | Individual balances (used in product testing and release making decision):   1. Have print out facility 2. The print out captures:    1. Balance id    2. Date & Time |  |  |  |
|  |  |  |  | 4. | Site has a defined policy for user rights:   1. Analyst 2. Reviewer 3. Administrator 4. Guest |  |  |  |
|  |  |  |  | 5. | Is there a pre-defined procedure for protection of data during the maintenance (Service Engineer have administrator rights)? |  |  |  |
|  |  |  |  |  | **Instrumentation** |  |  |  |
|  |  |  |  | 6. | The computer system is password protected; all the personnel have dedicated windows log in and software log in user name & password? |  |  |  |
|  |  |  |  | 7. | The computer system have adequate measures to prevent the following:   1. Change of date & time 2. Cut, Copy, Paste, Rename & delete option (disabled through mouse and keyboard) |  |  |  |
|  |  |  |  | 8. | Check Recycle bins for any files & folders related to analytical data |  |  |  |
|  |  |  |  | 9. | Audit Trail:  Is enabled for all instruments having associated computer system?  If not, paper based audit trail are maintained? |  |  |  |
|  |  |  |  | 10. | Audit Trail review:   1. System Audit trail is reviewed at a specified interval 2. Individual test audit trail is reviewed and is a part of analytical report 3. Verify Audit trail for one of the tests; audit trail should capture the actual reason for change or edit |  |  |  |
|  |  |  |  | 10. | Verify that adequate procedures are in place for System Suitability & Sample Analysis Check: |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Applicable to: | | | |  |  | **Observation** |  | COMMENTS (NOTE: comments are mandatory if response if “No”) |
| API | Excipient | BC/RW | PKG/Dist | **B.** | **Computer System** |  |  |
|  |  |  |  | **Sr. No.** | **Item** | **Yes/Document Number** | **No** | **Remark** |
|  |  |  |  |  | **GENERAL** |  |  |  |
|  |  |  |  | 1. | Is the computer validated for its intended use?   * You are looking for a set of requirements that define the following:   + What functions do the systems performs – including alarm and error conditions   + Security – What types of roles are in the system and what do the roles have access to   + What are the critical data fields and records   + How is the data backup |  |  |  |
|  |  |  |  |  | **What functions does**  **the computer perform** |  |  |  |
|  |  |  |  |  | * Audit Trail:   Is enabled for all instruments having associated computer system?  If not, paper based audit trail are maintained? |  |  |  |
|  |  |  |  |  | * Audit Trail review:   + System Audit trail is reviewed at a specified interval * Individual test audit trail is reviewed and is a part of analytical report   + Verify Audit trail for one of the tests; audit trail should capture the actual reason for change or edit or deletion and date/time stamp of the event |  |  |  |
|  |  |  |  |  | * The computer system has adequate measures to prevent the following:   + Change of date & time   + Cut, Copy, Paste, Rename & delete option (disabled through mouse and keyboard)   + Inactivity time out |  |  |  |
|  |  |  |  |  | * Verify the date/time on the computer is correct |  |  |  |
|  |  |  |  |  | **SECURITY** |  |  |  |
|  |  |  |  |  | * For Instruments - The computer system is password protected; all the personnel have dedicated windows log in and software log in user name & password? |  |  |  |
|  |  |  |  |  | * PLCs- used in the manufacturing, testing or maintaining the system - Are there unique individual user accounts and each for individual user |  |  |  |
|  |  |  |  |  | * Are critical process parameter changes performed by someone other than user and/or supervisors |  |  |  |
|  |  |  |  |  | * Do sops exist on the approval and removal of roles/users |  |  |  |
|  |  |  |  |  | * Are access reviews periodically performed and documented |  |  |  |
|  |  |  |  |  | * Is there a pre-defined procedure for protection of data during the maintenance (Service Engineer have administrator rights)? |  |  |  |
|  |  |  |  |  | **What are the critical data fields and records** |  |  |  |
|  |  |  |  |  | * Are the critical data fields defined in the requirements document * How are changes to these data fields done? By who and are audit trails reviewed for the changes |  |  |  |
|  |  |  |  |  | * PLC has adequate control to prevent changes in process parameters eg: The display shows the parameters as per specification but actual processing time has been changed in the PLC |  |  |  |
|  |  |  |  |  | * Individual balances (used in product testing and release making decision):   + Have print out facility   + The print out captures:   + Balance id   + Date & Time |  |  |  |
|  |  |  |  |  | **How is the data backed up** |  |  |  |
|  |  |  |  |  | * Do SOPs exist on how data is backed up that incudes how often and what happens if a failed back up occurs |  |  |  |
|  |  |  |  |  | * Has the back up of data been tested? What files are backed up? Does it include the meta data |  |  |  |
|  |  |  |  |  | * Has a restore of the backup been verified and how often does this happen. Is it defined in an SOP |  |  |  |
|  |  |  |  |  | * Check Recycle bins for any files & folders related to analytical data |  |  |  |

NOTES:

* When looking at security features ensure that the critical parameter changes are not performed by the person who approves or owns the data.
* When approving the data does the supervisor review the audit trail
* Control for accounts that can change critical parameters
* Password expiration required
* Account management required
* Maintain a list of users with access to the password
* Logout functionality (automatic Logoff or SOP enforcement)
* There are two different types of audit trials that need to be considered:

1. System Configuration Audit Trail
   * Tracks actions of System Administrator
   * Tracks changes to “rules” for operating the system
   * These types of audit trails should be reviewed as part of the system periodic review process.
2. Data Audit Trail
   * Tracks actions of Users, Reviewers, Approvers
   * Tracks changes to data
   * These types of data audit trail shall be reviewed every time the data is being reviewed. Review needs to include data + meaningful metadata