IPA

Innovation, Quality and Global Reach

Data Reliability Guideline

IPA
Innovation, Quality and Global Reach

Data Reliability Guideline

February 2017

Published by:
Indian Pharmaceutical Alliance
A-205 Sangam
14B S V Road, Santacruz (W)
Mumbai 400 054
India
E-mail: dgshah@vision-india.com

February 2017

Printed by:
Spenta Multimedia Pvt Ltd
Peninsula Spenta, Mathuradas Mill Compound
N. M. Joshi Marg, Mumbai 400 013

Contents

1. Preface

The IPA launched its Quality Forum (QF) in April 2015 to help Indian pharmaceutical manufacturers to achieve parity with global benchmarks in quality. The industry made a commitment to a multi-year journey to address key issues facing the industry and develop best practices. McKinsey & Co. joined this journey as a knowledge partner.

The QF focused on three priority areas. The first among them was to develop a comprehensive set of Data Reliability Guidelines. It took upon itself the challenge of establishing robust and seamless data management and documentation systems and processes. This initiative found great support from the US FDA, the UK MHRA and the EU EMA. The IPA wishes to acknowledge their contributions and commitment.

The IPA also wishes to acknowledge the CEOs of six member-companies who have committed their personal time, human resources and provided funding for this initiative.

This Guideline is the outcome of a concerted effort over the last 15 months by senior managers engaged in manufacturing, quality and regulatory functions of six IPA member-companies. They shared current practices, benchmarked these with the existing regulatory guidance's from the US FDA and other regulatory bodies such as UK MHRA, WHO, etc., developed a robust draft document and got it vetted by leading subject matter experts and regulatory agencies. The IPA acknowledges their hard work and commitment to quality.

This document, to be released at the IPA's 2nd Annual Conference 2017 in Mumbai, will be hosted on the IPA website www.ipa-india.org to make it accessible to all manufacturers in India and abroad.

2. Introduction and Background

- Managing data in pharmaceutical industry is challenging, especially when firms are experiencing growth of data volume at an exponential rate. While the industry realizes the magnitude and criticality of these issues, addressing them in time remains a challenge

- Suspicious data quality can result in severe consequences for the organization and ultimately jeopardize the reputation of the organization. All data generated requires close observation and immediate intervention in case of any anomaly. It is imperative that proper checks are put in place to avoid proliferation of bad data in the systems

- Implementing controls and maintaining data without first understanding the regulations and business processes can result in data of questionable authenticity, and may lead to regulatory, civil, or criminal action. Ensuring integrity of critical data and metadata is necessary

- Ensuring data reliability is not only a CGMP requirement; it is also a key enabler of effective management decision-making. Over a period of time, firms with reliable data systems are likely to benefit from informed decision-making based on greater transparency and accurate data from the shop-floor

- Data reliability is fundamental in a pharmaceutica l quality system (PQS) which ensures that medicines taken by consumers are of the required quality. Data reliability requirements apply equally to manual and electronic data

- Data reliability applies across the **data lifecycle,** that is

  — Collection of data (including raw data)

  — Processing and computation of data

  — Reporting of data

  — Retention of data, and

  — Archival/retrieval and authorized destruction

Data reliability is considered to be vital, since data should be complete as well as being accurate, legible, contemporaneous, original and attributable, commonly referred to as "ALCOA" ++ where '+' stands for 'Complete, Consistent, Enduring and Available.' A more detailed explanation is given later in this Guideline.

3. Scope

- This Guideline will be applicable to all functions and departments across an organization where GXP activities generate data through systems and processes, i.e.,
  - Manufacturing of finished drug products and drug substance for clinical trials, bioequivalence studies, and commercial distributions
  - Laboratories that develop methods or formulations intended to support a new drug application or laboratories that analyze samples generated from clinical trials
  - Contract manufacturing organizations
  - Contract research organizations
  - Contract testing laboratories
  - Pharmacovigilance
  - Contractors who provide GMP activities which could affect the quality of the drug reaching the patient
- It is applicable to data that is generated and stored by manual (paper–based), electronic, or hybrid systems. The practices within this document are intended to be incorporated into organizational data reliability standards and procedures in order to
  - Support the requirements set forth in the quality manual and standards
  - Define organizational CGXP data reliability requirements
  - Provide organizational data reliability expectations to be incorporated into internal audits, quality audits of suppliers, contract manufacturers, contract laboratories, self-inspections and risk reviews

4. Purpose

- The purpose of this Guideline is to
  - Describe the requirements of maintaining complete, accurate, truthful and verifiable data in all CGXP documents that are needed to be maintained as per regulatory requirements and various governmental regulations, laws, rules and statutes applicable to an organization in this matter
  - Describe the importance of data generation, maintaining data lifecycle, data governance and data reliability throughout manufacturing sites of an organization including contactors and service providers
  - Emphasize the paramount importance of ethics, agreements, and understand the regulatory implications of data falsification and fraud
- This Guideline will outline a holistic approach, with different elements necessary to help ensure the reliability of data throughout the product lifecycle. The key elements considered for overall data reliability guidelines are
  - Culture
  - Awareness and capability
  - Process design
  - Data reliability risk detection and mitigation
  - Technology and IT systems
  - Governance
- This Data Reliability Guideline focuses on ensuring quality, safety and efficacy – three attributes that are inseparable for all medicines manufactured

5. Definitions

- **Archiving:** Archiving is the process of protecting records from the possibility of further alteration or deletion, and storing these records under the control of dedicated data management personnel throughout the required records retention period

- **Audit Trail:** An audit trail is a process that captures details such as additions, deletions, or alterations of information in a record, either paper or electronic, without obscuring or over-writing the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its media, including the "who, what, when and why" of the action

- **Backup:** Backup refers to a true copy of the original data that is maintained securely throughout the records retention period. For example, the backup file shall contain data (including associated metadata) and shall be in the original format or in a format compatible with the original format and shall be maintained for the purpose of disaster recovery. The backup and recovery processes must be validated

- **Breach of Data Integrity (BDI):** It is a violation of the integrity of data. This means that the actions performed and the documents/records written do not reflect the truth and the reality which has taken place. Breaches of integrity can be observed during manufacturing and testing, inspection and post inspection

- **Computerized System:** Computerized System collectively controls the performance of one or more automated business processes. It includes computer hardware, software, peripheral devices, networks, personnel and documentation, e.g. manuals and standard operating procedures

- **Data:** Data means all original and master records and certified true copies of original records, including source data and metadata and all subsequent transformations and reports of this data, which are recorded at the time of the GXP activity, and allow full and complete reconstruction and evaluation of the GXP activity

- **Data Governance:** This refers to the sum total of arrangements which ensure that data, irrespective of the format in which it is generated, are recorded, processed, retained and used in order that a complete, consistent and accurate record throughout the data lifecycle is maintained

- **Data Integrity Assurance:** Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices. Data Integrity requires adherence to the criteria of ALCOA+ as mentioned earlier in this Guideline. The specific definitions are as below

Criterion	Meaning
Attributable	'Attributable' means information is captured in the record so that it is uniquely identified as executed by the originator of the data (e.g. a person, and/or a computer system).
Legible	The terms 'legible', 'traceable' and 'permanent' refer to the requirements that data are readable, understandable and allow a clear picture of the sequencing of steps or events in the record.
Contemporaneous	'Contemporaneous' is the process of documentation (on paper or electronically) at the time of the occurrence of an activity.
Original	'Original' data includes the first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GXP activity.
Accurate	'Accurate' means that data are correct, truthful, valid and reliable.
Complete	'Complete' means that all data from an analysis, including any data generated before a problem is observed, data generated after repeating part or all of the work, or re-analysis performed on the sample are contained the data record. For hybrid systems, the paper output must be linked to the underlying electronic records used to produce it.
Consistent	'Consistent' means that all elements of the analysis, such as the sequence of events, follow on and data files are date (all processes) and time (when using a hybrid or electronic systems) stamped in the expected order are contained in the record.
Enduring	'Enduring' means that all data have been recorded on authorized media which can be preserved for a period of time, e.g. laboratory notebooks, numbered worksheets, for which there is accountability, or electronic media. Data recorded on scrap paper or any other media which can be discarded later, e.g. backs of envelopes, laboratory coat sleeves or Post-It notes, etc. are not considered enduring.
Available	'Available' means that the complete collection of records can be accessed or retrieved for review and audit or inspection over the lifetime of the record.

- **Data Lifecycle:** This refers to a planned approach to assessing and managing risks to data in a manner commensurate with the potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the process by which data is created, processed, reviewed, analyzed, reported, transferred, stored and retrieved, and continuously monitored until retired

- **Data Owner:** An individual or a team who is responsible for data generation and storage

- **Data Reliability (DR):** Data Reliability is the degree to which a collection of data is complete, consistent and accurate throughout its data lifecycle. The collected data should be attributable, legible, contemporaneously recorded, accurate and should be an original or a true copy

- **Data Reliability Auditors (DRAs):** Data Reliability Auditors are independent auditors who report to the Corporate Quality (Data Reliability Cell-Head). The responsibility of these auditors is to conduct an independent reliability audit in order to confirm adherence to established requirements for data reliability in all the quality related processes

- **Data Reliability Governance:** It refers to all processes of governing by the Data Reliability Task Force through laws, norms, power or language

- **Data Reliability Task Force:** A 'Task Force' is a body which governs data reliability globally at all sites

- **Dynamic Record:** This refers to records in dynamic format, such as electronic records, that allows for an interactive relationship between the user and the record content. For example, electronic records in database formats allow the ability to track, trend and query data; chromatography records, maintained as electronic records, allow the user to reprocess the data, view hidden fields with proper access permissions, and expand the baseline to view the integration more clearly. Examples of dynamic data in quality control are chromatogram, spectrum, LIMS data, PLC and SCADA based data like -autoclave printouts, stability chamber monitoring records, KF titrator data, etc. Examples of dynamic data in ware houses would include SAP data base. In manufacturing, dynamic data would include BMS-Temperature and RH print outs, etc.

- **Electronic Data:** This includes data from ERP software used for controlling quality systems, laboratory electronic data and records, etc.

- **Ethics:** Ethics (also moral philosophy) is the branch of philosophy that involves systematizing, defending, and recommending concepts of right and wrong conduct

- **Exception Report:** This refers to a validated search tool that identifies and documents predetermined 'abnormal' data or actions, which require further attention or investigation by the data reviewer

- **GXP:** An acronym for the group of good practice guides governing the preclinical, clinical manufacturing and post-market activities for regulated pharmaceuticals, biologics, medical devices, such as GLP (good laboratory practices), GCP (good clinical practices), GMP (good manufacturing practices) and GDP (good documentation/distribution practices)

- **Hybrid System:** A Hybrid System is defined as an environment consisting of both electronic and paper-based records (frequently characterized by handwritten signatures executed on paper). A very common example of such a system is one in which the system user generates an electronic record using a computer-based system (e-batch records, analytical instruments, etc.) and then is required to sign that record as per the Predicate Rules (GLP, GMP, GCP, etc.). However, the system does not have an electronic signature option, so the user has to print out the report and sign the paper copy. Now, he/she has an electronic record and a paper/handwritten signature. The system has an electronic and a paper component, hence the term 'Hybrid System'

- **Metadata:** Metadata is the data that describes the attributes of other data, and provides context and meaning. Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data. It also permits data to be attributable to an individual. Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data. (For example, the number "23" is meaningless without metadata, such as an indication of the unit "mg."). Data should be maintained throughout the record's retention period with all associated metadata required to reconstruct the CGMP activity. The relationships between data and their metadata should be preserved in a secure and traceable manner. Among other things, metadata for a particular piece of data could include a date/time stamp for when the data was acquired, a user ID of the person who conducted the test or analysis that generated the data, the instrument ID used to acquire the data, audit trails, etc

- **Paper-based Data:** This includes recording formats (such as worksheets and logbooks), batch records, master records, green sheets, apex, but are not limited to documents alone

- **Quality Risk Management (QRM):** This refers to a systematic process for the assessment, control, communication and review of risks to the quality of the drug (medicinal) product across the product lifecycle (ICH Q9)

- **Raw Data:** This refers to original records and documentation, retained in the format in which they were originally generated (i.e. paper or electronic), or as 'true copies'. Raw data must be contemporaneously and accurately recorded by permanent means. In the case of basic electronic equipment which does not store electronic data, or provides only a printed data output (e.g. balance or pH meter or chart recorder), the printout constitutes the raw data

- **Senior Management:** This refers to the person(s) who direct and control a company or site at the highest levels with the authority and responsibility to mobilize resources within the company or site (ICH Q10 based in part on ISO 9000:2015)

- **Static Record:** A static record format, such as a paper or PDF record, is one that is fixed and allows no or very limited interaction between the user and the record content. For example, once they are printed or converted into static PDF files, chromatography records lose the capabilities of being reprocessed or enabling more detailed viewing of baselines or viewing of hidden fields. Examples of static data in quality control include pH melting point results reported in worksheets, or in paper logbooks; in warehouses, material de-dusting records, goods receipt notes, container physical verification records; in manufacturing, paper-based BMR in which complete activity of batch manufacturing is recorded, cleaning records of equipment's and instruments, etc.

- **Subject Matter Experts (SMEs):** A subject-matter expert (SME) or domain expert is a person who is an authority in a particular area or topic

- **True Copy:** A true copy is a copy of an original recording of data that has been certified to confirm it is an exact and complete copy that preserves the entire content and meaning of the original record, including in the case of electronic data, all metadata and the original record format as appropriate

- **Wrongful Act:** Wrongful act means employee conduct that raises significant questions regarding data reliability involving fraud, falsification and untrue statements, misconduct, wrongdoing or other acts that subvert the integrity of data for a regulated product that is required to be maintained in accordance with company policies, standards of procedures, or in accordance with applicable laws, regulations or legislative directive of regulatory authority or authorities

6. Responsibilities

- Management is responsible for
  - Ensuring that this Guideline is implemented across the entire organization in order to ensure that a robust and sustainable data management system and governance is in place
  - Establishing and maintaining organization-wide commitment to data reliability as an essential element of the quality system
  - Ensuring that personnel are not subject to commercial, financial and other pressures or conflicts of interest that may adversely affect data reliability
  - Making staff aware of the relevance of data reliability and its importance
  - Creating a work environment in which staff is encouraged to communicate failures and mistakes related to data reliability so that corrective action can be taken
  - Building systems and controls which prevent employees from altering or falsifying data
  - Creating channel(s) for employees to report any breaches in data reliability to senior management
  - Ensuring adequate information flow between staff at all levels
  - Discouraging any management practices that might be expected to inhibit the active and complete reporting of data reliability related issues
  - Reviewing quality matrix related to data reliability and key performance indicators of the quality management system
  - Encouraging employees to take an open-door approach and to take appropriate actions as per open-door privileges for employees
  - Taking appropriate disciplinary actions on employees for unethical conduct for data reliability.
  - Site Management shall be responsible for identifying SMEs for each function
  - Understanding resource constraints that may lead to breach in data reliability and/or integrity and for communicating to staff that such resource constraints should never lead to breach in data integrity
- Subject Matter Experts (SMEs) are responsible for
  - Performing data process lifecycle mapping, gap assessment, risk identification and mitigation.
  - Developing data reliability checklists and review processes.
  - Designing and updating training materials and imparting trainings as required.
- Data Reliability Compliance Head is responsible for
  - Maintaining overall data governance functionality

  - Notifying to Global Quality Head and Senior Management about incidence and discrepancies raised during data reliability inspections by Data Reliability Auditors
  - Identifying root cause for data reliability issues in association with site management and SMEs and providing corrective and preventive action according to regulatory inspections
  - Providing guidance to the respective SMEs for identifying risk associated with data reliability and proposing suitable corrective and preventive action and monitoring implementation and effectiveness
  - Providing inputs in overall improvement in quality metrics

- Data Reliability Auditors are responsible for
  - Performing scheduled and unscheduled data reliability assessments (DRAs) and inspections at sites as per authorized data reliability checklists with the help of trained data reliability auditors
  - Ensuring compliance related to the discrepancies identified during the inspection

- All Employees are responsible for
  - Following this Guideline. Responsibilities related to data reliability will be communicated to each level of employee through a code of conduct document as mentioned in Annexure 1 and each employee will acknowledge the same

7. Culture

- Culture is the foundation for a strong data reliability mindset. Data reliability culture can be improved through training, communication and change management. Common understanding, awareness of impact, ownership and leadership support is required for developing a culture

- This will aid in creating an environment needed to facilitate every individual in guiding his/her own behavior to

  — Work in the interest of the organization

  — Manufacture quality drugs for the patients, and

  — Improve these behavioral aspects continually

- This section focuses on developing a data reliability mindset, a mandate for each level of the employee, developing best practices and the required actions to be taken in case breaches in data integrity are discovered

- Employee responsibilities related to data reliability will be communicated to each level of employee as a code of conduct and every concerned employee will acknowledge the same

- Employees have a duty to engage in appropriate conduct to ensure that all stake holders can trust employee decisions that are based on data and information which are accurate, thoughtful and complete. **(Refer to Annexure 1: "Code of conduct for Data Reliability")**

- A culture of compliance is born out of this foundation and it shapes the decisions and actions taken by the employees of an organization. Hence, an organization should have a corporate policy on Ethical Quality Conduct. Each employee should also take the pledge for ethical quality conduct as a commitment to quality (Refer to Annexure 2: "Ethical Quality Conduct")

- Analysis of employees

  — HR will analyze employees on appropriate factors for behavioral aspects related to data reliability during the hiring process and will continue to carry this out throughout the employee's career in the organization

  — HR will use benchmark practices and deploy scientific and objective methodology in the selection process of employees to ensure a greater sense of fairness and transparency in this process. The organization will examine employees' past behavioral records by data mining and will analyze employees' intentions and attitudes towards data integrity. Based on these intentions and attitudes, in combination with perceived behavioral controls, the organization will predict future behaviors of employees and utilize these predictions in job assignment and human resource decisions

  — The organization will also monitor and analyze changes in behavior and attitudes of existing employees based on these parameters and utilize the findings in job assignment and human resource decisions

- The key behavioral aspects for the absence of reliable data could be the following

  — **Institutional bad habits:** Leadership fails to demonstrate the appropriate behavior. An example of a performance measure that drives wrong behavior is a focus on short-term gains

  - **Management using 'Rule by Fear' method with employees (for example, 'you do what you are told').** This leads to a culture of fear and blame and an inability of employees to challenge the status-quo

  - **Poor education:** This could lead to bad decisions or inappropriate behavior based on knowing 'How' but not 'Why'

  - **Poor attitude toward problems:** This could lead to a 'victim' mindset rather than a learning mindset, in that problems are seen as "bad" rather than "opportunities to improve"

  - **Complex systems and systems with inappropriate design:** These can encourage and, at times, even force bad practices

  - **A hierarchy which does not enable employees:** A constructive, enabling hierarchy is needed to provide employees with the knowledge and confidence to make the correct decisions

  - **Panic, stress and fatigue:** This can lead to negative behavior like fight, flight or freeze

  - **Lack of personnel integrity and honesty:** These are exemplified by attitudes of "don't care" and "I won't get caught". Such attitudes are displayed by employees with very little pride in what they do

- These key behaviors are indicators or triggers for BDI, and should be assessed by the organization throughout the hiring process as well as employee engagement and employment during his or her career in the organization

- **Open-door to Management:** An employee should be encouraged to take advantage of an open-door route to organization top management when it comes to raising compliance issues and discussing potential compliance concerns pertaining to data reliability

- **Whistleblower policy:** In order to create enduring value for all stakeholders and ensure the highest level of honesty, integrity and ethical behavior in all its operations, the Company should formulate a **Whistleblower Policy** in addition to the existing Code of Conduct that governs the actions of the employees

  - This whistleblower policy shall aspire to encourage all employees to report suspected or actual occurrence(s) of illegal, unethical or inappropriate events (behaviors or practices) that affect the Company's interest and image due to data reliability issues

  - Management shall be available to respond to questions and concerns if an employee does not feel comfortable talking with his/her supervisor; they also may directly contact the Senior Management of the company through a helpline for concerns related to data reliability. Reporting to the helpline may be made anonymously. Management shall take appropriate action as required upon receiving the information through the helpline. The helpline number will be easily accessible to each employee

- **Reporting of data integrity failures to regulatory bodies**

  - When issues relating to data validity and reliability are discovered, it is important that their potential impact on patient safety and product quality, and on the reliability of the information used for decision-making and applications are examined as matters of top priority

  - Respective health authorities shall be notified if the investigation identifies material impact on patients, products, reported information or on application dossiers

  - Individuals who observe data integrity issues can also report suspected issues of this nature that may affect the safety, identity, strength, quality, or purity of drug products to respective drug regulatory authorities or combination of regulatory agencies and the words "CGMP data integrity" shall be included in the subject line

  - For product marketed in India, CDSCO/DCGI shall be notified for any failures and breaches observed in data integrity

  - For USFDA, where it is the reporting authority for such matters, notifications should be sent to Druginfo@fda.hhs.gov

  - For Europe and other agencies, the respective qualified person will be notified for further communication with agencies

- **Disciplinary actions:** Disciplinary action shall be taken against employees who are found to be responsible for unethical conduct related to data reliability requirements

  - Impact on quality due to the unethical conduct of the employee shall be assessed through the applicable quality management system procedure at the site. However, as a part of corrective action, employee will be warned and prevented from performing GXP activities

  - The organization shall formulate and publish clear disciplinary practices to address situations where an employee is found engaged in illegal or unethical conduct related to data reliability. While misconduct is evaluated on a case-by-case basis, the organization will take corrective actions in a consistent manner so as to ensure that such action is appropriate under the circumstances and has the intended deterrent effect. Penalties for compliance violation may include termination of the employee at the sole discretion of the organization

  - The organization shall take every possible measure to prevent and correct issues that can lead to breaches in data reliability. While evaluating data reliability issues, the organization will look into the root cause of the systemic dysfunction rather than individual misconduct. During inspection by regulatory authorities and in the course of internal review, if a breach in data reliability is discovered, and/or misconduct is observed, then the concerned individual shall be removed from performing GXP operations

- **Town Hall Meeting:**

  - The Management shall proactively create global awareness at all the manufacturing sites about importance of data, through actions such as conducting town hall meetings. Such meetings shall be conducted when a serious situation arises and Management wants to convey a message on the organization's stand on data reliability

  - Subject matters of communication during town hall meetings shall be such as mentioned below, but need not be limited to these

    - The organization is committed to "doing the right thing when even no one is watching."

    - The behavior of employees must reflect their commitment to work in the interest of the organization and manufacture quality drugs for patients and to continually improve the ability of the organization to do so

    - Data reliability is important because it ensures the safety, efficacy and assurance of the quality of the drugs that consumers will use, and also because it helps to strengthen the trust that regulatory bodies place on the organization

    - Non-reliable data lead to recalls, warning letters, importing alerts, injunctions and/or seizures, as well as decrees from regulatory bodies

    - Intentional acts by employees that do not support data reliability are subject to disciplinary actions

- The organization shall recognize and reward employees for their contributions towards creating and developing a sustained data reliability culture. The evaluation criteria for reward and recognition should be

    - Consistent adherence to data reliability guidelines

    - No cases of breaches in data integrity in a particular month

    - Efficient and effective efforts of the employee related to the execution of DR guideline

8. Awareness and Capabilities

- Data reliability might be compromised if employees are not aware of the requirements related to data reliability for GMP activities and/or Quality-related processes that are performed by them. The individual's capabilities will be improved through training and awareness

- The organizational management at all levels will ensure that personnel under their responsibility, including contractors and consultants, have the appropriate qualification, experience and training required in assuring data reliability awareness

- Employees will be made aware of the specific requirements related to data reliability for the activities to be performed by them; they will also be trained to maintain current awareness of applicable laws, regulations and legislative directives that pertain to documentation and record keeping. Such trainings will be imparted on a regular basis through mandatory and refresher training, based on his/her job profile, i.e. Operator, Supervisor, or Manager

- Available GMP trend/regulatory landscape, for example, Monitoring Warning Letters, 483's, WHO-NOC, Health Canada Inspection Tracker, EUDRAGMP website, etc. across the industry and applicable regulatory guidelines will be taken into consideration for updating the training related documentation on a regular basis

- The organization shall build the requirement for data integrity into Quality Agreements with contractors, and create awareness among staff so they can assist with this endeavor, and report concerns proactively. Quality agreements shall be in place between manufacturers and suppliers and contract manufacturing organizations (CMOs) with specific provisions for ensuring data integrity across the supply chain. This may be achieved by setting out expectations for data governance, and transparent error/deviation reporting by the contract acceptor to the contract giver. There shall also be a requirement to notify the contract giver of any data integrity failures identified at the contract acceptor site

- The employee-to-supervisor feedback process, related to data reliability, shall be taken as an opportunity to impart and improve training and awareness modules. Such training would be in the form of quizzes in order to assess the effectiveness of the training

- The company shall establish and maintain an employee Learning Management System which will include the fundamental training requirements pertaining to documentation of GXP activities, including concepts and principles of data reliability, and how employees are to report suspected data reliability issues to company management

- Following aspects shall be covered in data reliability training, but the topics need not be limited to these

  — Data reliability and assurance using ALCOA++ criteria

  — Impact and consequences of data integrity violation

  — GDP (Good Documentation Practices) in paper-based and electronic systems

  — Expectations from a paper-based system

  — Expectations from an electronic system, including assuring integrity of electronic records, restricting access, establishing access control, user privileges, review of audit trials, administrative controls and other related matters

- Good Chromatographic Practices
- Identifying unreliable lab results for analytical process including mobile phase, suitability solutions, sample preparation, integration peaks
- Recording of observations during document review and audits
- Data governance
- Risk management for data reliability
- Role-based training for doers
- Training for SMEs
- Data review (paper and electronic)

9. Process design

- All the activities related to quality and/or GMP shall be designed so as to support data reliability across the data lifecycle in order to ensure that data is complete and meet the ALCOA criteria

- **Design for paper-based system**

  - Paper formats shall be controlled and accounted manually. Wherever possible, electronic systems shall be implemented to control and account for paper formats. Archival mechanisms shall be established in such a manner that paper records are secured. Wherever possible, paper records shall be archived with help of electronics having full control over protecting data in its original context

  - Accurate, legible and contemporaneous recording of paper data shall be monitored and verified with little loss of time from when the data was recorded. Risk-based review mechanisms shall be included in the design

- **Given below are dos and don'ts for Good Documentation Practices that shall be followed by the organization while doing documentation design**

- **'Dos' requirement for GDP**

  - DD/MM/YY and HH:MM formats shall be followed

  - Pens using indelible (permanent) inks of specified colors shall be used

  - GXP data shall be recorded directly on approved and authorized formats

  - Alterations made to handwritten entries shall be made in the following manner

    - A single line should be marked through the error followed by signature and date

    - Alterations shall permit reading of original information

    - Reason/s for the alterations shall be recorded

  - Modifications, changes and corrections in the master document shall be carried out through Change Control Procedure only. (No handwritten corrections shall be allowed on master documents.)

  - Design of recording format shall provide sufficient space and shall have provisions to record entries, signatures and record date/time (as applicable)

  - 'NA' shall be used with signature and date

  - In multiple blank spaces/rows/columns, a diagonal single line across the whole field or space shall be used, 'NA' shall be recorded with signature and date, and a brief justification shall be recorded

  - On draft documents intended for review, the word 'DRAFT' shall be used as a watermark, or a stamp with the word 'DRAFT' shall be used to mark all pages

  - Critical significant steps in documents shall be identified and the same shall be required to be checked by a second person while performing the task

  - Actual observations shall be recorded in the records. However, in certain formats such as a checklist, the recording of ‘Yes’ or ‘No’ shall be used to indicate whether the activity was performed or not

  - For analysis and in manufacturing, SOP/BMR/STP shall be followed step by step, that is sequentially, and documentation should happen concurrently

  - MS® Excel sheets used for calculation shall be validated

  - Signature Specimen Records for short (initial) and full signature shall be maintained, wherein each employee involved in GXP activities shall give a specimen of his/her signature and initials to ensure that the signature is traceable to the correct member of the staff

  - In cases where the original documents have attachment(s), there shall be clear indications about the number of attachments. Traceability (Parent-Child Relationship) shall be maintained in chronological order

  - While handling thermal paper, the procedure of signature, followed by photocopying and attaching the thermal paper with the photocopy shall be followed

  - All weight slips, printouts, chromatograms, spectrum, etc. shall be signed after completion of the activity. Print-outs pasted in the record shall have the relevant signatures across the printouts

  - Documents shall be maintained without any damage

  - Electronic records are equally important and are given due attention by regulatory agencies

- **‘Don’ts’ for GDP**

  - Handwritten corrections on Master Documents are not permitted

  - Use of ditto marks (e.g.____” ____) to fill repetitive entries is not permitted

  - Use of third brackets ‘{ }’ is not allowed for signature against multiple entries

  - Use of pencil or any removable and water soluble ink is not permitted

  - Use of eraser or ink remover or whitener is not permitted

  - Recording of data on unauthorized documents (e.g. post-it-notes, sticky sheets, scrap paper, personal notebooks), glass boards and black/white boards, etc. is not permitted

  - Overwriting, multiple crossing of the original entry/data and similar practices are not permitted

  - An entry made by a person on a GMP document but not signed and dated by the person who has made the entry is not accepted as authentic

  - Pre-dating or back-dating entry is strictly not permitted

  - Destruction and/or deletion of a record, document or report because of any error or mistake are strictly not permitted. Such a record, document or report is still required for reasons of traceability

  - Deliberately amending or destroying records, documents or reports to hide or falsify data is strictly forbidden. Such actions shall lead to strict disciplinary action

- **Control on blank forms**
  - Control on blank forms shall be done as part of the good documentation practices of the organization. Blank forms (including, but not limited to, worksheets, laboratory notebooks, and MPCRs) shall be controlled by the quality unit or by another document control method. For example, numbered sets of blank forms may be issued as appropriate and shall be reconciled upon completion of all issued forms. Incomplete or erroneous forms shall be kept as part of the permanent record along with written justification for their replacement

- **Signature Practices**
  - The same person shall not sign for multiple roles for one activity
  - ***Done by***
    - 'Done by' means 'performed by' and the person is the doer
    - The doer is a person who is responsible for the activity by means of preparation, doing or performance
    - The 'done by' signature identifies the person who actually did the work and documented it. Thus, the 'done by' signature is attributable to the person performing the activity or generating the data
    - The doer is the person who actually performs the activity and shall record or make entry of observations by him/ her followed by signature and date
  - ***Checked by***
    - This identifies the person who witnessed the activity being performed
    - The checker is a person proficient in the task performed and has been trained to perform the activity
    - The checker verifies that the doer has recorded contemporaneously
    - The checker has watched and/or witnessed the activity being performed. The checker may also perform the 'supervisory recording' (see below)
    - For the checker to sign, the document must have the signature of the doer. The checker cannot be the only individual to sign the document
    - All the critical stages/steps shall be checked by another person
  - ***Checked and Recorded by: (supervisory recording, recording by scribes)***
    - 'Checked and recorded by' shall carry the initials or signature of a person who is checking or supervising the activity and recording the information of the activity performed, and the readings of an operation which are recorded contemporaneously
    - The 'Checked and recorded by' part of the recording process shall be used only if the operator (doer) performing the operation is unable to initial and date immediately, due to working in a confined or restricted space, or to avoid intervention in the process
    - The use of 'supervisory recording' (scribes) to record activity on behalf of another operator shall be considered 'exceptional' and should take place only when normal documenting processes can place the product or activity at risk, e.g. in manufacturing steps such as addition of material in batch or

documenting line interventions by sterile operators

  - Each department shall maintain a list of the activities to which the process of "supervisory (scribe) recording" of the documentation applies. This shall be preapproved by QA

- ***Verified by***
  - The 'verified by' signature identifies the person who ensured that the work was performed and documented correctly
  - He or she verifies that sequential steps were performed and the doer has recorded the entries, based on objective evidence, associated records/logs, etc.
  - The verifier cannot perform the 'supervisory recording'
  - For the verifier to sign a document, it is must to have signature of the doer. The verifier cannot be the only individual to sign the document; e.g. a document signed 'Line Clearance by QA' which is signed only by the verifier shall be considered inadmissible

- ***Reviewed by***
  - The 'reviewed by' signature identifies the person who ensured that the work was performed and documented correctly (possibly at a later time)
  - 'Reviewed by' is the initials or signature of the person who reviews the document or record in order to confirm its accuracy and completeness, clarity and legibility, including checking of the calculations if applicable
  - The reviewer is a person who is responsible for reviewing the documents based on evaluation of supporting data, documents and/or references attached and the checker's comments

- ***Approved By (or Authorized By)***
  - The 'Approved by' signature identifies the person who evaluates the work performed to ensure it was done accurately, completely, and in accordance with procedures and/or documentation practices
  - 'Approved by' indicates approval to proceed to the next stage or process
  - The approver is a person who is responsible for approving or authorizing the documents based on evaluation of the critical steps, summary, and final conclusion or comments by the reviewer
  - The approver may also review the documents for clarity, understanding and decision making

- ***Helper or Assistant***
  - The 'helper' provides assistance to the 'doer' in order to make it easier for the latter to perform physical activities
  - Helpers are persons who perform motor activities and help the doers and the supervisors in physical handing, such as moving of trolleys, lifting of bags and containers, etc. Since the helper is only performing physical activities, in the sense of definition, the officer or the person getting such activities done through instructions will be the 'doer'

- *Designee*
  - The designee is a person who is allocated signature and decision-making authority in absence of his/her superior as per the Deputation Matrix of the organization
  - The deputation matrix shall be prepared by site and support functions
  - The allocation of designee is based on his/her knowledge, experience and competency; the designee shall be from the same function

- **Design of electronic system**
  - All computerized systems used by organizations shall be evaluated, controlled and managed in accordance with GMP and GDP requirements
  - To assure the integrity of electronic data, computerized systems will be validated at a level appropriate for their use and application. Validation will address the necessary controls to ensure the integrity of the data, including original electronic data and any printouts or PDF reports
  - The depth and scope of validation will depends on the diversity, complexity, and criticality of the computerized application
  - Systems shall be assessed to identify data integrity risks and/or vulnerabilities to manipulation
  - All computerized systems that have the potential for impact on product quality shall be designed and managed to ensure protection from accidental or deliberate manipulation, modification or any other activity that may impact data integrity
  - Users will be adequately involved in validation activities to define critical data and data lifecycle controls that assure data integrity

- **Qualification and Validation of Computerized Systems**
  - Risk assessments shall be in place for each system emphasizing the required controls to ensure data integrity
  - Validation shall be performed for each system and a report shall be in place stating at least the following items
    - Critical system configuration and controls for restricted access to configuration and any changes made therein
    - A list of currently approved users
    - Privileges for each user of the system
    - Identity and role of the System Administrator
    - Frequency of review of audit trails and system logs
    - Procedures for new system user creation, deleting users, changing of privileges, backing up, recovery and archiving
    - Original data shall be retained with relevant metadata in formats that allow the reconstruction of process

- Companies should have a Validation Master Plan in place
- Systems shall be challenged with defined tests before their routine use to ensure they conform to acceptance criteria
- Specific tests in DQ, IQ, OQ and PQ shall be included to challenge data integrity risk areas during qualification testing
- Computerized systems shall be evaluated periodically, at a pre-determined frequency, based on risk assessment depending upon criticality, in order to ensure that they remain in validated state. This evaluation shall include deviation, changes, upgrade history, performance and maintenance
- Interfaces shall be designed and assessed in such a way that it allows complete and accurate data transfer between systems

- **Records**
  - **Static Records**
    - The expectations from paper records include controls for retention of original paper records or certified true copies of original paper records, but are not limited to, static format records
    - The records shall also include written procedures, training, review and audit, and self-inspection of processes defining conversion, as needed, of original paper records to true copies, which shall be done in the following steps: copies are made of the original paper records, preserving the original record format, the static format, as required (e.g. photocopy, PDF files, etc.)
  - **Dynamic Records**
    - **Expectations from electronic records**
      These shall include written procedures, training, review and audit and self-inspection of processes defining conversion, as needed, of original electronic records to true copies which shall be done in the following steps

      1. Copies are made of the original electronic data set, preserving the original record format, the dynamic format, as required (e.g. backup copy of the entire set of electronic data and metadata using a validated backup process)
      2. A second person verifier or a technical verification process (such as use of a technical hash function) shall confirm successful backing up, whereby a comparison is made of the electronic backup copy to the original electronic data set to confirm that the copy preserves the entire content and meaning of the original record (i.e. all of the data and metadata are included, no data is missing in the copy, dynamic record format is preserved as important for record meaning, and the file was not corrupted during the execution of the validated backup process)
    - Preserving the original electronic data in electronic form is also important since data in dynamic format facilitates greater usability of the data for subsequent processes. For example, temperature logger data maintained electronically facilitates subsequent tracking and trending and monitoring of temperatures in statistical process control charts
    - There are a few special risk management considerations for retention of original records and/or certified true copies. Certified true copies of electronic records shall preserve the dynamic format of the original electronic data as essential to preserving the meaning of the original electronic data. For example, the original dynamic electronic spectral files created by instruments such as FT-IR, UV/Vis, chromatography systems and others can be reprocessed, but a PDF file or printout is

fixed or static and the ability to expand baselines, view the full spectrum, reprocess and interact dynamically with the data set would be lost in the PDF file or printout. As another example, preserving the dynamic format of clinical study data captured in an electronic case report form (eCRF) system allows searching and querying of data, whereas a PDF file of the eCRF data, even if it includes a PDF file of audit trails, would preclude such search and query of the content

- **System Security**
  - All systems shall be designed and configured with adequate security measures to prevent unauthorized access, changes or deletion of data.
    Examples are given as below but are not limited to
    - Individual Login IDs and passwords shall be allotted to users of the system
    - No shared Login credentials shall be assigned
    - A list of authorized users with privileges shall be maintained
    - Administrator access shall be controlled and other users shall not have access to change clock settings and deletion of any data
    - System administrator should be an independent person who is not involved or interested in outcome of data generated
    - Physical security shall be provided for servers and PLC nodules
  - Usage of electronic signatures must have appropriate controls to ensure identity and traceability
- **Audit Trails**
  - The purpose of an audit trail for electronic record systems is to provide assurance of the integrity of the electronic record and the associated raw data. Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operations

    Audit Trail Regulatory Requirements
    - Even if there are no predicate rule requirements to document, for example, date, time, or sequence of events in a particular instance, it may nonetheless be important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the records. The audit trails shall always be enabled, or other appropriate measures deployed, on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on product quality and safety and record integrity
    - The system shall enable the recording of the unique identity of operators entering or confirming critical data. Any entry or alteration of critical data shall be authorized and recorded with the reason for the change. Consideration shall be given to building into the system the creation of a complete record of all entries and amendments (a system generated 'audit trail'). Audit trails need to accurately reflect changes. For example, if a relevant electronic record is created using a number of data fields, all these data fields need to be linked within the audit trail. The aim is to know at any given time point what the information was. Audit trails need to be available and convertible to human readable form

- **Content of the Audit Trail**
    - The audit trail shall be inextricably linked to the electronic record. It shall be secure and not have the facility for editing or deleting, hence providing a permanent record
    - The main function of the audit trail is to provide assurance for the integrity of the electronic record. For each entry the following information shall be recorded
        - Date and time stamp
        - Name of the user making the change (unique ID)
        - Link to the record (Batch No, Record ID)
        - Original value
        - Changed value
        - Reason for change
    - This shall provide the same level of assurance to the record integrity as that of a paper record, that is, if in a process a correction or change is made and the operator makes a correction striking though the initial value, enters the new value, provides reason for change and signs and dates the entry, recording the data and events on paper or through electronic means must have the same level of assurance of data integrity
    - The audit trail can also provide a record of invalid attempts to log on to the system, to demonstrate the security of the system
- Electronic copies can be used as accurate reproductions of paper or electronic records, provided that the copies preserve the content and meaning of the original data, which includes associated metadata, while preserving the static or dynamic nature of the original records
- **Systems with audit trails**
    - Where systems have an audit trail, the organization shall develop processes for reviewing the audit trail for assuring record integrity. The checking of an audit trail can be labor intensive and therefore the most cost effective method shall be sought. Where records receive a final approval (batch record, change control or deviation), the point of approval of the record may be the most efficient time to check the record. For large systems, such as Enterprise Resource Planning (ERP) systems where thousands of transactions can take place, an audit trail review by exception may be taken, that is, when an error is detected. Personnel responsible for record review under CGMP shall review the audit trails that capture changes to critical data associated with the record as they review the rest of the record
    - Audit trails that capture changes to critical data shall be reviewed with each record and before final approval of the record. Audit trails subject to regular review shall 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
    - Processes shall be designed so that quality data required are created, maintained and are prevented from modification. For example, chromatograms shall be sent to long-term storage (archiving or a permanent record) upon run completion instead of at the end of a day's run
    - Storing data electronically in temporary memory, in a manner that allows for manipulation,

before creating a permanent record, i.e. electronic data that are automatically saved into temporary memory do not meet CGMP documentation or retention requirements

    - » There shall be technical and procedural controls to meet CGMP documentation practices for electronic systems. For example, a computer system, such as a Laboratory Information Management System (LIMS) or an Electronic Batch Record (EBR) system can be designed to automatically save after each separate entry. This would be similar to recording each entry contemporaneously on a paper batch record to satisfy CGMP requirements. The computer system could be combined with a procedure requiring data be entered immediately when generated

    - » Whatever methods are employed, the approach shall be justified and documented

- — **Systems without audit trails**

    - » Where systems do not provide the facility to change data, for example a data logging system used to capture process data, like temperature, and the data is stored securely, an audit trail shall not be necessary. However, such a decision must be documented

    - » In the case where an audit trail is not being employed, a security process must be put in place, validated and controlled via Standard Operating Procedures (SOPs). This shall ensure that only authorized users have access to the system, controls between configuration and operation are separated and that only administrators have access to the operating system

    - » Alternative methods shall be employed to provide assurance of the integrity of critical parameters. Procedures can be put in place to verify, prior to use, the critical parameters (including Control and Alarm Setpoints) to assure that they are set to the validation and process requirements. This shall be documented within the batch record for computerized control systems and in laboratory analysis or sample records for laboratory instrumentation

- — The organization shall purchase and upgrade software that includes electronic audit trail functionality

- — Audit trail functionalities should be configured properly to capture general system events and activities relating to the acquisition, deletion, overwriting of and changes to data

- — Audit trails should be verified during validation of the system

- — Where audit trail facilities are not available, alternative arrangements must be implemented, e.g. administrative procedures, secondary checks and controls

- — Audit trail functionality must be enabled and locked at all times

- — Policy and processes shall be implemented for the review of audit trails in accordance with risk management principles

- — Audit trails of each batch should be reviewed prior to the release of the batch

- — Ongoing reviews of audit trails shall be conducted by quality unit based on criticality and complexity of system

- — Procedure shall be in place to address and investigate any discrepancy found in audit trail

- ■ **Configuration and design control in IT systems**

    - — The validation activities shall ensure that the configuration settings and design controls for GDP are enabled and managed across the computing environment, including both the software application and operating systems environment. For example, such activities shall include, but are not limited to

    - » Documenting configuration specifications for commercial off-the–shelf (COTS) systems as well as user–developed systems, as applicable
    - » Restricting security configuration settings for system administrators to independent persons, where technically feasible
    - » Disabling configuration settings for system administrations to independent persons, where technically feasible
    - » Disabling configuration settings that allow over-writing and reprocessing of the data without traceability
    - » Restricting access to time/date stamps
  - — For systems to be used in clinical trials, configuration and design controls shall be implemented to protect the blinding of the trial, for example, by restricting access to randomization data that may be stored electronically
  - — Data security will be designed so as to protect the data from loss and unauthorized access
- ■ **Data capture and entry**
  - — Manual entry should be made by authorized individuals only and the system should record details such as who made the entry and when it was made
  - — Data should be entered in specified format which is controlled by the software
  - — All manual entries should be verified by a second operator or by computerized means
  - — Audit trail shall capture changes made
  - — Validation shall be performed of the interface between the data generation, acquisition, processing and recording systems to ensure the accuracy and completeness of data
  - — Data which are captured by the system should be stored in a format that is not susceptible to manipulation or loss
  - — Time stamp shall be generated automatically by the system when data is entered
  - — Procedures shall be in place for any changes and modifications to original data. Changes made must be documented, reviewed and approved
- ■ **Review of electronic data**
  - — Critical data, identified through risk assessment, shall be reviewed and verified to conclude that activities were executed correctly and changes made to original data, if any, are authorized
  - — The review of data-related audit trails should be part of the routine data review
  - — SOPs shall be in place that describes how to review audit trails including actions to be taken on identification of any serious issues which may have impact on product quality
- ■ **Storage, archival and disposal of electronic data**
  - — Data must be stored in its entirety along with metadata, including audit trails
  - — Control shall be put to prevent data storage on unauthorized media such as USB drives, etc.

- Written procedures shall govern periodic data archival and backup processes
- Backed up data shall be stored in physically isolated locations to survive in the event of disasters and shall be secured to prohibit unauthorized access, alteration and deletion
- A procedure for restoration of data shall be available to allow reconstruction of the activity in future
- Approved procedures should be in place for the disposal of electronically stored data

- **Data lifecycle**
  - Data Lifecycle Process Mapping (DLPM) shall be conducted by the organization. The objective of the process mapping shall be to identify the risk to data integrity in the current process of acquiring, processing, reviewing, reporting and retaining data forms. The outcome of the mapping shall include suggestions for redesigning the data process including data flow and associated business process, as well as listing residual risk and proposed frequency for review and monitoring of this risk to identify opportunities for continuous improvements
  - Data lifecycle process mapping and associated risk assessment will be done for each business process to identify all data and records generated in each process
  - DLPM and risk assessment will help the organization identify current gaps in the system and will give the organization the opportunity to implement additional effective controls
  - Data lifecycle process mapping will be performed with a pre-defined protocol. Refer to the following Annexures
    - **Annexure 3: Reference Protocol for Data Lifecycle Process Mapping for Manufacturing Stage: Granulation**
    - **Annexure 3a: Probability of Errors generated from various Data Generation Sources and Mitigation Plans; and**
    - **Annexure 3b: Monitoring of Manufacturing Process and Recording of Process Parameters with their Quality Attributes)**
  - Process mapping shall be done for each process throughout the lifecycle of a drug. The process with the individual documents involved in the process from start point to end point, each process step, description, data involved in the process, SOPs, etc., shall be reviewed against the mapping
  - In addition to this, the equipment, instruments, and software involved in the process shall be identified. Equipment and instruments including those generating the electronic data shall be identified. Separate data lifecycle process mapping shall be performed for stand-alone systems
  - Brain-storming sessions shall be conducted to evaluate all challenges pertaining to process gaps with SMEs with cross functional training, to address the gaps. Finally, gap closure shall be performed to identify critical priorities and the actions resulting from the same shall be implemented for better compliance with respect to all processes
  - Validation shall include assessing risk and developing quality risk mitigation strategies for the data lifecycle, including controls to prevent and detect risks throughout the steps of
    - Data creation and capture
    - Data processing

        - Data review
        - Data reporting, including handling of invalid data and atypical data
        - Data retention and retrieval
    - For example, validation activities might include, but shall not be limited to
        - Determining the risk-based approach to reviewing electronic data and audit trails based upon process understating and knowledge of potential data impact to product and patient
        - Writing SOPs defining review of the original electronic records and including meaningful metadata such as audit trails and review of any associated printouts or PDF records
        - Documenting the system architecture and data flow including flow of electronic data and all associated metadata, from the point of creation through till archival and retrieval
        - Ensuring that the relationship between data and metadata are maintained intact throughout data lifecycle
- **SOPs and training**
    - The validation activities shall ensure that adequate training and procedures are developed prior to release of the system for GXP use. These shall address
        - Computerized systems administration
        - Computerized system use
        - Review of electronic data and meaningful metadata, such as audit trails, including training that may be required in system features that provided users with the ability to efficiently and effectively process data and review electronic data and metadata
    - Validation shall also cover controls to ensure that good data management practices, for both electronic data and associated paper data, are implemented as deemed appropriate for the system type and its intended use
    - Data process shall be designed to adequately mitigate and control and continuously review the data integrity risks associated with the steps of acquiring, processing, reviewing, and reporting data, as well as the physical flow of the data and associated metadata across this process through storage and retrieval
    - Good data process design shall ensure and enhance controls, for each step of the data process, wherever possible, such that each step is
        - Consistent
        - Objective, independent and secure
        - Simple and streamlined
        - Well-defined and understood
        - Automated
        - Scientifically and statistically sound
        - Properly documented according to GDP

- **Data collection and reporting:** All data collection and reporting will be performed following GDP and applying risk-based controls to protect and verify critical data

- **Data processing:** To ensure data integrity, data processing should occur in an objective manner, free from bias, using validated/qualified or verified protocols, processes, methods, systems, equipment and according to approved procedures and training programs

- **Data review and data reporting:** Data shall be reviewed and, wherever appropriate, evaluated statistically after completion of the process to determine whether outcomes are consistent and compliant with established standards. The evaluation should take into consideration all data, including atypical or suspect data or rejected data, together with the reported data. This shall include a review of the original and electronic records

- **Data retention and retrieval:** Retention of paper and electronic records has been discussed in the section above, including measures for backup and archival of electronic data and metadata

- **Data management of quality processes:** Quality processes that have impact on data reliability shall be identified across the manufacturing, packaging, warehousing, engineering, quality-control and quality assurance operations. All these processes, like recording of batch manufacturing activities, batch testing activities, batch packaging activities, operation of GMP software, handling of QMS activities, document control, validations, reviews, etc. shall be visited for their design so as to evaluate if these are user-friendly for supporting data reliability. Quality processes shall be inspected for data recording design and shall be improved with the objective of preventing accidental breaches. **(Refer to Annexure 5: Data Quality Design Considerations and Controls)**

- **Exclusion of CGMP data**

  Any data created as part of a CGMP record must be evaluated by the quality unit as part of release criteria and maintained for CGMP purposes. Electronic data generated to fulfill CGMP requirements shall include relevant metadata. In order to exclude data from the release criteria of the decision-making process, there must be valid, documented, and scientific justifications for its exclusion. The requirements for record retention and review do not differ depending on the data format; paper-based and electronic data record-keeping systems are subject to the same requirements

10. Technology and IT Systems

- Technology and IT systems are helpful in achieving data reliability. Opportunities of uses of IT systems shall be rolled out across the quality related processes

- The organization shall continuously evaluate the IT options that are available and the systems that can be implemented practically. A visionary approach shall be derived and implemented in a timely manner

- The IT framework identifies the elements of IT that shall be considered as a minimum baseline, in managing systems, networks, devices and data, so as to ensure that they are secure, protected appropriately from risk, adequately tested and controlled, and developed and maintained in line with corporate objectives

- The organization shall determine the type of technology that can be implemented based on the complexity, since the amount of controls available in the systems increase with the increase in complexity of the systems. This can be done by identifying risks due to the newly introduced technology, e.g. implementing backup procedure to prevent data loss. Also, the organization shall evaluate the amount of reduction in the initially identified risk by applying the controls that the technology facilitates to mitigate the identified risk

- The organization shall also ensure that the system is selected, implemented and used as per documented procedures, i.e. procedures for qualification and validation of equipment and software. Appropriate installation and operational qualifications should demonstrate the suitability of the computer hardware and software to perform assigned tasks and handle all respective challenges with respect to data integrity

- **Validation of Workflow on Computer Systems**

  — A workflow, such as creation of an electronic Master Production and Control Record (MPCR), is an intended use of a computer system which shall be checked through validation. If the computer system is validated, but it is not validated for its intended use, then it cannot be known for certain whether the workflow will run correctly

  For example, qualifying the Manufacturing Execution System (MES) platform, a computer system ensures that it meets specifications; however, it does not demonstrate that a given MPCR generated by the MES contains the correct calculations. In this example, validating the workflow ensures that the intended steps, specifications, and calculations in the MPCR are accurate. This is similar to reviewing a paper MPCR and ensuring all supporting procedures are in place before the MPCR is implemented in production

- Data reliability shall be incorporated while evaluating software before implementation

- Vendors shall be evaluated and be required to distribute instruments and equipment, at affordable cost, that will help in global compliance with data integrity requirements

- The following IT SOPs shall be addressed with Technology and IT systems

  — IT system maintenance

  — Physical security

    - Logical security
    - Incident and problem management
    - System change control
    - Configuration management
    - Code development
    - Disaster recovery
    - Contingency planning
    - Virus control and systemic software program bug management
    - Data backup, restoration and retrieval
    - IT system retirement
    - Network and server qualification
- Following intermediate guidelines shall be addressed with Technology and IT systems
    - Overall CSVMP (Computer System Validation Master Plan)
    - User access control and authority level management
    - Password lifecycle management
    - Process and implementation plan of IT systems in quality processes for maintaining data reliability
    - Electronic signature policy
    - Risk assessment and mitigation for legacy and stand-alone systems
    - Desktop policy
    - IT administrator policy
    - Backup policy
    - Alarm lifecycle management for GXP controls
- Development of a robust IT frame work shall include maintaining systems, networks, devices and data, ensuring that they are protected from risk, adequately tested, validated, controlled and maintained
- Electronic signatures with the appropriate controls can be used instead of handwritten signatures or initials in any CGPM required record. An electronic signature with the appropriate controls to securely link the signature with the associated record fulfills this requirement. Electronic signatures should document the controls used to ensure that they are able to identify the specific person who signed the records electronically
- There shall be restriction to alter specifications, process parameters, or manufacturing or testing methods by technical means where possible (for example, by limiting permissions to change settings or data)

- Only authorized personnel shall make changes to computerized MPCRs, or other records, or input laboratory data into computerized records. The organization shall implement documentation controls to ensure actions are attributable to a specific individual

- Login IDs and passwords must not be shared. When login credentials are shared, a unique individual cannot be identified through the login and the system would thus not conform to the CGMP requirements

- The organization shall carry out IT threat assessment like hacking with respect to electronic data, and take a risk-management approach to protecting data reliability

- All the GMP activities and quality related processes shall be evaluated for implementation of the IT systems with the objective of migrating from paper-based documentation to electronic documentation, and upgradation of the existing IT systems to improve controls for data reliability requirements. An evaluation and action plan shall be documented, implemented and periodically reviewed

- Electronic systems are categorized as computerized systems and non-computerized systems

- All computerized systems shall be assessed so as to comply with 21 CFR Part11 /EU annex 11 requirements

- All non-computerized systems shall be assessed for data integrity risk assessment

- Gaps assessment for legacy IT systems shall be carried out with respect to 21 CFR part 11/EU annexure requirement's to identify data reliability risk

- Incidents related to computerized systems that could affect the quality of intermediates or APIs or the reliability of records or test results shall be recorded and investigated

- Changes to computerized systems shall be made according to a change procedure and shall be formally authorized, documented, and tested

- Records shall be kept of all changes, including modifications and enhancements to the hardware, software, and any other critical component of the system. These records shall demonstrate that the system is maintained in a validated state

- Risk identification prioritization and mitigation shall be carried out. Appropriate action plan shall be prepared so as to complete the action in a phased manner using procedural controls

- Technology alone cannot entirely eliminate data integrity issues. There are still people and manual processes involved that must be accounted for, monitored, and improved. Therefore, the organization must take a holistic approach to address data integrity issues and apply the necessary designs and controls across all spheres of influence

11. Risk detection and mitigation

- Risk management approach for data reliability implies that risk assessment shall be performed by trained SMEs who will be involved in providing key quality indicators that are affected during data reliability inspection

- Detail risk assessment with respect to data reliability shall be carried out as per ICH Q9 principles. An example related to Data reliability Risk assessment and mitigation evaluation is mentioned in point **5.12** of **Annexure-3 Reference Protocol for Data Lifecycle Process Mapping for Manufacturing Stage: Granulation**

- All the risks and failures effects associated with the data process lifecycle steps should be identified. There may be more than one failure mode or failure affect for each process step. Once all failure modes have been identified, the scoring can take place to allow ranking of the risk through guidance on quality risk management

- Scores must be provided for failure modes and effects by severity of the risk with data reliability and ease with which these could be detected. The rankings must be justified and rationale should be provided

- Data reliability risk can be classified into three levels: Severity (S), Occurrence (O) and Detection (D). Based on the level of risk classification, overall risk criticality can be identified as high, medium and low

- The risk priority number (RPN) is arrived at by multiplying classification scores, that is, (S) X (O) X (D)

- Potential improvements shall be identified for failures with a RPN. If, however, during evaluation a mitigating activity is identified that can reduce RPN, then this shall be captured as a recommended corrective and preventive action. **(Refer to Annexure 7: Risk Assessment Table for Data Recording and Process Control)**

- This table is to be used for risk assessment for data recording and process control. Potential improvements shall be identified for failures with an RPN (Risk Priority Number). During evaluation, risk mitigation measures need be identified with current controls that can reduce RPN, and such measures need to be captured as recommended corrective and preventive action. The amount of effort used for risk control should be proportional to the risk, and a suitable due date and classification commensurate with the label of the risk has to be assigned to each section. When it is not possible to reasonably reduce the risk to the acceptable level or to achieve it quickly, a proper justification must be provided

- **Risk Management Approach to Data Governance**

  — Where long-term measures are identified in order to achieve the desired state of control, interim measures shall be implemented to mitigate risk, and shall be monitored for effectiveness. Where interim measures or risk prioritization are required, residual data integrity risks shall be communicated to senior management, and kept under review. Reverting from automated or computerized to paper-based systems will not remove the need for data governance. Such retrograde approaches are likely to increase administrative burden and data risk, and prevent the continuous improvement initiatives

  — Not all data or processing steps have the same importance to product quality and patient safety. Risk management steps as mentioned in **Annexure 3 point 5.12** shall be utilized to determine the importance of each data and processing step. An effective risk management approach to data governance shall take into account data criticality (impact on decision making and product quality).

Factors to consider regarding data criticality include

  - Which decision/s does the data influence?
  - What is the impact of the data to product quality or safety?

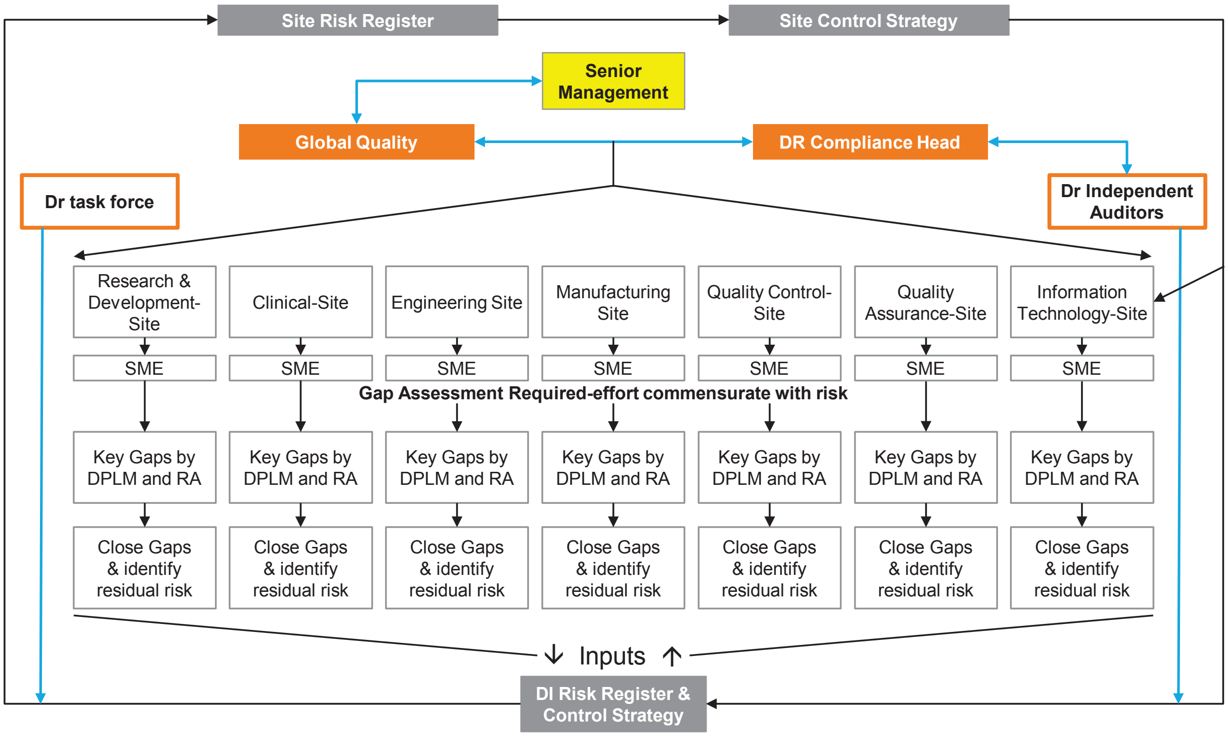
- Risk assessments shall focus on a business process (e.g. production, QC), evaluate data flows and the methods of generating data, and not just consider IT system functionality or complexity. Factors to consider include

  - Process complexity
  - Methods of generating, storing and retiring data and their ability to ensure data accuracy, legibility, indelibility
  - Process consistency and degree of automation / human interaction
  - Subjectivity of outcome and/or result (i.e. is the process open-ended or well defined?)

12. Governance

- Data governance refers to the sum total of arrangements that have been put in place in order to ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle. The organization shall appoint a Task Force to govern the overall data reliability process. A robust data governance approach will ensure that the data is complete, consistent and accurate, irrespective of the format in which data is generated, used or retained
- Data reliability shall be governed through training and implementation of data reliability related policies including this Guideline
- The organization shall establish and execute an audit program for data reliability that utilizes independent auditors who are qualified by education, experience and training to evaluate the quality systems used for collecting, analyzing, reporting and retaining information and data
- The audit program shall include periodic audit to confirm adherence to established requirements for data reliability
- Management shall be notified of critical data reliability findings that directly impact the quality of products and have potential of serious regulatory concerns. The relevant data reliability information shall be included in the site quality metrics and will be monitored as per a pre-determined process and frequency
- The data governance structure is provided below

Data Governance Structure



*DPLM: Data process life cycle mapping, RA: Risk Assessment

- **Data Reliability Assessment by Data Reliability Auditors**

  Data reliability assessment shall be part of the self-inspection program of the organization

  - Data Reliability Auditors will be responsible for performing scheduled/unscheduled data reliability assessments (DRA) and inspections at sites as per the authorized data reliability reference checklists referred to below. **(Refer to Annexure 4: Data Reliability Inspection Checklist, and Annexure 6: 21 CFR PART 11 Assessment)**

  - The Data Integrity Assessment team shall verify that the document contents comply with and reflect the applicable regulations and the relevant parts of applicable currently authorized product/project regulatory applications (Product Specification Files, Manufacturing and Marketing Authorizations). Documents shall be uniquely identified by suitable means, including version identification where appropriate, with a suitable descriptive title. Constituent pages are unambiguously identified in such a way that completeness is evident, e.g. pagination of the document shall follow the protocol Page 1 of 4, Page 2 of 4, etc.

  - All forms of documentation and records shall be legible and clear with regard to purpose, function and detail, and all types of GXP documents generated or used shall be properly defined and procedures adhered to

  - Documentation for records shall provide for accurate and sufficient recording of the various processes and evaluation of observations

  - Records shall be available for review and audit-inspection over the lifetime of the product as defined by ICH-Q10

  - The data reliability officers shall also verify the applications that manage access to such records for the purpose of use. These shall be configured so that only authorized persons can access appropriate levels of records, and only approved equipment is used to access records, and that records are not altered during use (e.g. the archiving environment and equipment)

  - The data reliability officer shall verify that records have been made and retained to demonstrate that in manufacturing, testing, monitoring and essential support processes, the applicable quality principles and regulations have been followed and all the precautions, steps, checks and actions have been taken or made as required, so that products conform with the requirements such that patient safety is assured. There must be controls in place to ensure integrity of data

  - Entries shall be clear, legible and indelible. If an unstable medium (e.g. heat-sensitive paper) cannot be avoided or if a document is damaged, then a non-degrading accurate copy must be retained with the original

  - Manual entries into records shall be made at the time each action is taken and each result is obtained, i.e. contemporaneously, or as soon as possible thereafter, so that all relevant activities, parameters, results and persons responsible are identified. Completed production records shall be signed and dated by the persons performing the operations

  - Any alteration, change or correction made to an entry on a record must permit the reading of the original information, and the reason for the change must be clearly evident and recorded where possible. The change(s) must be dated, and signed or logged in an audit trail

  - Manual recording of data generated during critical operations (in writing or by computer data entry) must be checked by an authorized second operator unless such checks are performed by validated electronic means

- Any suspicion that the integrity of data has not been maintained shall be investigated

- All persons contributing and the source document(s) used shall be identified in the record. All data recorded for the purpose of supporting quality decisions shall be retained, including the primary 'raw' data that are consolidated for presentation in the principal record. The traceability of information flow must be ensured

- If a record includes information in the form of codes, then that record must also contain either the means to interpret those codes, or an unambiguous reference to a document that explains the meaning of the codes; further, that document must be retained until the retirement or expiry of the last record in which the reference has been used

- The proper functioning of devices and systems for recording data shall be regularly checked and verified by suitable means (e.g. calibration, re-validation) by an authorized person. Systems used to record critical data/information must be equipped with audit trail capabilities

- **Risk Management Approach to Data Governance**

  - Where long-term measures are identified in order to achieve the desired state of control, interim measures shall be implemented to mitigate risk, and shall be monitored for effectiveness. Where interim measures or risk prioritization are required, residual data integrity risks shall be communicated to senior management, and kept under review. Reverting from automated or computerized to paper-based systems will not remove the need for data governance. Such retrograde approaches are likely to increase administrative burden and data risk, and prevent the continuous improvement initiatives

  - Not all data or processing steps have the same importance to product quality and patient safety. Risk management steps as mentioned in point 10 above shall be utilized to determine the importance of each data and processing step. An effective risk management approach to data governance shall take into account data criticality (impact on decision making and product quality). Factors to consider regarding data criticality include

    - Which decision/s does the data influence?

    - What is the impact of the data to product quality or safety?

  - Risk assessments shall focus on a business process (e.g. production, QC), evaluate data flows and the methods of generating data, and not just consider IT system functionality or complexity. Factors to consider include

    - Process complexity

    - Methods of generating, storing and retiring data and their ability to ensure data accuracy, legibility, indelibility

    - Process consistency and degree of automation / human interaction

    - Subjectivity of outcome and/or result (i.e. is the process open-ended or well defined?)

    The outcome of a comparison between electronic system data and manually recorded events (e.g. apparent discrepancies between analytical reports and raw-data acquisition times) could be indicative of malpractices

- **Establishing a Data Governance Structure**

  For establishing a data governance structure, there should be coordination of people, processes, and technology in order to manage and optimise the use of data as a valued enterprise asset. This will determine the exercise of authority, control, and shared decision-making (planning, monitoring, and enforcement) over the management of data assets

— The Data Governance Maturity Assessment (DGMA) model shall comprise the following

  » Open discussion with stakeholders at all levels

  » One-on-one interviews, group workshops, consulting SMEs

  » Pre-determined questions to be answered and maturity level determined

  » Current state maturity to be identified, together with the desired state

  » It must be ensured that the process is educational and continuous

The success of the data governance initiative will be highly dependent on a proper Maturity Assessment. A typical set of steps will comprise the following

Step 1 – Identification and preparation for interviews & workshops

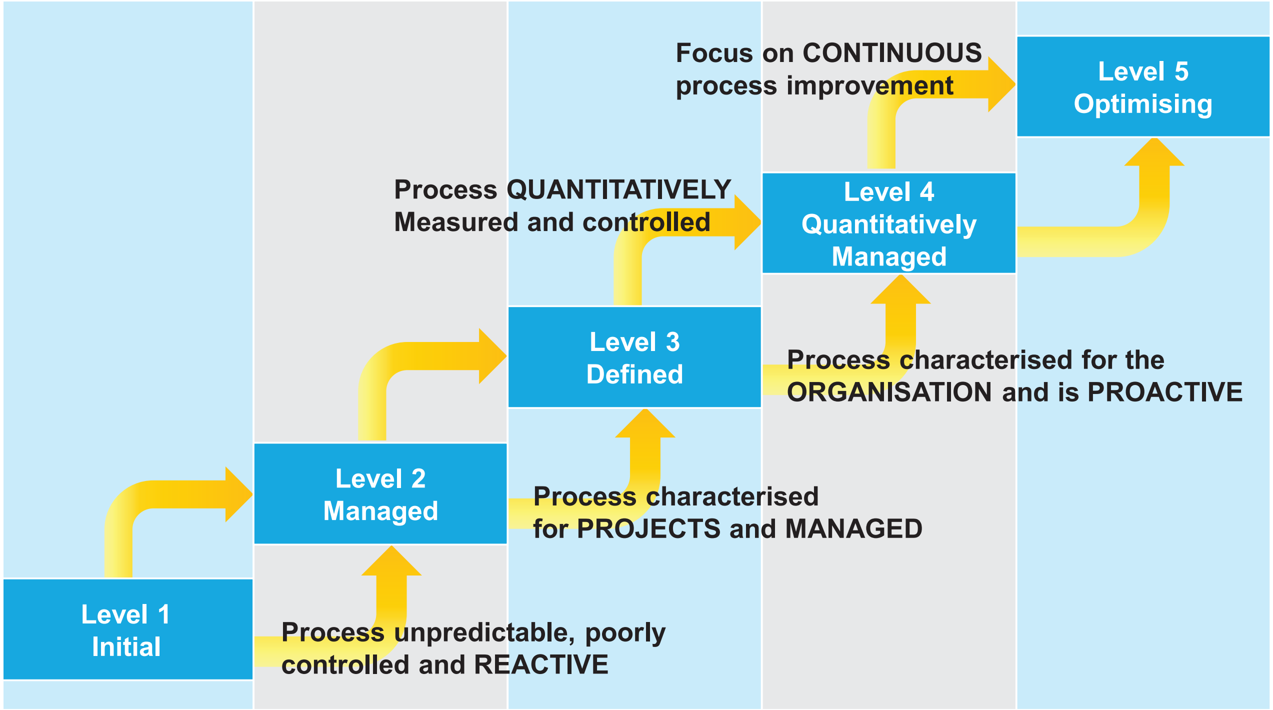
Step 2 – On-site workshops and interviews with key stakeholders in business and IT

Step 3 – Conducting the Maturity Assessment

Step 4 – Assimilation of findings, analysis, prioritisation of gaps and developing roadmap

Step 5 – Presentation of final Maturity Assessment

- Based on the maturity assessment of data governance in an organization, the appropriate data governance maturity model for the organization can be established
- There are a total of 5 levels for identification of data governance of a site or an organization
- The levels are Level 1 (Initial), Level 2 (Managed), Level 3 (Defined), Level 4 (Quantitatively Managed) and Level 5 (Optimizing), as shown in the diagram below


Focus on CONTINUOUS process improvement
Level 5 Optimising
Process QUANTITATIVELY Measured and controlled
Level 4 Quantitatively Managed
Level 3 Defined
Process characterised for the ORGANISATION and is PROACTIVE
Level 2 Managed
Process characterised for PROJECTS and MANAGED
Level 1 Initial
Process unpredictable, poorly controlled and REACTIVE

- Based on the data maturity assessment, an organization can evaluate the current status of data governance, associated gaps, and identify the probable risks associated with such gaps. It can then respond with improved processes and reach levels 3 and 4 (where there are defined processes, and data is quantitatively managed at an enterprise level)

- **Investigation of Wrongful Act:**

  — The organization shall establish and follow procedures for conducting an independent, fairly balanced and documented review, and if warranted, an in–depth documented investigation of any alleged falsification, fabrication, or other conduct that raises a question about the integrity of data

  — Such investigation shall be conducted at the direction of legal counsel to help ensure that documents are properly identified and preserved and that the company receives appropriate advice and legal advice regarding the conduct of such investigation. The investigator(s) shall possess the education, experience, and training to enable the person to conduct data integrity investigation

  — An independent investigation shall serve to identify potential gaps in systems, processes, procedures and/or practices by individuals or the organization that could raise questions about data integrity. Such investigations shall also serve to assess the legal implications of known or suspected wrongful acts and possible reporting to regulatory authorities

  — Independent investigations into conduct that raises a question about the integrity of data shall identify all person or persons found to be involved during such investigations, and describe in detail their actions or activities related to the conduct. Such investigation shall also determine the scope of the questionable conduct. For example, the investigation shall determine whether the same or similar conduct or practices may have happened in other instances or could have impacted other data, and if so, the investigation needs to be extended to these events, activities, and practices

  — Data reliability auditors shall bring the discrepancies identified, if any, to the attention of Corporate Quality for review and shall discuss the same with the site quality group as well

  — Corporate Quality shall notify the discrepancies to the site Quality Head for investigation and CAPAs

- **Data Integrity Failure, Observation, Action Plan and Remediation Process**

  — If data reliability failure is observed during self or regulatory inspection, then the following three key activities shall be undertaken

  1. Comprehensive Evaluation

  2. Risk Assessment

  3. Remediation and Management Strategy

  1. Comprehensive Evaluation

     » During investigation or post inspection, the investigation shall carry out a comprehensive evaluation of the extent of the inaccuracy of the reported data, in order to arrive at a detailed action plan based on the extent of the deficient documentation practice pertaining to data reliability

     » The organizational structure and personnel responsibilities shall be examined, specifically of the following areas

       • Nature of management involvement

    - SOPs (Standard Operating Procedures)
    - Contract Agreements

  - The investigation shall determine actual and factual root cause of the problem, i.e. find out who and what the real source of the problem
  - A comprehensive evaluation shall include a detailed description of strategies and procedures for finding the scope of the problem. Such an evaluation shall be comprehensive, thorough and complete
  - The evaluation report shall list the records, application and other documents that have been or will be examined
  - Scope of evaluation shall include interviewing identified people and personnel involved in the process
  - The investigation shall examine those involved in the data integrity breach and other related systems that could have the same problems with raw materials, components and ingredients, testing records, production and process records, and equipment

2. Risk Assessment
   - The organization shall assess the potential effect on the drug product and drug substance quality manufactured and released for distribution to all markets
   - The organization shall determine the effect of deficient documentation practices on the quality of the drug product released for distribution. Following issues will be evaluated
     - Were Out–of–specification (OOS) drugs shipped?
     - If yes, what is impact on patients?
     - Even if no OOS drugs were shipped, it will be important for the organization to maintain appropriate preventive controls
3. Remediation and Management Strategy
   - Data reliability identification and associated CAPA (Corrective Action and Preventive Action plan)
     - Management strategy shall include the details of global corrective actions and preventive actions
   - The key elements of CAPA will be
     - Analysis of findings
     - Recommendation of third party auditors and inspection
     - Corrective action
     - Time table for CAPA
     - Identification of responsible persons
     - Procedures for monitoring the plan

    - Global CAPA for data reliability shall always strive to implement technological controls over procedural controls. The organization shall take advantage of the latest technologies and evolution thereof and move towards a zero-tolerance approach on data integrity

    - As part of CAPA, the site where data reliability issue has been observed shall describe the actions the site management responsible are taking or will take, such as contacting customers, recalling product, conducting additional testing and or adding measures to the stability programs to assure stability, monitoring of complaints, and other steps to assure quality of product manufactured under the violative conditions

    - In addition to CAPA, the site management will also be required to describe other actions, such as revision of procedures, implementation of new controls, training or re-training of personnel, etc., to prevent recurrence of CGMP violations, including breaches of data reliability, using the data governance plan discussed earlier in this Guideline

    - The organization shall take corrective action as required to confirm the accuracy, completeness and truthfulness of all the data and information contained in the submissions(s) and provide the regulatory authority with corrected or additional data or information as applicable

- **Data Reliability Remediation**

  - Remedial measures in relation to data reliability shall be designed with the objective of reconstructing the process through actual available records and reports, with the complete negation of any possibility of data falsification, omission, hiding and substitution

  - While carrying out remediation, a comprehensive remediation plan shall be prepared by the organization in order to carry out investigation based on actual and factual data to understand the probable root cause(s) of the problems, e.g. lack of awareness, intentional act, emphasis on quantity over quality, shortage of manpower, performance and business pressure, inadequate process and technology, lack of effectiveness of training or any other reason(s). Accordingly, the organization shall prepare the appropriate Corrective and Preventive Action (CAPA). There shall be full Management support to bring and enhance quality culture elements for building better data reliability culture

  - The organization shall be committed to voluntary remediation activities along with regulatory bodies in order to correct the problems through detailed examination of inefficient processes

  - Management approach and monitoring shall be driven by a zero-tolerance approach to data integrity

13. References

- FDA, Guidance May 2010, Compliance Program Guide 7346.832 Pre-Approval Inspections
- FDA, Guidance for Industry 21 CFR Part 11, August 2003, CFR part 211, 803. Electronic Records; Electronic Signatures – Scope and Application
- Health Canada Inspection Tracker, 2016, http://www.hc-sc.gc.ca/dhp-mps/pubs/compli-conform/tracker-suivi-eng.php
- ISPE FDA 3rd Annual GMP Conference, June 2014, Baltimore MD, USA: "FDA Perspective: Current Inspectional and Compliance Issues in Data Integrity." Carmelo Rosa
- Pharmaceutical Inspection Co-operation Scheme, Oct 2015, Guide to PE009-8: Chapter 4
- European Commission, Eudralex, 30 June 2011;"Computerized System", The rules governing medicinal products in the European Union, Vol. 04, GMP guideline, Annex 11
- Therapeutic Goods Administration; Australian Code GMP for human blood, blood components, human tissues and human cellular therapy products, Version 1.0,April 2013, Sections 400 – 415
- FDA/CDER/Office of Compliance presentation; March 2014, Karen Takahashi, Senior Policy Advisor
- ISPE; 2005; GAMP 5 (Good Automation Practices): Validation of Laboratory System
- ISPE; 2007; GAMP 5 (Good Automation Practices): Validation of Electronic Data Archiving
- MHRA, March 2015, GMP Data Integrity Definitions and Guidance for Industry
- MHRA, July 2016, GXP Data Integrity Definitions and Guidance for Industry, Draft Version for Consultation
- WHO, Sep 2015, Draft Guidance on Good Data Management Practices, QAS/15.624
- PDA, Sep 2015 Draft on Elements of Code of Conduct for Data Integrity in Pharmaceutical Industry, released
- WHO TRS 996, 2016, Annex 5, Guidance on Good Data and Record Management Practice
- FDA Draft Guidance, April 2016; Data Integrity and Compliance with CGMP Draft Guidance for the Industry
- Pharmaceutical Inspection Convention, 10 August 2016, P1 041-1 (Draft 2)
- European Medicines Agency, Aug 2016 (EMA) Good Manufacturing Practice (GMP) Guidance to ensure the Integrity of Data: Questions and Answers on GMP and Data Integrity

14. Abbreviations

- FDA: Food and Drug Administration
- MHRA: Medicines and Healthcare Product Regulatory Agency
- PQS: Pharmaceutical Quality System
- GMP: Good Manufacturing Practice
- SISPQ: Strength, Identity, Safety, Purity and Quality
- SME: Subject Matter Expert
- DRA: Data Reliability Assessment
- ICH: International Conference on Harmonization
- GLP: Good Laboratory Practice
- GCP: Good Clinical Practice
- IT: Information Technology
- LIMS: Laboratory Information Management System
- SAP: Systems, Applications, and Products
- WHO-NOC: World health Organization – Notice of Concern
- BMR: Batch Manufacturing Record
- BPR: Batch Packaging Record
- SOP: Standard Operating Procedure
- COTS: Computer Off-The-Shelf
- CFR: Code of Federal Regulations
- RPN: Risk Priority Number
- CAPA: Corrective Action and Preventive Action

15. Revision History

Revision No	Effective Date	Reason for Review	Remark (s)

Annexure 1:
Code of conduct for data reliability

Annexure 1

Code of conduct for data reliability

RESPONSIBILITIES OF AN EMPLOYEE RELATED TO DATA RELIABILITY

- Every employee has a duty to perform their GXP functions in an ethical manner that meet company requirements and industry standards as articulated in the company requirements, and in accordance with all relevant laws, regulations and legislative directives of regulatory authorities.
- Every employee is required to collect, analyze, report and retain information and data in a manner that accurately, truthfully and completely represents what actually occurred, in either paper or electronic format or both, in accordance with company policies and procedures and applicable laws.
- Every employee shall adhere to the requirements of the established documentation systems and are not permitted to record any data on unofficial, unauthorized or uncontrolled record.
- Employees must sign or initial on original records with date and time in a contemporaneous manner.
- Employees shall never record the signature or initials of another person or pre-date or back-date entries on any record.
- Employee shall not discard, destroy or modify the raw data or original records in any way.
- Employees who enter data or verify accuracy of data or perform other activities including GXP data shall contemporaneously enter data in accordance with established policies and procedures.
- Employees shall not engage in any conduct that calls into question the reliability of data (such as falsifying data, making unauthorized changes, destroying, deleting or over- writing data.)
- Employees who review or evaluate electronic data shall follow established procedures and verify that all relevant data and information have been included in relevant records and reports.
- Employees shall provide factual information about any incident or event for which he/she may have firsthand knowledge about what happened.
- Employees shall notify the Management if they become aware or have reason to suspect that others have falsified data, made unauthorized changes, caused destruction or have indulged in any other conduct that calls into question the integrity of data.
- An employee shall not delay, deny or limit access to records or refuse to permit inspection by duly authorized officials of regulatory authorities, except as may be specified in a written procedure.
- Every employee is responsible for his/her own conduct in order to maintain a bond of trust between the company and its stakeholders, namely the patients, health care providers and regulators.
- Employees shall have the option of reporting such issues anonymously if they so choose and if local laws permit.
- Employees shall notify responsible management of the company if they become aware of any potential data integrity issue regardless of its cause. This includes issues impacting data reliability such as those attributable to errors, omissions or wrongful acts.

Management:

Name:

Signature and Date:

Read and understood by:

Name:

Employee No.:

Signature and Date:

Annexure 2:
Pledge – Code of ethical quality conduct

Annexure 2

PLEDGE – CODE of ETHICAL QUALITY CONDUCT

We, at **XX,** believe that, being a manufacturer of health-care products, our foremost responsibility is to provide safe, efficacious and high quality medicines to our customers.

We acknowledge that ethical production, quality assurance and social responsibility are core values in our business. We agree to abide by **XX** Good Manufacturing Practices, Quality Management System and Ethical Practices such as honesty, truthfulness, integrity and transparency.

To ensure these, I, as an employee of **XX,** take a pledge that I shall

- Exercise the highest standards of moral and ethical behavior, honesty, objectivity, integrity and diligence in the performance of my duties and responsibilities.
- Adhere to the basic philosophy of the GMP system: "Document what you do, and do as per the approved documents".
- Ensure that the data produced by me are scientifically sound, real, authentic, accurately documented and not manipulated.
- Share information of my work, observations and knowledge gained with my seniors and colleagues, which may be useful for the investigation and understanding of root cause(s) of the problems (system and/or product failures) and in deriving appropriate Corrective Action and Preventive Action (CAPA).
- Ensure that all company records and documentation, regardless of their nature, shall be truthfully recorded and maintained in accordance with corporate and regulatory requirements.
- Ensure that all data for which I am responsible shall be recorded truthfully, promptly, completely and accurately, and I shall never distort or disguise the true nature of any action, procedure, or transaction.
- Ensure that I shall sign only properly supported documents that I have reason to believe are accurate and truthful.
- Accept that purposely false or misleading information related to test results, production records, maintenance records, raw material cards, cleaning logs, calibration records or any other records shall not be tolerated and such action(s) will result in termination and /or other legal action. There will be no exception and no one is allowed to order me or ask me to act otherwise.
- Abide by this Code and report any violation or apparent violation of this Code.
- Abide by and respond to any future needs of the organization in case of violation of this Code even after I have left the company.

Management:

Name:

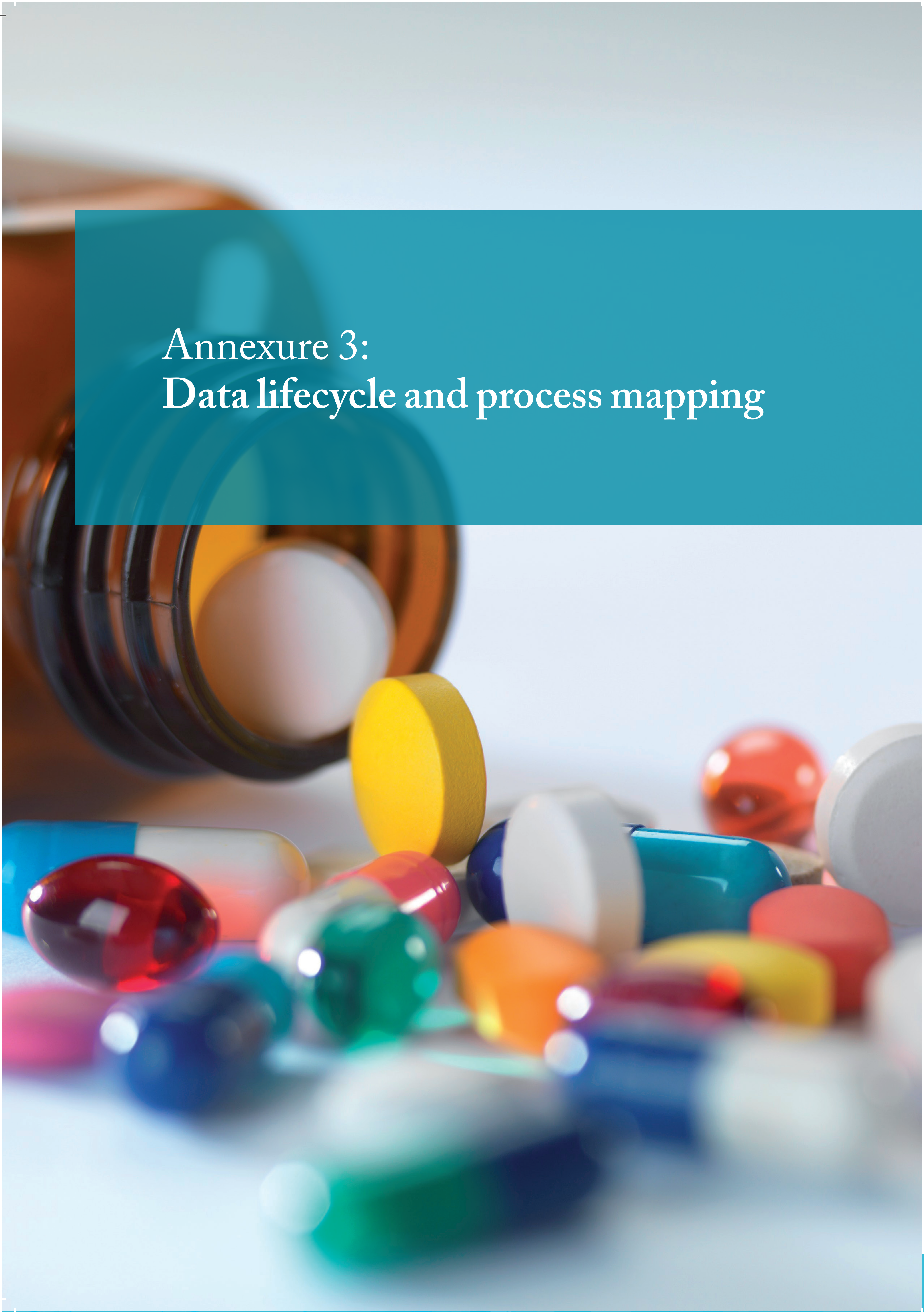
Signature and Date:

Read and understood by:

Name:

Employee No.:

Signature and Date:



Annexure 3:
Data lifecycle and process mapping

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

1 APPROVAL:

	Name	Designation & Department	Signature	Date
Prepared By				

	Name	Designation & Department	Signature	Date
Reviewed By				
Reviewed By				
Reviewed By				
Reviewed By				

	Name	Designation & Department	Signature	Date
Approved By				

2 DOCUMENT HISTORY:

Edition	Date		Author	Comments
01				

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

TABLE OF CONTENTS

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

3 Purpose of Data Lifecycle Pathway Mapping (DLPM):

The objective of this process mapping is to identify risks to data integrity in the current process of acquiring, processing, reviewing, and reporting from *receiving of material* to *final lubricated blend transfer to blend storage area* and to determine controls to mitigate and reduce data integrity risks. The outcomes of this mapping will include suggestions for redesigning the data process, including data flow and the associated business processes, as well as listing of residual risks and proposed frequency of review and monitoring of these risks to identify opportunities for continuous improvement.

4 Scope of Data Lifecycle Pathway Mapping:

The scope of this process mapping will be limited to the process *receiving of material* and *final lubricated blend transfer to blend storage area*. This protocol is limited to CHL facility.

5 Process Mapping Team Lead and Team Members:

Departments involved in Process Mapping	Name of person

6 Abbreviations/Definitions:

a)	NA	: Not Applicable
b)	QA	: Quality Assurance
c)	QC	: Quality Control
d)	SOP	: Standard Operating Procedure
e)	LOD	: Loss on drying
f)	LC	: Line clearance
g)	RMG	: Rapid Mixer Granulator
h)	FBP	: Fluidized Bed Processor
i)	HMI	: Human Machine Interface

7 Process description:

Granulation is a manual process wherein primary powder particles are made to adhere to form larger, multi-particle entities called granules. It is the process of collecting particles together by creating bonds between them. The granulation process is divided into two categories - wet granulation and dry granulation.

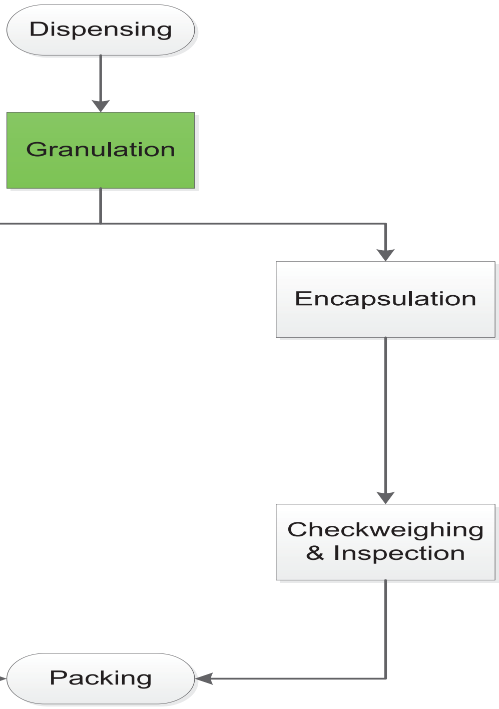
Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

8 Definition of Process Scope/Boundaries:

Process Start Boundary	Process End Boundary
Granulation plan from planner	Final lubricated blend transfer to blend storage area

9 Process Schematic and Description:



Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Granulation is a routine process and responsible associates are well-versed with the granulation activity.

Process Step	Description	Data involved in process	SOPs
1. Material received	• Check challan copy and other relevant documents. • Check the materials as per Checklist. • Material receipt observation report (SOP/ABC/ZZ). • Checklist for material receipt (SOP/ABC/ZZ). • Cross-verify the materials with vendor list, as per SOP/ABC/ZZ).	• Paper: Material receipt	• SOP/ABC/ZZ – Checklist generated through SAP Tcode ZMMCL by warehouse supervisor. • SOP/ABC/ZZ – Manual checklist filled.
2. Weighing and dedusting	• Dedust materials. • Physically weigh materials. • Generate weight slip(s). • Affix the weight label(s). • Generate label (s) for identification of materials.	• Paper/Electronic: Gross weight slip	• SOP/ABC/ZZ – Cleaning of equipment and area. • SOP/ABC/ZZ – Maintenance, calibration, cleaning and operation of balances. • SOP/ABC/ZZ – SOP for status label.
3. SAP entry	• Enter the material details into SAP. • Enter quantity per unit as per challan copy. • Enter actual quantity received/delivered. • Select storage location. • Allot mfg. date and exp. date as mentioned in COA; prepare GRS/GRN as per SOP (SOP/ABC/ZZ).	• Electronic: SAP entry	• SOP/ABC/ZZ – Usage and Entry in SAP. • SOP for preparation of GRN/GRS. • SOP/ABC/ZZ – Allotment for manufacturing and expiry dates.
4. Sampling	• QC person performs the sampling under sampling booth. • Record booth running time. • Record the DP and HEPA filter pressure. • Record RH/Temp and Environmental monitoring.	• Paper: Equipment cleaning checklist. • Paper: Equipment usage logbook • Paper: Area usage log book • Paper: Balance calibration logbook • Paper: Area cleaning logbook • Paper: Labeling on container	• SOP/ABC/ZZ – Sampling of RM. • SOP/ABC/ZZ – Cleaning of equipment and area. • SOP/ABC/ZZ – Maintenance, calibration, cleaning and operation of balances. • SOP/ABC/ZZ – Entries in log books. • SOP/ABC/ZZ – Cleaning of equipment. • SOP/ABC/ZZ – Recording of RH, Temp. and Humidity in log books.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
			• SOP/ABC/ZZ – Common status label. • SOP/ABC/ZZ – Good documentation practices. • SOP/ABC/ZZ – Status label on container "SAMPLED BY QC".
5. Manufacturing Plan	• Planner gives area wise granulation plan to granulation department through mail or hard copy. • Granulation shift in charge take a printout of area wise plan and affix to respective granulation area door for reference.	• Manual Plan /Printout	• SOP/ABC/ZZ – SOP for production. • Planning and circulation of plan for manufacturing of product.
6. Complete cleaning and balance calibration	• During the process: • Affix 'IN USE FOR' labels on the equipment. • After completion of process/ operation, remove the labels from the equipment. • Tear off labels and discard in dust bins. • Affix 'To be cleaned' label to equipment and change area status to 'TO BE CLEANED'. • Production executive to issue equipment cleaning checklist by taking printout or bound logbook from QA department. • QA person shall enter details in format issuance register. • Cleaning start and end times should be recorded in respective equipment log book and area cleaning logbook. • Cleaning should be done as per equipment cleaning checklist and recording of the same should be done online. • Some portable equipment and accessories should be cleaned in wash area and record of such cleaning activity should be recorded in wash area. • Cleaned labels attached to the respective equipment's and area status update as CLEANED after completion of cleaning. • After complete cleaning, calibration of the balances should be done as per frequency given in SOP and this	• Paper: Equipment cleaning checklist. • Paper: Equipment usage logbook. • Paper: Area usage log book. • Paper: Balance calibration logbook. • Paper: Area cleaning logbook. • Paper: Format issuance register. • Paper: Cleaning activity record. • Paper: 'To Be Cleaned' label • Paper: 'Cleaned' label.	• SOP/ABC/ZZ – Cleaning of equipment and area. • SOP/ABC/ZZ – Maintenance , Calibration, cleaning and Operation of Balances • SOP/ABC/ZZ – Entries in log books • SOP/ABC/ZZ – Cleaning of equipment. • SOP/ABC/ZZ – Recording on RH, Temp. and Humidity in log books. • SOP/ABC/ZZ – Common status label. • SOP/ABC/ZZ – Good documentation practices.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
	is to be recorded in respective balance calibration log books. • Daily cleaning of area should be done in first and second shift and this is to be entered into the area cleaning record. • Cleaning checklist should be attached to BMR. • During campaign manufacture for next batch, general cleaning of area and equipment should be done and the same recorded in area and equipment logbooks.		
7. Environmental conditions and pressure difference checking and recording	• Checking and recording of the temperature and relative humidity done by manual writing in BMR from digital or manual hygrometer present in area. • Checking of pressure difference of area done from differential pressure gauge reading outside the door of area at the time of line clearance. • During processing, temperature and relative humidity checking and recording done manually as per frequency given in BMR. • Minimum and maximum temperature and humidity recording of R.M. Day Store, Batch Staging, Tablet Hold, by manual recording in format from digital display.	• Paper: Batch Manufacturing Record (BMR). • Paper: Environmental Monitoring Record • Paper – Minimum and maximum temperature and humidity record.	• SOP/ABC/ZZ – Environmental monitoring (temperature, humidity, pressure differential). • SOP/ABC/ZZ – Good Documentation Practices.
8. Line Clearance of area & equipment	• Production executive shall issue line clearance checklist from QA. • QA person shall enter details in document issuance register. • Production technical supervisor shall fill the checklist and check cleanliness against checklist. • Production and QA persons shall check the area and equipment and sign on line clearance checklist. • 'Cleaned' label should be torn off and 'IN USE FOR' label should be affixed.	• Paper: Batch Manufacturing Record. • Paper: Equipment usage logbook. • Paper: Line clearance checklist. • Paper: Label generation.	• SOP/ABC/ZZ – Line clearance of area and equipment. • SOP/ABC/ZZ – Filling the area and equipment log books. • SOP/ABC/ZZ – Issuance of checklist and entry into inward register. • SOP/ABC/ZZ – Label status generation.
9. Material verification	• Operator takes material from dispensed material staging area. • If balance of required capacity is available in area then verification of dispensed material done inside the granulation area and if balance not available in area then verification	• Paper: Batch Manufacturing Record. • Paper: Dispensing label.	• SOP/ABC/ZZ – Entries in logbook (balance usage logbook, entry-exit of material in area) • SOP/ABC/ZZ – Filling of document.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
	done outside the area like in front of production office. • Verification of material is done by cross checking the product details on label with BMR & dispensed material weight or dispensed label with weight written in BMR in presence of production technical supervisor. • Executive checks the material and signs in 'Verified by' column in BMR.		
10. Sifting/ Sizing	• Sifting/sizing done by using sifter. • Before start of sifting activity, sieve integrity should be checked visually and recorded in BMR. • As per sequence given in BMR, sifting of material to be done by manual loading of material on sifter or with the help of elevator if material is in IBC. • After completion of sifting, sieve integrity should be checked again and recorded in BMR. • Recording of sifting start and end times done in BMR and logbook. • If sieve integrity fails to meet the acceptance criteria, then 'Reject' label is to be affixed to sieve and sieve scrap transfer note is filled up, and sieve is transferred to scrap room. • Select the sieve (mesh) size.	• Paper: Batch Manufacturing Record. • Paper: Equipment usage logbook. • Paper: Area usage log book.	• SOP/ABC/ZZ – Filling of Document. SOP/ABC/ZZ – Issuance, use and filling of Log Books. • SOP/ABC/ZZ – Operation, cleaning and maintenance of vibratory/mechanical sifter. • SOP/ABC/ZZ – Filling of logbooks (area equipment, RH, Temp., humidity, etc.). • SOP/ABC/ZZ – Checking of integrity of sieve (mesh).
11. Premixing	• Production associate loads the material in bin blender and transfers the bin to blending area. • Production associate places the bin inside the cage of bin blender and set the blending speed (Fast/slow) and time as per BMR. • Blender starts in auto mode in front of supervisor and start time is recorded in BMR and log book. • After completion of blending activity, blender automatically stops and end time is recorded in BMR & blender log book.	• Paper: Batch Manufacturing Record. • Paper: Equipment usage logbook.	• SOP/ABC/ZZ – Operation, cleaning and maintenance of blender. • SOP/ABC/ZZ – Filling document. • SOP/ABC/ZZ – Entries into log book (area, equipment, environmental sequential logbooks). • SOP/ABC/ZZ – Status labeling. • SOP/ABC/ZZ – Line clearance in respective area.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
12. Compaction	• Bin containing premixed material loaded in hopper of roll compactor. • Production associate sets roller speed, feeder speed and other parameters as per BMR and records them in BMR. Production supervisor shall verify and sign on BMR. • Start time and end times of compaction activity recorded in BMR and equipment log book from wall clock. • During compaction in process, recording done as per frequency given in BMR by production associate; production supervisor checks this and signs on BMR.	• Paper: Batch Manufacturing Record. • Paper: Equipment usage logbook. • Electronic data: PLC setting.	• SOP/ABC/ZZ – Filling of document. • SOP/ABC/ZZ – Operation, cleaning and maintenance of roller compactor. • SOP/ABC/ZZ – SOP for access into PLC software and level of security. • SOP/ABC/ZZ – Filling of area, equipment log books.
13. Binder/ Slurry/ Solution preparation	• Binder/slurry or solutions like drug loading solution, sub coating solution, barrier coating solution, enteric coating solution are prepared by using overhead stirrer, homogenizer or in binder preparation vessel. • The quantity of purified water required for process is collected in a vessel and weighed in balance. Weight is manually recorded in BMR from balance display or printout is attached with signature and date. • Water A.R. No. is recorded in BMR from water A.R. No. file maintained in production office. • As per specification of BMR, settings in HMI of stirrer or homogenizer and speed and time are recorded manually in BMR and logbook.	• Paper: Batch Manufacturing Record. • Paper: Equipment usage logbook • Paper: Water A.R. No. file.	• SOP/ABC/ZZ – Operation, cleaning and maintenance of stirrer/mechanical stirrer. • SOP/ABC/ZZ – Operation, cleaning and maintenance of homogenizer. • SOP/ABC/ZZ – Filling document. • SOP/ABC/ZZ – Filling of area, equipment log books. • SOP/ABC/ZZ – Addition of water during binder preparation.
14. Wet Granulation	• Operator logs into HMI of RMG/FBD in level 1. • As per BMR specification, parameter settings are done in RMG or FBP. • Operation of RMG is done for time given in BMR for different steps and time monitoring is done from wall clock. Recording of start time and end time are done in BMR from wall clock reading to BMR.	• Paper: Batch Manufacturing Recording. • Paper: Equipment logbook. • Paper: Machine printouts.	• SOP/ABC/ZZ – Filling of document. SOP/ABC/ZZ – Issuance, use and filling of log book. • SOP/ABC/ZZ – Operation, cleaning and maintenance of FBD/FBP/FBC. • SOP/ABC/ZZ – Operation, cleaning

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
	• Observed machine parameters are recorded in BMR manually from HMI display to BMR. • During operation of FBP, online parameter print is generated as per frequency set. At the end of operation, operator will check this print against BMR specification and will attach it to BMR after his signature. • Production executive will verify and check the granulation activity as per BMR instructions and sign this into BMR & log book. • Recording of start and end time is done manually in BMR and log book from wall clock.		and maintenance of RMG. • SOP/ABC/ZZ – Filling of area, equipment usage logbook.
15. Milling/ Screening	• Milling/screening of material is done by multi mill, comminuting mill, colloid mill, hammer mill, ball mill, co mill, and/or oscillating granulator. • Speed of operation and screen size are fixed as per parameter given in BMR. • Milling start time, end time, speed, screen size, screen ID, and screen integrity are recorded manually in BMR and log book.	• Paper: Batch Manufacturing Record. • Paper: Equipment usage logbook. • Paper: Screen inventory record.	• SOP/ABC/ZZ – Operation, cleaning and maintenance of equipment. • SOP/ABC/ZZ – Filling of document. • SOP/ABC/ZZ – Filling of area, equipment usage logbook. • SOP/ABC/ZZ – Specification, checks and storage of screen.
16. Drying of granules	• Drying of granules is done by using FBD. • Operator logs into HMI of FBD in level 1. • As per BMR specifications, inlet temp., exhaust temp., product temp., drive speed and % flap opening are sets in HMI of FBD. • Supervisor logs into HMI of FBD in level 2 and sets minimum and maximum parameters as per BMR for inlet temperature, product temperature and exhaust temperature. • As per frequency given in BMR, production associate records drying parameter from HMI of FBD to BMR, either manually or using print-outs. • Manual recording of drying start and end time are done in BMR and log book from wall clock.	• Paper: Batch Manufacturing Record. • Paper: Equipment logbook. • Paper: Machine printouts.	• SOP/ABC/ZZ – Filling of document. • SOP/ABC/ZZ – Filling of area, equipment usage logbook. • SOP/ABC/ZZ – Operation, cleaning and maintenance of equipment. • SOP/ABC/ZZ – Operation, cleaning of finger beg. • SOP/ABC/ZZ – Operation of printer attached to the FBD.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
	• During operation of FBD, online parameter print is generated as per frequency set. At the end of operation, operator checks this print against BMR specifications and signs it and then attaches it to BMR. • Production executive verifies or checks the activity as per BMR instructions, and signs in BMR and log book.		
17. Blending & lubrication	• Blending and lubrication is done in cage bin blender. • Quantity of lubricant to be added is calculated on the basis of yield of blend. • Production technical assistance logs into HMI of blender and sets the blending speed (fast/ slow) and time as per BMR. • Blender starts in auto mode in front of supervisor and start time is recorded from wall clock to BMR and log book. • After completion of blending activity, blender automatically stops and end time is recorded manually from wall clock to BMR and blender log book.	• Paper: Batch Manufacturing Record. • Paper: Equipment logbook.	• SOP/ABC/ZZ – Operation, cleaning and maintenance of equipment. • SOP/ABC/ZZ – Filling of document. • SOP/ABC/ZZ – Filling of area, equipment usage logbook.
18. Sampling	• As per specification, QA makes label in ExcelTM sheets and prints them on sticker label and attaches to glass vials. • Cleaned sampling rod is taken from respective area and according to sampling quantity, die selection is done. • When blend is ready for sampling, operator informs QA to proceed for sampling. • QA takes sample of blend by using sampling rod and records sampling details in log book of sampling rod and in BMR. • After sampling, QA records sample quantity in BMR and signs on sample.	• Paper: Batch Manufacturing Record. • Paper: Equipment logbook. • Paper: Sampling plan. • Paper: Request analysis.	• SOP/ABC/ZZ – Usage of sampling rod. • SOP/ABC/ZZ – Sampling procedure (collection of sample from blender). • SOP/ABC/ZZ – Selection of rod and die for sampling. • SOP/ABC/ZZ – Cleaning and maintenance of sampling rod and dies. •
19. Weighing and unloading of lubricated blend	• Weighing of lubricated blend is done on balance and recording is done manually from balance. The 'In Process' status label is displayed and recorded in BMR by operator.	• Paper: Batch Manufacturing Record. • Paper: 'In process' label.	• SOP/ABC/ZZ – Unloading of materials. • SOP/ABC/ZZ – Usage and issuance of poly

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
	• Production technical assistance cross checks weighing and product details on 'In process' label and signs on 'In process' label and BMR. • Unloading of blend is done in double-lined poly bag or triple-laminated aluminum bag and a silica bag is placed in between two poly bags if such an instruction is given in BMR. • 'In process' label is placed in between two poly bags, and one label is attached on aluminum bag with product details and weighing details on label. • Sealing of bag is done as per instructions given in BMR. • Recording of weighing details is done manually from balance display to BMR.	• Paper: Use of balance.	bag/triple-laminated aluminum bag. • SOP/ABC/ZZ – Status labeling. • SOP/ABC/ZZ – Weighing of materials. • SOP/ABC/ZZ – Usage of balance.
20. Yield reconciliation	• After completion of granulation activity or in between different stages of granulation, production executive does yield reconciliation by calculating actual yield against theoretical batch size and records it in BMR. • Second production executive cross checks yield reconciliation and signs in 'Checked By' column of BMR.	• Paper: Batch Manufacturing Record.	• SOP/ABC/ZZ – Filling of document.
21. Sieve receipt, inventory, usage and disposal	• After receiving new sieve mesh size, diameter, silicon molding/ bonding quality, dent, integrity, MOC and coding details are checked manually and recorded in new sieve receipt & certification checklist. • Cleaning of new sieve is done in wash area and this is recorded in cleaning activity record. • If any sieve fails to meet integrity or any other defect during inventory checking, the same is disposed by recording details on sieve scrap transfer note and the sieve is transferred to scrap yard.	• Paper: New sieves receipt and certification checklist. • Paper: Cleaning activity record. • Paper: Sieve inventory record. • Paper: Sieve scrap transfer note.	• SOP/ABC/ZZ – Checks integrity and storage of sieves.
22. Finger bag/ Filter bag Control &	• After receiving new finger bag, physical parameters are checked	• Paper: New filter bag receipt checklist.	• SOP/ABC/ZZ – Usage of filter bag.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Process Step	Description	Data involved in process	SOPs
integrity Checking	and recorded in New Filter Bag Receipt Checklist. • Coding of filter bag is done. • Cleaning of filter bag is done. • Filter bag issuance and usage details are recorded in Filter Bag Usage Record. • If the filter bag fails to meet integrity or it completes three year of usage, it is disposed of and this is recorded by a written remark on New Filter Bag Receipt Checklist.	• Paper: Filter bag usage record. • Paper: Inventory record for FBP/FBD filter bags.	• SOP/ABC/ZZ – Handling, checking and cleaning of filter bag. • SOP/ABC/ZZ – Destruction of finger/filter bag.
23. Calibration of IPQC instrument	• Moisture balance: • Calibration of moisture balance is done on a daily basis. • Daily calibration is done as per SOP and calibration printouts are taken and attached to file; recordings are also done in log book titled 'Internal Calibration and Weight check of Moisture Analyzer'. • Calibrations are done by external agency for weight and temperature as per schedule. Certificates of calibration are provided by external agency and same are archived.	• Paper: Log book of internal calibration and weight check of moisture analyzer. • Paper: Calibration printouts. • Paper: Calibration certificates.	• SOP/ABC/ZZ — Operation, cleaning, maintenance and calibration of Moisture Analyzer.

9.5 Process Flow Diagram:

Refer Annexure 3a: Probability of errors generated from various data generation sources and its mitigation plan.

Refer Annexure 3b: Manufacturing Process Flow Diagram.

10 Questions to be considered for Data Integrity:

Sr. No.	Critical thinking questions
1	Does the process involve electronic/paper data? Is the data Attributable/Legible and permanent/Contemporaneous/Original (or True copy)/Accurate (ALCOA)?
2	Does the process have a standard operating procedure?
3	Is the data reviewed?
4	Is data review part of an existing SOP?
5	Is there training for data review?
6	Is there training for data entry in GMP documents?
7	Is the process operated and/or controlled manually, automatically or both?
8	Is the data created during the process manual or electronic?
9	Is there any control over blank paper templates for data recording?
10	Is the recording of date/time manual or electronic?

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

11	Are the time/date settings in restricted control?
12	Is issuance and archival of document in control?
13	Is the electronic record/electronic signature of the process relevant?
14	Is the system validated for its intended purpose?
15	Have the functions of the computerized system along with the process been taken into consideration?
16	What part of the system has been validated by the relevant team of the organization or by/from the vendor validation package?
17	Is the backup/restore system automated or manual?
18	Is the backup/restore system adequate and periodically verified?
19	Does the backup include the transaction log/system audit trail?
20	Is the archiving process adequate and periodically checked?
21	Is the archiving processes verified to ensure that the record content is preserved?
22	Is the archiving process secure and does it include audit trail where relevant? (Is the audit trail data archived together with the current data?)
23	Is there a periodic exercise of retrieval (or verification) processes to verify their continuing operations?
24	Is the archiving foreseen for the whole retention period? (Does this also include the backup of the system audit trails?)
25	Is the hardware/software secure and do they comply with the CFR standards?
26	Are the operating systems and/or application software up-to-date with latest versions and security patches?
27	Has it been verified that the hardware and software do not allow uncontrolled access (e.g. open ports, generic users, blank passwords, etc.)?
28	For complex systems, does the system capture "transactions" (i.e. important operations) with an electronic signature that captures the metadata (i.e. user name, date, and time)? (In Manufacturing Execution Systems (MES), an electronic signature is often required by the system in order for the record to be saved and become permanent).
29	Is the electronic data reviewed?
30	Is data review (including electronic data, meta data, and audit trail review) part of an existing SOP?
31	Is there training for electronic data review?
32	Does the review of electronic data include meaningful meta data (data that describe the attributes of other data, and provide context and meaning)?
33	Have the critical meta data been identified?
34	Is an automatic data capture machine or a printer attached to the equipment?
35	Can the print-out be considered the raw data?
36	Is all the relevant data printed, or are there important information for data integrity such as date and time that are added manually?
37	Will the print-out be available for the whole lifecycle (e.g., since thermal prints fade with time, are other alternatives provided for in the process)?
38	When there is meta-data in the system (e.g., configuration settings or "recipes" on manufacturing equipment) are they validated and "locked"?
39	Is there proper segregation of duties in the system (with separate access)?
40	How many administrators have rights in the system?
41	Is access to equipment/instrument settings restricted to a number of administrators commensurate with the number of end users and/or complexity of the system to prevent intentional or accidental alteration of quality parameters?

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

42	Are administrator rights limited to individuals with no “conflict of interest”? System Administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) should not be assigned to individuals with a direct interest in the data (data generation, data review or approval).
43	Is there access to the clock of the system? Is the clock automatically updated when time changes?
44	If the system has an audit trail, is there an audit trail review of “relevant” audit trail (with GXP relevance such as data creation, processing, modification and deletion, etc.)?
45	Is there a mechanism to confirm that a review of the audit trail has taken place?
46	If the system does not have an audit trail, is there a “paper” system (e.g., equipment log) to demonstrate that changes to data have been permitted until a fully audit-trailed system (integrated system or independent audit software using a validated interface) becomes available?
47	Is there a process to review “critical” data (including meta-data)?
48	What are the different access levels and to who are they granted? Is there a potential conflict of interest?
49	Are there shared logins?
50	Does the operator/analyst have access only to his/her assigned tasks?
51	If the system does have an audit trail, does it capture the relevant information depending on the complexity/simplicity of the system? Is there traceability of changes to relevant data, timestamp and a reason provided?
52	Has the possibility of the application of deleting, changing or disabling the audit trail been verified?
53	Has the level of access that can delete, change, or disable the audit trail been verified?
54	Has it been verified if the application has any possibility of changing security settings or if they are “locked” after the validation?
55	Has it been verified if a change in configuration settings is reflected in the audit trail?
56	Has the level of access that can delete or change the configuration settings/recipes been verified?

11 Process Inputs:

- Batch Manufacturing Record.
- SOP.

12 Process Dependencies:

- Batch Manufacturing Record.
- SOP.

13 Process Outputs:

- Executed Batch Manufacturing Record.
- Equipment log book.
- Environmental conditions and pressure difference checking and recording format.
- Line clearance checklist.
- In-process control recording formats.
- Sieve receipt, inventory, usage and disposal record.
- Finger bag/Filter bag control and integrity checking record.
- Batch Report and its electronic data.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

14 Critical Data and Metadata:

Critical Data	Meta Data
Batch Manufacturing record	Standard operating procedure(s), equipment/systems usage log, equipment print outs.
Recipe	Audit trail, system in/out log.
Electronic record: Batch Report	Audit trail, system in/out log, alarm log, system usage log.
Environmental conditions and pressure difference record	Area usage log book
Line clearance checklist	Area cleaning log book.
In-process control record	Equipment log book for IPQC instrument and its calibration record.
NA	Time monitoring of clock and HMI of equipment.
NA	Finger bag/Filter bag control & integrity checking record.
NA	Sieve receipt, inventory, usage and disposal records.
NA	Backup data of electronic system.

15 Records Management Flow Description:

Record Type: **Electronic records**	
Process Step	**Description**
Acquire Data	Backup data of electronic system.
Transfer Data	Backup.
Storage and Retrieval of Data	Server.

Record Type: **Batch records (Manual)**	
Process Step	**Description**
Acquire Data	• Recording of environmental condition details in BMR from digital or manual hygrometer present inside the area. • Equipment start and end times recorded from wall clock. • Product parameter recorded from HMI display of machine to BMR.
Transfer Data	Hand over to QA.
Storage and Retrieval of Data	Archive in document cell by QA, retrieval on request.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

Record Type: **Formats**	
Process Step	**Description**
Acquire Data	• Checking and recording of the temperature and relative humidity done by manual writing on Environmental Monitoring Record and minimum/maximum temperature and humidity record from digital or manual hygrometer. • Line clearance checklist is used for checking and recording of cleanliness of area and equipment and calibration status of balance. • Sieve receipt, inventory, usage and disposal. • Finger bag/Filter bag control and integrity checking.
Transfer Data	Attached to BMR. Transfer to document storage room.
Storage and Retrieval of Data	Some formats are attached to BMR and archived with QA document cell. Other formats are archived in production Document Room.

Record Type: **Instrument printout / output data**	
Process Step	**Description**
Acquire Data	• Product parameter printed on machine printouts. • In process result of LOD printed on LOD printouts.
Transfer Data	Attached to BMR.
Storage and Retrieval of Data	Archive with QA with BMR.

Record Type: **Log books**	
Process Step	**Description**
Acquire Data	• Equipment start and end times recording done from wall clock. • Product name and batch number recorded from BMR. • Area and equipment cleaning details. • Calibration details of balance and equipment. • In format issuance log book, recording are done for details for which format is issued, with unique number. • In cleaning activity log book and area cleaning log book, details of cleaning are recorded.
Transfer Data	• From log book, manual recording of previous batch details done on equipment cleaning checklist, line clearance checklist, BMR and labels.
Storage and Retrieval of Data	• Document Room.

16 Risk Assessment Mitigation and Evaluation

Methodology

- Identify all risks and failure effects associated with the process steps:
  There may be more than one failure mode or failure effect for each process step. Once all failure modes have been identified the scoring can take place to allow ranking of the risks.
- Score the failure modes and effects by severity of the risk, and the ease of which it would be detected.
- Justify the ranking

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

FMEA Model (Example 1)

Sr. No.	Process Step/Unit Operation /Item	Failure/ Unwanted Event	SEV (S)	Cause/ Process Failure	OCC (O)	Current Controls	DET (D)	RPN (S×O×D)	Risk Accepted? (Yes/No)	Recommended Actions/ CAPA	Ranking after actions			
											SEV	**OCC**	**DET**	**RPN**
(a)	**(b)**	**(c)**	**(d)**	**(e)**	**(f)**	**(g)**	**(h)**	**(i)**	**(j)**	**(k)**	**(l)**			

(a) **Sr. No.:** This is sequential number.

(b) **Process Step/Unit Operation/Item:** The process step being evaluated should be listed. The process map, SOPs, supplier document or batch records can provide this information. The team should determine how detailed this information should be in order to facilitate the assessment.

(c) **Failure/Unwanted Event:** Potential or identified failure or unwanted event should be mentioned.

(d) **SEV – Severity (S):** A severity value should be assigned by determining the severity of the failure or unwanted event in relation to patient safety.

(e) **Cause/Process Failure:** Potential causes of failures should be listed. A cause is an unknown or a foreseeable failure associated with the said process. There may be multiple causes for each failure type; therefore, they should be listed individually, since they will be evaluated separately.

(f) **OCC – Occurrence (O):** An occurrence value should be assigned by determining the likelihood that the cause of failure will take place. Historical or empirical data should be used where possible (e.g. process capability data) to estimate this value.

(g) **Current Controls:** The existing procedural or design controls that detect, reduce or eliminate the cause of failure from occurring should be listed. The controls in place should be considered when determining the detection ranking. If there are no controls, the likelihood of detection is low, resulting in a high-risk ranking.

(h) **DET-Detectability (D):** A detectability value should be assigned by determining the detectability of the cause. Detectability is important because it facilitates the identification and correction of failures before the cause can harm the patient. If the event cannot be detected, then the occurrence and severity have to be low. It is very important to be as objective as possible in ranking the likelihood of detection. Historical or empirical data should be used where possible. The ranking system for Detectability is the reverse of the Severity and Occurrence rankings. A high detectability has a low ranking.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

FMEA Model (Example 1 continued)

Score for S, O & D:

SEVERITY		
Level	**Patient Effect**	**Process Effect**
10	Patient gets affected fatally.	Irreparable damage to batch/product. Product quality attributes are affected. Possible regulatory deficiency/customer query.
7	Patient is not affected fatally but deemed efficacy is not achieved. However, the effect is not noticeable.	Reprocessing is possible without affecting the quality attributes.
4	Patient is not affected fatally but deemed efficacy is not achieved. However, the effect is noticeable and manageable.	Manufacturing related deviations not affecting the quality of the product.
1	No impact on patient.	No impact on Process and Quality.
PROBABILITY OF OCCURRENCE		
Level	**Design**	**Process**
10	Certainty: availability of prior knowledge, information, reference that the phenomenon shall occur.	Probability of occurrence high.
7	Uncertainty: No information available, but there exists the possibility of surprise or unexpected results.	Significant probability of occurrence.
4	Uncertainty: No information available but further study is necessary.	Remote probability of occurrence.
1	Availability of prior information indicating that the phenomenon shall NOT occur.	Virtually no probability of occurrence.
DETECTION		
Level	**Process Control**	**Analytical Control**
10	In-process checks/parameters/systems/ procedural controls are not available.	No analytical technique/procedure is available.
7	In-process parameters/procedural controls to be established.	Qualitative detection technique to be implemented.
4	In-process parameters/procedural controls to be established.	Quantitative detection technique to be implemented.
1	In-process test/checks/parameters/systems are available.	Multiple analytical tests support detection/measurement of required attributes.

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

- Scoring for S, O and D shall be done on a scale of 10. [1 is considered as least-to-no risk and 10 as the highest risk. The possible score in this range can range from 1 (1 x 1 x 1) to 1000 (10 x 10 x 10). Since 1 represents the least-to-no risk state, minimal risk score can be 3].
- Values in the table are indicative. If required, the scale can be expanded within the range of 1 – 10.

FMEA Model (Example 1 concluded)

Acceptance Criteria (Risk Acceptability Decision):

Significance of Risk Priority Number (RPN = S x O x D)			
Risk priority number	**Nature of impact**	**Acceptance criteria**	**Mitigation (action/status)**
1-100	No impact	Fine	No mitigation is required since it is a residual risk.
101-199	Indirect impact	Mediate	Mitigation shall be done.
More than 200	Direct Impact	Cease	This is to be resolved with appropriate action.

Note: *The approach mentioned above is an illustration. For individual risk assessment, risk description, tools and acceptance criteria should be defined in advance. Caution should be used when prioritizing risks or areas for remediation on just the RPN number. For example, a process step that has 10 for severity, 10 for occurrence, and 1 for detection does not really have the same level of risk as a process step that has 10 for severity, 1 for occurrence, and 10 for detection although they both have the same RPN.*

Annexure 3

REFERENCE PROTOCOL for DATA LIFECYCLE PROCESS MAPPING for MANUFACTURING STAGE: GRANULATION

17 SUMMARY & CONCLUSIONS:

Data Lifecycle Pathway Mapping for "RECEIVING OF MATERIALS TO GRANULATION" process should be performed as per pre-defined protocol, and the mapping should be done for this process with the individual documents involved in the process from start point to end point.

Process steps, descriptions, data involved in process, SOPs, etc. should be reviewed against the mapping.

In addition, as far as the equipment involved in granulation process are concerned, it is possible that some of the equipment generate electronic data, while some are stand-alone systems. It is suggested that a separate data lifecycle process mapping should be performed for the stand-alone system available at Production Department.

Brainstorming sessions shall also be conducted to evaluate and/or address the process gaps with the cross functional trained SMEs.

Finally, after identifying gaps, FMEA (Failure Mode Effective Analysis) shall be performed to identify the critical priorities and appropriate actions that should be taken. The same will be implemented for the better compliance with respect to the granulation process.

Refer also to Annexure 3a – Probability of errors generated from various data generation sources and its mitigation plan, and Annexure 3b – Manufacturing Process Flow Diagram.

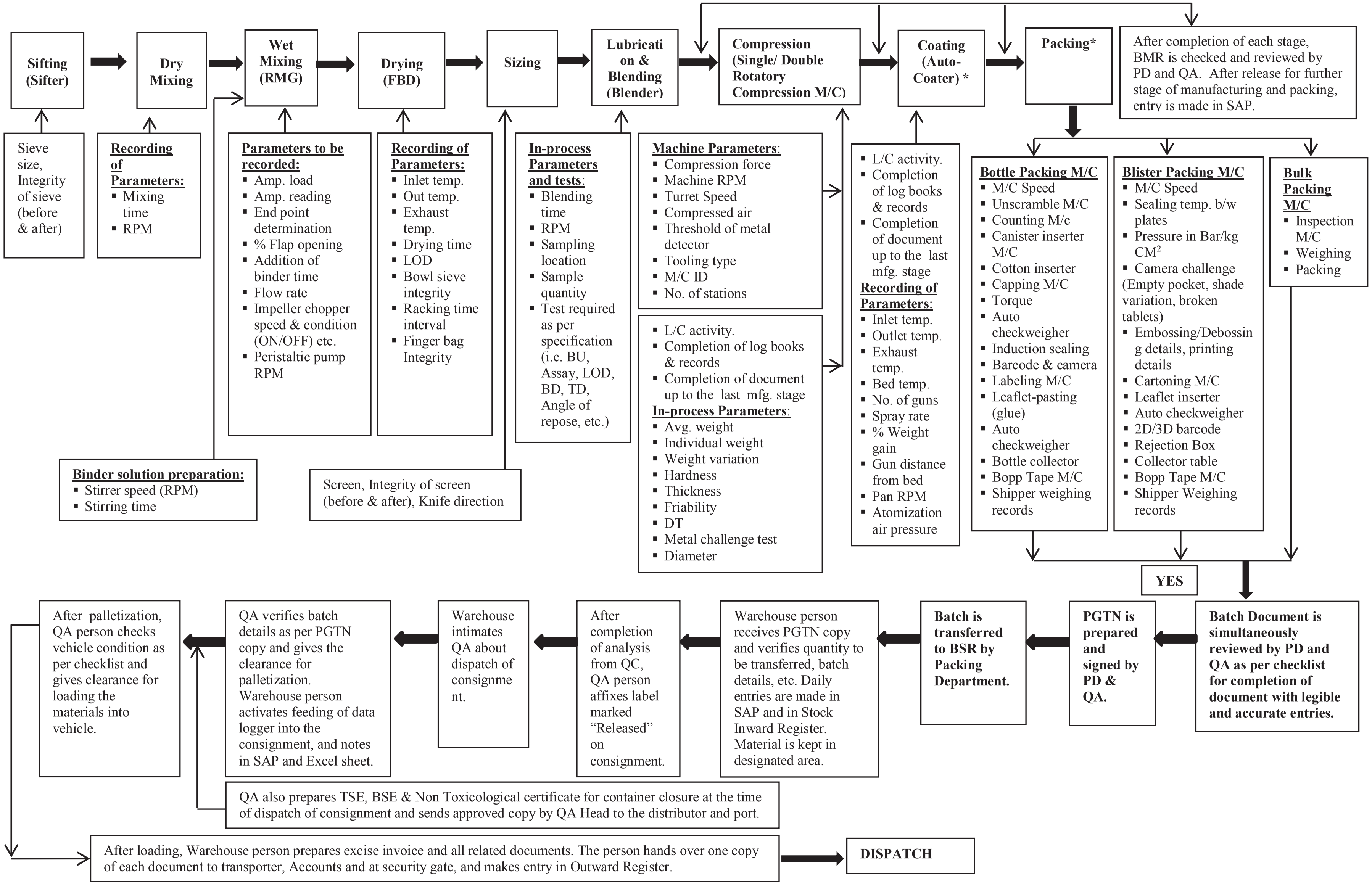
Annexure 3a

PROBABILITY of ERRORS GENERATED from various DATA GENERATION SOURCES and MITIGATION PLANS

Sources of Data Generation	Probability of Errors	Mitigation Plan
From recording	Human error; wrong data.	Read and record; data should be recorded contemporaneously and verified by a second person.
From writing	Incomplete information; wrong interpretation; illegible; misunderstanding; incorrect way of presentation; prescribed documentation practices not followed.	Raw data should be maintained; data should be verified by a second person.
From manual feeding	Entries made in wrong places; entries not contemporaneous; human error; data not readable.	A second person should verify the feed data.
From transcriptions	Data not readable; data transcribed incorrectly.	Transcribed data should be verified against original data.
Oral sources	Wrong interpretation.	Investigation should be reviewed by SME.
By measurement	Human error; manual measurement reading and recording; measurement equipment not calibrated.	Cross-verification by a second person at the same time should be done; digital measuring devices should be made available.
Electronic data	Not synchronized with equipment or global clock.	Regular calibration should be done.
From statistics or analytics	Feeding of data may be wrong due to manual entry.	The entered data should be verified by a second person, and the verified data should be entered into a validated sheet.
By electronic scanning	No barcode detection or smudging of barcode line.	The data should be verified by a second person. The earlier record should be destroyed to prevent confusion.
By printing	Inappropriate printing; printing not legible.	A second person should verify the printed data.
From barcode details	Barcodes incorrect; incorrectly placed, illegible, or incorrectly transcribed.	Second person verification should be done.
From visual scanning	Seeing and recording error.	This should be verified by a second person.
From videography footage	Recordings not checked regularly; over-writing.	Verification of review, including settings of cameras should be done.
From drawings	Layout design, shape and size.	Sources should be approved and authenticated, and accompanied by clear instructions.

Annexure 3b

MONITORING of MANUFACTURING PROCESS and RECORDING of PROCESS PARAMETERS with their QUALITY ATTRIBUTES



Sifting (Sifter) → **Dry Mixing** → **Wet Mixing (RMG)** → **Drying (FBD)** → **Sizing** → **Lubrication & Blending (Blender)** → **Compression (Single/ Double Rotatory Compression M/C)** → **Coating (Auto-Coater) *** → **Packing***

After completion of each stage, BMR is checked and reviewed by PD and QA. After release for further stage of manufacturing and packing, entry is made in SAP.

Sieve size, Integrity of sieve (before & after)

Recording of Parameters:
- Mixing time
- RPM

Parameters to be recorded:
- Amp. load
- Amp. reading
- End point determination
- % Flap opening
- Addition of binder time
- Flow rate
- Impeller chopper speed & condition (ON/OFF) etc.
- Peristaltic pump RPM

Binder solution preparation:
- Stirrer speed (RPM)
- Stirring time

Recording of Parameters:
- Inlet temp.
- Out temp.
- Exhaust temp.
- Drying time
- LOD
- Bowl sieve integrity
- Racking time interval
- Finger bag Integrity

Screen, Integrity of screen (before & after), Knife direction

In-process Parameters and tests:
- Blending time
- RPM
- Sampling location
- Sample quantity
- Test required as per specification (i.e. BU, Assay, LOD, BD, TD, Angle of repose, etc.)

Machine Parameters:
- Compression force
- Machine RPM
- Turret Speed
- Compressed air
- Threshold of metal detector
- Tooling type
- M/C ID
- No. of stations

- L/C activity.
- Completion of log books & records
- Completion of document up to the last mfg. stage

In-process Parameters:
- Avg. weight
- Individual weight
- Weight variation
- Hardness
- Thickness
- Friability
- DT
- Metal challenge test
- Diameter

- L/C activity.
- Completion of log books & records
- Completion of document up to the last mfg. stage

Recording of Parameters:
- Inlet temp.
- Outlet temp.
- Exhaust temp.
- Bed temp.
- No. of guns
- Spray rate
- % Weight gain
- Gun distance from bed
- Pan RPM
- Atomization air pressure

Bottle Packing M/C
- M/C Speed
- Unscramble M/C
- Counting M/c
- Canister inserter M/C
- Cotton inserter
- Capping M/C
- Torque
- Auto checkweigher
- Induction sealing
- Barcode & camera
- Labeling M/C
- Leaflet-pasting (glue)
- Auto checkweigher
- Bottle collector
- Bopp Tape M/C
- Shipper weighing records

Blister Packing M/C
- M/C Speed
- Sealing temp. b/w plates
- Pressure in Bar/kg CM^2
- Camera challenge (Empty pocket, shade variation, broken tablets)
- Embossing/Debossing details, printing details
- Cartoning M/C
- Leaflet inserter
- Auto checkweigher
- 2D/3D barcode
- Rejection Box
- Collector table
- Bopp Tape M/C
- Shipper Weighing records

Bulk Packing M/C
- Inspection M/C
- Weighing
- Packing

YES

Batch Document is simultaneously reviewed by PD and QA as per checklist for completion of document with legible and accurate entries.

PGTN is prepared and signed by PD & QA.

Batch is transferred to BSR by Packing Department.

Warehouse person receives PGTN copy and verifies quantity to be transferred, batch details, etc. Daily entries are made in SAP and in Stock Inward Register. Material is kept in designated area.

After completion of analysis from QC, QA person affixes label marked "Released" on consignment.

Warehouse intimates QA about dispatch of consignment.

QA verifies batch details as per PGTN copy and gives the clearance for palletization. Warehouse person activates feeding of data logger into the consignment, and notes in SAP and Excel sheet.

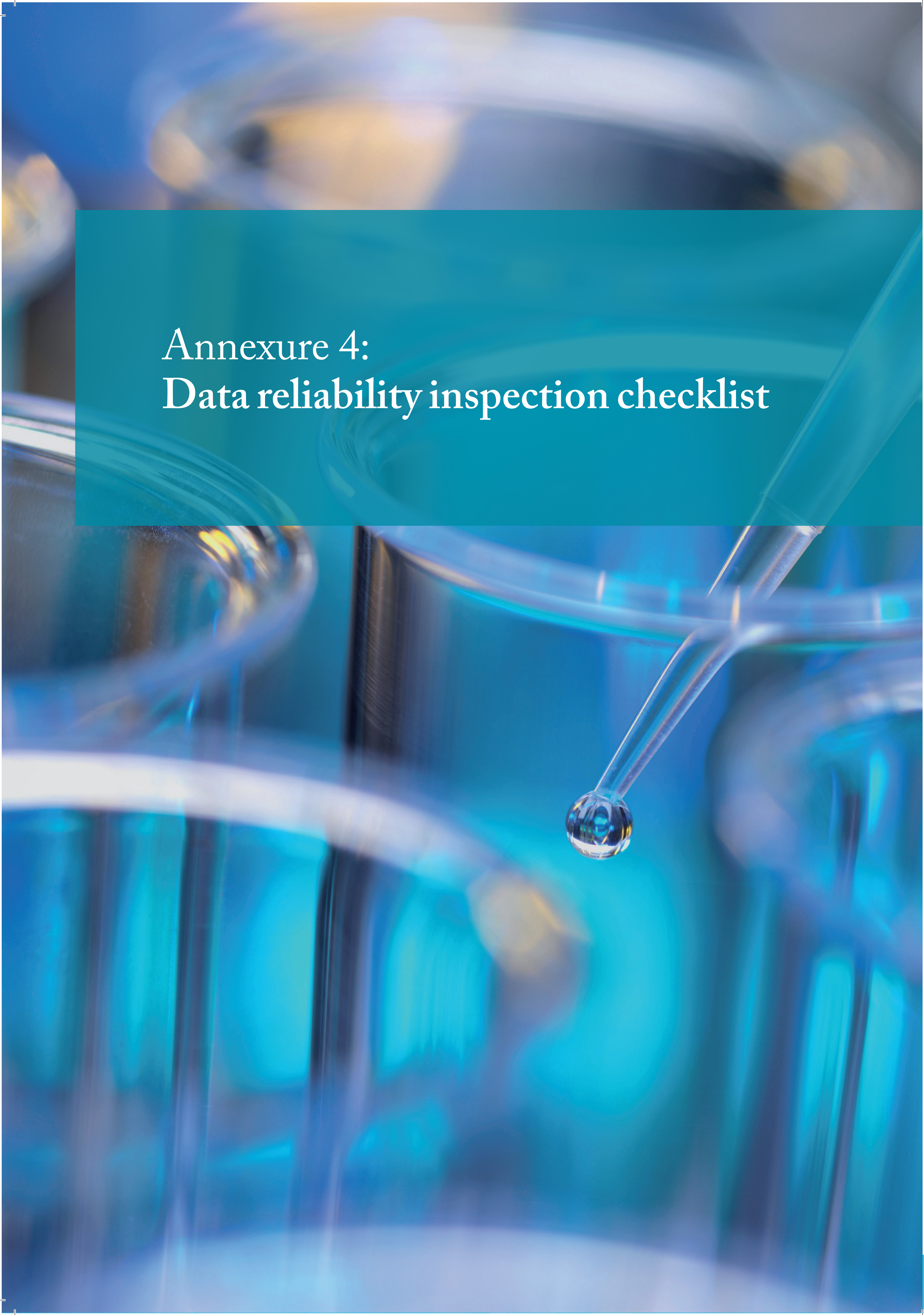
QA also prepares TSE, BSE & Non Toxicological certificate for container closure at the time of dispatch of consignment and sends approved copy by QA Head to the distributor and port.

After palletization, QA person checks vehicle condition as per checklist and gives clearance for loading the materials into vehicle.

After loading, Warehouse person prepares excise invoice and all related documents. The person hands over one copy of each document to transporter, Accounts and at security gate, and makes entry in Outward Register.

DISPATCH

Annexure 4:
Data reliability inspection checklist



Annexure 4

DATA RELIABILITY INSPECTION CHECKLIST

Date of Inspection	
Name of Inspector	
Name of the Site	
Area/Areas Inspected	
Inspection Report No.	

Sr. No.	EVALUATION CRITERIA	DOCUMENTS/ACTIVITIES	DISCREPANCIES
TRAINING, AWARENESS AND DATA MANAGEMENT			
1	Have all the employees taken the Pledge of Quality? (This is to be verified with site HR and the records for a sample of the employees should be checked).		
2	Is basic data reliability training module a part of the induction program for new employees? Are data reliability training programs conducted on a regular basis? Are all employees trained on the basics of data integrity? (The records of a sample of employees – current and new – are to be verified and confirmation obtained).		
3	Are data reliability inspections performed at the site by QA?		
4	Do site GDP SOPs include data reliability requirements?		
5	Are the specimen signatures available for all the personnel who sign the GMP documents and records for GMP activities? Are those signatures traceable on the GMP records? (This is to be cross-verified by examining an adequate number of documents as a sample).		
6	Are online documentation verified throughout the facility?		
7	Is an activity documented by the same person who performed the activity?		
8	Are OOS test results investigated? (Investigations of OOS results that are examined during data review should be verified).		
10	Are uncontrolled documents being used at the site for recording the original data and then transcribed into a controlled document? Is any GMP document being trashed? (A few drawers/ cupboards/waste bins and trash yards in different areas should be checked at random to see whether such activities are occurring).		
11	Is an instrument that is under evaluation connected to the server or is it a stand-alone system? (This is to be verified and recorded accordingly).		
12	Do Windows applications installed in a PC have features for individual ID and password? Are these activated?		
13	Are the date and time settings identical for all instruments?		
	Any other criteria:		

Annexure 4

DATA RELIABILITY INSPECTION CHECKLIST

PAPER SYSTEMS			
1	Are all paper formats controlled at QA? Do all formats (loose or bonded) have format numbers? Is complete reconciliation being conducted by QA? Is each bonded book individually numbered in chronological order?		
2	Is the recording of data that are recorded and maintained for all the GMP activities being done at the site? Has the person responsible signed the document with his/her name, date and time (for time-based activities)? (This is to be verified by examining different types of documents available at the site).		
3	Are critical activities being checked by a second person to ensure accuracy of data (This should be verified, and steps taken to ensure that print–outs, wherever required, are attached with the raw data).		
4	Have modifications to records been justified and signed with the name of the relevant person, together with date and time? Have the applicable GDP procedures been followed in doing so?		
5	Has data been recorded using permanent ink? (Pencils and/or correction fluids are strictly not permitted).		
6	Are records being archived in the QA after completion of the activities? Are such records being issued by QA after following the required procedures that are in place for tracking and traceability?		
	Any other criteria:		
ELECTRONIC SYSTEMS			
1	Are the electronic systems validated and are the relevant documents available?		
2	Are the date and time settings identical or different for all instruments, including stand-alone systems?		
3	Do instrument softwares have the feature of unique login ID and password? What is the frequency for changing the password and is this aligned with the SOP?		
4	Are user accesses granted as per the applicable procedure? Is the Admin QA or IT? Are at least two admins available? Is the 'Delete' option deactivated?		
5	Are the audit trails activated? (It must be ensured that no data or audit trail is deleted, that no data is renamed without proper justification, and that data is not saved as or renamed for another batch).		
6	Is the frequency for creating data folders appropriate? Can the data folders be saved as, copied, deleted or moved to other folders? What are the controls in place?		
7	Does the data that has been transcribed manually from electronic to paper records, or from paper to electronic records, match with each other identically?		
8	Are the data being saved in the authorized folders only? (It must be verified that no hidden folders or unwanted data are available.		
9	Is the data signed either electronically, or manually on the paper copy?		

Annexure 4

DATA RELIABILITY INSPECTION CHECKLIST

10	Is proper checking being done to ensure that Word or Excel programs available with users do not have raw data stored, and that no non-validated or uncontrolled calculation sheets are available?		
11	Is backup of the electronic data being performed on a regular basis as per the applicable procedure?		
	Any other criteria:		
STAND-ALONE SYSTEMS			
1	Are date and time settings locked for all stand-alone systems?		
2	Is critical data checked for accuracy if the relevant printed record is not available?		
3	Does the stand-alone system have sufficient memory for data storage? Is the data being backed up as per approved procedures? If the stand-alone system is not capable of storing the data, is the paper data being secured by the approved procedures?		
4	Is the stand-alone system being used by authorized personnel only? (The records available in the stand-alone system should be verified with paper data).		
	Any other criteria:		
CHROMATOGRAPHIC SYSTEMS			
1	Are there any interrupted or aborted sample set sequences? Have these has been conducted with proper documentation and investigation?		
2	Check the sample set sequence in the system and cross-verify with hard copy attached with the raw data. Is the sequence followed the same as defined in the SOP or in the method of analysis? Check the name of the analyst who prepared the sequence and cross-check this against the log book or raw data.		
3	Check the processing date and time for the sample set sequence. Check the name of the analyst who processed the sequence and cross-check this against the log book or raw data.		
4	Has the complete sample set sequence processing been done using the same processing parameters? If there are variations, have these been justified?		
5	Are there raw data files with similar names or overwritten files in the relevant data folders or other repositories?		
6	Do the date and time appearing on raw data files in the sequence match with respect to run time mentioned in the sequence and the method of analysis?		
7	Has manual integration been done? If so, has this been justified and authorized by the manager?		
8	Have additional SST and standard injection runs been done in the sequence? If so, have these been justified and authorized by the manager?		

Annexure 4

DATA RELIABILITY INSPECTION CHECKLIST

9	Check the following actions in audit trail: ‘Delete’, ‘un processed’, ‘re-processed’, ‘overwrite’, ‘changed’, ‘rename’, etc. Check if in the search option the related files and folders are showing results for such actions.		
10	Does the chromatogram have integration bias?		
11	Any other criteria:		
MICROBIOLOGY LAB			
1	Is the area monitoring data accurately documented on the paper documents if electronic prints are not available?		
2	Verify sample inward records with available samples for analysis. Report if any sample does not have the requisite inward record.		
3	Verify that disinfectant solutions used for lab cleaning available when required.		
4	Are all the plates available in the lab fully traceable?		
5	Are cultures that are used for testing in stock as and when required?		
Data Backup :			
1	Check that data backup is done as per the appropriate SOP.		
2	Any other criteria:		

Annexure 4

DATA RELIABILITY INSPECTION CHECKLIST

Summary of Observations:

Inspected By (Name):
Signature and Date:

Annexure 5:
Data quality design consideration and controls

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
<u>Attributable:</u> Who acquired the data of the performed action (or modification) and when.	The need to append and/or modify a record is likely to increase in complexity in a paper-based system; a computerized system must be defined, procured and configured to meet the applicable regulatory record requirement.	1. There should be definitions of separate User roles (based on record of involvement) for all Users of a system. For example, a 'User' may be a 'Creator' with the ability and authority to write records; or he/she can be a 'Reviewer' with the ability and authority to append and/or modify a record; or he/she can be an Administrator with the authority to delete a record.	1. A user of the system should not have more than one role.
		2. Each User, regardless of role, must have a unique user ID to access the system. Typically, this is handled most efficiently via a centralized network (e.g., Active Directory Groups).	2. If possible, the services should be utilized of a system administrator who is independent from the department responsible for electronic records (e.g. IT), or one that does not have any vested interest in the data results from the given system.
	Applicable tasks/deliverables: 1. System requirements/user requirements and/or assessments must define the intended system record types and Annex 11/21 CFR Part 11 applicability.	3. An Annex 11/Part 11 assessment should be performed to verify that all expected regulatory requirements including audit trail and electronic record/signature attributes where applicable (e.g., secure) are being met.	3. System administrators should not generate or review data.

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
	2. Prior to procurement, vendor assessment and product demonstration should be performed to aid in determining design and configuration needs and any potential compliance risk.	4. Security settings within the application must be designed and configured to prevent non-administrators from accessing the ability to disable compliance-related settings such as those related to audit trail, user management, and signatures.	4. Users who are not Administrators should not be in a local Administrators group or form a part of the Power/Super Users group.
	3. Design and configuration documentation shall include the specific post-installation attributes that must be set in order to meet the requirements of the system.	5. Security settings outside of the application must be designed and configured to only allow the minimum level of user-permissions required for the application to function. A few specific considerations are given below as illustrations: a) If a database is used, it should be located and administered in a qualified infrastructure, independent of the application client computer, with no user access to the raw data or database location outside of the application. b) If the computer system is stand-alone, security controls need to be in place to limit the user's ability to modify or delete raw data, metadata and audit trail information.	5. The use of shared and generic log-on credentials must be avoided to ensure that personnel actions documented in electronic records and signatures can be attributed to a unique individual.
			6. Implement SOP direction (and associated training) to identify the importance of data integrity and define procedural controls as necessary to secure the data flow within the process and prohibit the overwriting or deleting of data. For some (e.g., stand-alone) systems, this may involve a hybrid electronic/paper approach and maintaining a continuous session on the systems, with additional reviews if needed.

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
Legible: Data is permanent and easily read by a human.	Applicable tasks/deliverables: 1. Prior to procurement, vendor assessment and product demonstration should be performed to aid in determining design/configuration needs and assess any potential compliance risk.	1. There should be controlled configuration and use of any record annotation tool in a manner that may result in data display and print being obscured.	1. There should be strict implementation of SOP directions (and associated training) in order to emphasize the importance of data integrity. Such inputs should define procedural controls as may be necessary in order to ensure that no data is obscured during use and output (e.g. in a hardcopy format). Such procedures should be reviewed where applicable to ensure legibility and consistency with good documentation practices.
	2. Design and configuration documentation should include the specific post installation attributes that must be set in order to meet the requirements of the system.	2. There should be verification of record and report output against on-screen or originally entered data, including metadata.	
Contemporaneous: Document is prepared at the time of activity (or promptly thereafter).	Applicable tasks/deliverables: 1. Prior to procurement, vendor assessment and product demonstration should be performed to aid in determining design/configuration needs and assess any potential compliance risk.	1. An Annex 11/part 11 assessment should be performed to verify that all expected regulatory requirements including audit trail and electronic record/signature attributes where applicable (e.g. secure) are being met.	1. Users who are not Administrators should not be in a Local Administrator group or in a Power or Super User group.
	2. Design and configuration documentation shall include the specific post-installation attributes that must be set to the requirement of the system. a) Specific considerations need to be made relative to what centralized	2. It must be verified that a user cannot change system date, time and time zone on the computer that the application uses to stamp such information. a) This can be controlled centrally, for example, by defining a specific	2. There must be strict implementation of SOP directions (and associated training) in order to emphasize the importance of data integrity and overall good documentation practices, even if the computer

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
	(e.g. domain) security can be implemented versus stand-alone/local security. b) Specific considerations need to be made relative to the need for and definition of centralized and synchronized time stamping.	organization unit (group) where computers in this group only allow a network administrator to change these attributes. b) If this is handled locally on a stand-alone computer, it must be ensured that the users cannot be in the local administrators group.	system is providing the necessary information.
		3. If the system is an enterprise-level system where use may span multiple time zones, verification need to be made relative to a consistent centralized time for the system, regardless of access point and this time must be synchronized to a traceable source.	
Accurate: Data is correct including context and meaning (e.g. metadata) and edits thereof.	Applicable tasks/deliverables: 1. Prior to procurement, vendor assessment and product demonstration should be performed to aid in determining design and configuration needs and assess any potential compliance risk.	1. An Annex 11/part 11 assessment should be performed to verify that all expected regulatory requirements including audit trail and electronic record/signature attributes where applicable (e.g. secure) are being met.	1. A procedure or set of procedures (and associated training) should be implemented that will dictate the acceptable and consistent data management practices for the system including how an original data record should be processed and saved, how it may be reviewed or how it can have metadata associated with it (e.g.,

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
			signature), how it can be historically retrieved, backed up and restored, and other related practices.
	2. Design and configuration documentation should include the specific post-installation attributes that must be set in order to meet the requirement of the system. a) Specific consideration should be given to defining any custom or process–specific calculations, reporting, or critical process parameters, and critical quality attributes that may require data validation, calibration or supplemental risk assessment and verification.	2. Specific verification and/or validation documentation (e.g. tests plans, scripts, protocols, traceability matrix, etc.) must define, challenge, conform, and trace the accuracy of the defined data collection, processing and reporting for the system.	2. A procedure or set of procedures (and associated training) must be implemented in order to ensure that the required calibration frequency of any instrument associated with critical systems is achieved, and monitored.
<u>Complete:</u> A Data Record includes all data (passing or otherwise) from all action taken to obtain the required information, including metadata (e.g. audit trail) and edits.	Applicable tasks/deliverables: 1. Prior to procurement, vendor assessment and product demonstration should be performed to aid in determining design and configuration needs and assess any potential compliance risks.	1. An Annex 11/part 11 assessment should be performed to verify that all expected regulatory requirements including audit trail and electronic record/signature attributes where applicable (e.g. secure) are being met.	1. A procedure or set of procedures (and associated training) should be implemented in order to clearly identify the company's data integrity definitions and expectations.

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
	2. Design and configuration documentation should include the specific post-installation attributes that must be set in order to meet the requirement of the system.		2. A procedure or set of procedures (and associated training) should be implemented in order to dictate the acceptable and consistent data management practices for the system including how an original data record should be processed and saved, how it may be reviewed or how it can have metadata associated with it (e.g., signed), how it can be historically retrieved, backed up and restored, and other related practices.
			3. A procedure or set of procedures (and associated training) should be implemented in order to dictate the steps required for addressing out of tolerance results and process deviations.
			4. A procedure or set of procedures (and associated training) should be implemented in order to dictate the steps required for performing an audit trail review and the desired frequency of such a review.

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
Consistent: Data is created in a repeatable and comparative manner (traceable).	Applicable tasks/deliverables: 1. Prior to procurement, vendor assessment and product demonstration should be performed to aid in determining design and configuration needs and assess any potential compliance risk.	1. Specific verification and validation documentation (e.g. tests plans, scripts protocols, traceability matrix, etc.) must define, challenge, conform, and trace the consistency of the defined data collection, processing and reporting for the system. a) This may include, but need not be limited to, the following: i. Equipment and instrument qualification ii. Software and system qualification iii. Method validation iv. Process validation	1. A formal set of policies, plans or procedural documentation should be drawn up and implemented (along with associated training) dictating the system development and maintenance lifecycle along with the applicable method and process validation expectations.
	2. Design and configuration documentation should include the specific post-installation attributes that must be set in order to meet the requirement of the system. a) Specific consideration should be given to defining any custom or process-specific automated processing and/or workflow or specific sequencing of events.		2. A procedure or set of procedures (and associated training) should be implemented in order to clearly dictate the acceptable and consistent data management practices for the system including how an original data record should be processed and saved, how it may be reviewed or how it can have metadata associated with it (e.g., signature), how it can be historically retrieved, backed up and restored and other related practices.

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
<u>Enduring</u>: Stored on media proven to be stable for the record retention period.	Applicable tasks/deliverables: 1. Prior to procurement, vendor assessment and product demonstration should be performed in order to aid in determining design and configuration needs and assess any potential compliance risk.	1. Specific verification and validation documentation (e.g. tests plans, scripts protocols, traceability matrix, etc.) must define, challenge, conform, and trace the ability of the system to store and retrieve records of the entire duration of a record's retention period.	1. A formal set of policies, plans or procedural documentation should be drawn up and implemented (along with associated training) dictating the minimum retention period of the record types affected by the system.
	2. Requirement, design and configuration documentation must include the specific post-installation attributes that must be set in order to meet the intended use and the future state functions of the system. a) Specific consideration should be given to identifying the specific record types (e.g., records dictated by regulation, i.e., by predicate rule) and what is the record's respective retention period. b) Specific consideration and definition should be given to the technology and media type that will best satisfy the day-to-day use and the long-term retention and usability of the affected stored records.	This may include, but need not be limited to, the following: i. Vendor/media life span information ii. Media reliability information iii. Media use schedule iv. Restoration verification	2. A procedure or set of procedures (and associated training) should be implemented in order to clearly dictate the acceptable and consistent data backup process, schedule, media types, on-site and off-site schedules, archive, and restoration activities.

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
Available: Readily accessible in human readable form for review throughout the retention period of the record.	Applicable tasks/ deliverables: 1. Prior to procurement, vendor assessment and product demonstration must be performed in order to aid in determining design and configuration needs and assess any potential compliance risk.	1. Specific verification and validation documentation (e.g., test plans, scripts, protocols, traceability matrix, etc.) must define, challenge, confirm, and trace the ability of the system to retrieve and restore data in the time frame necessary for internal and external review. a) This may include, but need not be limited to, the following: i. Verification of restoration capability from all media types ii. Verification of restoration capability from all backup schedules (e.g., on-site and off-site). iii. Verification of archive retrieval capability	1. A formal set of policies, plans or procedural documentation should be drawn up and implemented (along with associated training) dictating the minimum retention period of the record types affected by the system.
	2. Requirements, design and configuration documentation should include the specific post-installation attributes that must be set to meet the intended use and the future state functions of the system. a) Specific consideration and definition needs to be given to identifying the specific record types (e.g. records dictated by regulation, i.e. by predicate rules) and the record's respective retention period. b) Specific consideration and definition needs to be given to the technology and media type that will best satisfy the day-to-day use,		2. A procedure or set of procedures (and associated training) should be implemented in order to clearly dictate acceptable and consistent data backup processes, schedules, media types, on-site and off-site schedules, archive, restoration, and other related practices.
			3. Procedural and periodic tests should be performed to verify the ability of the system to retrieve archived electronic data from storage locations.
			4. Taking into account the possibility of the presence of decommissioned and/or retired or archived systems, there may be a need

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

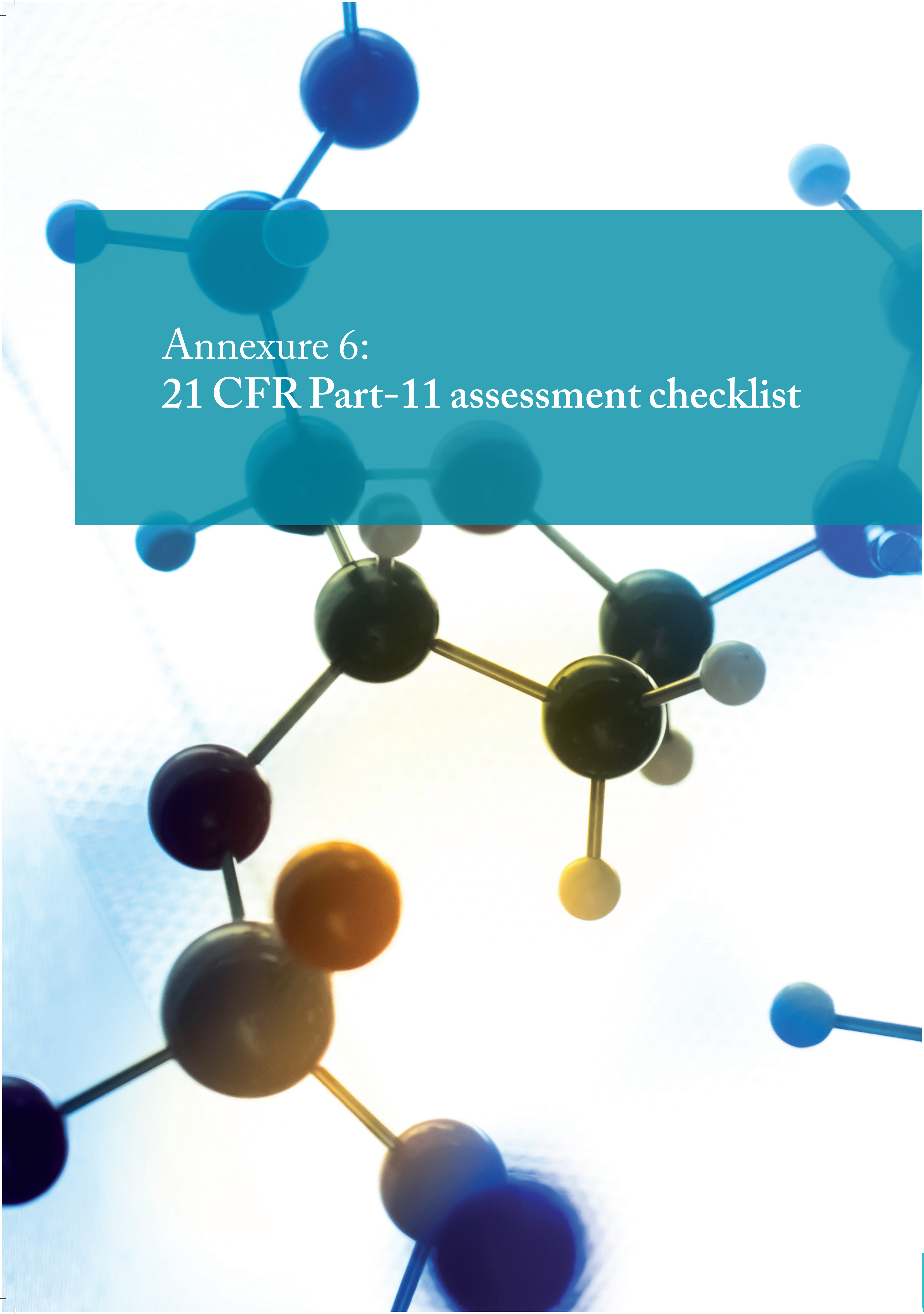
Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
	the long-term retention capability, and the retrieval time requirements.		for provisioning of suitable reader equipment, such as software, operating systems and virtualized environments, etc., to view the archived electronic data when required. A policy in this respect should be in place and implemented as required.
Original: First recording of data, raw or source- data or a certified true copy.	Applicable tasks/ deliverables: 1. Prior to procurement, vendor assessment and product demonstration should be performed to aid in determining design and configuration needs and assess any potential compliance risk.	1. An Annex 11/part 11 assessment should be performed in order to verify that all expected regulatory requirements including audit trail and electronic record/signature attributes where applicable (e.g. secure) are being met.	1. A formal system of development and implantation cycle should be followed in order to ensure that process-specific considerations and/or evaluations are being met and that the development or test environment is advantageous for proving a design prior to formal end-use environment verification.
	2. Design and configuration documentation should include the specific post-installation attributes that must be set in order to meet the intended use and the future state functions of the system. a) Specific consideration and definition needs to	2. Security settings outside of the application must be design and configured to only allow the minimum user permission for the application to function. Specific considerations should be given to the following:	2. A procedure or set of procedures (and associated training) should be implemented that clearly dictate the acceptable and consistent data management practices of the system including how an original data record should

Annexure 5

DATA QUALITY DESIGN CONSIDERATION and CONTROLS

Example of Data Quality Concern	Design/Implementation Consideration	Verification Consideration	Pitfalls to Avoid/ Management Consideration
	be given to the implementation of centralized (e.g. domain) security versus stand-alone/local security configuration. b) In the case of a stand-alone system, consideration needs to be given to process and procedural data flow and whether automatic or manual functions will be required. A folder or folders may need to be created for either write permission with deny append or read and execute with permission to write. In addition, permission inheritance needs to be recorded and included in the appropriate documentation.	a) If a data base is used, it should be located and administered on a qualified infrastructure, independent from the application client computer with no user access to the raw data and/or database location outside of the application. b) In the case of a stand-alone system, a user should not have full control of the records or audit trail location. Ideally, a user should only have permissions to read, write, and execute, with the functional denial of modify, write over and delete activities.	be processed and saved, how it may be reviewed or how it can have metadata associated with it (e.g., signature), how it can be historically retrieved, backed up and restored, and other related activities.

Annexure 6:
21 CFR Part-11 assessment checklist



Annexure 6

21 CFR Part-11 ASSESSMENT CHECKLIST

Instrument	
Make	
Model	
Software & Version No.	
Instrument ID No.	
Manufacturer Serial No.	
Windows Operating System	

SR. No	Parameters	Observation	Signature & Date
Password policy			
1	Software should have Individual User Accounts and such Accounts should be password-protected.	Yes/No/NA	
2	Password and User ID policy (Individual unique ID and Password, minimum length and strength of ID and Password) should be available.	Yes/No/NA	
3	The software should automatically limit the number of failed login attempts.	Yes/No/NA	
4	The software should automatically record unauthorized login attempts.	Yes/No/NA	
5	The software should electronically require users to change their passwords at regular intervals.	Yes/No/NA	
6	The software should automatically password-protect computer systems when idle for short periods of time.	Yes/No/NA	
7	When logging in for the first time, the system should ask for both User ID and Password. For all further transactions, the system may prompt for Password only.	Yes/No/NA	
8	The system should allow resetting of Password under authorized personnel login in case the User Account is locked.	Yes/No/NA	

Annexure 6

21 CFR Part-11 ASSESSMENT CHECKLIST

SR. No	Parameters	Observation	Signature & Date
User Management System and Privileges			
9	The user level is defined based on functionality and authority; e.g., Analyst, Reviewer, Lab Manager, Administrator, etc.	Yes/No/NA	
10	Privileges like delete, copy, cut, paste, rename, etc. should not be allowed at Analyst and Reviewer levels.	Yes/No/NA	
11	A user should not be able to delete an account once created in the system. The system should allow deactivating the user account if the user no longer exists in the system or that account is not required in the future. However, the right to delete such an account should remain with the Administrator.	Yes/No/NA	
Electronic Data			
12	Electronic data and reports should be human readable and suitable for inspection and review.	Yes/No/NA	
13	Content like 'Performed by' with date and time stamp, 'Print by' with date and time stamp, 'Reviewed by' with date and time stamp, information related to system and analysis parameters, etc. should be available as and when required.	Yes/No/NA	
Electronic Data Storage (See also Data Backup)			
14	Generated data should be stored in a protected drive.	Yes/No/NA	
15	Generated data shall not be edited or altered without authorization.	Yes/No/NA	
Audit Trail			
16	The system should track all creations, modifications, and deletions performed in the system. All activities should be logged between login and logout with time and date stamps along with user details.	Yes/No/NA	
17	All hardware related errors and warnings should be logged in an audit trail (system audit trail).	Yes/No/NA	
18	All entered data must be maintained. Original data must not be obscured when changes are made. The system shall maintain revision history for all changes made.	Yes/No/NA	
19	Time and date stamps will change automatically, and shall be locked and not editable unless performed by an authorized user, who shall be defined through user rights distribution.	Yes/No/NA	

Annexure 6

21 CFR Part-11 ASSESSMENT CHECKLIST

SR. No	Parameters	Observation	Signature & Date
20	The computer system shall be designed such that it would require a user to record the reason for change through the use of authorized login and password.	Yes/No/NA	
21	Software should automatically record identity of the individual who made a change or changes.	Yes/No/NA	
22	The system shall prevent modification and/or deletion of the audit trail.	Yes/No/NA	
23	Audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records, and these shall be available for agency review if required.	Yes/No/NA	
Electronic Signature			
24	Electronically signed documents should have the following automatically generated content: • The printed name of the person signing. • The date and time when the signature was executed. • The meaning associated with the signature. The above must be included as part of any human readable form of the electronic record.	Yes/No/NA	
25	There should be a unique ID and Password for an electronic signature.	Yes/No/NA	
26	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be exercised, copied or otherwise transferred to falsify an electronic record by ordinary means.	Yes/No/NA	
27	Each process using an electronic signature should be electronically logged in an audit trail with time and date stamp and user ID.	Yes/No/NA	
28	The system shall not allow any two users to have the same user ID or password.	Yes/No/NA	
Data Backup			
29	The software shall have the facility for automatic data backup to any client or connected central server.	Yes/No/NA	
30	It should be checked to see if any manual data backup facility and/or procedure are available.	Yes/No/NA	

Annexure 6

21 CFR Part-11 ASSESSMENT CHECKLIST

SR. No	Parameters	Observation	Signature & Date
31	As and when required, backed up data should be available for review purposes. There should be systems available so that backed up data can be restored, archived, and retrieved in original form. The restored copy should be identical with the original copy.	Yes/No/NA	
32	Backup data should be stored in a secured way with restricted access. Any access to the storage area should be logged with reason for access under the supervision of authorized personnel.	Yes/No/NA	
Other			
33	Users shall not be able to save or relocate the result files; it should be controlled only through the software.	Yes/No/NA	
34	Users shall not have rights to create folders or projects in the system. These rights shall rest only with the Administrator.	Yes/No/NA	
Validation			
35	Does a defined computer system validation policy exist?	Yes/No/NA	
36	Are all computer systems-based instruments and/or equipment involved in activities that are covered by the validation policy?	Yes/No/NA	
37	Have all the effects of changes been carefully evaluated before and after making such changes?	Yes/No/NA	
Training			
38	Is there a defined training program designed for authentication practices?	Yes/No/NA	
39	Are there specific written operating procedures in place?	Yes/No/NA	
40	Are system administrators and users trained in Part 11 and related regulations?	Yes/No/NA	

Done By:

Name of Department:

Signature and Date:

Annexure 7:
Risk assessment for data recording and process control

Annexure 7

RISK ASSESSMENT for DATA RECORDING and PROCESS CONTROL

SR	Event/Risk	Effect of failure	Severity (S)	Cause	Occurrence (O)	Current control	Detection (D)	RPN	CAPA
1	Levels of access	Unauthorized person may access the restricted and/or critical portion of the program.	5	This may impact the final outcome of results and/or equipment operation. This may change the specification and/or parameters set in the recipe. This may delete older data from system.	3	Define the level of access in place for all the applicable equipment in production. In general, the equipment is provided with following level of passwords: a. Operator b. Supervisor c. Administrator Training on equipment operation is provided to all operators. Verification of level of access is a part of the validation document.	1	15	No CAPA
2	Privileges for access level are not provided	Unauthorized person may access the operation of equipment or program. Untrained operators may operate the system and/or equipment.	5	This may impact the final outcome of results and/or equipment operation. The procedure does not define the requirement for password. The URS does not describe the requirement for access control. During the validation activities, level of access are not verified.	3	Levels of access are defined in SOP. URS/Qualification document described the specific level of control. Verification of privileges is a part of the validation document Additionally operators are assigned to particular equipment based on their experience and training on that particular equipment.	1	15	No CAPA

Annexure 7

RISK ASSESSMENT for DATA RECORDING and PROCESS CONTROL

SR	Event/Risk	Effect of failure	Severity (S)	Cause	Occurrence (O)	Current control	Detection (D)	RPN	CAPA
3	Modification of date, time and time zone	This may result in loss of data integrity.	4	Administrator controls are not in place and is not part of validation process.	3	All the infrastructure system is provided with administrative controls and the same is demonstrated during the infrastructure/system qualification.	1	12	No CAPA
4	Training of individual using the system not done	This may impact directly on the anticipated results. This may result in creating data integrity issues.	4	Trained operators are not employed on an instrument and/or equipment for a particular activity.	3	The access by the operator to the individual systems is through the login ID and password. Additionally operators are assigned to a particular equipment based on their experience and training on that particular equipment.	2	24	No CAPA
5	Non Compliance to ALCOA	Document may not be complying to ALCOA	5	Documents can be edited at any point of time. Documents are not readable or not stored permanently. Date and time are incorrectly updated. No traceability of activity is possible through the system. No certification is done on the document. Action done cannot be traced.	5	A document or data cannot be edited without change control or without documentation. All documents are printed with doer's name (i.e. balance, moisture content, etc.). Audit trail functionality is not available to all the peripheral equipment (i.e., balance, hardness tester, moisture analyzer balance, DT, friability, etc.). For data pertaining to production equipment, the entries done in BMR are online and are cross-verified by production supervisor and quality assurance at defined stages, conforming to the ALCOA standards.	3	75	All documents should be printed with instrument ID, doer's name, date and time. All activities should be traceable through audit trails.

Annexure 7

RISK ASSESSMENT for DATA RECORDING and PROCESS CONTROL

SR	Event/Risk	Effect of failure	Severity (S)	Cause	Occurrence (O)	Current control	Detection (D)	RPN	CAPA
6	Signature does not contain name, date, time and signature.	Document cannot be traced, i.e. on which date activity has been done and who has done the activity cannot be determined for certain.	8	Software/system available does contain signature along with name, date and time.	4	E-signature not available at a particular site.	4	128	Where E-signature is applicable and available, documents are automatically printed with date, time and name.
7	No password uniqueness	Document cannot be tracked to the specific doer of a particular activity.	7	The system has a common username and password for all. Authority of document will be lost. No tracking of document is possible.	5	Common password is used for IPQA instruments, i.e. balance, pH meter, hardness tester, friability, etc., that are not attached with system. All these systems and equipment do not have an audit trail function.	5	175	Validation should be carried out to ensure that wrong password or user name cannot open an unauthorized document. Password should be assign for individual instruments. Equipment and instruments should comply with 21 CFR Part 11.
8	No periodic revision of password	If an unauthorized person acquires a password and uses it without being detected, then that person has access for an indefinite period.	3	No system is available for changing the password.	3	The system automatically prompts for new password after a pre-determined period.	2	18	No CAPA

Annexure 7

RISK ASSESSMENT for DATA RECORDING and PROCESS CONTROL

SR	Event/Risk	Effect of failure	Severity (S)	Cause	Occurrence (O)	Current control	Detection (D)	RPN	CAPA
9	No data backup	Data may be lost. Evidence of root cause of an incident or investigation may be lost.	5	No system or SOP is available for backup of data.	2	SOP and system are available for backup and archiving of electronic data.	1	10	Periodic verification of data backup should be done by Audit team.
10	No listing of all the computerized systems	Periodic inventory updating is required of systems to ensure that all such instruments are covered and maintained under the GXP environment.	3	No system is in place to ensure the inventory control of all the systems.	3	SOP and system are in place to maintain inventory control of all the systems. Equipment list is also updated with incorporation of any new equipment and/or instrument in the area.	1	9	No CAPA
11	No application of Risk Management for extent of validation and data integrity controls	Product quality may be affected. Data integrity may be affected.	6	Risk management SOP is not available. No procedure is available to identify the extent of data integrity controls. No trained persons are available to evaluate the risks involved in the system.	4	Risk management SOP is available. Functional risk assessment is carried out to ensure the extent of validation. Training should be given to all concerned for the evaluation of risk.	1	24	No CAPA

Annexure 7

RISK ASSESSMENT for DATA RECORDING and PROCESS CONTROL

SR	Event/Risk	Effect of failure	Severity (S)	Cause	Occurrence (O)	Current control	Detection (D)	RPN	CAPA
12	No additional checks for manually entered data	Incorrect parameters may get uploaded or fed in. This may result in data integrity issues.	3	No SOP or system is available for checks on manually entered parameters. Wrong data may be reported. Wrong interpretation of data may take place.	2	Verification of manually entered data is a part of the SOP. All the critical equipment are operated by using PLC and audit trail functions are present in individual critical systems.	1	6	No CAPA
13	No change management procedure	Changes may take place without review and approval. Impact of the changes will not be evaluated properly. All the affected departments may not aware of the changes being done and the impact thereof.	4	No SOP is available for changing the system, including the procedure and documentation.	2	All changes are addressed through change management and/or change control SOPs. After initiation of the proposed changes, the changes are circulated with all the impacted departments to evaluate the proposed changes as are applicable.	1	8	No CAPA
14	No periodic evaluation of computerized systems	Over a period of time, the system may not perform as efficiently as intended	5	No defined procedure is in place to periodically evaluate the system. This may affect the final output or result.	3	SOP for computerized system is in place to ensure periodic evaluation of the system.	1	15	No CAPA

Annexure 7

RISK ASSESSMENT for DATA RECORDING and PROCESS CONTROL

SR	Event/Risk	Effect of failure	Severity (S)	Cause	Occurrence (O)	Current control	Detection (D)	RPN	CAPA
15	No integrity, accuracy and ability to restore the backup data	Older data may be corrupted or even lost. Evidence of older data may also be lost.	6	Backing up of data is not done using the right or correct process or device. No procedure is in place to assure integrity of backed up data.	4	SOP and system is available for back-up and archival of electronic data. As per the procedure, accuracy of the backup data is verified at defined frequency.	1	24	No CAPA
16	Reporting of data	Wrong data is reported. Loss of raw data may occur.	5	This may affect the quality of the final product.	2	All raw data are attached with the document and same is verified by supervisor.	1	10	No CAPA

Annexure 7

RISK ASSESSMENT for DATA RECORDING and PROCESS CONTROL

Conclusion:

Based on the assessment, it can be inferred that the available controls are adequate to control, and monitor the processing and retention of data with consistent quality.

Current quality systems are adequate and sufficient to ensure safety, identity, strength, purity and quality of the product. However, as a measure of abundant precaution, the following steps will be taken to further strengthen our quality systems.

Sr. No.	Recommendations	Target Implementation Date	Responsible Person
1.	All equipment and systems shall be operated through a PLC system.		
2.	All equipment and instruments shall be operated through login ID and Password protection.		
3.	Installation of an ‘Access control system’ to avoid entry of unauthorized personnel into process area will be implemented, so as to avoid any issues related to data integrity.		
4.	E-signature documents shall be implemented.		
5.	Frequency of audits for data restoration can be increased on the basis of criticality of incident and observed failures.		

Done By: **Name of Department:** **Signature and Date:**	**Checked By:** **Quality Assurance :** **Signature and Date:**

Published by:
Indian Pharmaceutical Alliance
A-205 Sangam
14B S V Road, Santacruz (W)
Mumbai 400 054 India
E-mail: dgshah@vision-india.com