GUIDELINES

Data Integrity & Computer System Validation

Developed by the Federal State Institute of Drugs and Good Practices with the support of PQE Group

Acknowledgements

This guideline was produced by a task team led by Federal State Institute of Drugs and Good Practices representatives (Vladislav Shestakov, Natalia Chadova, Tatiana Nikolko, Igor Falkovskiy, Vladimir Orlov, Nadezhda Arkhipova, Madina Sottaeva, Vyacheslav Goryachkin and Sergey Orlov) with contribution of PQE group (Gilda D'Incerti, Danilo Neri and Yuriy Sandler).

Contents

I. GENERAL PROVISIONS

1. INTRODUCTION

In order to ensure the Patient Safety and the Product Quality, Minpromtorg (Ministry of Industry and Trade) has issued the Order of Minpromtorg of Russia dated 14 June 2013 No. 916 "On the approval of Rules of Good manufacturing practices" (Registered in the Russian Ministry of Justice on 10 September 2013 No. 29938). This regulation is intended to define the minimum requirements that a manufacturer must meet in order to assure that their products are consistently high in quality, from batch to batch, with respect to their intended use. The control measures required to be implemented are based upon the Regulated Data (i.e. information relied upon by the manufacturers to ensure Patient Safety and Product Quality) which shall be created and maintained integer within the entire Product Life Cycle allowing to reconstruct the activities performed.

The Regulated Data management has evolved in the latest decade in line with the ongoing development of supporting technologies (such as the increasing use of electronic data capture, automation of systems and use of remote technologies) and the increased complexity of supply chains and ways of working (for example, via third party service providers). Systems to support these ways of working can range from manual processes with paper records to the use of fully computerized systems.

The Annex 11 to the Regulation No. 916 "On the approval of Rules of Good manufacturing practices" defines the regulatory requirements for GMP critical Records managed through Computerized Systems: these requirements are ultimately focused to ensure the Integrity of those data managed through automated systems.

The principles of data integrity apply equally to both manual and computerized systems and shall not place any restraint upon the development or adoption of new concepts or technologies.

Data Integrity is defined as "the extent to which all data are complete, consistent and accurate, throughout the data lifecycle" and is fundamental in a pharmaceutical quality system, which ensures that medicines are of the required quality. Poor data integrity practices and vulnerabilities undermine the quality of records and may ultimately undermine the quality of medicinal products.

Data integrity applies to all elements of the Quality Management System and the principles herein apply equally to data generated by electronic and paper-based systems; these data have to be assessed for finding potential vulnerabilities and taking steps to design and implement good data governance practices in order to ensure that data integrity is maintained.

The measures addressed by this Guidance are oriented to expected to ensure effectiveness of the inspection processes to the drug manufactures, which is strictly based upon the veracity of the evidence provided to the inspectors and ultimately upon the integrity of the underlying data. It is critical to the inspection process that inspectors can determine and fully rely on the accuracy and completeness of evidence and records presented to them.

This guidance aims to promote a risk-based approach to data management that includes data risk, criticality and lifecycle. Users of this guidance need to understand their data processes (as a lifecycle) to identify data with the greatest GMP impact. From that, the identification of the most effective and efficient risk-based control and review of the data can be determined and implemented.

The requirements and methods addressed by this guidance are aligned with the expectations defined in the relevant guidances released by the most important associations (i.e. WHO, PIC/S, ICH, ISPE)

This guidance shall be considered as a means for understanding the position of the Pharmaceutical and Medical Development Department of Ministry of Industry and Trade of Russian Federation, and Federal State Institute of drugs and Good Practices on data integrity and the minimum expectation to achieve compliance. The guidance does not describe every scenario so interaction with the regulatory authorities is encouraged where your approach is different to that described in this guidance.

II. FIELD OF APPLICATION

2. PURPOSE

This guidance is oriented to establish a process that integrates sound organizational practices, effective risk-based processes and compliance with regulatory expectations to ensure the integrity of those records determined to have a potential impact on Patient Safety and Product Quality.

As Data integrity applies to all elements of the Quality Management System, the Guidance is oriented to define the expectations for Critical Records managed through paper documents and through the Computerized Systems, focusing on the Computer Validation requirements, which is the key requirement to ensure the records integrity.

The targets of this Guidance are:

- Support inspectorates in the interpretation of GMP requirements in relation to data integrity and the conduct of inspections.
- Provide consolidated, illustrative advises to Regulated Companies on risk-based control strategies which enable the existing requirements for data integrity and reliability to be implemented in the context of modern industry practices and globalized supply chains.
- Facilitate the effective implementation of data integrity elements into the routine planning and conduct of GMP supplier qualification process
- Define a procedural framework to meet the regulatory requirements for Computerized System management set forth by the Annex 11 to the Regulation No. 916 “On the approval of Rules of Good manufacturing practices” (issued on June 14 2013).

3. SCOPE

This document applies to records generated, maintained and/or stored, manually or electronically, from creation through archival, in support of their GMP processes established by pharmaceutical companies to assure that their manufactured products are consistently high in quality, from batch to batch, for their intended use.

Data integrity requirements set forth by this Guidance apply equally to manual (paper) and electronic data, generated or used within any process determined to have a potential impact on Patient Safety and Product Quality within the different stages of the manufacturing and distribution of a Pharmaceutical Product.

In case one critical process is outsourced, the organization that outsources work has the responsibility for the integrity of all results reported, including those furnished by any subcontracting organization or service provider (see section 10).

In case the Regulated Data are created, managed and maintained through Electronic Records, the associated Integrity is ensured by the relevant Computerized System. As a consequence, this Guidance applies to all Computerized Systems determined to have a GMP impact, i.e. which may potentially affect the Patient Safety and Product Quality.

III. BASIC CONCEPT

4. DATA INTEGRITY PRINCIPLES

Regulatory Authorities worldwide have always depended upon the knowledge of organizations that develop, manufacture and package, test, distribute and monitor pharmaceutical products. Implicit in the assessment and review process is trust between the regulator and the regulated company (i.e. the pharmaceutical company) that the information submitted in dossiers and used in day-to-day decision-making is comprehensive, complete and reliable. The data on which these decisions are based shall therefore be complete as well as being **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal and **A**ccurate, commonly referred to as "ALCOA".

The control measures to ensure Data Integrity shall be embedded in the Pharmaceutical Quality System, which guarantees that medicines are of the required quality. Data integrity applies to all elements of the Pharmaceutical Quality System and the principles herein apply equally to data generated by electronic and paper-based systems. Organizations shall follow good documentation practices (GDocP) in order to assure the accuracy, completeness, consistency and reliability of the records and data throughout their entire period of usefulness – that is, throughout the data life cycle.

The effort and resource assigned to data integrity control shall be commensurate with the risk to product quality, and shall also be balanced with other quality resource demands. The Pharmaceutical companies shall design and operate a procedural framework which provides an acceptable state of control based on the data integrity risk, and which is fully documented with supporting rationale.

The responsibility for good practices regarding data management and integrity lies with the manufacturer or distributor undergoing inspection: these entities have full responsibility and a duty to assess their data management systems for potential vulnerabilities and take steps to design and implement good data governance practices to ensure that data integrity is maintained.

Management has the ultimate responsibility for the assignment of resources and the implementation of control measure oriented to minimize the potential risk to data integrity, and for identifying the residual risk.

The organization of Regulated Companies needs to take responsibility for the systems used and the data they generate. The organizational culture shall ensure data is complete, consistent and accurate in all its forms (i.e. paper and electronic): every operator involved with collection, submission or maintaining data shall be made aware of Data Integrity expectations and continuously monitored.

The stakeholders of process/es outsourced to Third parties which affect the clinical studies, manufacturing, product QC or distribution, are responsible to ensure that the Third parties comply with this policy.

4.1 ALCOA+ Requirements

To ensure that decision making is well informed and to verify that the information is reliable, the events or actions that informed those decisions shall be well documented. As such, Good Documentation Practices (GDocPs) are key to ensuring data integrity, and a fundamental part of a well-designed Pharmaceutical Management System. The application of GDocPs may vary depending on the medium used to record the data (i.e. physical vs. electronic records), but the principles are applicable to both.

The key principles both paper-based and electronic-based recordkeeping are summarized by the acronym ALCOA (Attributable, Legible, Contemporaneous, Original, and Accurate) which have been extended adding the other attributes (Complete, Consistent, Enduring and Available) now termed ALCOA+.

The ALCOA+ expectations reported in the following ensure that events are properly documented and data can be used to support informed decisions.

Attributable. It shall be possible to identify the individual and/or the Computerized System who performed the recorded task. The need to document who performed the task / function, supports that the function was performed by trained and qualified personnel. This applies to changes made to records as well: corrections, deletions, changes, etc.

Legible. All records must be legible – the information must be readable during its retention period. This applies to all information that would be required to be considered Complete, including all Original records or entries. Where the 'dynamic' nature of electronic data (see related definition in section 5.2) is significant to the content and meaning of the record, the ability to interact with the data using a suitable application shall be preserved within the Retention Period (i.e. data shall be maintained in an electronic format which allow to interact with data for elaborations, trending).

Contemporaneous. The evidence of actions, events or decisions shall be recorded as they take place. This documentation shall serve as an accurate attestation of what was done, or what was decided and why, i.e. what influenced the decision at that time.

Original. The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state shall remain available in that state.

Accurate. Ensuring results and records are accurate is achieved through many elements of a robust Pharmaceutical Quality System. This can be comprised of:

- Equipment-related factors such as qualification, calibration, maintenance and computer validation.
- policies and procedures to control actions and behaviors,
- data review procedures to verify adherence to procedural requirements
- deviation management including root cause analysis, impact assessments and CAPA
- Trained and qualified personnel who understand the importance of following established procedures and documenting their actions and decisions.

Complete. All information that would be critical to recreate an event is relevant. The level of detail required for an information set to be considered complete would depend on the criticality of the information. A complete record of data generated electronically includes relevant metadata.

Consistent. Good Documentation Practices shall be applied throughout any process, without exception, including deviations and changes that may occur during the process.

Enduring. Part of ensuring records are available is making sure they exist for the entire period during which they might be needed. This means they need to remain intact and accessible as an indelible/durable format.

Available. Records must be available for review at any time during the required retention period, accessible in a readable format to personnel responsible for their review whether for routine release decisions, investigations, trending, annual reports, audits or inspections.

Together, these elements aim to ensure the accuracy of information, including scientific data, which is used to make critical decisions about the quality of products.

5 MAIN DEFINITIONS

5.1 Acronyms

«CSV»	Computerized Systems Validation
«ER»	Electronic Record
«ERES»	Electronic Record & Electronic Signature
«ERP»	Enterprise Resource Planning
«ES»	Electronic Signature
«FAT»	Factory Acceptance Testing
«GAMP»	Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture (issued by ISPE)
«GxP»	Good 'X' Practice where 'X' is used as a collective term for GCP – Good Clinical practice, GLP – Good Laboratory Practice GMP – Good Manufacturing Practice GPvP – Good Pharmacovigilance Practice
«HW»	Hardware
«IQ»	Installation Qualification (i.e. Configuration Testing)
«ISPE»	International Society for Pharmaceutical Engineering
«LIMS»	Laboratory information management system
«OQ»	Operational Qualification (i.e. Functional Testing)
«OS»	Operating System
«PC»	Personal Computer
«P&ID»	Piping and Instrumentation Diagram
«PCS»	Process Control System
«PIC/S»	Pharmaceutical Inspection Convention-Pharmaceutical Inspection Co-operation Scheme
«PLC»	Programmable Logic Control
«PQ»	Performance Qualification (i.e. Requirement Testing)
«QC»	Quality Control
«QMS»	Quality Management System
«QRM»	Quality Risk Management
«R&D»	Research & Development
«RACI»	Responsible, Accountable, Consulted, Informed
«RAI»	Risk Assessment Index
«RFI»	Request For Information
«RT»	Requirements Testing
«SAT»	Site Acceptance Testing
«SME»	Subject Matter Expert
«SOP»	Standard Operating Procedure
«SW»	Software
«WHO»	World Health Organization

5.2 Definitions

«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.

«Computerized System» - A computerized system collectively controls the performance of one or more automated business processes. It includes computer hardware, software, peripheral devices, networks (if any), personnel and documentation, (e.g. manuals and standard operating procedures).

«Computerized System Validation» - Computerized Systems Validation is the confirmation by examination and provision of objective evidence that computerized system (hardware and software) specifications conform to user needs and intended use, and that all requirements can be consistently fulfilled.

«Data» - Information derived or obtained from raw data (e.g. a reported analytical result). Data shall meet the following ALCOA+ requirements:

A - Attributable to the person generating the data
L - Legible and permanent
C - Contemporaneous
O - Original record (or 'true copy')
A – Accurate
'+' is referring to the additional measures ensuring that data are Complete, Consistent, Enduring, and Available.

«Data Lifecycle» - Encompass all phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive/retrieval and destruction. The procedures for destruction of data shall consider data criticality and, where applicable, legislative retention requirements. Archival arrangements shall be in place for long term retention of relevant data in compliance with legislation.

«Data Processing» - A sequence of operations performed on data in order to extract, present or obtain information in a defined format. Examples might include: statistical analysis for Annual Product Review. The traceability of any human defined parameter used within data processing activities shall be ensured. Audit trails and retained records shall allow reconstruction of all data processing activities regardless of whether the output of that processing is subsequently reported or otherwise used. If data processing has been repeated with progressive modification of processing parameters this shall be visible to ensure that the processing parameters are not being manipulated to achieve a more desirable end point.

«Data Review» - There shall be a procedure that describes the process for data review and approval. Data review shall also include a review of relevant metadata (i.e. audit trails). Review shall be based upon original data or a true copy. Data review shall be documented. A procedure shall describe the actions to be taken if data review identifies an error or omission. This procedure shall enable data corrections or clarifications to be made in a GMP compliant manner, providing visibility of the original record and audit trail traceability of the correction, using ALCOA+ principles

«Dynamic Record» - Records in dynamic format, such as electronic records that allow 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.

«Metadata» - Metadata is data that describes the attributes of other data, providing context and meaning. Typically, this data describes the structure, data elements, inter-relationships and other characteristics of the data. It also permits data to be attributable to an individual (or if automatically generated, to the original data source). Metadata forms an integral part of the original record. Without metadata, the data has no meaning.

«Original record» - Data as the file or format in which it was originally generated, preserving the integrity (accuracy, completeness, content and meaning) of the record, e.g. original paper record of manual observation, or electronic raw

data file from a computerized system. This data must permit full reconstruction of the activities resulting in the generation of the data.

«Primary Record» - Record which takes primacy in cases where data that are collected and retained concurrently by more than one method fail to concur.

«Regulated Data» - Data used for GMP purposes, required by GMP Regulations, relied upon for operations, which might affect the Patient Safety and Product Quality.

«Sample Turn-Around Time» - The Sample Turn-Around Time is the temporal period between the sample creation up to the completion of analyses related to the sample. In short, it is the time needed to complete all the analyses for a batch. This factor shall be defined adequately since, if the expectation is a short turn-around time, the operators might be inclined to violate the data integrity in order to meet the expected period.

«Regulated Company» - a Company which has to comply with GMP requirements upon legal obligations or business reasons.

«Static Record» - A static record is a fixed-data document such as a paper record or an electronic image. Examples of a static record include list of training records or a static image created during the data acquisition

«True Copy» - A copy of original information has to be an exact copy having all the same attributes and information of the original record. True copy must preserve integrity, accuracy, complete content, date formats, electronic signature, authorizations and full audit trail. The process of making a true copy (either printed or electronic) must be certificated, fully described and the copy has to be verified by applying date and signature on paper or by applying a validated electronic signature. A true copy may be retained in a different electronic file format to the original record, if needed, but must retain the equivalent static/dynamic nature of the original record.

IV. DATA INTEGRITY ENABLERS

6. Data governance system

6.1 Data governance system

Data governance is the sum of total of arrangements which provides assurance of data integrity. These arrangements ensure that data, irrespective of the process, format or technology in which it is generated, recorded, processed, retained, retrieved and used will ensure a complete, consistent and accurate record throughout the data lifecycle.

Data governance shall address data ownership and accountability throughout the lifecycle, and consider the design, operation and monitoring of processes/systems to comply with the principles of data integrity including control over intentional and unintentional changes to data.

Data governance systems shall be integral to the Pharmaceutical Quality System (QMS) for each GMP stage of the Pharmaceutical Life Cycle: the QMS shall address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes / systems in order to comply with the principles of data integrity, including control over intentional and unintentional changes to and deletion of information.

An effective data governance system will demonstrate Management’s understanding and commitment to reliable data governance practices including the necessity for a combination of appropriate organizational culture and behaviors (section 7.4) and an understanding of risk associated to data and data lifecycle. Expectations for Data Integrity shall be communicated to personnel at all levels in a documented manner; the communications shall set forth to require open reporting of violations observed by operators to the relevant responsible persons and to allow personnel to recommend improvements oriented to prevent data falsifications. This reduces the incentive to falsify, alter or delete data.

Data Governance systems shall include staff training with regard to the importance of data integrity principles and the creation of a working environment that enables visibility, and actively encourages reporting of errors, omissions and undesirable results.

The extent of Management's knowledge and understanding of data integrity can influence the organization's success of data integrity management. Management must know their legal and moral obligation (i.e., duty and power) to prevent data integrity lapses from occurring and to detect them, if they shall occur.

6.2 Risk management approach to data governance

Quality risk management (QRM) is essential for an effective data Management Program. The effort and resources assigned to data and record management shall be commensurate with the risk: the risk-based approach to record and data management shall ensure that adequate resources are allocated and that control strategies for the assurance of the integrity of GMP data are commensurate with their potential impact on product quality and patient safety and related decision-making.

As not all data or processing steps have the same importance to product quality and patient safety, risk management shall be utilized to determine the importance of each data/processing step. An effective risk management approach to data governance shall be based upon Risk to Data Integrity determined by the following factors:

- Data criticality (impact to decision making and product quality)
- Exposure to violation (opportunity for data alteration and deletion, and likelihood of detection / visibility of changes by the manufacturer's routine review processes). The exposure is determined by the potential to be deleted, amended or excluded without authorization and the opportunity for detection of those activities and events.

The risks to data may be increased by complex, inconsistent processes with open-ended and subjective outcomes, compared to simple tasks that are undertaken consistently, are well defined and have a clear objective.

Reduced effort and/or frequency of control measures may be justified for data that has a lesser impact to product or patient safety; if those data are obtained from a process that does not provide the opportunity for amendment without high-level system access or specialist software/knowledge.

Organizations are expected to implement, design and operate a documented system that provides an acceptable state of control based on data integrity risk with supporting rationale. An example of a suitable approach is to perform a data integrity risk assessment (DIRA) where the processes that produce data or where data is obtained are mapped out and each of the formats and their controls are identified and the data criticality and inherent risks documented.

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 / result (i.e. is the process open-ended or well defined?)
- Outcome of a comparison between of electronic system data and manually recorded events could be indicative for malpractices (e.g. apparent discrepancies between analytical reports and raw-data acquisition times).

6.3 Data Life Cycle

The data lifecycle refers to how data is generated, processed, reported, checked, used for decision-making, stored and finally discarded at the end of the retention period. Data relating to a product or process may cross various boundaries within the lifecycle. This may include data transfer between manual and IT systems, or between different organizational boundaries; both internal (e.g. between production, QC and QA) and external (e.g. between service providers or contract givers and acceptors).

Data governance, as described in the previous section, must be applied across the whole data lifecycle to provide assurance of data integrity. Data can be retained either in the original system, subject to suitable controls, or in an appropriate archive.

Data may be generated by recording:

- **On paper**, a paper-based record of a manual observation or of an activity. Data generated manually on paper may requires independent verification if deemed necessary from the data integrity risk assessment or by another requirement. Consideration shall be given to risk-reducing supervisory measures, specifically for data associated to high criticality
- **Electronically**, using a tool that ranges from simple machines (equipment) to complex computerized systems. The inherent risk to data integrity related to equipment and computerized systems may differ depending upon the degree to which the system (generating or using the data) can be configured, and the potential for manipulation of data during transfer between computerized systems during data lifecycle. The use of available technology, suitably configured to reduce data integrity risk, shall be promoted. Simple electronic systems with no configurable software and no electronic data retention (e.g. pH meters, balances and thermometers. In any case a thorough system assessment is mandatory since all the systems mentioned as examples may have a very complex structure) may only require calibration, whereas complex systems require 'validation for intended purpose' (see section 8.1). It is important not to overlook systems of apparent lower complexity. Within these systems, it may be possible to manipulate data or repeat testing to achieve the desired outcome with limited opportunity for detection (e.g. stand-alone systems with a user-configurable output such as ECG machines, FTIR, UV spectrophotometers).
- **Using a hybrid system** where both paper-based and electronic records constitute the original record. Where hybrid systems are used, it shall be clearly identified the Primary Records (in any case all evidences shall be reviewed and retained). Hybrid systems shall be designed to ensure they meet the desired objective.
- **Other means** such as photography, imagery, and chromatography plates. Where the data generated is captured by a photograph or imagery (or other media), the requirements for storage of that format throughout its lifecycle shall follow the same considerations as for the other formats, considering any additional controls required for that format.

Raw data is defined as the original record (data) which can be described as the first-capture of information, whether recorded on paper or electronically. Irrespective of the format (paper or electronic), Raw Data shall meet ALCOA+ requirements. Information that is originally captured in a dynamic state shall remain available in that state. Raw data must permit full reconstruction of the activities. Where this has been captured in a dynamic state and generated electronically, paper copies cannot be considered as 'raw data'.

Raw data is defined as the original record (data) which can be described as the first-capture of information, whether recorded on paper or electronically.

Irrespective of the format (paper or electronic), Raw Data shall meet ALCOA+ requirements. Information that is originally captured in a dynamic state shall remain available in that state.

Raw data must permit full reconstruction of the activities.

In case dynamic data (according to the definition of this guidance) have been captured, paper copies cannot be considered as 'raw data'. In case technological constraints do not allow to preserve the dynamic nature of records, the available options should be assessed based on risk and the importance of the data over time.

The directives for archiving are included in the section 8.4.2.

In the case of basic electronic equipment that does not store electronic data, or provides only a printed data output (e.g. balances or pH meters), then the printout constitutes the raw data. Where the basic electronic equipment does store electronic data permanently and only holds a certain volume of data before overwriting; this data shall be periodically reviewed, where necessary reconciled against paper records, and extracted as electronic data where this practice is supported by the equipment itself.

ALCOA+ requirements applies also to Metadata (see 5.2).

6.4 Organizational Requirements

6.4.1 Quality culture

The impact of organizational culture, behavior driven by performance indicators, objectives and senior management behavior on the success of data governance measures shall not be underestimated. The data governance policy (or equivalent) shall be endorsed at the highest levels of the organization.

Management shall create a work environment (i.e. Quality Culture) that is transparent and open, where personnel is encouraged to freely communicate failures and mistakes, including potential data reliability issues, so that corrective and preventive actions can be taken.

Organizational reporting structure shall permit the information flow between personnel at all levels. Good data governance in 'open' cultures may be facilitated by employee empowerment to identify and report issues through the Quality System. In 'closed' cultures, a greater emphasis on oversight and secondary review may be required to achieve an equivalent level of control due to the social barrier of communicating undesirable information. The availability of anonymous escalation to senior management may also be of greater importance in this situation.

Management can foster quality culture through the following:

- Ensure awareness and understanding of expectations (e.g. Code of Ethics and Code of Conduct);
- Lead by example, management shall demonstrate the behaviors they expect to see
- Ensure accountability for actions and decisions;
- Stay continuously and actively involved;
- Set realistic expectations, considering limitations which place pressures on employees;

6.4.2 Code of ethics and policies

A Code of Values & Ethics shall reflect Management's philosophy on quality, achieved through policies (i.e. a Code of Conduct) that are aligned to the Quality Culture and develop an environment of trust, where all individuals are responsible and accountable for ensuring patient safety and product quality.

The company's general ethics and integrity standards need to be established and known to each employee and these expectations shall be communicated frequently and consistently.

Code of Conduct policies shall clearly define the expectation of an ethical behavior, such as honesty. This shall be communicated to and be well understood by all personnel. The communication shall not be limited only to knowing the requirements, but also to why they were established and the consequences of failing to fulfill the requirements. Unwanted behaviors, such as deliberate data falsification, unauthorized changes, destruction of data, or other conduct that compromises data integrity shall be addressed promptly. Disciplinary actions shall be taken, when warranted. Similarly, conforming behaviors shall be recognized appropriately.

6.4.3 Training Programs

Personnel shall be trained in data integrity policies and agree to abide by them. Management shall ensure that personnel are trained to understand and distinguish between proper and improper conduct (including deliberate falsification), and shall be made aware of the potential consequences.

In addition, key personnel, including managers, supervisors and quality unit personnel, shall be trained in measures to prevent misdemeanors and detect suspicious data.

Management shall also ensure that when recruiting and periodically afterwards (as needed) all personnel is trained in procedures to ensure GDocP for both paper and electronic records.

6.4.4 Pharmaceutical Quality System Enhancement

The application of modern quality risk management principles and good data management practices to the current Pharmaceutical Quality System serves to modernize the Quality System in order to meet the challenges that come with the generation of complex data.

The company's Pharmaceutical Quality System shall be able to prevent, detect and correct weaknesses in the system or their processes that may lead to data integrity lapses. The company shall know their data life cycle and integrate the appropriate controls and procedures such that the data generated will be valid, complete and reliable. Specifically, such control and procedural updating may be in the following areas:

- Risk assessment and management
- Investigation programs (oriented to prevent Data Integrity violations and/or to investigate observed violations)
- Data review practices
- Computer software validation
- Vendor/contractor management
- Training program to include company's data integrity policy and data integrity SOPs
- Self-inspection program to include data integrity
- Quality metrics and reporting to senior management.

Critical thinking skills shall be used to determine whether control and review procedures effectively achieve their desired outcomes. An indicator of data governance maturity is an organizational understanding and acceptance of residual risk, which prioritizes actions. An organization which believes that there is 'no risk' of data integrity failure is unlikely to have made an adequate assessment of inherent risks in the data lifecycle. The approach to assessment of data lifecycle, criticality and risk shall therefore be examined in detail. This may indicate potential failure modes which can be investigated during an inspection.

6.4.5 Quality metrics for Data Integrity

There shall be regular management reviews of quality metrics, including those related to data integrity, such that significant issues are identified, escalated and addressed in a timely manner. Caution shall be taken when key performance indicators have been selected in a way that gives data integrity a low importance and priority.

Quality metrics shall address the following type of actions:

- **Preventive**, oriented to oversee the rules expected to prevent Integrity failures (e.g. Operators/Supervisor Data Integrity Awareness Rate, Sample Turn Around Time)
- **Corrective**, oriented to monitor the completion and outcome of records compliance vs ALCOA+ requirements (e.g. Electronic Records Assessed Rate, Integrity Corrective Action Rate)
- **Monitoring**, oriented to supervise the number of actual integrity failures and the relevant follow up (e.g. Data Integrity Internal Verification Rate, Spontaneous Integrity Failures Rate, i.e. Reported by operators)

These metrics, aimed to demonstrate management commitment to ensure the integrity of GMP Data Management, shall have an independent expert periodically verifying the effectiveness of their systems and controls.

7. REQUIREMENTS FOR REGULATED PAPER RECORDS

7.1 QMS for Record Management

The effective management of paper based documents is a key element of Pharmaceutical QMS in any stage of the Product Life Cycle. Accordingly, the documentation system shall be designed to meet GMP requirements and ensure that documents and records are effectively controlled to maintain their integrity.

In all cases where Paper Records are generated and relied upon to ensure Patient Safety and Product Quality, these records must be controlled and must remain reliable throughout the data lifecycle, i.e. meeting the ALCOA+ requirements.

Procedures outlining good documentation practices and arrangements for document control shall be available within the QMS. These procedures shall specify:

- How master documents and procedures are created, reviewed and approved for use during their life-cycle
- Generation, distribution and control of templates used to record data (master, logs, etc.)
- Retrieval and disaster recovery processes regarding records
- Process of working copies generation for routine use, with specific emphasis on ensuring copies of documents, (e.g. SOPs and blank forms) are issued and reconciled for use in a controlled and traceable manner
- Guidance for the completion of paper based documents, specifying how individual operators are identified, data entry formats and amendments to documents are recorded
- How completed documents are routinely reviewed for accuracy, authenticity and completeness
- Processes for the filing, retrieval, retention, archival and disposal of records

7.2 Record Creation

7.2.1 Records Generation

Paper records shall be created according to the following measures:

- All documents shall have a unique identification number (including the version number) and shall be checked, approved, signed and dated.
- Use of uncontrolled documents shall be prohibited by local procedures; similarly, the use of temporary recording practices, (e.g. scraps of paper) shall be prohibited.
- Document design shall provide sufficient space for manual data entries, to ensure that handwriting data are clear and legible. What data is to be provided for each entry has to be clearly specified.
- Documents shall be stored in a manner, which ensures appropriate version control.
- Unauthorized or inadvertent changes to Master copy (in soft copy) shall be prevented
- Unauthorized or inadvertent changes to Master copy (i.e. form attached to an SOP and copied to fill out the form) shall be prevented
- Risk of someone inappropriately using and/or falsifying a record ‘by ordinary means’ (i.e. not requiring the use of specialist fraud skills) has to be reduced to an acceptable level.

For template records stored electronically, the following precautions shall be in place:

- Access to master templates shall be controlled
- Process controls for creating and updating versions shall be clear and practically applied/verified
- Master documents shall be stored in a manner which prevents unauthorized changes

Master copies shall contain distinctive marking so to distinguish the master from a copy, e.g. use of colored papers or inks to prevent inadvertent use.

An index of all the template records shall be maintained by QA organization. This index shall mention for each type of template record at least the following information: title, reference number including version number, location (e.g., documentation database, effective date, next review date, etc.).

Records shall be appropriately controlled in the production areas by designated persons or processes. These controls shall be carried out to minimize the risk of damage or loss of the records and ensure data integrity.

7.2.2 Records Distribution

Paper Regulated Records shall be distributed according to the following measures:

- Updated versions shall be distributed in a timely manner, ensuring that only the current approved version is available for use
- Obsolete master documents and files shall be archived and their access restricted.
- Any issued and unused physical documents shall be retrieved and destroyed accordingly
- Issuing shall be controlled using a secure stamp, or paper color code not available in the working areas or another appropriate system.
- Blank documents shall be identified through a unique identifier, the creation of each document shall be numbered and recorded

7.2.3 Record Processing & Completion

- Handwritten entries must be made by the person who executed the task.
- Unused, blank fields within documents shall be crossed-out, dated and signed.
- Handwritten entries shall be made in clear and legible writing
- The completion of date fields shall be done in the format defined for the site (E.g. dd/mm/yyyy or mm/dd/yyyy)
- Filling out operations shall be contemporaneous
- Records shall be indelible. The use of pencils is not allowed
- Records shall be signed and dated using a unique identifier that is attributable to the author.
- The traceability of any user defined parameters, within data processing activities, shall be ensured. Records shall allow reconstruction of all data processing activities, regardless of whether the output of that processing is subsequently reported or otherwise used. If data processing has been repeated with progressive modification of processing parameters, this shall be visible to ensure that the processing parameters are not being manipulated to achieve a more desirable end point.
- Corrections to the records must be made in such way that full traceability is maintained, including:
    - Cross out what is to be changed in a way keeping the initial data readable (e.g. with a single line).
    - Where appropriate, the reason for the correction must be clearly recorded and verified if critical.
    - Who and when the change has been made (Initials and date).

7.3 Records Review

The approach to reviewing specific record content, such as critical paper records and associated correction shall be oriented to ensure that ALCOA+ requirements are verified and all applicable regulatory requirements are met.

There shall be a procedure that describes the process for review and approval of data. Data review shall be documented and the record shall include a positive statement regarding whether issues were found or not, the date when review was performed and the signature of the reviewer.

A procedure shall describe the actions to be taken if data review identifies an error or omission. This procedure shall enable data corrections or clarifications to provide visibility of the original record, and traceability of the correction, using ALCOA+ principles.

In case of outsourced processes, the pharmaceutical company shall ensure that critical data generated by the supplier are reviewed; the responsibilities for data review must be documented and agreed by both parties.

7.4 True Copies

7.4.1 True copies of Paper Records

Copies of original paper records (e.g. analytical summary reports, validation reports etc.) are generally very useful for communication purposes, e.g. between companies operating at different locations. These records must be controlled during their life cycle to ensure that the data received from another site (sister company, contractor etc.) are maintained as “true copies” where appropriate, or used as a “summary report” where the requirements of a “true copy” are not met (e.g. summary of complex analytical data).

A true copy shall ensure that the full meaning of the data are kept and its history may be reconstructed.

Original records and true copies must preserve the integrity of the record. True copies of original records may be retained in place of the original record (e.g. scan of a paper record), if a documented system is in place to verify and record the integrity of the copy. Organizations shall consider any risk associated with the destruction of original records.

7.4.2 Paper records generated from Computer Systems

Paper records generated by very simple electronic systems, e.g. balances, pH meters or simple processing equipment which do not store data provide limited opportunity to influence the presentation of data by (re-)processing, changing of electronic date/time stamps. In these circumstances, the original record shall be signed and dated by the person generating the record and the original shall be attached to batch processing records.

This approach is allowed only for very simple systems and for records whose content is static.

A static record format, such as a paper or electronic record, is one that is fixed and allows little or no interaction between the user and the record content. For example, once printed or converted to static electronic format records lose the capability of being reprocessed or enabling more detailed viewing of baselines.

Conversely, Records in dynamic format, such as electronic records, allow an interactive relationship between the user and the record content. For example, electronic records in database formats allow the user to track, trend and query data; chromatography records maintained as electronic records allow the user or reviewer (with appropriate access permissions) to reprocess the data and expand the baseline to view the integration more clearly.

Many electronic records are important to retain in their dynamic (electronic) format, to enable interaction with the data. This shall be justified based on risk. For these type of Records, the maintenance of the sole Paper Records and the deletion of the corresponding Electronic Records shall be prohibited.

7.5 Records Retention

The retention period of each type of records shall (at a minimum) meet those periods specified by the relevant GMP requirements. Consideration shall be given to other local or national legislation that may stipulate longer storage periods. The records can be retained internally or by using an outside storage service subject to quality agreements.

Archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period.

7.6 Records Disposal

A documented process for the disposal of records shall be in place to ensure that the correct original records are disposed of after the defined retention period. The system shall ensure that current records are not destroyed by accident and that historical records do not inadvertently make their way back into the current record stream (e.g. historical records confused/mixed with existing records.)

A record/register shall be available to demonstrate appropriate and timely destruction of retired records.

Measures shall be in place to reduce the risk of deleting the wrong documents. The access rights allowing deletion of records shall be limited to few persons.

In case of printouts which are not permanent (e.g. thermo transfer paper) a verified (‘true’) copy may be retained, and it is possible to discard the non-permanent original. Paper records may be replaced by Scans provided that the principles of ‘true copy’ are addressed (see section 7.4).

8. REQUIREMENTS FOR REGULATED ELECTRONIC RECORDS

Regulated Electronic records (i.e. generated and relied upon to ensure Patient Safety and Product Quality) are managed through a large variety of computerized systems used by companies to assist in a significant number of operational activities. These range from the simple standalone to large integrated and complex systems, many of which have an impact on the quality of products manufactured. It is the responsibility of each regulated entity to fully evaluate and control all computerized systems and manage them in accordance with GMP requirements.

Organizations shall be fully aware of the nature and extent of computerized systems utilized, and assessments shall be in place that describe each system, its intended use and function, and any data integrity risks or vulnerabilities that may be susceptible to manipulation. Particular emphasis shall be placed on determining the criticality of computerized systems and any associated data, in respect to product quality.

All computerized systems with potential impact on product quality shall be effectively managed under a mature quality framework, which is designed to ensure that systems are protected from acts of accidental or deliberate manipulation, modification or any other activity that may impact on data integrity.

When determining data vulnerability and risk, it is important that the computerized system is considered in the context of its use within the business process.

In order to ensure that Regulated Electronic records are meeting the ALCOA+ requirements the relevant Computerized Systems shall ensure Reliability, Security, Traceability, Inspect ability and Accountability.

These requirements are reflected in the Annex 11 to the Regulation No. 916 “On the approval of Rules of Good manufacturing practices” which defines the regulatory requirements for GMP critical Records managed through Computerized Systems, which are oriented to ensure the Integrity of those data managed through automated systems.

8.1 Computer System Validation

Computerized systems shall comply with regulatory requirements and associated guidance, which include the Validation requirement: systems shall be validated for their intended purpose which requires an understanding of the computerized system’s function within a specific company process.

Computerized System Validation (CSV) is the documented process of “achieving and maintaining compliance with applicable GMP regulations and fitness for intended use by the adoption of principles, approaches, and life cycle activities within the framework of validation plans and reports and by the application of appropriate operational controls throughout the life of the system”.

To assure the integrity of electronic data, computerized systems shall be validated at a level appropriate for their use and application. Validation shall address the necessary controls to ensure the integrity of data, including original electronic data and any printouts or PDF reports from the system. In particular, the approach shall ensure that ALCOA+ requirements will be met and that data integrity risks will be properly managed throughout the data life cycle. Therefore it is required the implementation and confirmation during validation of computerized systems and subsequent change control, that all necessary controls to ensure the integrity of Data are in place and that the occurrence of errors in the data is minimized.

The validation activities shall ensure that configuration settings and design controls for Data Integrity are enabled and managed across the computing environment (including both the software application and operating systems environments). Activities include, but are not limited to:

- documenting configuration specifications for commercial off-the-shelf systems as well as user-developed systems, as applicable
- restricting security configuration settings for system administrators to independent personnel, where technically feasible
- disabling configuration settings that allow overwriting and reprocessing of data without traceability
- restricting access and implementation of time/date stamps.

The acceptance of vendor-supplied validation data in isolation from system configuration and users intended use is not acceptable. In isolation from the intended process or end-user IT infrastructure, vendor testing is likely to be limited to functional verification and may not fulfil the requirements for performance qualification.

This document integrates a risk-based Computerized System Validation methodology into business processes, specifying documentation required for each of the validation phases, and responsibilities to each step in the validation process. Section 9 of this document integrates industry best practices for risk-based computerized system validation, incorporating guidance and methodology from guidelines released by the most important associations (i.e. PIC/S, ISPE).

8.1.1 Data capture/entry

Systems shall be designed for the correct capture of data whether acquired through manual or automated means.

For manual entry:

- The entry of data shall only be made by authorized individuals and the system shall record details of the entry, the individual making the entry and when the entry was made
- Data shall be entered in a specified format that is controlled by the software, validation activities shall verify that invalid data formats are not accepted by the system
- All manual data entries shall be verified, either by a second operator, or by a validated computerized means in case the entried data may have an impact on Product Quality and Patient Safety
- Changes to entries (including reason) shall be captured in the audit trail and reviewed by an appropriately authorized and independent person, according to the relevant risk to Product Quality and Patient Safety
- For automated data capture:
- The interface between the originating system, data acquisition and recording systems shall be validated to ensure the accuracy of data
- Data captured by the system shall be saved into memory in a format that is not vulnerable to manipulation, loss or change
- The system software shall incorporate validated checks to ensure the completeness of data acquired, as well as any metadata associated with the data
- Any necessary changes to data must be authorized and controlled in accordance with approved procedures. For example, manual integrations and reprocessing of laboratory results must be performed in an approved and controlled manner. The firm's Quality Unit must establish measures that ensure that changes to data are performed only when necessary and by designated individuals.

8.2 Security

8.2.1 System Access

User access controls, both physical and electronic, shall be configured and enforced to prohibit unauthorized access to, changes to and deletion of data.

Individual Login IDs and passwords shall be set up and assigned for all staff needing to access and utilize the specific electronic system. Shared login credentials do not allow traceability to the individual who performed the activity; for this reason, shared passwords (even if justified for reasons of financial savings) must be prohibited.

In case the system does not include the functionality for access control (e.g. if it does not require password or a shared user account is to be used), one of the following equivalent control measures shall implemented:

- Paper-based manual log providing traceability of accesses to the system
- Third-party software which allows to limit the access to the system to pre-authorized operators

The suitability of these alternative methods shall be justified and documented.

8.2.2 User Authorizations

Full use shall be made of access controls to ensure that people have access only to functionality that is appropriate for their job role, and that actions are attributable to a specific individual. Companies must be able to demonstrate the access levels granted to individual staff members and ensure that historical information regarding user access level is available.

Access controls shall be applied to both the operating system and application levels. Individual login at operating system level may not be required if appropriate controls are in place to ensure data integrity (e.g. no modification, deletion or creation of data outside the application is possible).

Administrator access to computer systems used to run applications shall be controlled. General users shall not have access to critical aspects of the software, e.g. system clocks, file deletion functions, etc. System Administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) shall not be assigned to individuals with a direct interest in the data (data generation, data review or approval).

User Authorization scheme shall ensure the Segregation of Duties.

8.2.3 Backup

The Backup and recovery processes shall be documented through a procedure defining the backup operations and the restore steps to be executed in case of need. The Backup and recovery processes shall be tested to ensure the capability to fully recover data and a metadata in case of system failure. A mechanism (either automatic or manual) of backup verification shall be in place to ensure that it has functioned correctly.

Backup and recovery processes shall be documented (e.g. addressed by a procedure), validated and periodically tested. Each back up shall be verified to ensure that it has functioned correctly.

Routine backup copies (i.e. media where backup data are saved) shall be stored in a remote location (physically separated) in the event of disasters.

8.2.4 Data Migration Verification

Data transfer/migration is the process of transferring data and metadata between storage media types or computerized systems. Data migration where required may change the data format for making it usable or visible on an alternative computerized system.

Data transfer/migration procedures shall include a rationale, and be robustly designed and validated to ensure that data integrity is maintained during the data lifecycle.

8.3 Traceability

8.3.1 Audit Trail

System shall ensure the automatic capture of audit trail, which is a form of metadata that contains information associated with actions that relate to the creation, modification or deletion of regulated Electronic record. An audit trail provides secure recording of life-cycle details such as creation, additions, deletions or alterations of information in a record, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the “who, what, when and why” of the action.

Audit trails records shall be in an intelligible form and have at least the following information:

- Name of the person who made the change to the data;
- Description of the change
- Time and date of the change
- Reason for the change

Audit trail functionalities must be enabled and locked at all times. As the other functionalities oriented to ensure the Data Integrity, Audit trails shall be verified during validation of the system.

System shall rely upon appropriately controlled/synchronized clocks for recording timed events to ensure reconstruction and traceability, including information of the time zone where this data is used across multiple sites. Operators shall be not allowed to change the Time reference and/or the Time zone.

In case systems lack appropriate automatic audit trails, paper based record to demonstrate changes to GMP critical data shall be implemented only as an interim action until a fully audit trailed (integrated system or independent audit software using a validated interface) system becomes available.

8.3.2 Audit Trail Review

The Audit Trail data related to Regulated Electronic Records shall be audited by the regulated user in order to verify that operations have been performed correctly and whether any change (modification, deletion or overwriting) has been made to the original information in electronic records. All changes must be duly authorized.

The review of relevant data-related audit trails shall be part of the routine data review within the approval process.

The frequency, roles and responsibilities of audit trails review shall be based on a risk assessment according to the GMP relevance of the data recorded in the computerized system. For example, for changes to electronic data that can have a direct impact on the quality of the medicinal products, it would be expected to review the audit trail at each and every time the data is generated or at the point of use of the data (i.e. when data is relied upon for a GMP critical decision).

The regulated user shall establish a SOP that describes in detail how to review audit trails. The procedure shall determine in detail the process that the person in charge for the audit trail review shall follow.

The audit trail activity shall be documented and recorded. The records shall be maintained together with the other GMP relevant documents.

8.4 Inspectability

8.4.1 Electronic Copies

System shall allow to create generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the Inspectors.

8.4.2 Archiving

Data shall be archived periodically in accordance with written procedures. Archived copies shall be physically secured in a separate and remote location from where back up data is stored.

Data shall be accessible and readable and its integrity maintained for all the period of archiving.

There shall be in place a procedure for restoring archived data in case an investigation is needed. The procedure in place for restoring archived data shall be regularly tested.

When legacy systems can no longer be supported, consideration should be given to maintaining the software for data accessibility purposes (for as long possible depending upon the specific retention requirements). This may be achieved by maintaining software in a virtual environment.

Migration to an alternative file format that retains as much as possible of the ‘true copy’ attributes of the data may be necessary with increasing age of the legacy data. Where migration with full original data functionality is not technically possible, options should be assessed based on risk and the importance of the data over time. The migration file format should be selected considering the balance of risk between long-term accessibility versus the possibility of reduced dynamic data functionality

8.4.3 Disposal

Procedures shall be in place that describe the process for the disposal of electronically stored data. These procedures shall provide guidance for the assessment of data and allocation during retention periods, and describe the manner in which data that is no longer required is disposed of.

8.5 Accountability

8.5.1 Electronic signature

Electronic signatures used in place of handwritten signatures must have appropriate controls to ensure their authenticity and traceability to the specific person who electronically signed the record(s).

The use of electronic signatures shall be appropriately controlled with consideration given to:

- How the signature is attributable to an individual.
- How the act of ‘signing’ is recorded within the system so that it cannot be altered or manipulated without invalidating the signature or status of the entry.
- How the record of the signature will be associated with the entry made and how this can be verified.

- The security of the electronic signature i.e. so that it can only be applied by the 'owner' of that signature.

It is expected that appropriate validation of the signature process associated with a system is undertaken to demonstrate suitability and that control over signed records is maintained

Where a paper or pdf copy of an electronically signed document is produced, the metadata associated with an electronic signature shall be maintained with the associated document.

Electronic signature or E-signature systems must provide for "signature manifestations" i.e. a display within the viewable record that defines who signed it, the associated role (where possible), and the date (and time, if significant) and the meaning of the signature (e.g. verified or approved).

An inserted image of a signature or a footnote indicating that the document has been electronically signed (where this has been entered by a means other than the validated electronic signature process) is not adequate. Where a document is electronically signed then the metadata associated with the signature shall be retained.

9. RISK BASED VALIDATION LIFE CYCLE

According to this Guidance (section 9.1.1), the Computer Validation process is the ultimate step to ensure the Integrity of the electronic data created and maintained for regulated purposes.

Computerized systems that may have an impact on product or service quality and data integrity are subject to GMP regulations and need to be validated. The purpose of this section is to define the computerized system validation process, throughout the entire system life cycle according to the relevant most important guideline (PIC/S, GAMP) and to provide a procedural framework to meet the requirements set forth by Regulation No. 916 "On the approval of Rules of Good manufacturing practices". This section related to the Computer Validation process defines the activities to be executed before the system is released, and those process to be established during operations until the system is retired.

The validation process provides documented proof enabling to conclude with a high degree of assurance that a computerized system operates as defined in its specifications, as well as to quality and regulatory requirements, in a constant and reproducible manner. In addition, the Validation process shall provide documented evidence that the system includes the automated functionalities oriented to ensure that the GMP critical Electronic Records meet the 'ALCOA+' requirements.

This guidance promotes a risk-based approach to the specification, design, and verification of computerized systems that have the potential to affect product quality and patient safety through the following phases:

- Requirements & Planning: The Planning phase is oriented to address the required activities, responsibilities, procedures, and timelines based upon the risk associated to the System. The implementation project is based upon the User Requirement Specifications (URS) document oriented to detail the Business and User needs (in terms of business processes, compliance processes, and technical and non-functional standards) to be defined in the initial stages of the implementation project.
- Specifications & Build: based upon the URS, a set of specifications documents is created by the supplier/Implementer in order to define the system Design / Configuration. The number and level of detail of the specifications may vary depending upon the type of system and its intended use. A design Review phase is executed including the creation of a Traceability Matrix to demonstrate the relationship between specifications and the corresponding requirements and the execution of Source Code Review in case of custom built system.
- Testing & Acceptance: System Verification is oriented to confirm that specifications have been met: this may involve multiple stages of reviews and testing depending on the type of system, the development method applied, and its use. Testing shall be based upon the outcome of Functional Risk assessment.
- Release: the system is formally accepted for use and release into the operating/production environment in accordance with a controlled and documented process, including the approval from the business process owner, technical owner and quality unit representatives.
- Operation through Supporting Processes: after release, the system will be managed through the Supporting processes oriented to maintain the validated status

- Retirement: when the system is retired, the data maintained by the system shall be made available within the Retention period

It would be normally expected that a prospective validation for computerized systems is conducted; however, for systems already installed, it may be acceptable to perform retrospective validation based on an assessment of all historical records for the existing computerized system.

9.1 Computerized System and Categories

The computerized system shall be considered as composed of all computer hardware, firmware, installed devices, and software controlling the operation of the computer. The controlled function may be composed of equipment to be controlled and operating procedures that define the function of such equipment, or it may be an operation which does not require equipment other than the hardware in the computerized system

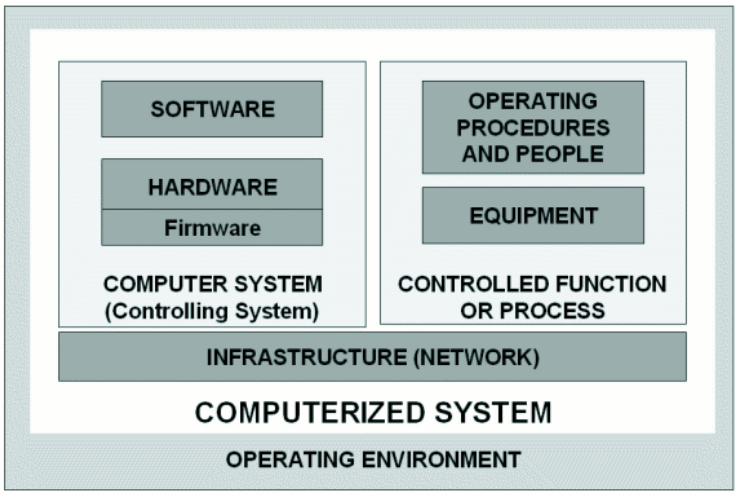

Figure 1 - Good Practices for Computerised Systems in Regulated "GXP" Environments, PI 011-3 25 September 2007

According to this definition the Computerized System shall be considered as including not only the SW Application but all the other entities (connected instruments, IT infrastructure, personnel) which may affect the GMP critical process(es) executed through the System. Each entity shall be documented and maintained under control in order to achieve the validated status.

There is generally increasing risk of failure or defects with the progression from standard software and hardware to custom software and hardware. The increased risk derives from a combination of greater complexity and less user experience. When coupled with risk assessment and supplier assessment, categorization can be part of an effective quality risk management approach.

Most systems have components of varying complexity, such as an operating system, un-configured components, and configured or custom components. In order to facilitate the determination of the appropriate validation strategy and depth, the following categories have been defined.

Category	Type	Description	Example
1	Infrastructure Software	Infrastructure elements link together to form an integrated environment for running and supporting applications and services.	– Established or commercially available layered software (operating systems, database managers, programming languages, middleware, ladder logic interpreters, statistical programming tools, and spreadsheet packages (but not applications developed using these packages) – Infrastructure software tools (e.g. network monitoring software, batch job scheduling tools, security software, anti-virus, and configuration management tools) –
3	Not Configured Products	Run-time parameters may be entered and stored, but the software cannot be configured to suit the business process	– Firmware-based applications – Commercial Off-the-Shelf Software (COTS) – Instruments
4	Configured Products	Software, often very complex, that can be configured by the user to meet the specific needs of the user's business process. Software code is not altered.	– Laboratory Information Management System (LIMS) – Data Acquisition Systems – Supervisory Control and Data Acquisition (SCADA) – Enterprise Resource Planning (ERP) – Clinical Trial Monitoring – Distributed Control System (DCS) – Adverse Drug Reaction (ADR) Reporting – Chromatography Data System (CDS) – Electronic Document Management System (EDMS) – Building Management System (BMS) – Customer Relationship Management (CRM) – Spreadsheets – Simple Human Machine Interface
5	Custom Applications	Software custom designed and coded to suit the business process	– Internally and externally developed IT applications – Internally and externally developed process control applications – Custom ladder logic – Spreadsheets (macro)

Generally, the level of detail and depth of the Validation documentation shall increase with the System category

Complex computerized systems can consist of multiple components that may fall into various categories. In this case, the system shall be categorized according to the highest category of the multiple components

In case one or a limited number of components are customized, the system can be still classified as category 4, specifying the list of customized components which have to be classified as category 5

9.2 System Inventory and GMP Risk Assessment

Regulated companies shall have an inventory of all computerized systems in use. This list shall include reference to:

- Name, version number, system supplier, system owner, location and main function (i.e. intended use) of each computerized system;
- Evaluation of the Risk associated to the System and to the relevant Record(s) maintained by the System (e.g. direct GMP impact, indirect impact, no impact)
- Current validation status of each system and reference to existing validation documents.

Risk assessments shall be in place for each system, specifically assessing the necessary controls to ensure data integrity. The level and extent of validation for data integrity shall be determined based on the criticality of the system and process and potential risk to product quality, e.g. processes or systems that generate or control batch release data would generally require greater control than those systems managing less critical data or processes

Validation scope shall include GMP compliance criteria, ranked for product/process quality and data integrity risk criticality, shall the system fail or malfunction. This process represents one of the most important pre-requisites of Validation Master Planning, in that it is essential to assign priorities and attention to those systems, which may have an impact on Product Quality, Patient Safety and Data Integrity. The risk analyses and the results, together with reasoning for critical or non-critical classifications, shall be documented. Risks potentially impacting on GMP compliance shall be clearly identified.

Automated equipment can be listed in a separate list, it is necessary to avoid duplication of positions in the lists of automated and computerized equipment.

9.3 Supplier Assessment & Quality Agreement

When third parties (e.g. suppliers, service providers or internal IT department) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between Regulated Company and any third party, and these agreements shall include clear statements of each party responsibilities.

Potential and existing Vendors for GMP systems (Computerized System vendors and service providers) are assessed based on the business risk and impact of the considered service or Computerized System.

Assessment of Third Party Quality Systems, as a component of the risk assessment, is considered for determining the extent of validation and potential leveraging on their documentation to support the validation effort.

The target of third party assessment is to determine if computerized system vendors and service providers:

- Can provide a high quality product or service,
- Meet regulatory requirements,
- Have adequate quality processes in place.

Analysis of the system supplier must be performed in order to verify the capability of realizing a product according to Quality Standard and methodology. The assessment method chosen is based on the risk associated to the system, the complexity of the system, and previous experience with the vendor according to the vendor assessment procedure.

9.4 Requirements & Planning Phase

9.4.1 User Requirements Specification

A **User Requirements Specification** (URS) shall be created for all computerized systems. The purpose of the URS document is to define the "intended use" and functions of the system, including all essential requirements.

The extent and detail of requirements shall be commensurate with risk, complexity, and novelty, and shall be sufficient to support subsequent risk analysis, specification, configuration/design, and verification as required.

The User Requirement document specifies if data, managed by the system, is maintained in an electronic format and if data is used for operations having GMP Impact.

URS includes the following:

- Critical-To-Quality features
- Identification of Regulated Electronic Records (ER) maintained by the System and the Regulated Electronic Signature (ES) executed through the System
- Regulatory Requirements for Electronic Records and Electronic Signature Management (also termed ERES Regulations) considered as Applicable
- List of Business processes and associated Process Flows
- Other general type of requirements (e.g. operational requirements, data requirements, technical requirements, interface requirements, environment requirements, performance requirements, availability requirements, and security requirements) shall be included as needed based upon the system type/complexity

The Requirements shall be defined/agreed by the relevant Business Process Owner(s) and shall be listed in consistent naming conventions and with unique reference numbers.

URS are deemed as mandatory also in case of Retrospective validation in order to define the intended use of the system to be verified in the end-to-end final test.

9.4.2 Validation Plan

Validation Plan is a strategic document providing evidence that all the validation activities are adequately addressed, under management control, using a risk based approach.

The document shall identify the validation Life Cycle and the Validation scope through the identification of system boundaries; outcome of the Supplier Assessment shall be considered together with the conditions to leverage the documentations provided by Supplier.

The Validation Plan shall identify the validation documentation to be created with the relevant responsibilities (e.g. RACI table for validation deliverables) and the general acceptance criteria for the validation process.

The Validation Plan shall always be defined in case of new implementation and of major changes.

9.5 Specifications & Build Phase

Depending on system category and complexity, the specification documentation addressed by this section can be combined in a single document.

9.5.1 Functional Specification

The functional specifications shall provide a precise and detailed description of how the system covers the essential requirements for the computer system and external interfaces. This means descriptions of functions, performances and where applicable, design constraints and attributes. The document defines what the system shall do, and what functions and facilities are allowed by the system, including a list of design objectives for the system.

The document shall include details of functional descriptions of Company's system specific requirements, Usage diagrams, Flow charts, Process specifications, External interfaces specifications, Performance specifications, Security and control specifications, Configurable items, Logical data model details, Technology infrastructure specifications, Availability/maintainability specifications.

The Specifications shall be prepared and organized in a way that permits to trace each User Requirements against the corresponding functionalities and associated testing documentation, therefore allowing traceability through the life cycle from individual user requirements to associated tests. The high level description shall be broken down to the level of the individual functions; each function should have a coding system in order to be identified and allow traceability.

Functional Specifications shall be traced against User Requirements, allowing the execution of the Operational Qualification Protocol (i.e. Functional Testing) and the issuing of system's Design Specifications.

9.5.2 Configuration Specifications

The Configuration Specification document is defined in order to:

- describe the list of HW/SW components included in the Computerized System
- describe the system parameters (e.g. password length) which may impact one or more GMP functionality

The Configuration Specification identifies the System Configuration Baseline addressing the SW components and interfaces and the System Parameters, focusing on the configuration items which may affect the GMP functionalities.

A Security Matrix is created (included in the document or in a separated document) in order to identify the user profiles defined in the system and the related functions included. The assignment of the users to each profile shall be executed according to the security-related procedures.

The document shall also describe the IT landscape on which the software resides and how it is to be connected to any existing system or equipment. Therefore the document shall include also (or make reference to other document) a description of the system landscape and a specification of all elements shown on the Landscape (e.g. Operating systems, Middleware, Ancillary Software e.g. PDF viewer, System environments, Interfaces, Relevant IT Infrastructure components e.g. Servers).

9.5.3 Design Specifications

The SW design specifications are required for the customized components in order to provide a detailed, technical explanation of the Functional Specification in order to explain how the system does what is defined in the higher level specifications.

Software shall be designed in accordance with recognized design standards where appropriate. Design Specifications covering software design are required for custom applications: this type of documentation is not normally required for configurable products, where software design is normally reviewed or evaluated as part of supplier assessment.

Software design occurs at two levels. At the higher level it defines the software modules (sub-systems) that form the complete software system, the interfaces between these modules and also the interfaces to other external systems. At the lower level the design describes the operation of the individual software modules. For customized components,

the Design Specification shall document Software development components, Implementation units, User interface design, Interface design, Error handling procedures, and Physical data models.

9.5.4 Detailed Risk Assessment

Detailed Risk Assessment activities are required during the Specification and Build phases through the execution of Process and/or Functional Risk Analysis in order to identify the risks that may impact the correct or reliable functioning of the system at process and function level respectively.

The functional risk assessment identifies regulatory compliance and business risk severity against the existing functionality within the system and the supporting business processes.

The Validation teams along with the business process owner or representatives and technical teams prepare the risk assessment based on the User requirements and/or Functional/Configuration/Design Specifications.

The outcome of the Risk assessment shall include the results of process and/or functional risk analysis executed according to a predetermined methodologies

The Risk Assessment report shall define the Risk mitigation actions, including the testing scope and effort.

9.6 Testing & Acceptance Phase

The system testing is performed to ensure that computerized systems meet their predefined requirements, prior to system release.

The scope of the validation activities during the Test Phase, and the depth of the deliverable documentation, is dependent on scaling factors such as the system level of GMP risk (10.2) and the outcome of the Detailed Risk Assessment (10.5.4), which has identified the riskiest processes/functionalities where the testing shall be focused upon.

The test strategy shall define an appropriate approach to the testing of a specific system, based upon the following:

- Understanding of system components (GAMP categories), overall system complexity and system novelty;
- System GMP Risk Level
- Functional risk assessments outcome;
- Results of supplier assessments, if relevant.

The test strategy may vary widely, e.g., from a simple low GMP risk standard software to a complex high GMP risk software. It shall be defined as early in the project life cycle as feasible, and preferably in parallel with the development of system specifications.

System testing must be organized in different phases, each of them occurring at different stage of the system implementation in a continuous process of quality monitoring.

The testing includes:

- Vendor Testing (e.g. Commissioning Testing, Unit and Integration testing), executed by the SW Supplier according to its Quality System or to a predefined Quality & Project Plan,
- Validation Testing, executed in the qualification and/or production environment according to pre-defined protocols for the following Validation Testing phases:
    - Installation Qualification
    - Operational Qualification
    - Performance Qualification

In case the Supplier Assessment determines that the vendor's quality management and testing practices are appropriate, then testing done by the vendor as part of the software development lifecycle can be used to reduce the Validation test effort to be executed by the Regulated Company (Installation and Operational Qualification testing only). Testing documentation provided by the Supplier shall formally be assessed, reviewed and approved by the Regulated Company.

Any connected instrument/equipment and the relevant IT Infrastructure components which are included in the Computerized System are qualified before the initiation of the IQ stage to demonstrate the proper functioning and calibration of the connected instruments.

The testing documentation (e.g. qualification protocol) shall describes the approach to be taken for intended testing activities, the testing environment, the list of testing actions and relevant acceptance criteria, the testing results together with the identification and follow up of deviations (if any) and the criteria for phase acceptance. The testing phases may be combined (e.g. IQ/OQ session) where convenient; the output of the testing phases shall be documented.

9.6.1 System Environments

Tests shall be performed in an appropriately qualified environment according to a predetermined Test Plan and Test Specifications including predefined expected results.

The environments used for the development and/or implementation of a computerized system may differ depending on the system category and its complexity.

The establishment of Development, Qualification (also termed Quality or Validation) and Production environments is considered and shall be documented in the Configuration Specification and verified (at least for the Qualification and Production environment). Appropriate verification activities have to be executed in order to give documented evidence that Qualification and Production Environment are equivalent.

9.6.2 Data Migration

Data migration activities are highly dependent upon the specific technology and file structure of the electronic records being migrated.

Where possible, the data migration effort shall involve the use of software tools to automate some or all of the extraction, transformation, loading, and verification activities. The tools must be fit for intended use. The rigor of tool specification and verification activities must be commensurate with associated risks.

Data must be verified each time it is moved (either within a system platform or from one system to another) or its state is transformed.

This verification provides objective evidence that the data migration software tools are fit for intended use, and also provides a level of confidence in the overall migration process. A typical approach during this step is to work with a relatively small amount of data, which can later be completely verified to assure that no data errors occurred.

9.6.3 Installation Qualification Protocol

The Installation Qualification (IQ) (also termed Configuration Testing), is the verification activity of the installation and configuration of the hardware and software components of the system and related documentation.

This activity shall be performed after freezing the configuration which will be verified. Any change later made to the configuration, shall undergo the Change Management procedure.

The Installation Qualification session shall take into consideration the environment where tests will be executed. Generally a dedicated Test Environment is strongly recommended; appropriate controls shall be executed during IQ in order to give documented evidence that Test and Production Environment are equivalent.

The qualification of any connected instrument/equipment and of the relevant IT Infrastructure shall be considered as prerequisites for the IQ Testing phase.

The Installation Qualification Protocol defines the tests which shall be performed on the Computerized System; it shall contain at least the following verifications:

- proper HW and SW installation according to what reported in the technical specifications and in the system configuration baseline
- configuration setting according to what reported in the Configuration Specifications (where applicable)
- availability of system documentation

For standard software the vendor installation procedures/Manuals/Instructions can be used as Installation Qualification Protocol by documenting who installed and when.

9.6.4 Operational Qualification Protocol

The purpose of the Operational Qualification OQ is to demonstrate that the system and each of its identified critical functions/processes operates as defined in the related specification(s).

The testing must be based upon approved specifications (functional specifications, user requirements etc.) and the outcome of the Detailed Risk Assessment to define tests typologies. Worst case tests shall be done for critical functions and evidence of challenge testing shall be included, particularly system parameter limits, data limits and error handling.

If the system manages regulated electronic records and signatures, the Operational Qualification Protocol contains also the tests oriented to ensure the control measures to ensure Data Integrity (see section 9.1.1). Also if the general Regulatory Requirements testing is included in the documented controls executed by the Supplier, the OQ phase includes the verification of reliability of those functionalities which allow compliance with the Regulatory Requirements (e.g. Audit Trail, Security) as applicable to the specific environment and intended use of each regulated company.

Each test case shall be performed by using predefined data and scenarios. The results obtained shall be compared with the expected ones, deduced from the Functional Specifications.

If used, automated testing tools, employed for validation purposes, shall be assessed for their adequacy.

9.6.5 Performance Qualification Protocol

The Performance Qualification (PQ) phase (also termed Requirements Verification) is oriented to demonstrate that the system performs effectively and reproducibly, is fit for its intended use, and that both, the system and its operating environment (including users), are ready to go into production.

The PQ must be performed mainly by nominated user(s) representatives and shall be oriented to ensure:

- The IQ/OQ are completed and related reports approved (any deviation evaluated and addressed)
- All system related SOPs, installation/administration and user guides are approved and available
- All users who can access the system are trained and training records are available
- All users' accesses have been created in accordance with their skills and responsibilities
- Verification of the business processes supported by the system (end-to-end tests) based upon the outcome of the Detailed Risk Assessment (section 9.5.4)
- System and Data recovery in operational environment (data backup and restoration)

PQ Tests shall be done in the qualification environment. In case this approach is not possible for technical reasons, the PQ can be executed directly in the Production environment after repeating the IQ in the Production environment.

9.6.6 Traceability Matrix

The Traceability Matrix shall be created to demonstrate that:

- Business processes have been properly translated into system functionalities,
- System functionalities and business processes have been properly tested in the qualification test cases according to the outcome of the Detailed Risk Assessment.

9.7 Release Phase

The decision to release the computerized system to production has to be approved at least by the Business Process Owner and Quality Assurance. These roles determine the system validation status before authorizing deployment in the Production environment. This decision has to be formally documented in a section of the Validation Report or within a dedicated document.

9.7.1 Validation Report

The validation report summarizes the activities and associated documentation issued to demonstrate correct and complete execution of the Validation process, according to the validation plan. It provides an analysis of data collected during the Validation process and documents the validation activity results including any non-conformity or follow-up.

The Validation Report (or Validation Summary Report) shall include:

- Clear statement that the system is validated and released for operational use,
- Identification of possible restrictions,
- Confirmation that all activities have been performed according to the plan or to any approved deviation to the plan,
- Measurable evaluation of test results and confirmation of meeting the system acceptance criteria,
- Action plan (if appropriate),
- Updated Documentation List / Master Index, including the operational environment procedures, instructions and controls that govern the use and management of the system after System Release.

After the approval of the Validation report, the site Inventory shall be updated to reflect the validated status of the System and to include the reference to the validation report.

9.8 Supporting Processes

9.8.1 Security Management

Security procedures must be defined and implemented to provide a high level of protection of data from loss of confidentiality, integrity and availability with respect to the environment made by computers, networks, and programs.

The following processes are ensured throughout the entire Computerized System Life Cycle:

- Physical Security, which includes all appropriate precautions for access and environment control to protect computerized systems facilities from theft, destruction, uncontrolled change, or disruption.
- Logical Security:
    - Logical Security includes all precautions to protect programs and data against un-authorized access, misuse, or manipulation, e.g. virus protection, protection against external threats, procedures to identify Users, audit trail on data created, modified, or deleted,
    - Role-based security shall be implemented to ensure that GMP data are accessed only by preauthorized operators, according to the relevant role in the organization, preserving the Segregation of Duties. Security management procedures are applied to all users, including administrators, super-users, end users, and support staff (including supplier support staff),
    - The following control measured are ensured to:
- Establish and maintain security roles and responsibilities, policies, standards, and procedures,
- Perform security monitoring and periodic testing, e.g., manual check of system access log, automated notification of lockouts, testing of tokens (if any),
- Establish and maintain a list of those authorized to access the system.

The security configuration is documented in the System Configuration Specifications or in a dedicated document (e.g. Security Matrix). Access to the system is limited to operators with documented training.

The control measures for system-critical components (e.g. servers) are included and verified within the Infrastructure Qualification process.

9.8.2 Incident Management

An incident is any unplanned occurrence which prevents (or may prevent) or delays users, the system, an operation, or a service from proceeding with an assigned task. The Incidents are collected and managed to address the associated actions, which may result in an immediate local resolution, a Change Request or CAPA.

Incidents and their resolutions shall be tracked to monitor the performance of both the process and the automated system within which the incident occurred. This traceability usually is done using an incident log.

The process is intended to provide a high-level structure that is supported by detailed SOPs, and associated tools, which give guidance on the escalation and evaluation scenarios. This process may be supported by software tools.

9.8.3 Change Control

Change Management applies to computerized systems subject to validation throughout the system lifecycle from the Installation qualification phase to the retirement.

Change Management requires procedures that control and report the implementation of changes that may affect the configuration items (documentation. hardware, software) and/or the validation status of a system. This includes the tracking of changes (triggered by incidents or change requests) from their opening to their resolution.

The Change implementation process triggers the Configuration Management, which covers the identification, recording, and reporting of IT components, including their versions, constituent components and relationships.

The changes shall be performed according to the predetermined Change Management Procedure.

9.8.4 Backup & Restore

According to section 8.2.3, the backup is the process of copying records, data and software to protect against loss of integrity or availability of the original. Restore is the subsequent restoration of records, data or software when required.

These procedures are required to ensure the recovery of essential systems in the event of any system failures and consequent loss of data.

The reliability of the restore process is documented within the validation process.

9.8.5 Service Level Agreement

For most GMP medium or high systems a Service Level Agreement (SLA) with the system supplier and / or integrator must be defined in order to assure an adequate and timely maintenance / incident support and adequate secure storage if system documentation, created during the development, is retained at vendor ‘site

The SLA defines the mutual responsibilities between the Regulated Company and Supplier together with the relevant timing.

9.8.6 Business Continuity

The Business Continuity process includes the control measures oriented to ensure continuity of support for critical processes in the event of a system breakdown (e.g. a manual or alternative system).

For each system, the Business Continuity Plan addresses the following information:

- Alternate contingency procedures used in place of process steps that involve computerized systems access,
- Management plans and decision methods to be used during a computerized systems operations disaster,
- Business Continuity Identification of critical documents that need to be stored temporarily until computerized systems Operations are recovered,
- Tests of the contingency procedures.

The Business Continuity requirement is considered as strictly applicable only for those systems which supports time-critical processes, i.e. those systems which executes processes which cannot be interrupted without a potential impact on Patient Safety, Product Quality and Data Integrity. The need of a business continuity plan shall be defined in the Validation Plan.

As a subset of business continuity planning, plans shall be specified, approved, and rehearsed for the recovery of specific systems in the event of a disaster. These plans shall detail the precautions taken to minimize the effects of a disaster, allowing the organization to either maintain or quickly resume critical functions; special focus on disaster prevention, (e.g., the provision of redundancy for critical systems) is addressed by the Disaster Recovery Plan.

9.8.7 Archiving

In case the data are archived offline (i.e. not immediately available to users), an archive procedure defines where temporal periods and conditions for data archive are defined. The archive and retrieval process is documented and tested within the Validation Life Cycle.

9.8.8 Periodic Review

The Validation status of each GMP system is periodically reviewed in order to ensure that the validated status is maintained. The frequency and depth of the Periodic Review process is determined based upon the risk associated to the System. The related scheduling is included in the Validation scheduling defined in the Validation Master Plan. The Periodic Review process shall be executed according to a predetermined procedure.

9.8.9 Training & System usage procedures

For each GMP system, the SOPs defining use and operations process steps required to be executed by the users have to be issued. Moreover such procedures will contain section dedicated to specific and not day by day tasks as appropriate to each system, such as:

- Add, change, and delete Master Records
- Execute routine-periodic tasks (e.g. DB index rebuild),
- Prepare (select and sort, determine sequences, etc.) screen queries and printed reports of system data,
- Trigger user-controlled interfaces of data to/from other systems,
- Upload or download data to/from the workstation or remote data collection devices from/to the system,
- Audit Trail Review.

Training plans and training records shall be maintained to demonstrate to auditors, that the systems are being utilized by qualified and trained personnel.

9.9 Specific Validation Requirements

9.9.1 Global Systems Validation

Global Systems are those IT systems which are centrally managed and used at multiple sites of the Regulated Company; these systems can be centrally implemented and released or distributed for use at each site. For these systems, the Validation life cycle addressed by this procedure might be adapted in order to maximize the central creation of harmonized documentation and to minimize the validation effort at site level.

For each Global System, the validation approach shall be defined in a single Global validation Plan which identifies the global and site deliverables. The local implementation might be detailed in a site specific Validation Plan, created according to the above mentioned Global VP.

The Validation process for these systems may include a Global Validation Package oriented primarily to ensure the functional reliability of the System. Each site may formally accept the Global Validation deliverable and creates the local specification/testing documentation related to site-specific functionalities if any. The validation process shall include the verification of processes executed through the system at each single site.

The Global documentation has to be made accessible to the site in case of inspection. The local Validation approach is approved by the Global Team in order to ensure the harmonized and coherent approach.

The Local Team has to be trained in order to be aware of the strategy utilized for validation at Global and Local level.

9.9.2 Cloud-based System Validation

Where ‘cloud’ or ‘virtual’ services are used, attention shall be paid to understanding the service provided, ownership, retrieval, retention and security of data.

The responsibilities of the contract giver (i.e. Regulated Company) and acceptor (IT Service Provider) shall be defined in a technical agreement or contract. This shall ensure timely access to data (including metadata and audit trails) to the data owner and national competent authorities upon request. Contracts with providers shall define responsibilities for archiving and continued readability of the data throughout the retention period (see archive).

The following different types of services are nowadays provided to Regulated Companies:

- Software as a Service (SaaS) –Regulated companies use the applications running on an infrastructure owned by the IT Service Provider. Regulated Companies does not manage or control the underlying infrastructure or even individual application capabilities with the possible exception of limited user-specific application configuration settings
- Platform as a Service (PaaS) – Regulated Companies leverages IT infrastructure hosted by the IT Service Provider to run applications created using operating systems, programming languages and tools supported by the IT Service Provider. Regulated Companies does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but still has control over the deployed applications and possibly application hosting environment configurations
- Infrastructure as a Service (IaaS) – Owner leverages fundamental computing resources, such as processing, storage, networks, where Customer can deploy and run arbitrary software, which can include operating systems and applications. Customer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications and possibly limited control of selected networking components (e.g., host firewalls).

The reliability of the Computerized System used by the Regulated Company is always under the responsibility of Regulated Company, which shall document the relevant Validation process leveraging the documentation provided by the System provider.

The Validation Life Cycle shall be executed according to the previous sections ensuring that it is appropriately tested/validated with the following specific measures:

- The Supplier Assessment is executed on site and before the definition of the Validation strategy in the Validation Plan; the method for Supplier Assessment shall be based upon the risk associated to the system
- The Validation Plan takes into account the outcome of the Supplier Assessment phase
- The Validation documentation may leverage the Specifications, Installation Testing (i.e. IQ) and Functional Testing (i.e. OQ) documentation, provided by the Supplier in case these documents are found as adequate in the Supplier Assessment
- The effective status of the Service Level Agreement is verified in the IQ testing phase
- The Performance Qualification (PQ) / User Acceptance Test (UAT) is executed by the Regulated Company end user verifying that the system performs as intended by the user (based on the URS) throughout all anticipated operating ranges.

The selection of systems shall be executed through a robust supplier assessment on all the aspects of services provided. It is highly recommended the involvement of Auditors with IT expertise, in order to leverage testing of the cloud software, platform, and infrastructure and to verify if the cloud application is managed in a compliant and controlled manner. The IT Security audit shall be oriented at least to the following aspects:

- How the vendor notifies the Regulated Company for issues which affect data integrity, including but not limited to technical and hosting, related security breaches, software bugs, backup and restoration issues and/or the execution of a Disaster Recovery Plan;
- Security authorizations and Segregation of Duty requirements;
- Change Control process for enhancements, patches, upgrades
- Data retention requirements;
- Audit Trail and Event Log Monitoring;
- Access control mechanism;
- Identification and authentication mechanism;
- Encryption mechanism;
- Infrastructure qualification (even if the infrastructure is third-party managed)
- Validation package (specification and testing protocols). Any discovered gaps/non-conformities shall be addressed through corrective actions agreed by the Supplier and additional Validation activities within the implementation project (e.g. additional testing activity) performed by the Regulated Company.

For clouds applications consider only GAMP category 4 and 5; from a regulated organization's perspective, the configuration of cloud applications shall be treated as category 4, while any custom development for GMP significant interfaces or data supply, which communicates with the cloud application, shall be treated as category 5 and tested appropriately.

If a cloud based infrastructure (IaaS and PaaS) has been selected to be implemented, ensure that it is appropriately qualified according to section 10, either by the provider and/or by Regulated Company.

9.9.3 Spreadsheet Validation

Each spreadsheet shall be considered as a single Computerized System and therefore the critical spreadsheets shall be inventoried, risk assessed and validated accordingly.

Spreadsheet are commonly implemented for repetitive usage of calculation algorithm; the use of Excel as database (i.e. spreadsheet implemented to store and archive GMP data) shall be **prohibited** unless an automatic audit trail is ensured through additional measures.

As regards System category, the classification of an Excel spreadsheet depends on the type of operations the sheet performs on the GMP data according to the following:

- Category 3 (not configured): the spreadsheet simply uses native functions without configuration (e.g. data validation, conditional format)

- Category 4 (configured): the spreadsheet executes calculations through configured formulas (also formulas using basic functions of the excel e.g. plus, minus, division shall be considered as Category 4)
- Category 5 (custom): the spreadsheet employs custom macros, sophisticated or nested logic or look-up and similar functions

Each spreadsheet system shall be implemented considering the following factors:

- Secure the spreadsheet to ensure that only input cells can be populated (e.g. formulations cannot be intentionally or accidentally overwritten, development options is disabled)
- Configure security of accesses and authority checks, e.g. create the Excel spreadsheet in a dedicated folder, with the access privileges defined for all the users of the spreadsheet
- Execute any related calculation with a precision displayed on the screen and in reports
- Use of spreadsheet Variables (in Microsoft Excel termed Names) to facilitate the formula development (e.g. Instead of including into a formula the reference to the cell A4 , the cell A4 is defined with the Name "Quantity" and the string Quantity is included into a formula"
- Ensure that backup is correctly performed (for the spreadsheets stored in local directories)
- Protect time reference including time zone
- Ensure that the spreadsheet filled out is saved to a non-editable file (e.g. PDF format)
- In case of Spreadsheet used as template, configure the spreadsheet to allow only the Save As operation to a secured folder

The Validation Life Cycle deliverables required in sections 10.4-10.5-10.6-10.7 shall be created for each Spreadsheet although some documents can be merged together (e.g. single Functional Requirement URS/FS document).

9.10 IT Infrastructure Qualification

IT infrastructure supports networked systems involved in the production and management activities of Company's plants. Validated applications are required to run on qualified infrastructure.

Infrastructure Qualification provides the documented verification of the correct operation and the status of control of IT Infrastructure.

IT Infrastructure exists to support the primary business by providing: platform to run business applications, IT Infrastructure processes that facilitate a capable and controlled IT environment, general IT services (e.g. office tools, intranet facilities, file storage).

The following phases are associated to the qualification process of IT Infrastructure components:

- **Planning**: to address the required activities, responsibilities, procedures, and timelines, assuring that the Qualification Activities are executed in a systematic and controlled manner, based on a predefined strategy
- **Specification and Design**: to describes in detail the hardware and software structure of the IT Infrastructure components subject to qualification, assuring that the documentation, related to IT Infrastructure, is organized and integrated, to be easily managed and put under control
- **Testing**: to assure the IT infrastructure guarantees a reliable and accurate service
- **Reporting**: to summarize the results of the performed Qualification Activities
- **Operation:** to guarantee the maintenance of the Qualified status

The following Life Cycle activities shall be considered as mandatory for every GMP relevant IT Infrastructure components:

- GMP Impact Assessment
- Qualification Plan & Reporting
- Design Specification
- Installation and Operational Qualification Testing
- Supporting Processes:
- Change Management
- Configuration Management
- Backup & Restore
- Infrastructure Security

– Incident Management

These tasks for GMP components allow to ensure documented evidence of the state of control required for the GMP IT Infrastructure. The documentation created within the Life Cycle will constitute the IT Infrastructure Qualification documentation which provides documented evidence of proper functioning of IT Infrastructure, documenting that it is managed as indicated in the applicable guidelines.

The qualification process for IT Infrastructure, explicitly required by Regulation No. 916 “On the approval of Rules of Good manufacturing practices”, shall be executed according to a dedicated plan.

The IT Infrastructure Qualification is a prerequisite of the validation process related to the SW application(s) which run upon the IT infrastructure.

10. DATA INTEGRITY ASSURANCE FOR OUTSOURCED ACTIVITIES

Data integrity plays a key part in ensuring the security and integrity of external provided products and services. Data governance measures provided by a contract giver may be significantly weakened by unreliable or falsified data or materials provided by another supply chain partners. This principle applies to all outsourced activities, including suppliers of raw materials or contract manufacture / analytical services.

Initial and periodic re-qualification of suppliers and outsourced activities shall include consideration of data integrity risks and appropriate control measures.

It is important for an organization to understand the data integrity limitations of information obtained from the supplier (e.g. summary records and copies / printouts), and the challenges of remote supervision. The remote review of data within summary reports is a common necessity; however, the limitations of remote data review must be fully understood to enable adequate control of data integrity. It is essential that summary reports are viewed as transfer of data and that interested parties do not place sole reliance on summary report data. Prior to acceptance of summary data, an evaluation of the supplier’s quality system and compliance with data integrity principles shall be established through on-site inspection. The inspection shall ensure the veracity of data generated by the company, and include a review of the mechanisms used to generate and distribute summary data and reports

Companies shall conduct regular risk reviews of suppliers and outsourced activity periodically evaluating the extent of data integrity controls required.

Quality agreements shall be in place between Regulated Companies and suppliers/contract organizations (e.g. CMO) with specific provisions for ensuring data integrity across the supported process(es). 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. Audits of suppliers and service providers, conducted by the manufacturer (or by a third party on their behalf), shall include a verification of data integrity measures at the contract organization.

11. REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS

Deficiencies relating to data integrity failures may have different impact to product quality. Prevalence of the failure may also vary between the actions of a single employee to an endemic failure throughout the inspected organization.

In case a violation to data integrity is detected, consideration shall be primarily given to resolving the immediate issues identified and assessing the risks associated with the data integrity issues, considering also Historical Data review. The response by the company in question shall outline the actions taken.

The Regulated Company shall execute a detailed investigation, including a summary of all involved laboratories, manufacturing operations, and systems and a justification for any part of the operation that the regulated user proposes to exclude. The investigation shall include interviews of current and former employees to identify the nature, scope, and root cause of data inaccuracies. These interviews may be conducted by a qualified third party.

The investigation shall include an assessment oriented to:

- Evaluation of the extent of data integrity deficiencies at the facility, not limited to the single observed case, but verifying all other instances where violation may have occurred.
- Impact of an integrity violation on the Patient Safety and Product Quality shall be determined considering risks posed by ongoing operations, and any impact on the veracity of data submitted to regulatory agencies, including data related to product registration dossiers
- Identification of the root causes of data integrity lapses

Corrective and preventative actions taken to address the data integrity vulnerabilities and timeframe for implementation shall at least include:

- Interim measures describing the actions to protect patients and to ensure the quality of the medicinal products, such as notifying customers, recalling product, conducting additional testing, adding lots to the stability program, drug application actions, and enhanced complaint monitoring.
- Long-term measures describing any remediation effort and enhancement to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the data integrity.

12. REVISION HISTORY

Draft Version