ACTIVE PHARMACEUTICAL INGREDIENTS COMMITTEE

Practical risk-based guide for managing data integrity

Version 1, March 2019

PREAMBLE

This original version of this guidance document has been compiled by a subdivision of the APIC Data Integrity Task Force on behalf of the Active Pharmaceutical Ingredient Committee (APIC) of CEFIC.

The Task Force members are:

Charles Gibbons, AbbVie, Ireland

Danny De Scheemaecker, Janssen Pharmaceutica NV

Rob De Proost, Janssen Pharmaceutica NV

Dieter Vanderlinden, S.A. Ajinomoto Omnichem N.V.

André van der Biezen, Aspen Oss B.V.

Sebastian Fuchs, Tereos

Daniel Davies, Lonza AG

Fraser Strachan, DSM

Bjorn Van Krevelen, Janssen Pharmaceutica NV

Alessandro Fava, F.I.S. (Fabbrica Italiana Sintetici) SpA

Alexandra Silva, Hovione FarmaCiencia SA

Nicola Martone, DSM Sinochem Pharmaceuticals

Ulrich-Andreas Opitz, Merck KGaA

Dominique Rasewsky, Merck KGaA

With support and review from:

Pieter van der Hoeven, APIC, Belgium

Francois Vandeweyer, Janssen Pharmaceutica NV

Annick Bonneure, APIC, Belgium

The APIC Quality Working Group

1 Contents

1. General Section

1.1 Introduction

Data integrity refers to the accuracy, completeness and consistency of GxP data over its entire lifecycle. The steps that need to be overseen include the initial generation and recording, the processing (incl. analysis, transformation or migration), the outcome/use, the retention, retrieval, archive and finally the destruction.
Data integrity means that all the steps defined above are well managed, controlled and documented and therefore the records of the activities follow the ALCOA principles described in the guidelines.
The ALCOA and ALCOA+ principles have been in place for several years in the industry and are widely known and implemented. Achieving data integrity compliance, for paper, electronic and hybrid systems, requires translation of these principles into practical controls in order to assure GxP-impacting business decisions can be verified and inspected throughout the data lifecycle.

Currently available regulatory guidelines have been used to elaborate the approach outlined in this practical guide (see also section 7, References).

The current guidelines on data integrity require that companies complete data integrity criticality and risk assessments to ensure that the organizational and technical controls that are put in place are commensurate with the level of risk to quality attributes.

The guidelines emphasise the importance of creating and maintaining a working environment and organisational culture that supports data integrity. Companies should establish data governance programs that address technical, procedural and behavioural aspects to assure confidence in data quality and integrity.

This document will not describe all the elements required for a data governance program in detail. However, some foundational principles are given below:

- Organisational Culture

Organisational culture has the potential to increase the possibility for lapses in data integrity; intentional (e.g. fraud or falsification) or unintentional (e.g. lack of understanding of responsibilities and/or requirements). To reduce this potential, organisations should aspire to an open culture where subordinates can challenge hierarchy, and full reporting of a systemic or individual failure is a business expectation.

- Awareness

It is crucial that employees at all levels understand the importance of data integrity and the impact that they can have on GxP data with the authorisations assigned for their job roles. Training is a major component of raising awareness and should be conducted periodically. The ALCOA+ concepts, and the acronym itself, are widely used by regulators and industry and should be incorporated into the program (e.g. within staff training, policies etc.).

- System and Process Design

Compliance with data integrity principles can be encouraged through the consideration of ease of access, usability and location. For example:

  - Control over blank paper templates for GxP data recording
  - Control of spreadsheets used for calculations

  - Access to appropriate clocks for recording timed events
  - Accessibility of records at the locations where activities take place

  - User access rights and permissions that align with personnel responsibilities
  - Automation of GxP data capture where possible
  - Access to electronic GxP data for staff performing data review activities

- Management Commitment

Senior management should ensure that there is a written commitment to follow an effective quality management system and professional practices to deliver good data management. The commitments should include

- An open quality culture
- Data integrity governance
- Allocation of appropriate resources
- Data integrity training for staff
- Monitoring of data integrity issues with CAPA taken to address issues identified
- Mechanisms for staff to report concerns to management

1.2 Objectives and Scope

This document is based on general Data Integrity requirements and gathers practical experiences from a number of companies operating in the sector that can be used as guidance to others. It is not an all-inclusive list of requirements but proposes a comprehensive approach that companies can adopt to help carry out their data integrity risk assessments.

The guide is essentially practical and therefore, after the presentation of the approach and of the tools, the document includes some examples of executed assessments, categorisations and check lists that can be used by any company according to their individual needs. Each company can choose the appropriate tools and categorisations that apply to their own business processes and systems. This guidance applies to all GxP processes and GxP data used in the manufacture and analysis of APIs for use in human and veterinary drugs.

1.3 Definitions and abbreviations

Business process: a set of structured activities or tasks that produce a specific service for a particular customer or customers. It is often visualised as a flowchart of a sequence of activities with decision points.

Data: Facts, figures and statistics collected together for reference or analysis. All original records and true copies of original records, including source GxP data and metadata and all subsequent transformations and reports of these GxP data, that are generated or recorded at the time of the GxP activity and allow full and complete reconstruction and evaluation of the GxP activity.

Raw data: Raw data is defined as the original record (data) which can be described as the first-capture of GxP information, whether recorded on paper or electronically. Information that is originally captured in a dynamic state should remain available in that state.

Metadata: Metadata are data that describe the attributes of other data and provide context and meaning. Typically, these are data that describe the structure, data elements, inter-relationships and other

characteristics of data e.g. audit trails. Metadata also permit data to be attributable to an individual (or if automatically generated, to the original data source).

Data severity assessment: within GxP data, different levels of severity can be defined as a function of its use. Typically, this is linked to the stage of manufacturing following the principle of increasing GxP outlined in ICH Q7. Alternatively, other factors such as impact on final product quality can be taken into account to further differentiate between severity categories.

Data elements: (for the purpose of this document) individual GxP data items that are part of raw GxP data or metadata, e.g. an operator name, a test date.

Data Flow: diagram that maps the flow of information of any process or system (inputs, outputs, storage points and routes between each destination).

Data process mapping: generation of a visual representation of the creation and movement of data through the business process including documentation of the systems used.

Data Audit Trail: appropriate audit trail elements supporting the acquisition, sequencing, processing, reporting and retention of GxP data for the release of product. Including all relevant or significant GxP data generated, which may affect the product (such as: analytical method validation, stability analysis, multiple sample/test runs, etc.), as determined by a risk assessment.

LIMS: Laboratory Information Management System

MES: Manufacturing Execution System

PCS/DCS: process control systems (PCS) / distributed control systems (DCS)

Process mapping: activities involved in defining what a business entity does, who is responsible, to what standard a business process should be completed, and how the success of a business process can be determined.

System Audit Trail: a record of all administrator changes. The frequency of this review should be determined based on a risk assessment. This may be performed as part of the system periodic review as appropriate.

True copy: A copy (irrespective of the type of media used) of the original record that has been verified (i.e. by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original

1.4 Overall Data Integrity Approach

When assessing data integrity risks within an organisation, companies may focus immediately on those systems or areas that are the most obvious in this context, such as a particular software, a specific lab system or instrument etc. Doing so creates the risk of forgetting less visible but still important areas, processes or systems, or of failing to address integrity issues concerning data flows *between* controlled environments.

Therefore, this guide approaches data integrity in a holistic manner by looking at the organisation from a high-level business process perspective, subsequently diving deeper into underlying sub-processes and only at the end drilling down to individual activities or systems that involve GxP data.

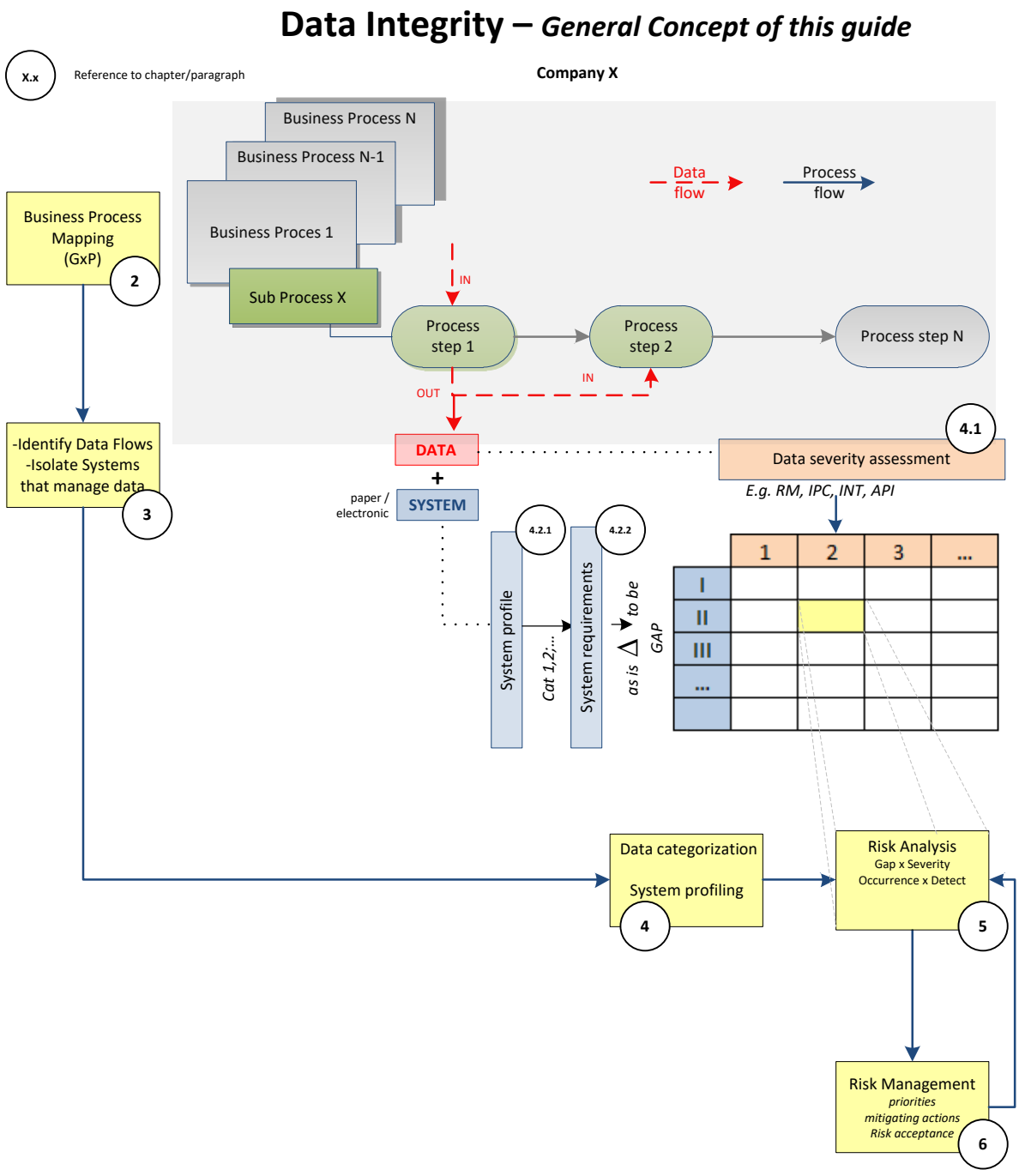
Figure 1 is a graphical representation of this approach and the sequence of steps that should help assessors to obtain a complete and profound data integrity risk assessment.

It should be noted that the proposed approach is suitable not only to assess risks related to systems or processes already present in the organisation but also to proactively evaluate the requirements of new systems.

Below is a short description of the sequence actions that are illustrated in the diagram. Details for the major steps will be further elaborated in the following sections of this guideline (those sections are also cross-referenced in Figure 1).

- ✓ Identify the company's high-level GxP business processes (or having links to GxP activities) (ref. to section 2)
- ✓ **Map** each of the GxP **business processes** and their sub-processes down to level of **process flows** that consist of individual activities (refer to section 0)
- ✓ Identify the **GxP data elements** and the way the **data flows** (IN/OUT) between the different process steps or activities (**Data Process Mapping**); (refer to section 0)
- ✓ Identify and **isolate** the individual **systems** (both paper and electronic) that manage (generate, store, transfer or process) GxP data (refer to section 0)
- ✓ Assign GxP data to a specific category based on a **severity assessment** (refer to section 4.1)
- ✓ Create a **profile** of each **system** based on the way GxP data is handled by that system (e.g. data generation, storage, processing, transfer or a combination thereof) and assign a category to the system based on its profile; (refer to section 4.2)
- ✓ Identify the **gap** between the "as is" state of the system and the desired state (i.e. the set of data integrity requirements linked to the particular system category) ; a check-list should be used to accomplish this task; (refer to section 4.3)
- ✓ **Analyse** the data integrity **risk** considering the gaps identified above, which is an assessment of the failure mode, using **severity**, **occurrence and detectability** that are part of the risk assessment methodology (e.g. FMEA); (refer to section 5)
- ✓ Establish a **remediation plan** to remediate the gaps and set **priorities** based on the magnitude of the risk (refer to section 6)

Figure 1 Data integrity management approach (General Concept)



2 Business Processing Mapping

Business Process mapping should be used in order to provide a global overview on all kinds of activities performed in a company, including operational, supportive and strategic processes. Examples include:

- Production (Development & Control of Master Batch Record, Manufacture of a Product)
- Laboratories (Analysis of Material Sample, Qualification & Calibration of Instruments)
- Control of Packaging & Labels
- Quality (Change Control, Complaint Management)
- Materials Management (Distribution of Final Product)
- Facilities and Equipment (Calibration)

This approach not only helps to visualize all activities sequencing within a process, but also interactions between these activities as well as interactions between processes.

Business Process Mapping is an approach to visually represent flows for given processes. It is intended to provide a clear schematic view of the activities performed, step by step from start to finish.

After defining which business processes are GxP relevant the next phase is to map them in detail. It is essential to form a cross functional team to perform the mapping which involves the relevant subject matter experts (SMEs) and business process owners. This is commonly done by identifying each step of the process, as an action or decision point, and to build the sequenced process. Depending on the level of detail, a step can also be subdivided in sub-steps (which can be mapped separately).

The examples displayed in section 8 illustrate the approach.

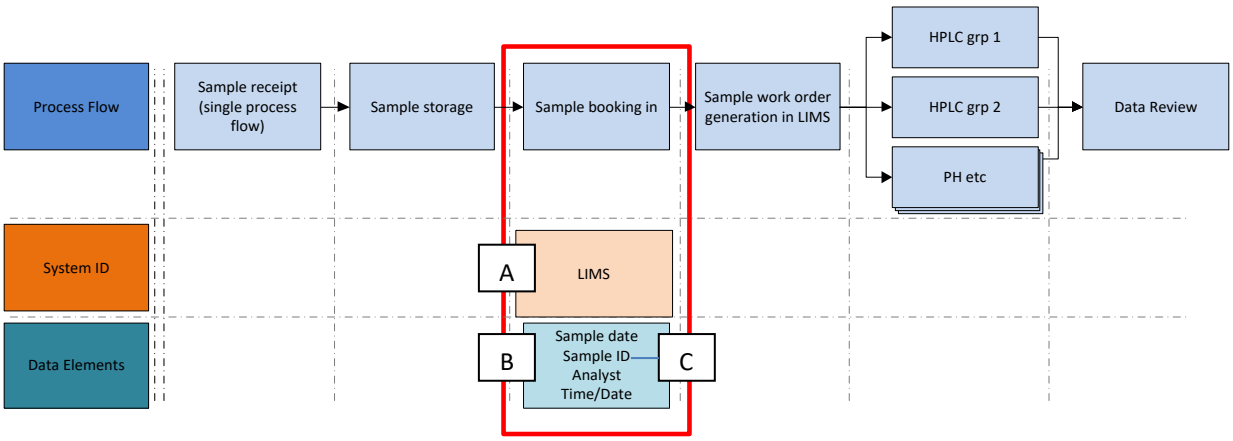
3 Data and System Identification

Following the execution of business process mapping including the mapping of sub-processes, the following steps are performed:

A. Identify the systems (both paper and electronic) involved in the processing of GxP data
B. Define individual GxP data elements
C. Identify GxP data elements that can be modified, deleted or re-processed after creation (at the non-administrator level i.e. either accidentally or deliberately).

The execution of these steps allows for efficiency in the execution of the risk assessment in the next stage of the process.

Figure 2 Example of an individual sub-process mapping (sample booking step)



4 Data and System Categorisation

4.1 Data Severity Assessment

A proposed approach is to use the stage of manufacturing as the primary determinant for severity classification (high-medium-low), following the principle of increasing GxP requirements outlined in ICH Q7. However, additional factors such as impact on final product quality can be considered to further differentiate within a severity category (high/very high – medium/medium high

Remark: in case certain GxP data, depending on its use, belongs to different severity categories the highest severity is maintained. (see also table 3 of chapter 5 'Risk assessment' to clarify severity rating)

- **High / very high severity data:** GxP Data generated during and directly associated with the final stage of API synthesis (direct impact on product quality / patient safety)

  Examples (not exhaustive):
  - Temperature of final crystallisation
  - Weighing and dispensing of critical raw materials
  - Analytical testing records of API
  - Calibration of instruments controlling critical process parameters
  - Calibration records of QC instruments
  - Cleaning records of a production equipment

- **Medium / medium high severity data:** GxP Data generated during and directly associated with the production of API intermediates and raw materials testing.

  Examples (not exhaustive):
  - Reaction conditions during API intermediate production
  - Analytical testing records of raw materials and intermediates (from regulatory starting raw material onwards)
  - Calibration of instruments controlling non-critical parameters
  - Records of in-process controls for API intermediate manufacture

- **Low severity data:** GxP Data that is GxP relevant but is not directly associated with raw material testing, API intermediate production or testing or API final stage production or testing.

  Examples (not exhaustive):
  - Records that do not directly impact operations and not described in the batch production record (BPR) or analytical methods
  - Location and transfers of materials (not temperature sensitive) or material transfer requests
  - Autoclave GxP data for waste media disposal
  - Operator access to production area
  - GxP data generated during the development of process or systems or equipment, prior to the validation or qualification
  - Shift scheduling
  - Planning data (production schedule)
  - Shift change notes
  - Time and attendance information (time and attendance system may not be qualified, but maybe used during investigations)
  - Safety training

- Analysis of chemicals before starting materials
- For information only in process controls

4.2 System Profiling

Once the system is identified, it can be further categorised based upon the GxP data that is generated in and by the system. This system categorisation will help selecting the necessary questions during the system assessment in the next step. (see section 4.3).

Remark: please note that these categories are different from categories as defined in GAMP guide since the focus here is on the data lifecycle instead of on the system.

4.2.1 System categorization

The following 6 categories are proposed.

Remark:

(1) It is important to evaluate the system in relation to all GxP data it processes. In case of different outcomes, the highest category is maintained. For hybrid systems both categories have to be taken in to account.

(2) It is important that the evaluation is done from the point of view of the system where the GxP data is generated and not where the GxP data is being transferred to.

Category 1: A non-electronic system. No GxP data are stored. Typical examples are bag sealers, pH paper, density meters, CAPA logbook.

Category 2: An electronic system and the generated GxP data is not stored and manually transferred on paper. Typical examples could include pH meters, balances, polarimeters with manual adjustable a wavelength, pressure gauge with display.

Category 3: An electronic system with some limited manual adjustable input data and the generated GxP data is not stored but printed out. Typical examples could be potentiometric titrators not connected to a PC, balances with printer.

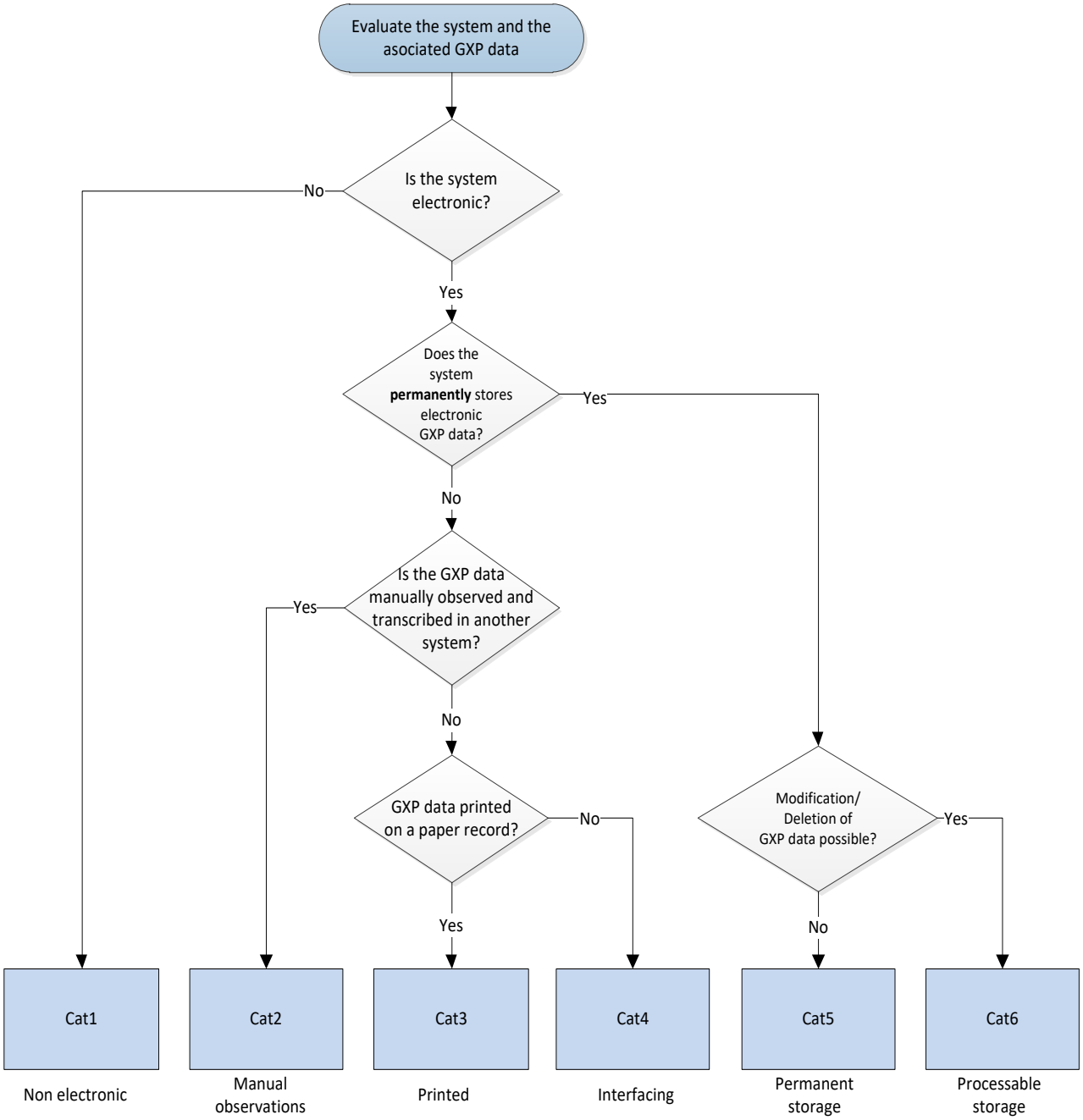
Category 4: An electronic system with some limited manual adjustable input data and the generated GxP data is not stored but sent via an interface to another system, e.g. a cat 5 or 6. Typical examples could be temperature sensors.

Category 5: An electronic system where GxP data are permanently stored, and these GxP data are not modified by the user to generate results (static GxP data). Examples could include UV instruments or IR instruments used for identification testing, in line particle size and TOC testing

Category 6: An electronic system where GxP data are permanently stored, and the GxP data can be processed by the user to generate results. Examples could be MES systems, ERP systems, chromatographic data systems, electronic deviations management system.

In order to facilitate this system categorization, below decision flow can be used (see Figure 3).

Figure 3 System categorization



4.2.2 System categorization requirements

It is important to follow the different chronological steps described in the previous and next chapters to assure review of all the GxP data and their severity. This process assesses the complete dataflow and enables identifying the appropriate remediation. The below described requirements for the different system categorisations can help in defining the actions at the end of the process (see Table 1).

a) Good documentation practices:

Good documentation practices are a general quality requirement and should be in line with the ALCOA principles, as described earlier in this document. This is applicable to all categories where GxP data is created. Starting from medium criticality up to high criticality (GxP activities) a process to control the issuance and reconciliation of documents/log books. In addition, GxP data should be reviewed.

b) Access control:

A system needs to be in place to control unauthorised access to systems.

c) User levels:

Depending upon a specific job responsibility, users can have different privileges in a system. An administrator will have more privileges in order to maintain the system and all the related GxP data, while an end-user only will operate the system and use the GxP data to generate results. This should achieve segregation of duties. Each user must have an individual ID and password to log into the system.

d) Audit trail:

The system should have a functionality to document the different activities that have taken place. Who has done what, when and why?

It is important to consider both the GxP data audit trail and the system audit trail.

e) Audit trail review:

An audit trail is only useful if there is a regular review of the activities that are stored in it. Depending upon the criticality of these stored GxP data the frequency of the review will increase and should be risk based.

f) Back-up / Restore / Archive

A process needs to be in place for the back-up of the electronic GxP data in order to guarantee that GxP data is retrievable, reproducible and unaltered for the retention period of the record. A test should be completed periodically to restore these GxP data confirming that it can still be read and is complete.

GxP Data (paper and electronic) are archived in a dedicated, protected and controlled environment. The record retention period should be defined in writing and depends upon the criticality of the GxP data.

Table 1 Minimum system requirements based on categories

Category	**Severity** (score)	**Good documentation practices**	**Access control**	**User levels**	**Audit trail review + frequency**	**Back-up / restore / archive**
Category 1 (non-electronic)	Low (1)	X	N/A	N/A	N/A	X
	Medium (2-3)	X + controlled issuance/reconciliation of docs	N/A	N/A	N/A	X
	High (4-5)	X + controlled issuance /reconciliation of docs	N/A	N/A	N/A	X
Category 2 (manual observations)	Low	X	N/A	N/A	N/A	X
	Medium (2)	X + controlled issuance/reconciliation of docs	N/A	N/A	N/A	X
	Medium (3)	X + controlled issuance/reconciliation of docs + risk-based witnessing of critical GxP data	N/A	N/A	N/A	X
	High (4-5)	X + controlled issuance/reconciliation of docs + risk-based witnessing of critical GxP data	N/A	N/A	N/A	X
Category 3 (printed)	Low (1)	X	N/A	N/A	N/A	X
	Medium (2-3)	X + controlled issuance/reconciliation of docs + printing of relevant GxP data	X[1]	N/A	N/A	X
	High (4-5)	X + controlled issuance/reconciliation of docs + printing of relevant GxP data	X[1]	N/A	N/A	X

[1] Access control only for securing time and date settings

Table 1 system requirements based on categories - continued

Category	Severity	Good documentation practices	Access control	User levels	Audit trail review (ATR)	Back-up / restore / archive
Category 4 (system sending GxP data via interfacing) (interface qualified as part of the system)	Low (1)	X	N/A	N/A	N/A	N/A
	Medium (2-3)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user (where human intervention is required)	N/A	N/A
	High (4-5)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user (where human intervention is required)	N/A	N/A
Category 5 (Permanent storage)	Low (1)	X	X	Administrator	N/A	X Monthly Back-up
	Medium (2-3)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	X System ATR every 2 years	X Weekly Back-up
	High (4-5)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	X System ATR: once per year	X Daily Back-up
Category 6 (Processable storage)	Low (1)	X	X	Administrator	N/A	X Monthly Back-up
	Medium (2)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	X Data ATR: risk based (e.g. spot check) System ATR: every 2 years	X Weekly Back-up
	Medium (3)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	X Data AT review: every batch System ATR: every 2 years	X Weekly Back-up
	High (4-5)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	Data: every batch System ATR: risk based, e.g. yearly	X Daily Back-up

4.3 System Assessment

To manage the individual risks relating to Data Integrity, it is necessary to assess the gaps within the individual systems and processes.

For all combinations of systems, processes and GxP data, it is necessary to challenge the following areas:

- Administrator Roles & Responsibilities
  → *Administrator role and responsibilities, Training*
- Security/User Access Control
  → *Access Approval, Authentication, Authorisation, Periodic Access Review*
- Signatures
  → *Electronic signatures, Wet Signatures*
- Data review
  → *Data review process, Double witnessing*
- Audit trail
  → *Audit trail review process, Functionality*
- Data lifecycle management
  → *Archival/Retrieval, Records Retention, Backup/Restore, (True) Copies, Dynamic GxP data*
- System life cycle management
  → *Calibration/Qualification/Validation, Periodic review, Change control, GxP Data migration, Risk management, Transient GxP Data Management*
- Time Stamps
  → *Access security, Daylight savings Time, Synchronization, Time/Date format and precision, Time zone*

These aspects have been documented in a detailed Data Integrity checklist and used to identify the current gaps (refer to Table 2).

The example checklist consists of 44 questions. Not all questions are applicable to all systems: based on the system profiling as defined on *section 4.2*, the system category (from 1 to 6) will guide the decision as to which questions apply.

Table 2 detailed data integrity checklist

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
1	System life cycle management	Calibration/ Qualification/ Validation	Is the system calibrated/qualified/validated in accordance with an approved life cycle management procedure? ***Comment:*** *Includes Paper based systems (procedures for paper batch records needs to be qualified completion of batch record, BRR, archival, …)*	1 / 2 / 3 / 4 / 5 / 6	Documented objective evidence shall be present showing that the system performs as intended. A life cycle management process shall be followed to implement the system. Calibration/ qualification/ validation documentation for the system shall be maintained during the lifetime of the system and retained in accordance with the companies Retention Schedule.			
2	System life cycle management	Change control	Are changes to the system controlled according to the sites change management process?	1 / 2 / 3 / 4 / 5 / 6	All changes to the original validated/ qualified state shall be captured in a Change Management process, including: - All system-, patch- and user roles changes; - All activities performed by Administrators; - GxP Data changes outside the system (database, flat files);			
3	System life cycle management	Data migration	Is data verification executed as part of computer system validation activities when GxP data is migrated from a source system to another system?	5 / 6	Data migration from a source system to another system requires GxP data verification as part of computer system validation activities. GxP Data shall be verified for completeness and accuracy			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					using a statistically relevant sample.			
4	System life cycle management	Transient Data Management	Are the requirements for temporary (interfacing) GxP data defined and documented? ***Examples:*** *data translations, compression, scan-rates, …*	3 / 4 / 5 / 6	Transient GxP Data (interface) requirements shall be defined.			
5	System life cycle management	Transient Data Management	Is the interface validated for intended use? ***Definition of 'Interface':*** *GxP Data in this interfacing system is received from a sending system and forwarded to a receiving system without permanent storage of GxP data in this interfacing system. These systems only transfer GxP data.* ***Note:*** *Connections like RS-232 cords, Moxa-boxes, USB-cables, etc. shall not be treated as interfaces since they do not have user or security management and they do not temporarily store raw GxP data before sending it to the receiving system. These connections shall be treated as being part of the sending system.*	4	The interface shall be validated for intended use. During the set-up and validation, it should be guaranteed that: - the GxP data residing at the receiving system is the exact representation of the GxP data generated at the sending system. - no business users are able to manipulate this temporary GxP data at the intermediate storage location.			
6	System life cycle management	User accounts	Are user accounts required specifically for system testing/qualification in the Production Environment disabled at the end of testing/qualification?	5 / 6	Business administrators shall ensure that if any user accounts are required specifically for system testing/ qualification in the production environment, these accounts are disabled at the end of testing/ qualification.			
7	System life cycle management	Periodic review	Is the system periodically reviewed and is the review documented according to a prescribed process?	1 / 2 / 3 / 4 / 5 / 6	On a periodic basis a system review shall evaluate the current range of functionality, deviation records, incidents, changes, problems, upgrade history, performance,			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					reliability, security and validation status reports. The period shall be defined based on risk.			
8	Data lifecycle management	Data capture/entry	Does the system enforces saving at the moment of GxP data entry?	2 / 3 / 4 / 5 / 6	The system should enforce saving immediately after critical GxP data entry. GxP Data entry prior to saving to permanent memory with audit trail (server, database) is considered to be temporary memory. The length of time that GxP data is held in temporary memory should be minimized.			
9	Data lifecycle management	Data capture/entry	Is a process or procedure in place to identify which system generates and retains the primary GxP data record, in case of discrepancy when the same information is captured by more than one system?	2 / 3 / 4 / 5 / 6	If the same information is captured by more than one system, a process or procedure shall be present to identify which system generates and retains the primary record, in case of discrepancy. The assigned primary record should provide the greatest accuracy, completeness, content and meaning.			
10	Data lifecycle management	Data capture/entry	Are good documentation and record management practices applied on non-electronic GxP data?	1 / 2	Good documentation and record management practices shall be applied on non-electronic GxP data.			
11	Data lifecycle management	Copies	Is a documented process in place to verify and record the integrity and authenticity of the copy when exact or true copies are retained in place of the original GxP data record?	1/ 3 / 5 / 6	Exact or true copies of original records may be retained in place of the original record (e.g. scan of a paper record) provided that a documented			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					process is in place to verify and record the integrity and authenticity of the true copy.			
12	Data lifecycle management	Retention	Are all GxP data (Including meta data and audit trail data) retained in accordance with the companies Retention Schedule and applicable GxP	1 / 2 / 3 / 4 / 5 / 6	GxP Data generated, including paper records, system records and corresponding audit trail entries, shall be retained in accordance with the company's retention schedule and any applicable legal hold notices. GxP documents shall be maintained in a secured storage location that is reasonably accessible and readily available for review to responsible personnel.			
13	Data lifecycle management	Backup/restore	Is a risk-based approach used to define the strategy and the frequency for backup and restore and is the backup, restore strategy documented, validated and periodically tested?	5 / 6	Formal Data Backup procedures for all GxP relevant data shall be established, documented, validated and periodically tested. Backup storage time shall be based on company's requirements. Data Backups shall include both business GxP data and metadata and system GxP data. Data backup frequency shall be pre-determined. and shall be periodically performed per a risk assessment. Data Backups shall be performed prior to any system upgrade or maintenance activity. The process of restoring a Data Backup shall be checked with			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					a pre-defined frequency determined by a risk assessment and shall be documented according to the company's procedure.			
14	Data lifecycle management	Backup/restore	Is a scheduling system maintained for manual data backups and are manual backup processes traceable throughout the process of performing the activity?	5 / 6	For manual Data Backup, a scheduling system shall be maintained. The scheduling system shall track and notify the appropriate personnel when backup is required. Manual backup processes shall be traceable throughout the process of performing the activity.			
15	Data lifecycle management	Backup/restore	Does backup include all relevant raw GxP data, metadata and audit trail data?	5 / 6	Where computerized systems are used to capture, process, report or store raw GxP data electronically, data backups shall include both business GxP data, meta data and system GxP data. The items included in audit trail should be those of relevance to permit reconstruction of the process or activity.			
16	Data lifecycle management	Backup/restore	Are the backups stored in a secure location protected from unauthorized users/people?	5 / 6	The location of the backup shall be separated from the production system. The backup shall be stored in a secure location protected from unauthorized users/people, fire and water (sprinkler and other sources of water and moisture, fire			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					protection and housekeeping). Access to backup data shall not be provided to non-authorized user roles.			
17	Data lifecycle management	Backup/restore	Do changes to the Data Backups process follow a formal change control process?	5 / 6	Any changes to scheduled Data Backups shall follow the formal change management process.			
18	Data lifecycle management	Archival/retrieval	Does the system have an archival strategy documented and is the GxP data retrieval process periodically verified?	1 / 3 / 5 / 6	The system shall have an archival strategy documented. GxP Data and associated meta data shall be archived if system modifications impact the functionality to read or to process existing files. GxP Data shall be archived at the retirement of the system. Data archival storage time shall be defined per the company's Retention Schedule. GxP Data retrieval of archived records shall be tested on a periodic basis, as required by applicable regulation, using a statistically relevant sample.			
19	Data lifecycle management	Archival/retrieval	Are archived GxP data records stored in a secure location protected from unauthorized users/people, fire and water (sprinkler and other sources of water and moisture, fire protection and housekeeping)?	1 / 3 / 5 / 6	Archive records shall be locked such that they cannot be altered or deleted without detection and audit trail. Access to the archived GxP data shall be limited to the System Administrator. If GxP data are archived in a readable format (e.g. pdf files			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					stored in a controlled network folder), they may be made available to the business users for consultation purposes.			
20	Data lifecycle management	Dynamic data	Is dynamic GxP data kept in its dynamic state?	6	Raw GxP data that is generated electronically should remain in its dynamic (electronic) state if the ability to interact with the GxP data is critical to its integrity or later verification. Where the capability of the electronic system permits dynamic storage, it is not appropriate for low-resolution or static (printed / manual) GxP data to be collected in preference to high resolution or dynamic (electronic) GxP data.			
21	Data lifecycle management	Records	Are records protected against intentional or accidental modification or deletion throughout the record retention period?	1 / 3 / 5 / 6	Computerized system records shall be protected against intentional or accidental modification or deletion throughout the companies Retention Schedule. Appropriate controls shall be in place to ensure the integrity of the record throughout the companies Retention Schedule. These controls must prevent manipulation and/or unscheduled destruction of original hard copy paper as well as electronic documents			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					and must be validated in the case of electronic controls.			
22	Audit trail	Functionality	Is good documentation practice applied for paper records?	1 /2/ 3	Good documentation practice shall be applied at the creation and completion of paper records.			
23	Audit trail	Functionality	Is there an audit trail in place for user management and system settings?	2 / 3 / 4 / 5 / 6	Where computerized systems are used to capture, process, report or store raw GxP data electronically, the GxP data shall include user management- and system settings. The items included in audit trail should be those of relevance to permit reconstruction of the generation, modification and deletion of the user management- and system settings.			
24	Audit trail	Functionality	Is there an audit trail in place for GxP data supporting product release	5 / 6	Where computerized systems are used to capture, process, report or store raw GxP data electronically, system design should provide for the retention of full audit trails. The items included in audit trail should be those of relevance to permit reconstruction of the process or activity.			
25	Audit trail	Functionality	Do users or administrators have the ability to amend or switch off the audit trail?	2 / 3 / 4 / 5 / 6	End users shall not have the ability to amend or switch off the audit trail. If the system administrator has access to			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					disable the audit trail a procedure shall be in place to mitigate/prevent this.			
26	Audit trail	Audit trail review	Are audit trails reviewed according to the applicable procedures?	2 / 3 / 4 / 5 / 6	The company's requirements on audit trail review shall be taken into account and should be supported by a risk-based approach to define the process and frequency for execution.			
27	Audit trail	Audit trail review	Is an investigation initiated when data integrity issues are identified during the review?	2 / 3 / 4 / 5 / 6	If any risks or data integrity issues are identified during the audit trail review, an investigation shall be initiated according to the company's non-conformance handling procedures.			
28	Administrator Roles & Responsibilities	Administrator role	Is Segregation of Duties in place for the system?	1/ 2 / 3 / 4 / 5 / 6	Procedures shall be in place describing how the segregation of role functions is managed. The periodic access review shall include a check to ensure that the he users are assigned to the appropriate training curricula for their role and that the appropriate segregation of duties is in place. If required to have dual roles in a single account, a Quality management approved procedural mitigation shall be in place.			
29	Security/User Access Control	Access Approval	Is a procedure in place describing access approval, revocation and periodic access review?	1/ 2 / 3 / 4 / 5 / 6	Procedures shall be in place describing the access approval, revocation and			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					periodic review. Access to a system shall be limited to individuals with a business need to access the system. Access to the system shall be approved by the business system owner or documented delegate before access is granted. All training shall be completed prior to granting access to trainees. A check shall be performed at the time of granting access to a new role whether the user has rights that allow a conflict of interest (segregation of role functions). An approved procedural mitigation shall be in place if a conflict of interest is unavoidable within a single account. Documented evidence of verification of relevant training shall be present. When a user no longer requires system access, a procedure shall exist to disable access in a timely manner.			
30	Security/User Access Control	Access Approval	For contractors; Is an agreement in place with the service provider capturing the data integrity responsibilities of the service provider?	1/ 2 / 3 / 4 / 5 / 6	An agreement shall be in place with the service provider (Quality Agreement, Service Level Agreement, etc.), capturing the responsibilities of the service provider.			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
31	Security/User Access Control	Authentication	Is a procedure present that prohibits to operate and to sign under someone else's name?	1/ 2 / 3 / 4 / 5 / 6	Login IDs and passwords shall only be used by their genuine owner. Procedures and training are in place to ensure individual account access is not shared with other users. Procedures and training are in place to ensure that one user does not log on to a system to provide access to another user.			
32	Security/User Access Control	Authentication	Is the system designed and operating applying unique user specific login on the application system? No shared logins are allowed!	2 / 3 / 4 / 5 / 6	Group IDs and associated passwords (shared logins or generic user access) are not acceptable and shall not be used for accessing the application if the computerized system design supports individual user access. Each user account (internal and external personnel) must have a unique login ID and password. The lack of suitability of alternative systems shall be justified based on a review of system design, and documented. A paper-based method, described in controlled documentation, shall be available for providing traceability of user actions performed by a specific individual. Additional controls shall be in place, including a			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					log to track who & when used the generic account and what was performed.			
33	Security/User Access Control	Authentication	Are login IDs and passwords safeguarded to prevent unauthorized use?	2 / 3 / 4 / 5 / 6	Login IDs and passwords shall be safeguarded to prevent unauthorized use. The system shall only allow authorized users access to the system.			
34	Security/User Access Control	Authentication	Does the system require enforcing for password change at a defined interval?	2 / 3 / 4 / 5 / 6	The system must require enforcing for a password change at a defined interval.			
35	Security/User Access Control	Authentication	Does the system block user accounts if they have executed multiple unauthorized access attempts?	2 / 3 / 4 / 5 / 6	The system user accounts shall be blocked if they have executed multiple unauthorized access attempts.			
36	Security/User Access Control	Authentication	Is an investigation started according to the local sites event handling procedures in case that login credentials have been compromised and potentially misused?	2 / 3 / 4 / 5 / 6	A procedural control shall be present describing that an investigation shall be initiated according to the companies nonconformance handling procedures if login credentials have been compromised and potentially misused.			
37	Security/User Access Control	Authentication	Does an inactive/unattended computer system go into a non-accessible mode after a defined period of inactivity?	2 / 3 / 4 / 5 / 6	An inactive/unattended computer system shall go into a non-accessible mode after a defined period of inactivity.			
38	Security/User Access Control	Authorization	Are user roles and responsibilities pre-determined and documented in controlled documentation?	1 / 2 / 3 / 4 / 5 / 6	Users of computerized systems shall only have access to functionality within the system as required by their job role. User roles and responsibilities shall be pre-determined and			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					documented in controlled documentation			
39	Security/User Access Control	Periodic Access Review	Is a risk-based approach used to define the period for access review and is a procedure in place describing how and what to review (including a check for the appropriate training expectations for each role)?	1 / 2 / 3 / 4 / 5 / 6	A periodic review of access shall be performed at a period based on risk.			
40	Time Stamps	Synchronization	Is the system synchronized with an approved managed trusted time server (atomic clock)?	3 / 4 / 5 / 6	The system shall be synchronized with a managed trusted time server (atomic clock) or when synchronization to a trusted time source is not possible: the administrator shall periodically review the audit log time source for accuracy against a trusted time server (atomic clock), with a frequency defined by risk assessment. The administrator shall correct inaccuracies in system time according to the company's procedures. For server-based systems, the date and time shall be taken always from the server, not from (one of) the client components. All components producing time information shall be synchronized automatically with a managed trusted time server (atomic clock). Synchronization shall start at the start up of the system.			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
41	Time Stamps	Synchronization	For paper based manual observations: do the procedures ensure to make use of an approved managed trusted clock?	1	Procedures shall be in place to ensure the usage of an approved managed trusted clock when recording date and time notations on paper records?			
42	Time Stamps	Time and date format and precision	Are dates in a format that makes the day, month, and year and time zone clearly discernible?	1 / 2 / 3 / 4 / 5 / 6	Dates shall be in a format that makes the day, month, and year clearly discernible. If a 12-hour format is being used to record time, “AM” or “PM” must always be included in the time recorded (e.g. 12:43 PM) for every entry. Any format of AM or PM is acceptable, e.g. AM/PM, A.M./P.M., a.m./p.m., etc. if the meaning is clear in context. Calculations shall be verified for conversion between 24-hour and 12-hour format. The time & date format chosen shall be defined and consistently used.			
43	Time Stamps	Daylight savings	Is the system capable of taking a daylight-saving time switch to correct for summer or winter time?	3 / 4 / 5 / 6	When the system is technically not capable to take daylight-saving time switch into account automatically, specific arrangements need to be implemented and defined in a procedure for that system. These arrangements shall make sure that no GxP data are lost or overwritten. Additional notation may be required for clarity for those			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					two-time definitions whenever displayed or printed.			
44	Time Stamps	Access security	Can non-IT administrator roles change systems date and time settings (including time zone settings)?	3 / 4 / 5 / 6	Only system administrators shall have sufficient authority to change systems date and time settings. Non-administrator roles shall have read only access.			

5 Risk Assessment

The gaps identified by applying the checklist from the previous section, will feed into a risk assessment.

It is essential that the Risk Assessment process involves a truly scientific examination of Data Integrity controls and is not solely used to justify existing practices.

The risk assessment methodology should include general rules for scoring, minimum attendance at the risk assessment sessions, how the outcomes from the risk assessment should be tracked, and how the resultant risk assessments should be approved and archived.

In the example, the FMEA methodology is applied and the following general stages are distinguished (alternative methodologies described in ICH Q9 are acceptable):

A. Identification of Failure Modes: within the context of this guideline the failure modes are to be derived directly from the identified gaps in the previous section.

B. Assessment of Failure Modes using a structured formalized risk assessment.

C. Evaluation of risks using a Risk Priority Number (RPN) defined as follows
   RPN = Severity X Occurrence X Detectability

Figure 4 Risk Assessment example

A	B	C	D	E	F	G	H	I	J
ID#	**Checklist ID**	**Step**	**Function/Requirement or Data flow Step**	**Potential Failure Mode**	**Effect**	**Severity**	**Occurrence**	**Detectability**	**RPN**
1	N/A (Data process mapping)	Software: functionality	Data review	Users can run multiple analysis from the same sample without recording the first initial runs in the system	Testing into compliance.	4	1	4	16
2	ID44	Time Stamps	Access security	A non-IT administrator role is able to change systems date and time settings.	Analyst can misrepresent times of analysis to falsify on results.	4	2	4	32
3	ID26	Audit trail	Audit trail review	Relevant audit trails are not being reviewed since the system is not having a user friendly report to do so.	Possible inccorrect data used in making a batch release desicion, having possible impact on product quality and patients safety.	4	3	3	36
4	ID15	Data lifecycle management	Backup/restore	Backup does not include all relevant GxP metadata.	Permanent loss of GxP data	3	2	3	18

To build the FMEA, the individual gaps in ***'column A to E'*** are resulting out of:

- the data process mapping (*section 0*)
  → example: failure modes in manual transcribing GxP data from one system into the other
- the system assessment applying a checklist with some standard questions to be evaluated (*section 4.3*)

- **Severity *'column G'*:** Considers the worst possible consequence of a failure classified by the degree of injury, property damage, system damage and mission loss that could occur.

Table 3 example of severity scoring

5	Very high
4	High
3	Medium High
2	Medium
1	Low

Guidance with regard to assigning severity is given in section 4.1

- **Occurrence 'column H':** also called 'likelihood', is a numerical estimate of the likelihood that the failure mode will occur
  This variable is to be evaluated system by system / process by process / data set by data set.

Table 4 Example of occurrence scoring

4	The event is likely to occur / this event has occurred historically
3	The event is possible to occur / events of this nature have been historically reported
2	Is unlikely to occur / events of this nature have not been historically reported
1	Is very unlikely to occur / events of this nature have not been historically reported
0	Is technically not possible to occur / technically fail safe

- **Detectability *'column I'*:** also called 'effectiveness', is a numerical subjective estimate of the effectiveness of the controls to prevent or detect the cause or failure mode before the failure reaches the customer.
  This variable is to be evaluated system by system / process by process / data set by data set.

Table 5 Example of detectability scoring

4	No detection mechanism exists
3	Is likely to be detected after lot release
2	Is likely to be detected before lot release
1	Will be detected before lot release on each occasion

The evaluation of risk is attained in terms of RPN using the formula reported above. RPN are grouped in order to define three different levels of risk. The grouping is performed such that an equal number of combinations is present within each RPN group. With reference to the example above, the following RPN group thresholds apply:

Table 6 example of RPN grouping

RPN	Risk category
0-8	Low (green)
9-23	Medium (amber)
24-80	High (red)

6 Risk Management

Once the risk has been assessed, mitigation actions and priorities to address them should be defined.

According to the significance of the risk, short-term and long-term mitigation actions should be defined. These mitigations should lead to an increased control over process, GxP data or systems by acting on probability and/or detectability.

Some examples of short- and/or long-term remediation actions are reported later in the document (*section 8*).

After defining short-term and long-term mitigation actions, re-assess the risks to confirm the expected residual risk is acceptable.

Typically, risks identified as low can be accepted without any further action. Certain medium risks can still be accepted on a temporary basis provided no further mitigation actions are possible at the time of evaluation (e.g. upgrade of software nor alternative solution available from vendor). Such type of remaining medium risks should be periodically re-evaluated.

Actions should be defined and tracked in alignment with the company's CAPA and risk management procedures.

Figure 5 example of risk mitigation actions

ID#	Step	Potential Failure Mode	RPN	Intermediate Action	Severity	Occurrence	Detectability	RPN	Long term Recommended Action	Severity	Occurrence	Detectability	RPN
1	Software: functionality	Users can run multiple analysis from the same sample without recording the first initial runs in the system	16	Introduce a log book to be filled in for each run they start and run.	4	1	2	8	Update the software to go to the version which is storing all of the	4	1	1	4
2	Time Stamps	A non-IT administrator role is able to change systems date and time settings.	32	Restrict the access for that specific role in the system.	4	0	4	0	N/A (coverd by intermadiate action)	4	0	4	0
3	Audit trail	Relevant audit trails are not being reviewed since the system is not having a user friendly report to do so.	36	Implement some validated queries to pull by IT on a frequent basis and provide the data to the end user for review purposes.	4	2	2	16	Implement validated reports containing the validated queries giving the end user the possibility to pull and review the data with a higher frequency on its own.	4	1	1	4
4	Data lifecycle management	Backup does not include all relevant GxP metadata.	18	Run seperate backup runs for the relevant GxP meta data.	3	1	4	12	Include the relevant GxP meta data in the backup process of the related GxP raw data.	3	1	2	6

In the specific example, as a result of implementation of remediation action, residual risk is reduced to low / medium level on short term and to low level on long term basis.

7 References

ICH Q7 Good Manufacturing Practice for APIs

ICH Q9 Quality Risk Management

ICH international conference of harmonisation. (August 2009). *Q8(R2).*

MHRA. (March 2018). *'GxP' Data Integrity Guidance and Definitions'.*

PIC/S PHARMACEUTICAL INSPECTION CONVENTION. (Nov 2018). *GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY (PI 041-1 DRAFT 3).*

WHO. (September 2015). *GUIDANCE ON GOOD DATA AND RECORD MANAGEMENT.*

FDA, Data Integrity and Compliance with Drug CGMP - Questions & Answers - Guidance for industry, Dec 2018

8 Examples

8.1 Production Systems and Process Risk Assessment

1) Scenario:

The MES system is an IT platform, having several modules for serving end to end manufacturing purposes. For this example, the focus is on the production execution module, in particular the 'Synthesis' process module. Material GxP data is available and approved. Equipment is calibrated, configured under change control and in a clean status. Raw materials are available and approved. Users are trained and assigned the correct role. The recipes have lifecycle management guaranteeing change control and are in an approved status.

Sample labels are all created from a prepopulated template.

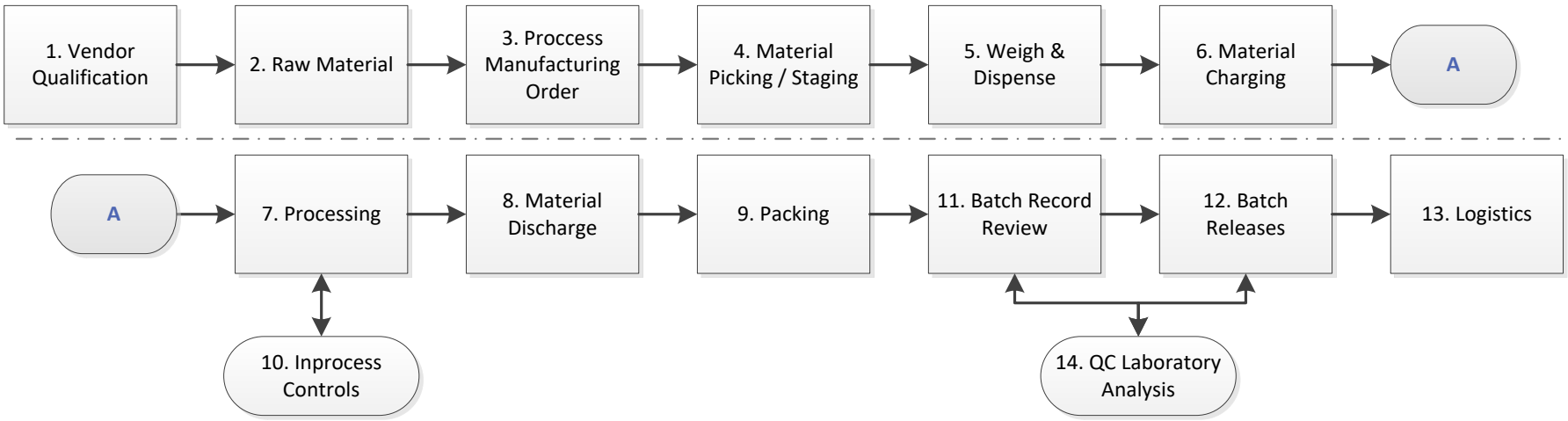
Remark:

The analytical instruments are not taking into account for this example as this is already covered under the lab system example.

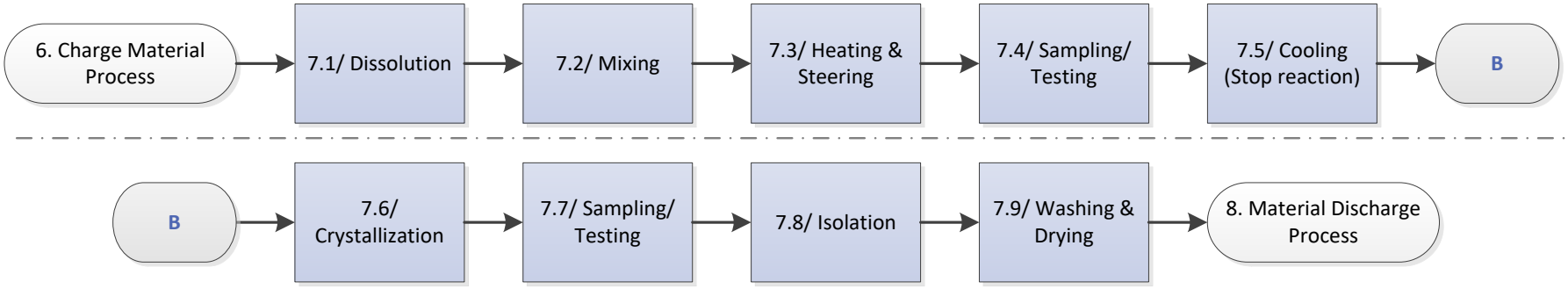
2) Business process mapping

The business process mapping utilizes the 6 FDA systems and their subsystems

➔ FDA Process: Production control system



➔ Sub Process: Processing (Synthesis)



2) Data (paper/electronic) and system identification

a. System identification: (see section 3 step A)

	7.1	7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9
Start	Dissolution	Mixing	Heating & Steering	Sampling/ Testing	Cooling (Stop reaction)	Crystallization	Sampling/ Testing	Isolation	Washing & Drying
GxP Data	electronic	electronic	electronic	paper/ electronic	electronic	electronic	paper/ electronic	electronic	electronic
System	MES PCS/DCS Data Historian	MES PCS/DCS Data Historian	MES PCS/DCS Data Historian	MES Analytical Instrument[2] Sample label LIMS	MES PCS/DCS Data Historian	MES PCS/DCS Data Historian	MES Sample label LIMS	MES PCS/DCS Data Historian	MES PCS/DCS Data Historian

[2] Instrument with DI requirements is not further discussed in this example as this is already covered in the lab system example.

b. Data Identification: (see section 3 step B)

Step	7.1 Dissolution	7.2 Mixing	7.3 Heating & Steering	7.4 Sampling/ Testing	7.5 Cooling (Stop reaction)	7.6 Crystallization	7.7 Sampling/ Testing	7.8 Isolation	7.9 Washing & Drying
System 1: PCS/DCS → Transferring and controlling GxP data from the equipment towards the Data historian and MES systems									
GxP Data elements	Speed of addition Steering Speed Vessel Temp Sludge Temp Pressure	Agitation speed Steering Speed Temperature*	Temperature* Pressure Speed		Temperature* Pressure Speed	Agitation speed Temperature Quantity added		Temperature*	Temperature Pressure
System 2: Data Historian → Recording of the continuous pressure/temperature/speed (trend) data, for permanent storage									
GxP Data elements	Speed of addition Steering Speed Vessel Temp Sludge Temp Pressure	Agitation speed Steering Speed Temperature	Temperature Pressure Speed		Temperature Pressure Speed	Agitation speed Temperature Quantity added		Temperature	Temperature Pressure
System 3: MES									
GxP Data elements	User ID Start Date & Time End Date & Time Equipment ID Ph Dissolution confr. Speed of addition Steering Speed Vessel Temp Sludge Temp Pressure	User ID Start Date & Time End Date & Time Equipment ID Duration* Agitation speed Steering Speed Temperature*	User ID Start Date & Time End Date & Time Equipment ID Temperature* Pressure Speed	User ID Start Date & Time End Date & Time Equipment ID Batch Material ID Storage Condition	User ID Start Date & Time End Date & Time Equipment ID Duration	User ID Start Date & Time End Date & Time Equipment ID Ph	User ID Start Date & Time End Date & Time Equipment ID Batch Material ID Storage Condition	User ID Start Date & Time End Date & Time Equipment ID Loss on drying Visual check result Duration	User ID Start Date & Time End Date & Time Equipment ID Quantity* Duration
System 4: LIMS									
GxP Data elements				Sample ID User ID Date/Time Quantity / Batch Material ID Sample result*			Sample ID User ID Date/Time Quantity / Batch Material ID Sample result*		
System 5: Sample Label									
GxP Data elements				Sample ID User ID Date/Time Quantity / Batch Material ID Storage Condition			Sample ID User ID Date/Time Quantity / Batch Material ID Storage Condition		

c. Highlight electronic GxP data that can be modified/deleted or re-processed after creation. (as indicated by an asterix in above table) (see section 3 step C)

3) Data and System categorisation

a. Data severity assessment (see section 4.1)

This example will focus on the MES system only. The PCS/DCS, Data Historian, Sample label and LIMS should be handled in a separate assessment.

The MES is used for intermediates and APIs manufacturing.
According to the severity definitions, the API categorisation results in **very high severity data**.

b. System profiling (see section 4.2, decision tree figure 3)

System 1: PCS/DCS -> cat 6
System 2: Data Historian -> cat 5
System 3: MES -> cat 6
System 4: LIMS -> cat 6
System 5: Sample label -> cat 1

c. System assessment: (according to checklist 4.3 table 2)
Only the gaps are in below overview.

Topic	Sub topic	Question	Acceptance criteria	Does the system meet the criteria?	Description of gap
Data lifecycle management	Retention	Are all GxP data (Including meta data and audit trail data) retained in accordance with the companies Retention Schedule?	Data generated, including paper records, system records and corresponding audit trail entries, shall be retained in accordance with the companies retention schedule and any applicable legal hold notices. GxP documents shall be maintained in a secured storage location that is reasonably accessible and readily available for review to responsible personnel.	No	The units of measures are not part of the backup and archiving data set. Since these is valuable information in interpreting the time, pressure, temperature notations they become GxP meta data to be retained during the applicable schedule and for disaster recovery purposes.
Audit trail	Audit trail review	Are audit trails reviewed according to the applicable procedures?	The companies requirements on audit trail review shall be taken into account and should be supported by a risk based approach to define the process and frequency for execution.	No	For some steps, the entered duration, temperature or quantity could be modified after the data has been saved. No audit trail is available.
Security/User Access Control	Authentication	Does an inactive/unattended computer system go into a non-accessible mode after a defined period of inactivity?	An inactive/unattended computer system shall go into a non-accessible mode after a defined period of inactivity.	No	The MES user sessions are not being locked automatically after a defined period of inactivity.
Security/User Access Control	Periodic Access Review	Is a risk based approach used to define the period for access review and is a procedure in place describing how and what to review (including a check for the appropriate training expectations for each role)?	A periodic review of access shall be performed at a period based on risk.	No	Periodic access review is not being performed for the administrator roles.
Time Stamps	Access security	Can non-IT administrator roles change systems date and time settings (including time zone settings)?	Only system administrators shall have sufficient authority to change systems date and time settings. Non-administrator roles shall have read only access.	No	The client PCs are not protected for unintentional changes towards the time and date settings. Since for the sampling step the PC's time and data notations are automatically being used, this is critical to be locked for manipulation.

4) Risk Assessment (FMEA to calculate the gaps and their current individual Risk Priority Numbers (RPN)) (see section 5)

ID#	Checklist ID	Step	Function/Requirement or Data flow Step	Potential Failure Mode	Effect	Severity	Occurrence	Detectability	RPN
1	8	Retention	Are all GxP data (Including meta data and audit trail data) retained in accordance with the companies Retention Schedule?	The units of measures are not part of the backup and archiving data set. Since these is valuable information in interpreting the time, pressure, temperature notations they become GxP meta data to be retained during the applicable schedule and for disaster recovery purposes.	Data can be lost.	5	4	1	20
2	14	Audit trail review	Are audit trails reviewed according to the applicable procedures?	For some steps, the entered duration, temperature or quantity could be modified after the data has been saved. No audit trail is available.	Manipulation of data possible.	5	3	4	60
3	17	Authentication	Does an inactive/unattended computer system go into a non-accessible mode after a defined period of inactivity?	The MES user sessions are not being locked automatically after a defined period of inactivity.	Possible misabuse of someones session and cridentials.	5	3	4	60
4	23	Periodic Access Review	Is a risk based approach used to define the period for access review and is a procedure in place describing how and what to review (including a check for the appropriate training expectations for each role)?	Periodic access review is not being performed for the administrator roles.	Risk on administrators access rights being misabused while people have moved position, possibly leading to uncontrolled changes in the system.	5	3	3	45
5	34	Access security	Can non-IT administrator roles change systems date and time settings (including time zone settings)?	The client PCs are not protected for unintentional changes towards the time and date settings. Since for the sampling step the PC's time and data notations are automatically being used, this is critical to be locked for manipulation.	Possible registration of incorrect/manipulated time & date notations for some steps.	5	2	4	40

5) Risk management (see section 6)

The above table shows that 4 of the 5 gaps have a high RPN (Red). Actions have been defined to address these issues immediately. Additional actions have also been defined to mitigate the other gaps

In the next table the RPNs are recalculated after implementation of the defined actions.

ID#	Potential Failure Mode	Effect	Severity	Occurrence	Detectability	RPN	Intermediate Action	Severity	Occurrence	Detectability	RPN	Long term Recommended Action	Severity	Occurrence	Detectability	RPN
1	The units of measures are not part of the backup and archiving data set. Since these is valuable information in interpreting the time, pressure, temperature notations they become GxP meta data to be retained during the applicable schedule and for disaster recovery purposes.	Data can be lost.	5	4	1	20	Assess and include the relevant meta data in the backup and archiving data set.	5	0	1	0	N/A				0
2	For some steps, the entered duration, temperature or quantity could be modified after the data has been saved. No audit trail is available.	Manipulation of data possible.	5	3	4	60	Implement procedure to prohibit users to change regsitered paramters after saving.	5	1	4	20	Upgrade the system to enable the audit trail functionality for these paramters.	5	1	1	5
3	The MES user sessions are not being locked automatically after a defined period of inactivity.	Possible misabuse of someones session and cridentials.	5	3	4	60	Configure the system to go into a non-accessible mode after a defined period of inactivity?	5	0	4	0	N/A				0
4	Periodic access review is not being performed for the administrator roles.	Risk on administrators access rights being misabused while people have moved position, possibly leading to uncontrolled changes in the system.	5	3	3	45	Implement a process and procedure to execute the periodic review of administrator accounts.	5	1	1	5	N/A				0
5	The client PCs are not protected for unintentional changes tow ards the time and date settings. Since for the sampling step the PC's time and data notations are automatically being used, this is critical to be locked for manipulation.	Possible registration of incorrect/manipulated time & date notations for some steps.	5	2	4	40	Implement a process to prohebit for changing the date and time settings on the PC.	5	1	4	20	Lock the date and time setting on the PC.	5	0	4	0

To close out the risk in a documented and formal way, an additional column can describe the objective evidence that has been implemented to remediate the gaps.

ID#	Potential Failure Mode	Effect	RPN	Intermediate Action	Severity	Occurrence	Detectability	RPN	Long term Recommended Action	Severity	Occurrence	Detectability	RPN	References
1	The units of measures are not part of the backup and archiving data set. Since these is valuable information in interpreting the time, pressure, temperature notations they become GxP meta data to be retained during the applicable schedule and for disaster recovery purposes.	Data can be lost.	20	Assess and include the relevant meta data in the backup and archiving data set.	5	0	1	0	N/A				0	1) Inclusion of the relevant meta data in the backup and archiving data set under change control.
2	For some steps, the entered duration, temperature or quantity could be modified after the data has been saved. No audit trail is available.	Manipulation of data possible.	60	Implement procedure to prohibit users to change regsitered paramters after saving.	5	1	4	20	Upgrade the system to enable the audit trail functionality for these paramters.	5	1	1	5	1) Operational procedure 2) Change control for system upgrade including audit trail functionality 3) Audit trail review procedure adapted including the review of the related data
3	The MES user sessions are not being locked automatically after a defined period of inactivity.	Possible misabuse of someones session and cridentials.	60	Configure the system to go into a non-accessible mode after a defined period of inactivity?	5	0	4	0	N/A				0	1) Configuration of the system sessions settings under change control.
4	Periodic access review is not being performed for the administrator roles.	Risk on administrators access rights being misabused while people have moved position, possibly leading to uncontrolled changes in the system.	45	Implement a process and procedure to execute the periodic review of administrator accounts.	5	1	1	5	N/A				0	1) Procedure on periodic review of administrator accounts.
5	The client PCs are not protected for unintentional changes towards the time and date settings. Since for the sampling step the PC's time and data notations are automatically being used, this is critical to be locked for manipulation.	Possible registration of incorrect/manipulated time & date notations for some steps.	40	Implement a process to prohebit for changing the date and time settings on the PC.	5	1	4	20	Lock the date and time setting on the PC.	5	0	4	0	1) Operational procedure to prohebit for changing date and time settings. 2) Change control for locking the date and time settings on the PC's.

8.2 Laboratory Systems and Process Risk Assessment

1) Scenario:

The UV device is a stand-alone instrument, not connected to a network. This device is delivered with a standard desktop computer with Windows 7 as the operating system. The weighing activities are completed using balances that are connected to a printer. These balances are calibrated, and calibration status is controlled and verified through procedure. The balance configuration is locked. The access to the balance is segregated from lab personal.
Prepared analytical worksheets are available for the UV-assay test and these sheets are part of the documentation control process.

2) Business process mapping

For this example, the business process mapping is done through the 6 FDA systems and their subsystems.

➔ Laboratory control system -> Sample Analysis -> UV-Assay

The sub-process is as follows:

2) Data (paper/electronic) and system identification
   a. System identification (see section 3 step A)

	1	2	3	4	5	6
Start	Preparation sample/Ref	Instrument Prep	Measurements	Result process	Result reviewing	Result reporting
GxP Data	Paper	paper/electronic	electronic	paper	paper/electronic	electronic
System	Raw data sheet (RDS) balance	RDS UV instrument	UV instrument	RDS	RDS UV instrument	LIMS

a) Data Identification (see section 3 step B)

Step	1. Preparation sample/Ref	2. Instrument Prep	3. Measurements	4. Result process	5. Result reviewing	6. Result reporting
System 1: RDS						
GxP Data elements	Method ID Sample ID Ref-sample ID Analyst Date and time Balance ID Weights (ticket) Solvents/Reagents ID	Method ID Sample ID Ref-sample ID Analyst Date and time UV ID SST data		Run ID UV absorbances (print or manual) Calculated assay(s)	Reviewer ID Date and time Comments Documentation Audit trail review	
System 2: Balance						
GxP Data elements	Date/Time* Configuration					
System 3: UV						
GxP Data elements		Date/Time* Configuration* Analyst Method ID SST data	UV absorbances* Meta data* (run ID, analyst, time and date, sequence, sample ID, ..)		Raw data Audit trail data	
System 4: LIMS						
GxP Data elements						Sample ID Analyst ID Date and time Sample result

b. Highlight electronic GxP data that can be modified/deleted or re-processed after creation. (asterix in above table) (see section 3 step C)

3) Data and System categorisation

a. Data severity assessment: (see section 4.1)

For this exercise we only continue with the UV-instrument. The raw GxP data sheets (RDS), the balances and LIMS are out of the scope. These systems should be handled in a separate assessment.

The UV-instrument is used for RM, intermediates and APIs. According to the severity definitions, we will apply the API categorisation which will result in very high severity.

b. System profiling: (see section 4.2, decision tree figure 3)

System 1: RDS -> cat 1
System 2: Balance -> cat 3
System 3: UV-instrument -> cat 6
System 4: LIMS -> cat 6

c. System assessment: (according to checklist 4.3 table 2)
Only the gaps are in below overview.

Topic	Sub topic	Question	Acceptance criteria	Does the system meet the criteria?	Description of gap
Data lifecycle management	Data capture/entry	Does the system enforces saving at the moment of GxP data entry?	The system should enforce saving immediately after critical data entry. Data entry prior to saving to permanent memory with audit trail (server, database) is considered to be temporary memory. The length of time that data is held in temporary memory should be minimized.	No	It is possible that data is not saved at the end of the measurement. The system is asking if data need to be saved or not.
Data lifecycle management	Backup/restore	Is a scheduling system maintained for manual data backups and are manual backup processes traceable throughout the process of performing the activity?	For manual Data Backup, a scheduling system shall be maintained. The scheduling system shall track and notify the appropriate personnel when backup is required. Manual backup processes shall be traceable throughout the process of performing the activity.	No	There is no system in place for back-up and storage of standalone systems. (not connected to a network) There is no fixed schedule.
Data lifecycle management	Backup/restore	Do changes to the Data Backups process follow a formal change control process?	Any changes to scheduled Data Backups shall follow the formal change management process.	No	See question 14
Audit trail	Functionality	Is there an audit trail in place for user management and system settings?	Where computerized systems are used to capture, process, report or store raw data electronically, the data shall include user management- and system settings. The items included in audit trail should be those of relevance to permit reconstruction of the generation, modification and deletion of the user management- and system settings.	No	No user management audit trail available
Security/User Access Control	Authentication	Does the system require enforcing for password change at a defined interval?	The system must require enforcing for a passwords change at a defined interval.	No	The system doesn't rquire periodic password change.
Time Stamps	Access security	Can non-IT administrator roles change systems date and time settings (including time zone settings)?	Only system administrators shall have sufficient authority to change systems date and time settings. Non-administrator roles shall have read only access.	No	All users can change date and time. (including time zone)

4) Risk Assessment (FMEA to calculate the gaps and their current individual Risk Priority Numbers (RPN)) (see section 5)

Checklist ID	Step	Function/Requirement or Data flow Step	Potential Failure Mode	Effect	Severity	Occurrence	Detectability	RPN
8	Data capture/entry	Does the system enforces saving at the moment of GxP data entry?	It is possible that data is not saved at the end of the measurement. The system is asking if data need to be saved or not.	Data can be lost.	5	3	4	60
14	Backup/restore	Is a scheduling system maintained for manual data backups and are manual backup processes traceable throughout the process of performing the activity?	There is no system in place for back-up and storage of stand alone systems. (not connected to a network) There is no fixed schedule.	Data can be lost.	5	4	2	40
17	Backup/restore	Do changes to the Data Backups process follow a formal change control process?	see question 14	see question 14	5	4	2	40
23	Functionality	Is there an audit trail in place for user management and system settings?	No user management audit trail available	User levels can be changed. (e.g. an analist can receive admin rights)	5	3	4	60
34	Authentication	Does the system require enforcing for password change at a defined interval?	The UV systems doesn't require periodic pasword change.	Possible misabuse of someones password	5	1	4	20
44	Access security	Can non-IT administrator roles change systems date and time settings (including time zone settings)?	Date and time settings (including time zones) are accessable by all users.	Time of creating data can be adulterated.	5	2	4	40

5) Risk management (see section 6)

The above table shows that 5 of the 6 gaps have a high RPN (Red). Actions have been defined to address these issues immediately. Additional actions have also been defined to mitigate the other gaps

In the next table the RPNs are recalculated after implementation of the defined actions.

Checklist ID	Step	Potential Failure Mode	Effect	RPN	Intermediate Action	Severity	Occurrence	Detectability	RPN	Long term Recommended Action	Severity	Occurrence	Detectability	RPN
8	Data capture/entry	It is possible that data is not saved at the end of the measurement. The system is asking if data need to be saved or not.	Data can be lost.	60	Introduce a procedure to describe the different steps for the user during UV analysis, including a review process at the end.	5	2	2	20	Update the software to go to the version which is storing automatically all of the runs.	5	1	1	5
14	Backup/restore	There is no system in place for back-up and storage of stand alone systems. (not connected to a network) There is no fixed schedule.	Data can be lost.	40	Introduce a manual back-up process	5	2	2	20	Install a full automated back-up system with a defined customized interval	5	1	1	5
17	Backup/restore	see question 14	see question 14	40	See question 14	5	1	1	5	NA since short term inmplementation is sufficient				0
23	Functionality	No user management audit trail available	User levels can be changed. (e.g. an analist can receive admin rights)	60	Install a logbook and periodic user/access review	5	2	2	20	Even the new software doesn't have the audit trail function for user management	5	2	2	20
34	Authentication	The UV systems doesn't require periodic pasword change.	Possible misabuse of someones password	20	Implement a procedure to regularly change of passwords	5	1	2	10	Implement automatic password rules in system. (or update software)	5	0	1	0
44	Access security	Date and time settings (including time zones) are accessable by all users.	Time of creating data can be adulterated.	40	Include a procedure to define R&R towards time and date settings and include check in the periodic review.	5	1	4	20	Update the software to include user level access on date and time settings (including time zone)	5	0	1	0

To close out the risk in a documented and formal way, an additional column can include a reference to the objective evidence that has been implemented to remediate the gaps.

Checklist ID	Step	Potential Failure Mode	Effect	Long term Recommended Action	Severity	Occurrence	Detectability	RPN	References
8	Data capture/entry	It is possible that data is not saved at the end of the measurement. The system is asking if data need to be saved or not.	Data can be lost.	Update the software to go to the version which is storing automatically all of the runs.	5	1	1	5	1) Change control document upgrade UV software 2) Qualification report of UV software NameX, version xx 3)Training records analists 1, 2, x
14	Backup/restore	There is no system in place for back-up and storage of stand alone systems. (not connected to a network) There is no fixed schedule.	Data can be lost.	Install a full automated back-up system with a defined customized interval	5	1	1	5	1) Change control document connecting UV to network 2) Qualification report of back-up/restore sotware NameY, version xx
17	Backup/restore	see question 14	see question 14	NA since short term inmplementation is sufficient				0	1) Change control procedure version xx
23	Functionality	No user management audit trail available	User levels can be changed. (e.g. an analist can receive admin rights)	Even the new software doesn't have the audit trail function for user management	5	2	2	20	1) logbook reference xxx
34	Authentication	The UV systems doesn't require periodic pasword change.	Possible misabuse of someones password	Implement automatic password rules in system. (or update software)	5	0	1	0	1) Change control document upgrade UV software 2) Qualification report of UV software NameX, version xx
44	Access security	Date and time settings (including time zones) are accessable by all users.	Time of creating data can be adulterated.	Update the software to include user level access on date and time settings (including time zone)	5	0	1	0	1) Change control document upgrade UV software 2) Qualification report of UV software NameX, version xx