ACTIVE PHARMACEUTICAL INGREDIENTS COMMITTEE

Practical risk-based guide for managing Data Integrity

Revision 2, April 2022

PREAMBLE

This second 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

Danny De Scheemaecker, Janssen Pharmaceutica NV

Rob De Proost, Janssen Pharmaceutica NV

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

Fraser Strachan, DSM

Bjorn Van Krevelen, Janssen Pharmaceutica NV

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

Alexandra Silva, Hovione FarmaCiencia SA

Jean-Claude Van hove, S.A. Ajinomoto Omnichem N.V.

Erwin de Vries, Aspen Oss B.V.

Catarina Duarte – Hovione

Mar Valladrares, Esteve

Luisa Paulo - Hovione FarmaCiencia SA

Maarten Goud – Synthon

With support and review from:

Pieter van der Hoeven, APIC, Belgium

Annick Bonneure, APIC, Belgium

The APIC Quality Working Group

Revision History		
Version	**Changes**	**Date**
2.0	APIC Logo updates to APIC 30 Years logo. Preamble section updated with current contributors to the guide. Revision history section added. Definitions and abbreviations expanded to include additional terms. Section 4.1 revised to expand the details in "Medium / medium high severity data" and Examples. Section 4.3 additional text added to point to the new quick scan questions. New Table 2b simplified data integrity checklist added. New Section 7 Audit Trail Review Management added. Section 8 References updated to current revisions. Section 9 Examples renamed to Annexes and moved to standalone Annex documents.	Feb 2022
1.0	New Document	Mar 2019

1. General Section

1.1 Introduction

Data integrity refers to the accuracy, completeness, and consistency of CGxP 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+ 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 CGxP-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 8, **Error! Reference source not found.**).

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 CGxP 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 CGxP 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 CGxP data capture where possible
   - Access to electronic CGxP 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 CGxP processes and CGxP 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.

CDS: Chromatography Data System

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

Data Audit Trail: appropriate audit trail elements supporting the acquisition, sequencing, processing, reporting and retention of CGxP data. Including all relevant or significant CGxP 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.

Data elements: (for the purpose of this document) individual CGxP data items that are part of raw CGxP 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 severity assessment: within CGxP 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 CGxP 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.

Dynamic data: Dynamic means that the record format allows interaction between the user and the record content.

FMEA: Failure Mode Effects Analysis. A risk assessment tool.

LIMS: Laboratory Information Management System

MES: Manufacturing Execution System

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).

Original Data: See Raw Data definition.

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.

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

System Audit Trail: a record of changes or events associated with the configuration of the system including administration and security.

System Log: The automatically produced and time-stamped documentation of events relevant to a particular system.

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 CGxP 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 CGxP business processes (or having links to CGxP activities) (ref. to section 2)

- ✓ **Map** each of the CGxP **business processes** and their sub-processes down to level of **process flows** that consist of individual activities (refer to section 2)
- ✓ Identify the **CGxP data elements** and the way the **data flows** (IN/OUT) between the different process steps or activities (**Data Process Mapping**); (refer to section 2)
- ✓ Identify and **isolate** the individual **systems** (both paper and electronic) that manage (generate, store, transfer, or process) CGxP data (refer to section 2)
- ✓ Assign CGxP 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 CGxP 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 checklist 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)

. . . .

Data Integrity – *General Concept of this guide*
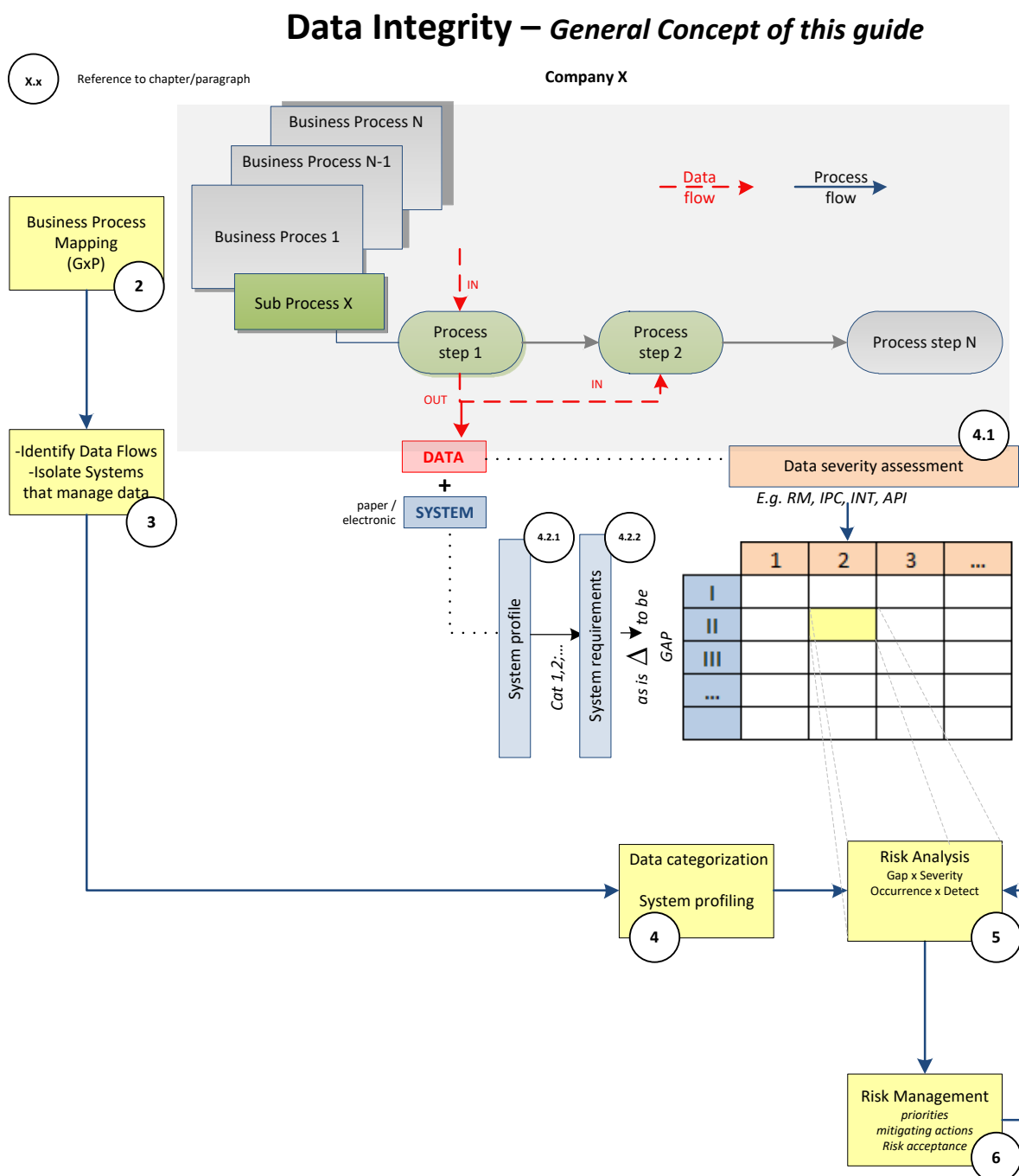
2 Business Processing Mapping

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 CGxP 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 referred to in Error! Reference source not found. 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 CGxP data
   B. Define individual CGxP data elements
   C. Identify CGxP 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)
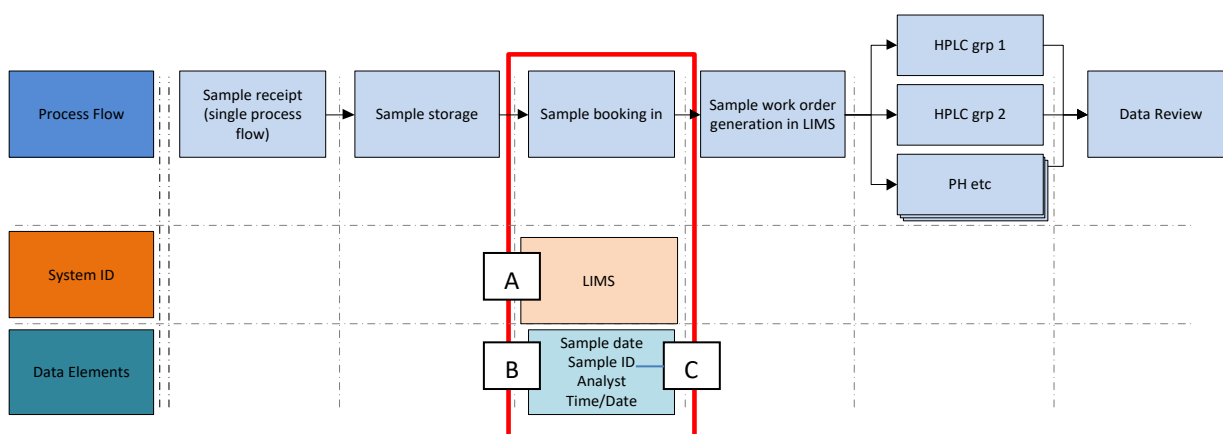
4 Data and System Categorisation

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 CGxP 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 CGxP 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:** CGxP 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:** CGxP Data generated during and directly associated with the production of API intermediates and raw materials testing; configuration data that control the correct execution of the process, as defined in SOP or manufacturing and testing directions.

  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
  - Item master data of the ERP that govern the approval process
  - Setpoint in the DCS that control critical process operating parameters, for example in recipes or fixed manually setpoints.

- **Low severity data:** CGxP Data that is CGxP 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 CGxP data for waste media disposal
  - Operator access to production area

- o CGxP data generated during the development of process or systems or equipment, prior to the validation or qualification
- o Shift scheduling
- o Planning data (production schedule)
- o Shift change notes
- o Time and attendance information (time and attendance system may not be qualified, but maybe used during investigations)
- o Safety training
- o Analysis of chemicals before starting materials
- o For information only in process controls

4.2 System Profiling

Once the system is identified, it can be further categorised based upon the CGxP 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 CGxP data it processes. In case of different outcomes, the highest category is maintained. For hybrid systems both categories have to be taken into account.

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

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

Category 2:   An electronic system and the generated CGxP 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 CGxP 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 CGxP 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 CGxP data are permanently stored, and these CGxP data are not modified by the user to generate results (static CGxP 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 CGxP data are permanently stored, and the CGxP 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
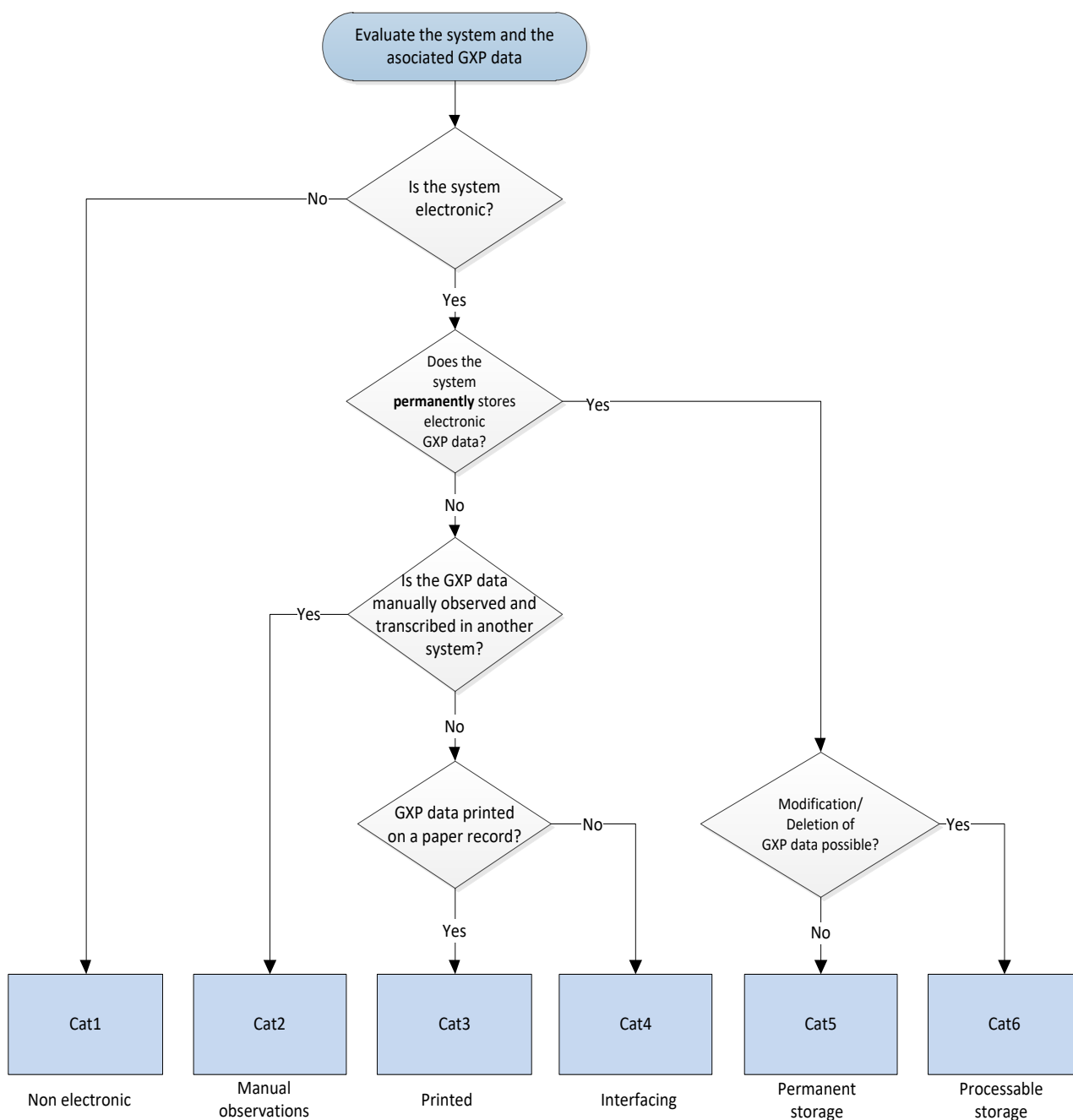
4.2.2   System categorization requirements

It is important to follow the different chronological steps described in the previous and next chapters to assure review of all the CGxP 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 CGxP data is created. Starting from medium criticality up to high criticality (CGxP activities) a process to control the issuance and reconciliation of documents/logbooks. In addition, CGxP 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 CGxP data, while an end-user only will operate the system and use the CGxP 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 CGxP data audit trail and the system audit trail.

e) **Audit trail review:**

An audit trail is only useful if there is a review of the activities that are stored in it. Depending upon the criticality of these stored CGxP data the frequency of the review will increase and should be risk based. Refer to section 7.

f) **Back-up / Restore / Archive**

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

CGxP 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 CGxP data.

Table 1 Minimum system requirements based on categories

Category	Severity (score)	Good documentation practices	Access control	User levels	Audit trail review (ATR)	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 CGxP data	N/A	N/A	N/A	X
	High (4-5)	X + controlled issuance/reconciliation of docs + risk-based witnessing of critical CGxP 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 CGxP data	X[1]	N/A	N/A	X
	High (4-5)	X + controlled issuance/reconciliation of docs + printing of relevant CGxP data	X[1]	N/A	N/A	X

---

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

Table 1 Minimum system requirements based on categories - continued

Category	Severity	Good documentation practices	Access control	User levels	Audit trail review Risk Assessment (ATR)	Back-up / restore / archive
Category 4 (system sending CGxP 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 Ref section 7	X Weekly Back-up
	High (4-5)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	X System ATR Ref section 7	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 &Ref section 7 System ATR Ref section 7	X Weekly Back-up
	Medium (3)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	X Data ATR &System ATR Ref section 7	X Weekly Back-up
	High (4-5)	X + controlled issuance/reconciliation of docs, if any	X	Minimum 2: admin, end user	Data ATR &System ATR Ref section 7	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 CGxP 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 CGxP data*
- System life cycle management
  → *Calibration/Qualification/Validation, Periodic review, Change control, CGxP Data migration, Risk management, Transient CGxP 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.

As an alternative to detailed list of 44 questions, which involve a deep dive into the system, a more simple list can be used (refer to table 2.b.) e.g., in case a lot of systems need to be reviewed and there is a need for a quick/high level scan of the situation and identification of the main gaps (e.g., during an audit), or in case a very simple system needs to be assessed. Only questions that are applicable to the System Category should be used.

Table 2a 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; - CGxP 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 CGxP data is migrated from a source system to another system?	5 / 6	Data migration from a source system to another system requires CGxP data verification as part of computer system validation activities. CGxP Data shall be verified for completeness and			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					accuracy using a statistically relevant sample.			
4	System life cycle management	Transient Data Management	Are the requirements for temporary (interfacing) CGxP data defined and documented? *Examples:* data translations, compression, scan-rates, …	3 / 4 / 5 / 6	Transient CGxP Data (interface) requirements shall be defined.			
5	System life cycle management	Transient Data Management	Is the interface validated for intended use? *Definition of 'Interface':* CGxP Data in this interfacing system is received from a sending system and forwarded to a receiving system without permanent storage of CGxP data in this interfacing system. These systems only transfer CGxP 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 CGxP 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 CGxP data residing at the receiving system is the exact representation of the CGxP data generated at the sending system. - no business users are able to manipulate this temporary CGxP 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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					history, performance, 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 CGxP data entry?	2 / 3 / 4 / 5 / 6	The system should enforce saving immediately after critical CGxP data entry. CGxP Data entry prior to saving to permanent memory with audit trail (server, database) is considered to be temporary memory. The length of time that CGxP 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 CGxP 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 CGxP data?	1 / 2	Good documentation and record management practices shall be applied on non-electronic CGxP 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 CGxP 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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					paper record) provided that a documented process is in place to verify and record the integrity and authenticity of the true copy.			
12	Data lifecycle management	Retention	Are all CGxP data (Including meta data and audit trail data) retained in accordance with the companies Retention Schedule and applicable CGxP	1 / 2 / 3 / 4 / 5 / 6	CGxP 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. CGxP 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 CGxP 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 CGxP data and metadata and system CGxP data. Data backup frequency shall be pre-determined. and shall be periodically performed per a risk assessment. Data Backups shall be performed			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					prior to any system upgrade or maintenance activity. The process of restoring a Data Backup shall be checked with 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 CGxP data, metadata and audit trail data?	5 / 6	Where computerized systems are used to capture, process, report or store raw CGxP data electronically, data backups shall include both business CGxP data, meta data and system CGxP 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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					from unauthorized users/people, fire and water (sprinkler and other sources of water and moisture, fire 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 CGxP data retrieval process periodically verified?	1 / 3 / 5 / 6	The system shall have an archival strategy documented. CGxP Data and associated meta data shall be archived if system modifications impact the functionality to read or to process existing files. CGxP Data shall be archived at the retirement of the system. Data archival storage time shall be defined per the company's Retention Schedule. CGxP 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 CGxP 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.			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					Access to the archived CGxP data shall be limited to the System Administrator. If CGxP data are archived in a readable format (e.g. pdf files 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 CGxP data kept in its dynamic state?	6	Raw CGxP data that is generated electronically should remain in its dynamic (electronic) state if the ability to interact with the CGxP 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) CGxP data to be collected in preference to high resolution or dynamic (electronic) CGxP data. For Example, Chromatography data for additional processing.			
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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					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 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 CGxP data electronically, the CGxP 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 CGxP data supporting product release	5 / 6	Where computerized systems are used to capture, process, report or store raw CGxP data electronically, system design should provide for the retention of full audit trails. The items included in audit			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					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 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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					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 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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					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.			
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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					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 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.			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
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 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			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
					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.			
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.			

ID	Topic	Sub topic	Question	Category	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
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 CGxP data are lost or overwritten. Additional notation may be required for clarity for those 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.			

Table 3 b Simplified data integrity checklist

ID	Topic	Question	Acceptance criteria	Does the system meet the criteria?	Description of gap	Comments
1	System Validation	Has the system software been validated in accordance to the company's procedures and applicable regulatory requirements.	Software of systems for critical CGxP data must be validated			
2	Secured date & time stamps	Are actions performed via the system or data generated by the system date and time stamped ?	System date and time settings cannot be changed by users			
3	Security – User access – user authentication	Does the system prevent usage by authorized users only? Are all actions uniquely attributable to individual users?	System access must be password protected and each user should be logged in with own passwords to uniquely identify any actions an user has performed in the system			
4	User levels	Does the system allow for the configuration of different roles ?	As a minimum there should be a differentiation between an administrator and ordinary users. Ideally differentiation between users based on their role should be available			
5	Audit Trail / Audit trail review	Does the system have audit trail functionality ?	An audit trail for tracking system and data changes is available, enabled and periodically reviewed (based on a risk assessment)			
6	Autosave Raw (original) data	Does the system enforces saving upon entry of data	All data recorded by the system should be saved, no data can be discarded			
7	Data retention (back-up restore – delete)	Are the data generated by the system protected against accidental loss ?	All data must be backed-up to secured locations, the restore functionality has been tested, no data can be deleted			

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 2)
  → example: failure modes in manual transcribing CGxP 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 4 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 5 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 6 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 7 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, CGxP 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 **Error! Reference source not found.***).

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 Audit Trail Review Management

7.1 Types of Audit Trail

The data (including meta data) to be evaluated should include data directly related to manufacturing and control activities but also system data and configuration data that may affect the ability to control processes as expected and designed.

Typically audit trails and their associated reviews can be divided into two categories

Data Audit Trail: appropriate audit trail elements supporting the acquisition, sequencing, processing, reporting and retention of CGxP data. Including all relevant or significant CGxP 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.

System Audit Trail: a record of all administrator changes, examples given in section 7.4.

Operations conducted through the system should ideally be recorded in an audit trail. However often normal operations are recorded by system logs which may not have the same detail recorded. When data entered in the execution of such operations are time and date stamped, not modifiable, system logs and can be used for review purposes in place of or in combination with the audit trail. This decision should be supported by a formal assessment.

7.2 Data Audit Trail Review

The review of audit trail should be conducted systematically as due diligence in order to ensure that data used in support of the lot release is valid and correctly managed.

Some computerized systems may be pre-configured by the vendor to present changes or deletions of certain data or meta-data in a specific report, commonly referred to as an exception report, or to record and present specific data within audit trails. Other systems are not so configured as such, and the audit trail shows most, or all of the operations completed. For these systems, the audit trail functionality might require activation, either for all or for specific data items. Finally, some systems do not have audit trail functionality at all.

Independently from the vendor choices, the company should review and define which data should be subject to audit trail. This will ensure important data is captured and checked as well as limiting the amount of information to be checked, with potential associated benefits to system performance and the ability of users to read and analyse the audit trail information.

Therefore, the content and frequency of a data audit trail review should be based on a risk assessment which considers

- the potential impact of the data on product safety and efficacy
- the probability of a data integrity issue to occur
- the likelihood of detection of a data integrity issue once it has occurred.

An assessment that achieves the above will result in an effective and efficient audit trail review by delivering a rationale for

- which data should be included in the audit trail review.

- the frequency of audit trail review

7.3   Data Audit Trail Risk Assessment

Based on business process mapping, data and system identification as described in the previous chapters, CGMP data and associated systems should be assessed through risk management tools to identify the activities by which the data could be altered or deleted and their risk to product quality. The output is a defined risk level for each, which should guide the content and frequency of audit trail review.

Different frequency levels of the audit trail review can be identified as:

- Routine review at or prior to the lot release
- Periodic to assure that the system is correctly operated, configuration is adequately maintained (including system configuration, user configuration, audit trail configuration and business processes configurations) and data archive is integer (e.g., data deletions); different frequencies can be assigned if required (e.g., every 1, 3, 6 or 12 months).
- when a specific need arises in case of investigation
- Not required

The risk assessment can also guide, and provide justification for, the content of the audit trail review. Only the data or meta data relevant to the activity or activities identified as requiring review at that frequency needs to be included (this could be done by e.g., specific filters, queries, or exception reports within the audit trail functionality). This maximises the value and efficiency of the audit trail reviews.

The APIC Data Integrity taskforce has developed an FMEA template and methodology that can be used to document the potential data integrity breach scenarios and quantify the associated risks.

Severity scoring is based upon the Data Severity level and the CGMP impact of the specific failure mode under consideration.

Occurrence scoring takes into account the potential motivation of the person handling the data and also the complexity of the operation and/or opportunities to manipulate data.

Detectability scoring is based upon the potential for the failure mode to be identified in the absence of an audit trail review given the existing controls.

Refer to the associated Annex(es) for a detailed instruction on the method and practical examples of the approach outlined above.

7.4   System Audit Trail Review

- Examples of areas to be included, but not limited to;
  - Failed user log-in attempts
  - Data deletions
  - Configuration changes e.g., scan and compression rates, audit trail activation/deactivation, file path or database locations …
  - List of users and their authorisation levels
  - Significant errors, alerts or warnings as defined by company e.g., back up failures or issues
  - Remote access events (successful and unsuccessful)

- Typical frequency annual. Higher frequency may be necessary based upon factors such as the severity of the data, system usage and data audit trail review frequency. Shall be clearly risk based and justified.

7.5   Audit Trail Report and Assessment

The access and the analysis of audit trail log can be jeopardized by the complexity of record structures. Although the IT personnel can support the reviewers, so those who are not IT experts should be able to easily access and consult the audit trail information.

Adequate validated tools should be available to perform the review activity; such tools should guarantee readability, reproducibility, and assurance to access audit trail database in read only manner.

Tools, provided by IT department or by the software supplier can include

- structured queries validated, saved, and made available for use of specified users
- reports generated by the system or by external software

The company should define in written instructions the audit trail queries or reports to be used for different systems and different purposes. These instructions need to make clear

- which data is required to be reviewed
- how that data is presented in the audit trail or the associated query/report
- how changes / deletions to the data would be presented in the audit trail or associated query/report
- which data changes are acceptable in the routine use of the system, what justifications are required and acceptable in these instances and how/where these should be documented
- where and how the audit trail review and its outcomes should be documented e.g., in the system itself or via a separate GMP record

8   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). 'CGXP' Data Integrity Guidance and Definitions'.

PIC/S PHARMACEUTICAL INSPECTION CONVENTION. (August 2016). GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED - DRAFT.

WHO. TRS 996 Annex 05 (2016). GUIDANCE ON GOOD DATA AND RECORD MANAGEMENT PRACTICES.

9   Annexes

Refer to Annexes area of Website.