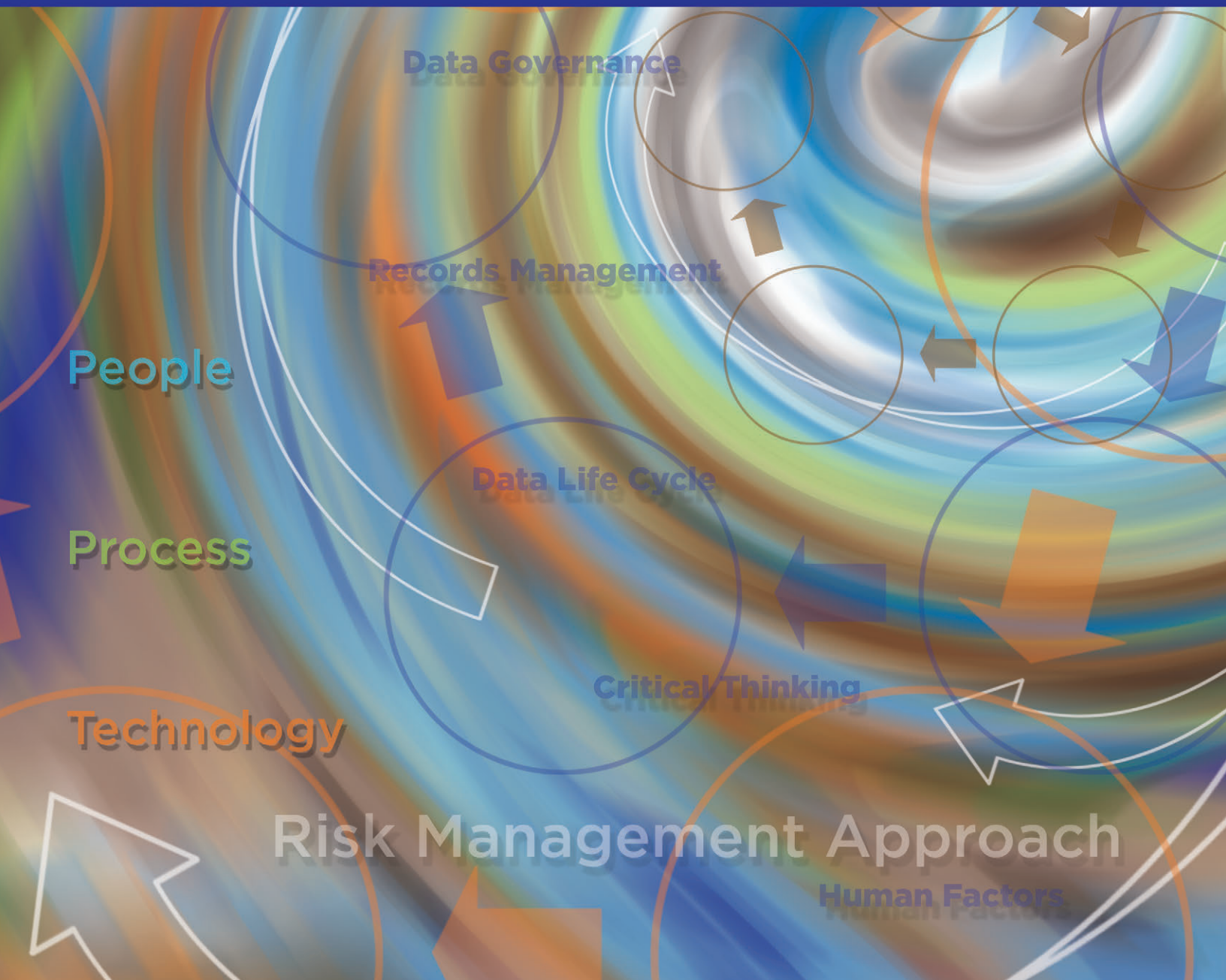
ISPE | GAMP

Records and Data Integrity GUIDE



This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Records and Data Integrity GUIDE

Disclaimer:
This Guide is intended to assist regulated companies in managing records and data throughout the data life cycle. ISPE cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability
In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, or the authors, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

© Copyright ISPE 2017. All rights reserved.

All rights reserved. No part of this document may be reproduced or copied in any form or by any means – graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems – without written permission of ISPE.

All trademarks used are acknowledged.

ISBN 978-1-936379-96-5

This Document is licensed to
Valrico, FL
ID number: 1568

Preface

The importance of data integrity is reflected in recent guidance, citations, and public comments of Regulators and Health Agencies. A number of companies have suffered serious regulatory and financial consequences as a result of unacceptable data integrity practices.

Patient safety is affected by the integrity of critical records, data, and decisions, as well as those aspects concerned with physical attributes of the product. That the phrase “patient safety, product quality, and data integrity” is commonly used in regulatory and industry guidance underlines this point.

The use of information technology and computerized systems in all aspects of life sciences continues to grow and has resulted in the generation of more data to support the development and manufacture of products. Key decisions and actions are routinely being made based on this data, and the integrity of the data, whether in electronic or paper form, is of paramount importance to the industry, the regulatory agencies, and ultimately the patient.

Industry will benefit from clear guidance on ensuring that the management of records and data forms an integral part of the Quality Management System, and is compliant with GxP requirements. This Guide intends to provide such guidance and is aligned with *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems*.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Acknowledgements

The *ISPE GAMP® Records and Data Integrity Guide* was produced by a Task Team led by:

Nigel Price	QCDI Ltd.	United Kingdom
Mike Rutherford	Eli Lilly and Company	USA
Sion Wyn	Conformity Limited	United Kingdom

The work was supported by the ISPE GAMP Community of Practice (CoP).

Core Team

The following individuals took lead roles in the preparation of this Guide:

Chris Clark	TenTenTen Consulting	United Kingdom
Colin Jones	Conformity Limited	United Kingdom
Tony Margetts	Factorytalk Co., Ltd.	Thailand
Mark Newton	Eli Lilly and Company	USA
Arthur “Randy” Perez	Novartis (retired)	USA
Chris Reid	Integrity Solutions Ltd.	United Kingdom
Lorrie Vuolo-Schuessler	GlaxoSmithKline	USA
Charlie Wakeham	Waters Australia Pty. Ltd.	Australia
Christopher White	Alexion Pharmaceuticals	USA
Guy Wingate	GlaxoSmithKline	United Kingdom

Regulatory Input and Review

Particular thanks go to the following for their review and comments on this Guide:

David Churchward	MHRA	United Kingdom
Stephen Grayson	MHRA	United Kingdom
Karl-Heinz Menges	Regierungspräsidium Darmstadt	Germany
Ian Thrussell	World Health Organization	United Kingdom

Subject Matter Expert Input and Review

Particular thanks go to the following for their review and comments on this Guide:

Monica Cahilly	Green Mountain Quality Assurance, LLC	USA
Robert McDowall	R.D. McDowall Ltd.	United Kingdom

The Team would like to special thanks to the Global GAMP Data Integrity Special Interest Group (SIG) for their efforts.

The Team Leads would like to express their grateful thanks to the many individuals and companies from around the world who reviewed and provided comments during the preparation of this Guide; although they are too numerous to list here, their input is greatly appreciated.

Company affiliations are as of the final draft of the Guide.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valid [illegible]
Purchase [illegible]

Downloaded on: 6/19/19 11:34 AM

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

www.ISPE.org

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table of Contents

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to
Carlos J. Cabrer
Padron, PE
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

1 Introduction

1.1 Background

The impact of record and data integrity issues can be significant on a regulated company. It can result in recalls of products, warning or untitled letters, import alerts, injunctions, seizures, Application Integrity Policy Invocations/legal action, and ultimately the potential for patient harm. These regulatory actions can also have a significant financial impact.

There has been increased regulatory focus on all aspects of data integrity, including publication of specific regulatory guidance on the topic, and increased number of citations in the area.

For the purposes of this Guide:

- Regulated data is information used for a regulated purpose or to support a regulated process.
- *"Metadata is data that describes 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."* [1].
- A regulated record[1] is a collection of regulated data (and any metadata necessary to provide meaning and context) with a specific GxP purpose, content, and meaning, and required by GxP regulations. Records include instructions as well as data and reports.
- *"Data Integrity is defined as the extent to which all data are complete, consistent and accurate throughout the data life cycle."* [1]
- The integrity of records depends on the integrity of underlying data, and signatures executed to electronic records should be trustworthy and reliable. See Appendix D3.

This Guide addresses paper records, electronic records, and hybrid situations, while encouraging a move away from hybrid situations, wherever practical.

1.2 Purpose

This *ISPE GAMP® Guide: Records and Data Integrity* provides principles and practical guidance on meeting current expectations for the management of GxP regulated records and data, ensuring that they are complete, consistent, secure, accurate, and available throughout their life cycle. This approach is intended to encourage innovation and technological advance while avoiding unacceptable risk to product quality, patient safety, and public health.

This Guide is intended as a stand-alone Guide. It is aligned with *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems* [3]. This Guide has been designed so that it can be used in parallel with guidance provided both in *ISPE GAMP® 5* [3] and other *ISPE GAMP® Good Practice Guides* [4].

Although the scope of this document is wider, it replaces the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures*.

The Standards Group
Created by
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

[1] Within the US regulatory framework regulated electronic records, and associated signatures, are subject to 21 CFR Part 11 [2]. For further information see Appendix D3.

For individual use only. © Copyright ISPE 2017. All rights reserved.

1.3 Scope

This guide addresses the integrity of GxP records and data used within the regulated life science industries including pharmaceutical, biological, and medical devices. The guidance is intended for regulated companies and suppliers of systems, products, or services in this area, as well as a useful reference for regulators.

Applicable life science regulations and guidance have been taken into account, and the following publications have been specifically considered:

- US Code of Federal Regulations (CFRs) [5] covering GCP, GLP, GMP, and medical devices
- US 21 CFR Part 11 [2] and associated guidance
- Relevant sections of EU GMPs including Chapter 4 [6] and Annex 11 [7]
- MHRA GMP Data Integrity Definitions and Guidance for Industry (Revision 1.1, March 2015) [1]
- MHRA GxP Data Integrity Definitions and Guidance for Industry (Draft version for consultation July 2016) [8]
- FDA Draft Guidance for Industry: Data Integrity and Compliance with CGMP [9]
- ICH Q9 Quality Risk Management [10]
- ICH Q10 Pharmaceutical Quality System [11]
- WHO Annex 5: Guidance on Good Data and Record Management Practices [12]
- PIC/S Draft Guidance: Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments (Draft 2 published August 2016) [13]

This Guide provides a method for managing risk to record and data integrity. Regulated companies may already have established risk management activities and tools, and this Guide does not intend or imply that these existing methods should be discarded, rather that they continue to be used as appropriate within the context of the overall risk management process described. Other methods or techniques giving documented evidence of adequate control, and ensuring appropriate security and integrity, may also be acceptable.

This Guide may also be useful in other regulated areas such as cosmetics and food, or in other areas or sectors where data integrity is important.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

1.4 Structure of this Guide

This Guide contains this introduction, a main body, and a set of appendices. It has been structured to meet the needs of various readers, and contains, in increasing level of detail:

1. Data integrity requirements, critical areas of regulatory focus and concern, and key concepts
2. A framework for data governance and the importance of human factors
3. A complete data life cycle approach as part of a Quality Management System (QMS), from creation to destruction
4. Further information on how to apply the Quality Risk Management (QRM) approach from *ISPE GAMP® 5* [3] to record and data integrity

For individual use only. © Copyright ISPE 2017. All rights reserved.

5. More detailed information, including “how to” guidance for specific topics, in a series of management, development, and operation appendices

1.5 Key Concepts

This section describes key concepts that apply throughout this Guide.

1.5.1 Risk Management Approach

A holistic and flexible risk management approach should be used to ensure the integrity of records and data. This is achieved by the application of appropriate controls to manage identified risks within the context of the regulated process. The effort required to assess and manage risk should be commensurate to the level of risk. Critical thinking and analysis skills should be applied to identify and adequately control risks to patient safety, product quality, and data integrity.

The QRM approach defined in *ISPE GAMP® 5* [3], following ICH Q9 [10], (and also detailed in Section 5) can be applied to identifying, assessing, and managing risks to data and record integrity.

A full understanding of the regulated process to be supported, including the intended use of data within the process, is fundamental. Data integrity cannot be achieved without a complete understanding of the data flow.

1.5.2 Data Governance

Data governance is the sum total of arrangements to ensure that data is recorded, processed, retained and used to ensure a complete, consistent, and accurate record throughout the data life cycle [1]. Data governance ensures formal management of records and data throughout the regulated company. Data governance encompasses the people, processes, and technology required for effective data handling. See Section 3.

1.5.3 Data Life Cycle

All phases in data life cycle from initial data creation, capture, and recording through processing (including transformation or migration), review, reporting, retention, retrieval, and destruction should be controlled and managed in order to ensure accurate, reliable, and compliant records and data. See Section 4.

Details of the life cycle will vary depending on the type of documentation. See Section 4.

Two main types of documents are defined by EU GMP Chapter 4 [6]:

This Document is licensed to

1. Instructions (directions or requirements) type, e.g., specifications, manufacturing formulae, processing, packaging, and testing instructions, SOPs, protocols, and technical agreements

Carlos I. Cabrer
Valrico, FL

2. Record/report type, e.g., batch records, laboratory testing results, certificates of analysis, reports

Regulated data should be controlled and managed, and integrity of the data ensured, e.g., following the principles and requirements described in this Guide. All regulated data is subject to GxP requirements for data integrity and good documentation practices.

A primary record is the record which takes priority in cases where data is collected and retained concurrently by more than one method, and the data does not correspond. The primary record attribute should be defined and documented, and should not be changed on a case by case basis. The UK MHRA [1] defines a primary record as:

> *“The record which takes primacy in cases where data that are collected and retained concurrently by more than one method fail to concur.”*

For individual use only. © Copyright ISPE 2017. All rights reserved.

Risk management principles should be used to ensure that the primary record provides the greatest accuracy, completeness, content, and meaning [1].

For example, high resolution or dynamic (electronic) data should be designated as a primary record in preference to low resolution or static (printed/manual) data. All relevant data should be considered when performing activities such as a risk-based investigation into data anomalies (e.g., out of specification results) [1].

1.5.4 Key Concepts Summarized by ALCOA and ALCOA+

Both the WHO Guidance [12] and the draft PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments [13] indicate that key concepts described by the ALCOA (and ALCOA+) acronyms can help to support record and data integrity.

The WHO Annex 5: Guidance on Good Data and Record Management Practices [12] states:

> *"The basic building blocks of good GXP data are to follow GDocP and then to manage risks to the accuracy, completeness, consistency and reliability of the data throughout their entire period of usefulness – that is, throughout the data life cycle.*
>
> *Personnel should follow GDocP for both paper records and electronic records in order to assure data integrity."*

PIC/S [13] further states:

> *"The application of GDocPs may vary depending on the medium used to record the data (ie. physical vs. electronic records), but the principles are applicable to both…" and "Some key concepts of GDocPs are summarised by the acronym ALCOA…"*

Along with the additional key concepts described by ALCOA+, PIC/S [13] goes on to state:

> *"Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions."*

Tables 1.1 and Table 1.2 provide information of how key concepts described by ALCOA and ALCOA+ should be applied throughout the data life cycle.

Table 1.1: ALCOA

Principle	Data Expectation
Attributable	• Attributable to the person or system generating the data • Identify the person or system performing an activity that creates or modifies data • Linked to the source of the data
Legible	• Readable and permanent • Accessible throughout the data life cycle • Original data and any subsequent modifications are not obscured
Contemporaneous	• Recorded or observed at the time the activity is performed
Original	• Original data is the first recording of data, or a "true copy" which preserves content or meaning
Accurate	• Free from error • No editing performed without documented amendments • Conforming to truth or standard

This Document is licensed to Carlos L Cabrer Valrico, FL ID number: 1568 Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 1.2: ALCOA+

Principle	Data Expectation
Complete	• All data, and relevant metadata, including any repeat or re-analysis performed
Consistent	• Application of good documentation practices throughout any process • The application of date and time stamps in the expected sequence
Enduring	• Recorded in a permanent, maintainable form for the retention period
Available	• Available and accessible for review, audit, or inspection throughout the retention period

1.5.5 Critical Thinking

Critical thinking is a systematic, rational, and disciplined process of evaluating information from a variety of perspectives to yield a balanced and well-reasoned answer. Critical thinking allows the effective interpretation of data and situations while avoiding personal biases, assumptions, and other factors [14].

The application of critical thinking skills allows the identification of gaps in data governance and processes, and assists in challenging the effectiveness of behavioral, procedural, and technical controls in achieving data integrity.

Critical thinking is an important component of data integrity, and many regulators are trained in critical thinking to help them more quickly to identify and assess risk to product quality and patient safety. PIC/S Guidance [13] states:

> *"Critical thinking skills should be used by inspectors to determine whether control and review procedures effectively achieve their desired outcomes."*

Elements of critical thinking include:

- Analyzing situations through gathering relevant details, and reviewing them carefully and objectively through applying knowledge and experience
- Gathering and evaluating information from different sources, understanding links between concepts and ideas, and identifying inconsistencies and errors in reasoning
- Analyzing situations and solving problems consistently, systematically, and logically
- Evaluating information in an open-minded manner to better interpret and understand all available data and signals
- Challenging and questioning ideas and assumptions in a rational and balanced manner
- Comparing, contrasting, and testing alternatives based on ambiguous, incomplete, or partial information
- Creating, developing, and applying new models from experience
- Designing new processes to meet changing process, technical, and regulatory needs

Critical thinking encourages a product quality driven and patient focused approach, rather than a document driven and purely compliance focused approach.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID#2184571568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Guide encourages regulated companies to apply critical thinking and promote its application through leadership, awareness, and training. This Guide encourages the application of critical thinking as part of a holistic top-down risk-based approach.

The identification of appropriate and effective controls within a specific process context, in accordance with an understanding of risks to patient and product, is encouraged.

1.5.6 GxP Computerized System Life Cycle

Data integrity is underpinned by well-documented, validated GxP computerized systems, and the application of appropriate controls throughout both the system and data life cycles.

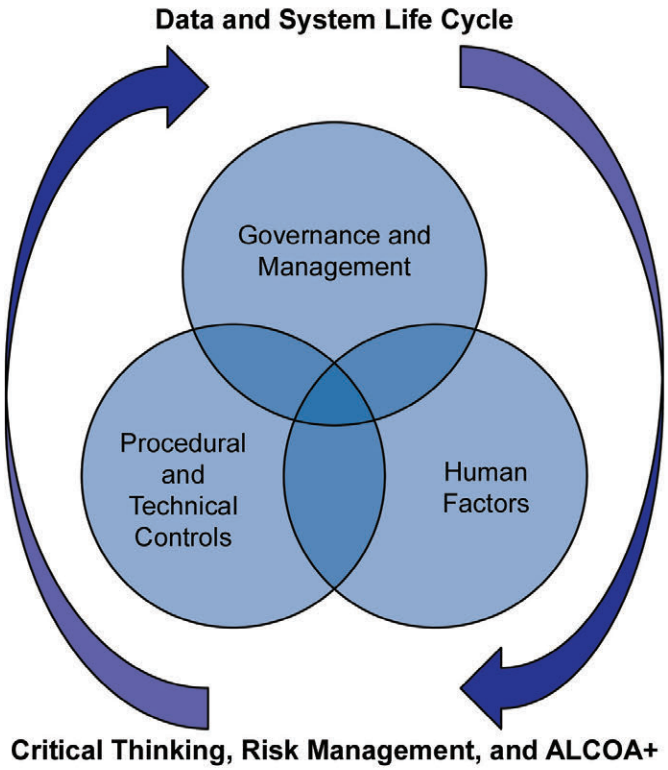
Multiple GxP computerized systems may be involved in supporting a data life cycle, as the data may be passed from system to system. To ensure data integrity all GxP computerized systems should be trustworthy and validated for intended use.

A system life cycle approach, such as described in *ISPE GAMP® 5* [3], should be applied to each GxP computerized system. Record and data integrity should be built-in and maintained throughout the GxP computerized system life cycle phases, from concept through project and operations, to retirement. The GxP computerized system life cycle activities should be scaled based on the complexity and novelty of the system, and potential impact on product quality, patient safety, and data integrity.

The inherent risk of standalone GxP computerized systems may be greater than for enterprise GxP computerized systems. Standalone GxP computerized systems may require different approaches. There should be sufficient effort placed on identifying and managing standalone systems, based on level of impact and vulnerability, when designing controls, defining the data life cycle, and applying the Data Governance Framework.

1.5.7 Summary of the Key Concepts

Figure 1.1: Key Concepts



licensed to
rer
568
9 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Data is managed through a controlled data management life cycle within a Data Governance Framework. A holistic risk management approach is applied to manage risks to data integrity and to ensure that the principles of ALCOA+ are met. The data life cycle may be supported by one or more computerized systems that should be trustworthy and compliant.

1.6 Key Terms

Regulated Data

Information used for a regulated purpose or to support a regulated process.

Metadata (MHRA, 2015 [1], MHRA, 2016 [8])

"Metadata is data that describes 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." [1] *"It also permits data to be attributable to an individual (or if automatically generated, to the original data source)."* [8]

Regulated Record

A collection of regulated data (and any metadata necessary to provide meaning and context) with a specific GxP purpose, content, and meaning, and required by GxP regulations. Records include instructions as well as data and reports.

Atypical / Aberrant / Anomalous Result (MHRA Out Of Specification Investigations Guidance [15])

"Results that are still within specification but are unexpected, questionable, irregular, deviant or abnormal. Examples would be chromatograms that show unexpected peaks, unexpected results for stability test point, etc."

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

2 Regulatory Focus

2.1 Introduction

It is a regulatory expectation that GxP data and records are complete, consistent, reliable, accurate, that their content and meaning are preserved, and that they are available and usable for the required retention period.

Specific areas impacting data integrity, which have been of particular regulatory focus and concern include:

- Lack of basic access control and security measures allowing unauthorized changes
- Shared user logins
- Missing or disabled audit trails
- Lack of contemporaneous recording of activities
- Failure to investigate data discrepancies
- Testing into compliance
- Incomplete collection, retention, and review of data for quality decisions
- Overwriting or deletion of original data
- Data falsification

The FDA [9] states:

> *"CGMP regulations and guidance allow for flexible and risk-based strategies to prevent and detect data integrity issues. Firms should implement meaningful and effective strategies to manage their data integrity risks based upon their process understanding and knowledge management of technologies and business models."*

2.2 Data Integrity Requirements

This section provides an overview of the data integrity expectations on regulated companies based on published regulatory guidance documents. It is an overview and should not be considered as all inclusive.

Regulated companies should have confidence in the quality and the integrity of the data used to make decisions impacting product quality and patient safety.

Data integrity controls for records should ensure that the accuracy, completeness, content, and meaning of data is maintained throughout the data life cycle. The principles of ALCOA+ should be applied.

MHRA states:

> *"The effort and resource applied to assure the validity and integrity of the data should be commensurate with the risk and impact of a data integrity failure to the patient or environment."* [8]

> *"The data governance system should be integral to the pharmaceutical quality system…"* [1]

This Document is Licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1368
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Regulated companies should implement meaningful and effective holistic strategies to manage risks to data integrity, based upon their process understanding and knowledge of technologies. Critical analysis skills should be applied to identify and adequately control risks to data integrity, and to investigate and address root causes if failures occur.

The impact on quality may be determined by considering the type of decisions or activities influenced by the data. Risk to data reflects its vulnerability to unauthorized or inadvertent deletion or amendment, and the opportunity for detection during routine review. Risk to data is typically increased by complex, inconsistent processes, with open ended outcomes that are open to subjective interpretation, compared to simple tasks that are consistent, well defined, and objective [8].

Regulated companies should maintain an inventory of systems generating and maintaining data and the capability of each system. An inventory of documents should be maintained within the Quality Management System (QMS) [6].

Data governance activities should be integral to the QMS [1]. Data governance activities should be supported by an organizational culture that enforces data integrity, led by senior management leadership and behavior. Senior management should:

- Take primary responsibility for data integrity by initially understanding the capabilities and limitations of existing processes, methods, environment, personnel, and technologies
- Subsequently ensure the allocation of necessary resources to address any identified limitations and maintain data integrity

As part of data governance, regulated companies should take the following three types of steps to achieve an acceptable level of data integrity:

- Behavioral
- Procedural
- Technical

2.2.1 Behavioral Steps

Senior management should take responsibility for establishing and maintaining a culture which supports data integrity. Data governance should address the:

- Ownership of data throughout the data life cycle
- Training of personnel in the importance of data integrity principles [8]
- Creation of a working environment that:
  - Enables visibility of errors, omissions, and atypical (aberrant) results [8]
  - Encourages transparent investigation and analysis

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/9/19 11:34 AM

Personnel should be trained in the importance of data integrity, and in the methods of detecting data integrity issues, as part of routine GxP training programs. See Section 3.3.7.

Senior management should also establish arrangements to ensure personnel are not subject to commercial, political, financial, and other pressures or conflicts of interest that may adversely affect the quality of their work and integrity of their data [12].

For individual use only. © Copyright ISPE 2017. All rights reserved.

The quality manual, or equivalent document, should include a quality policy statement of management's commitment to an effective QMS. The policy statement should include a code of ethics and a code of proper conduct which are intended to assure the reliability and completeness of data, including mechanisms for personnel to report any quality and compliance questions or concerns to management [12].

Implementation of an effective quality culture and data governance may be different in different locations. A single approach to quality management or data governance may not be effective in all situations, e.g., if cultural differences and dynamics challenge the societal acceptability of open reporting of problems, and challenging of hierarchy.

2.2.2 Procedural Steps

Regulated companies should implement systems and procedures to:

- To minimize the potential risk to data integrity [1]
- Identify the residual risk, using risk management techniques following the principles of ICH Q9 [10, 1]
- Assess risks associated with any third parties. This should include:
  - Consideration of the control of associated risks
  - How the risks may be addressed in contracts and quality/technical agreements

Data which is manually recorded requires a high level of supervision. Supervisory measures or technical controls should be considered to reduce risk. Examples include second person verification at the same time as the data entry is made or cross checks of related information sources [8].

Records should be accessible at locations where regulated activities take place. Ad hoc data recording and later transcription to official records should be discouraged and should not be necessary [1].

Access to blank paper templates for original data recording should be controlled, where appropriate. Reconciliation of blank paper templates and documentation may be necessary to prevent recreation of a record without control and traceability.

Blank forms (including worksheets, laboratory notebooks, and master production control records) should be controlled by the Quality Unit or by another document control method. For example, numbered sets of blank forms may be issued, as appropriate. The numbering of completed forms should be compared to the numbering of all issued blank forms to ensure that they match. Incomplete or erroneous forms should be kept as part of the permanent record along with written justification for their replacement [9].

This Document is licensed to
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

Regulated companies should allow and encourage correct performance of tasks and accurate recording of data, as required; regulated companies should control physical aspects such as space, equipment, and the timing of events to support these activities. Regulated records and data (including hybrid situations) should be held in secured areas. Appropriate access should be provided to all relevant data for personnel performing data checking activities.

2.2.3 Technical Steps

GxP computerized systems should be validated for intended use, supporting infrastructure qualified, and equipment qualified and calibrated as necessary.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Regulated companies should apply access controls to ensure that people have access only to functionality that is appropriate for their job role, and that actions are attributable to a specific individual [1]. Controls should prevent the unauthorized deletion or modification of regulated data and records, inside or outside the software application (e.g., limiting user rights). Regulated companies should be able to demonstrate the access levels granted to individual staff members and ensure that historical information regarding user access level is available [1]. User access arrangements should prevent (or if necessary log) unauthorized data amendments.

Basic access control measures should be established (e.g., unique usernames and private passwords, and policies and processes for their management). Shared logins or generic user access should not be used as they do not allow for traceability to an individual. Where the computerized system design supports individual user access, this function should be used [1].

Appropriate segregation of duties should be applied. Account privileges should be limited to those required for individuals to perform their duties, e.g., users, supervisors, Quality Unit and administrators.

Elevated privileges permitting activities such as data deletion, database amendment, or system configuration changes (e.g., system administrator rights), should not be assigned to individuals with a direct interest in the data (e.g., data generation, or data review or approval) [1].

Where possible automated data capture techniques should be applied to minimize the risk of data transcription error. Appropriately controlled and synchronized clocks should be available for recording timed events.

Computerized systems should be designed to ensure that the execution of critical steps is recorded at the same time as they are performed [8], and are individually traceable. The EU GMP Annex 11 [7] states that:

> *"Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail")."*

Audit trails are required when users create, modify, or delete regulated records during normal operation [16]. The reason for change or deletion of regulated data should be documented and be consistent with regulatory expectations. The EU GMP Chapter 4 [6] states that:

> *"Any alteration made to the entry on a document should be signed and dated; the alteration should permit the reading of the original information. Where appropriate, the reason for the alteration should be recorded."*

Audit trail functionality should be available, enabled, and verified. Routine data review should include audit trail review where relevant.

Data transfer or migration should be designed and validated to ensure that data integrity principles are maintained. Copies of records should preserve the integrity (accuracy, completeness, content, and meaning) of the original record. Backup and recovery processes should be validated and periodically tested. Security controls should be in place to ensure the data integrity of the record throughout the retention period. Security controls should be validated, where appropriate.

This Document is Licensed to
Carlos J. Cabrer
Valrico, FL
[illegible]
Downloaded on 6/10/19 11:34 AM

Archival arrangements should be established for the long-term retention of regulated data (this should be accurate and complete) in compliance with legislation. The procedures for destruction of data should consider data criticality and any applicable regulatory or legal requirements [1].

Where outsourced or cloud services are used, attention should be paid to understanding the service provided, ownership, retrieval, retention and security of data [8], and the role quality agreements can play in such understanding.

The physical location where the data is held, including the impact of any laws applicable to that geographic location, should be considered. The responsibilities of the service provider (particularly quality related aspects and requirements) should be defined in a technical/quality agreement or contract [8].

For individual use only. © Copyright ISPE 2017. All rights reserved.

3 Data Governance Framework

3.1 Introduction

This section describes a framework for data governance, covering:

- Definition and overview of data governance
- Elements of data governance
- Importance of human factors in data integrity
- Maturity levels for data governance

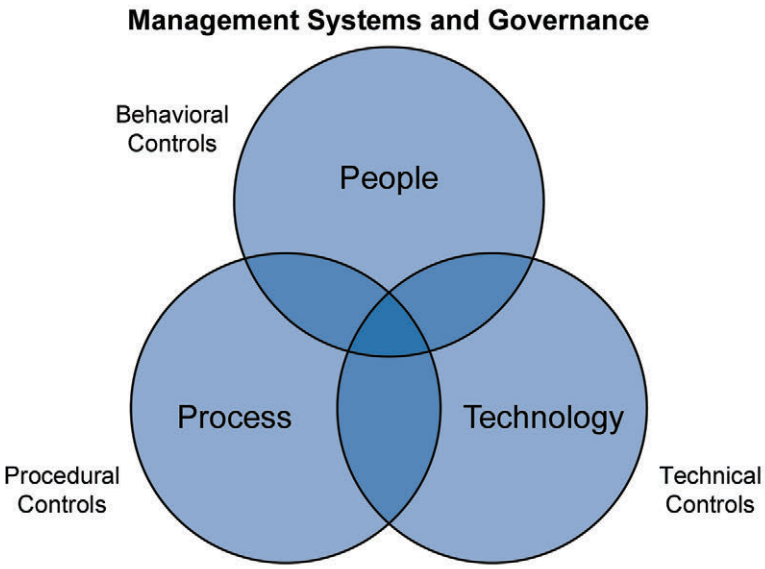
3.2 Overview

Data governance may be defined as (MHRA, 2015 [1]):

> *"The sum total of arrangements to ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data life cycle."*

Data governance ensures formal management of records and data throughout the regulated company. Data governance encompasses the people, processes, and technology required to achieve consistent, accurate, and effective data handling. Data governance provides the structure within which appropriate decisions regarding data related matters may be made according to agreed models, principles, processes, and defined authority. It may also be considered as a quality assurance and control approach for applying rigor and discipline to the process of managing, using, protecting, and improving organizational information.

Figure 3.1: Elements of the Data Governance Framework



nsed to
:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Elements of data governance are closely related to regulatory requirements. Data governance activities should be integral to the QMS [1]. A specific Corporate Data Integrity Program may be necessary to address any gaps in a regulated company's existing Quality Management System.

Senior management commitment and leadership is considered essential to the effectiveness of the data governance framework. Lack of explicit and demonstrable senior management commitment risks ineffective data governance.

Training should be provided for personnel on the importance of data integrity principles and policies [8]. All personnel should be encouraged to report instances of data integrity failures, bad practice, or falsification, without fear of penalty. Such reports should be fully and transparently investigated by senior management, including root cause analysis and the establishment of prevention or detection measures.

Data governance should also address data ownership and responsibilities throughout the data life cycle [1]. Individuals accountable and responsible for specific data, and its integrity and compliance, at various stages of the data life cycle should be defined and documented.

Regulated companies may recognize the need to manage data as a corporate asset. An executive level role, such as a Chief Data Officer (CDO) may be appointed to oversee this area.

The specification, design, validation, and operation of processes and systems should meet the defined requirements for regulated data integrity. This should include ensuring appropriate control over intentional, unintentional, authorized, and unauthorized changes to regulated data.

The risk to data integrity, especially as it may be related to risk to product quality and product safety should be managed by an established Quality Risk Management process, and defined as part of the QMS. This should include consideration of the risk to data integrity associated with any outsourcing of activities or use of service providers, which should be assessed and managed though appropriate formal agreements. Risk associated with use of summary reports or data should be considered, and this may include a review of the mechanisms used to generate and distribute summary data and reports, based on risk.

The data governance approach should be holistic, proportionate, and integrated (MHRA, 2015 [1]):

> *"The data governance system should be integral to the pharmaceutical quality system described in EU GMP chapter 1. The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality assurance resource demands. As such, manufacturers and analytical laboratories are not expected to implement a forensic approach to data checking on a routine basis, but instead design and operate a system which provides an acceptable state of control based on the data integrity risk, and which is fully documented with supporting rationale."*

This Document is licensed to
[redacted]
Valrico, FL
[redacted]
Downloaded on: 6/19/19 11:34 AM

Manual systems and paper based records may be a key area of data integrity failure. Risks associated with manual systems, including risks at the interface between manual and computerized systems, uncontrolled copies, and multiple inconsistent copies, should also be considered. Computerized systems related activities are only one part of the broader governance framework, and equivalent considerations are required for paper based systems and processes. See Appendix O2.

Human factors are a critical aspect of an effective Data Governance Framework, including the topics of cultural differences, human error, understanding and awareness, and motivation and behavior. See Section 3.4 and Appendix M3.

For individual use only. © Copyright ISPE 2017. All rights reserved.

3.3 Elements of the Data Governance Framework

The overall Data Governance Framework consists of the following elements:

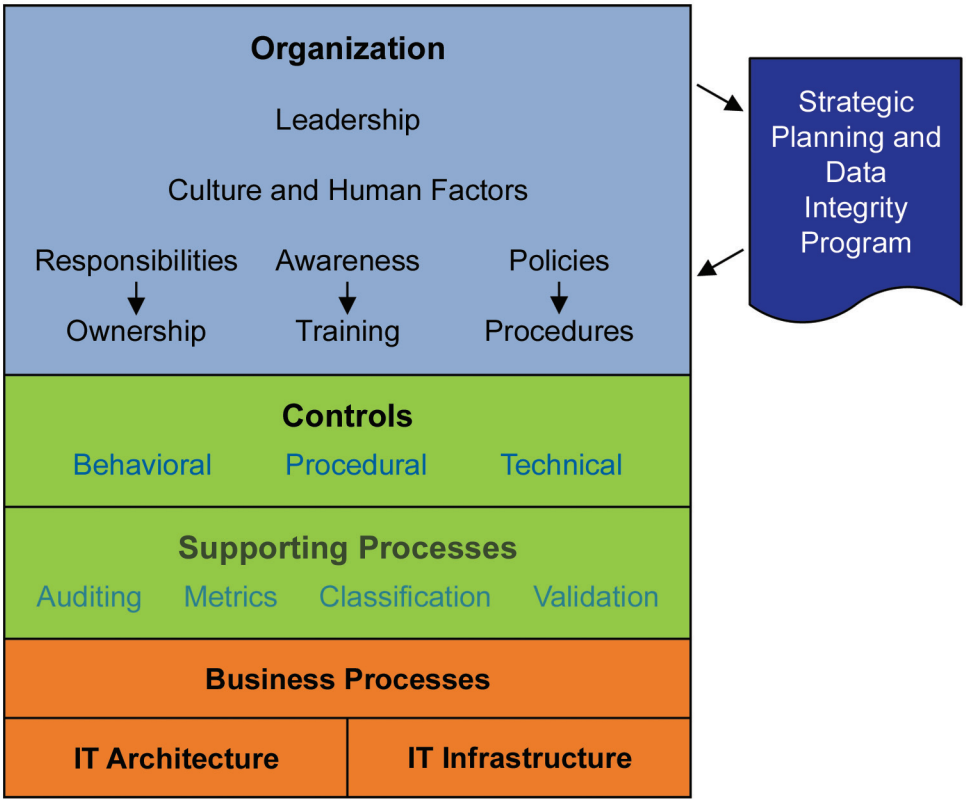
- Goals and objectives
- Organization and data ownership
  - Leadership and management responsibility
  - Roles and responsibilities
  - Policies and standards
  - Awareness and training
- Strategic planning and data integrity program
- Data life cycle
  - Quality risk management
  - Data management
  - Data incident and problem management
  - System access and security management
- Supporting processes
  - Auditing
  - Metrics
  - Classification
  - Validation
- IT architecture and infrastructure
- Maturity level model

This Document is licensed to
Carlos J. Cabrer
Validant S.L.
Downloaded on: 6/19/19 11:34 AM

The regulated company should define clear data governance goals and objectives, supported by a specific data integrity program, if necessary. Senior management should establish appropriate organizational structures to achieve these objectives, with clear polices, standards, and procedures, supported by appropriate training. Appropriate controls should be applied throughout the data life cycle, based on Quality Risk Management. Suitable supporting process (including system validation) and suitable IT architecture and infrastructure should be established. See Figure 3.2.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 3.2: Data Governance Framework



3.3.1 Scope and Objectives

Effective data governance requires regulated companies to be clear on the scope and objectives. General goals and objectives for data governance may include:

- Increasing consistency and confidence in decision making
- Decreasing compliance risk
- Improving data security and privacy
- Maximizing the potential business value of data
- Clarifying information ownership and accountability for data quality
- Minimizing or eliminating re-work
- Optimizing process effectiveness

Data governance activities may have a different scope and objective depending on the nature, situation, and the business context of the regulated company, and it is likely that some focus and prioritization will be required. Although the overall structures and concepts in this guide would be appropriate for many regulated companies, the discussion will concentrate on focus areas for a regulated company, specifically around compliance, regulated data quality, and managing risks to data integrity, and therefore, product quality and patient safety.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568

For individual use only. © Copyright ISPE 2017. All rights reserved.

Specific data governance goals and objectives for a regulated company may include:

- Demonstrating fitness for intended use through computerized system validation
- Assessing and controlling regulated data integrity risk
- Effective compliance with GxP regulations
- Minimizing inspection risk
- Compliance with various data privacy laws and regulations
- Ensuring adequate data security and access control
- Achieving these objectives effectively throughout a wide range of sites encompassing many local cultures and circumstances

For a regulated company, the key objectives should be product quality and patient safety, for which appropriate data governance delivering acceptable data integrity is considered a prerequisite.

Data governance goals, objectives, and scope should be defined and communicated by senior management, based on significant input from Business Process Owners, and Quality Unit and Information Technology functions.

3.3.2 Leadership and Management Responsibility

Senior management with executive authority has a responsibility across all levels of the regulated company to:

- Promote the requirements for data integrity
- Provide appropriate resources
- Resolve issues
- Define priorities
- Ensure that data integrity expectations are achieved

Senior management should also make personnel aware of the relevance of data integrity and the importance of their role in protecting the safety of patients and the reputation of the organization [12].

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

Senior management should lead by example and reinforce the messages by positive action, rewarding appropriate behavior, and taking the necessary management action when data integrity expectations and polices are not met.

It may be helpful to create a data governance council, or equivalent, ensuring adequate input from Business Process Owners, QU, and IT.

A data governance council, or equivalent, could play a key role in:

- Defining policies
- Taking decisions on roles and accountabilities
- Leading initiatives aimed at raising awareness

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Dealing with serious data related problems or incidents

Such a body would typically be led by a member of executive management, e.g., the chief data officer.

3.3.3 Organization and Data Ownership

Data ownership and responsibilities should be defined in the data governance framework and wider QMS. Individuals accountable and responsible for specific data, and its integrity and compliance, at various stages of the data life cycle should be defined and documented.

Data governance should not be regarded as primarily an IT issue, and IT is primarily a supporting role. While it may be an important role for computerized systems, IT has typically no involvement for non-electronic records and data.

Effective data governance in regulated companies requires communication and co-operation between Business Process Owners, Quality Assurance, IT department, and other technical support departments such as engineering, with sufficient support and leadership from senior management.

3.3.4 Key Performance Indicators

Leadership teams should monitor the progress of Data Integrity Programs, covering assessment and remediation activities, as well as monitoring the changing risk profile as work proceeds.

Typically, a small number of Key Performance Indicators (KPIs) will be identified for tracking in a summary dashboard. The nature and content of KPI Dashboards will vary depending on the specific needs, points of focus, and the priority of the data integrity work within the regulated company. Data for the selected KPIs should be readily available to avoid creating excessive work to collect supporting information. KPIs should be a predictor of the challenges ahead and should not just be to show what has been achieved.

KPIs should be clearly defined to promote consistency when the supporting data is collected. Ambiguous definitions can lead to misunderstandings when deciding exactly what to count and not count within the KPI being measured. KPIs should not give an over optimistic or pessimistic view that could impede effective management. Although leadership teams may like simple presentation of data (e.g., Red, Amber, Green status) over simplification should be avoided. Reporting should be accurate and based on metrics. Leadership should also be aware of different levels of risk tolerance across the regulated company.

3.3.5 Roles and Responsibilities

Two key roles associated with regulated Computerized Systems are defined in EU GMP Annex 11 [7] and *ISPE GAMP® 5* [3]:

This Document is licensed to

- Process Owner

Carlos J. Cabrer
Valrico, FL

- System Owner

The terms and definitions used in specific organizations and the boundaries between such roles may vary. The use of the terms in this guide and the role descriptions below are aligned with the definitions in *ISPE GAMP® 5* [3] and EU GMP Annex 11 [7].

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Process Owner

This is the owner of the business process or processes being managed. The process owner is ultimately responsible for ensuring that the computerized system and its operation is in compliance and fit for intended use in accordance with applicable SOPs. The process owner also may be the system owner. The process owner may be the de facto owner of the data residing on the system (data owner) and therefore, ultimately responsible for the integrity of the data. Process owners are typically the head of the functional unit using the system.

Specific activities may include:

- Approval of key documentation as defined by plans and SOPs
- Providing adequate resources (personnel including SMEs, and financial resources) to support development and operation of the system
- Ensuring adequate training for end users
- Ensuring that SOPs required for operation of the system exist, are followed, and are reviewed periodically
- Ensuring changes (including business process changes) are approved and managed
- Reviewing assessment/audit reports, responding to findings, and taking appropriate actions to ensure GxP compliance
- Ensuring that processes/systems are fit for the intended business use, and support data integrity
- Ensuring that data integrity risks are identified and controlled to acceptable levels

System Owner

The system owner is responsible for the availability, and support and maintenance, of a system and for the security of the data residing on that system. The system owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable SOPs. The system owner also may be the process owner (e.g., for IT infrastructure systems or systems not directly supporting GxP).

For systems supporting regulated processes and maintaining regulated data and records the ownership of the data resides with the GxP process owner, not the system owner.

The system owner acts on behalf of the users. The system owner for larger systems will typically be from IT or Engineering functions. Global IT systems may have a global system owner and a local system owner to manage local implementation.

This Document is Licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

Specific activities may include:

- Approval of key documentation as defined by plans and SOPs
- Ensuring that SOPs required for the maintenance of the system exist and are followed
- Ensuring adequate training for maintenance and support staff
- Ensuring changes (including technical changes) are managed
- System life cycle management, including system upgrade and replacement planning

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Ensuring the availability of information for the system inventory and configuration management
- Providing adequate resources (personnel including SMEs, and financial resources) to support the system
- Reviewing audit reports, responding to findings, and taking appropriate actions to ensure GxP compliance, in conjunction with the process owner
- Ensuring that systems are supported and maintained such that they are fit for the intended business use, and support data integrity
- Ensuring that data integrity risks are identified and controlled to acceptable levels

Data Steward

The term data steward is usually used in the context of data governance. The term may be used differently and may apply to different roles in the data governance framework. It may be a functional role, or included as part of a wider job description. Data stewardship activities may be embedded in the responsibilities of other roles, rather than being a new and specific individual role.

In this Guide a data steward is defined as a person with specific tactical coordination and implementation responsibilities for data integrity. A data steward is responsible for performing data usage, management, and security policies as determined by wider data governance initiatives, such as acting as a liaison between the IT department and the business.

Data stewards are typically members of the operational unit or department creating, maintaining, or using the data, e.g., personnel in the laboratories who generate, manage, and handle the data. Segregation of duties should seek to minimize conflict of interest in the data steward role, e.g. avoiding the granting of unnecessary administrator privileges to individuals responsible for functional review and approval of GxP data.

3.3.6 Policies and Standards

Data governance policies and standards should be established and communicated to all relevant staff.

Data policies define the expectations and rules covering the integrity, security, quality, and use of data during its life cycle. Data standards provide more detail on structure, format, definition, and use of data.

It should be clear who has responsibility for defining, reviewing, approving, and monitoring compliance with policies and standards. Such policies and standards may be developed by a data governance council, or similar.

This Document is licensed to
Valrico, FL
Downloaded on: 6/19/19 11:34 AM

Based on the policies and standards, practical procedures, typically in the form of SOPs should be established, defining key activities and processes related to data integrity and providing details on how to achieve the defined polices and standards. Examples include procedures for handling adverse event and complaint data and evidence, manual chromatography integration practices, and batch record assembly and review.

These policies, standards, and procedures as described above should be incorporated as an integral part of the overall QMS, and unnecessary duplication should be avoided.

3.3.7 Awareness and Training

Regulated companies should ensure sufficient training in the importance of data integrity principles and data governance activities, and awareness and training on regulatory requirements and organizational polices and standards.

For individual use only. © Copyright ISPE 2017. All rights reserved.

The aim is to achieve a state where all staff routinely follow accepted data integrity principles and practices, from a position of awareness and understanding, rather than depending on policing and technical controls to prevent users from doing the wrong thing.

For further information on training see Appendix M3.

3.3.8 Technology and Tools

Data governance technology and tools may be used to automate the definition, management, and enforcement of business rules at the data level.

Technology may assist in improving data quality and fitness for intended use by providing tools for data standardization and cleansing. Systems should be designed and configured to enforce integrity and consistency rules, ensuring conformance to defined policies and standards of the organization, and applying technical controls to minimize risks to data integrity. Other tools may include data reporting and visualization tools.

3.3.9 Strategic Planning and Data Integrity Program

Data governance initiatives and programs should be strategic and high level to provide a clear vision and direction to the regulated company, while also ensuring that critical immediate actions are prioritized, facilitated, and delivered. Effective data integrity initiatives and programs need senior management sponsorship at an appropriate level.

Short term needs should be addressed (particularly critical compliance requirements) while the wider aspects of data governance in the organization are being developed and overall maturity level increases.

Data governance programs should be scaled based on the size and complexity of the business unit, level of compliance risk, and potential impact on product quality and patient safety (MHRA, 2015 [1]).

> *"The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality assurance resource demands."*

Communication should clearly link the Data Integrity Program with immediate business objectives or regulatory compliance challenges and requirements, so that the value of the program is obvious to all stakeholders. A communication plan, and if necessary, a change management plan should be established to ensure ongoing stakeholder engagement and understanding, and a smooth transition to new ways of working.

A process should be established for systematically incorporating learning points, and building them into the program and sharing with stakeholders. A repository of items such as templates, checklists, example citations, and FAQs on an internal information sharing and collaboration site, or similar, should be considered.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID Number: 1568
Downloaded on: 6/19/19 11:34 AM

For further information on corporate data integrity programs, see Appendix M1. For further information on knowledge and information sharing, see Appendix M3.

3.3.10 Data Life Cycle and Data Management

The data life cycle, should be defined in standards and procedures. See Section 3.3.6.

Appropriate data management functions should implement the policies and standards established by the data governance framework, including:

- Data quality management
- Master and reference data management

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Data incident management
- Data inventory management

These activities and responsibilities should be integrated into existing roles and functions, where possible.

Data architecture models (which may be conceptual, logical, or physical) may be defined in the form of data flow diagrams, entity relationship diagrams, or system architecture diagrams. These together with data standards and procedures define how the data life cycle should be implemented within the regulated company. Higher level business process mapping and business process definition are prerequisites for the successful development of detailed data related flows and diagrams. See Appendix D2.

Data quality relates to the data's fitness to serve its intended purpose in a given context within a specified business or regulatory process. Data quality management activities address aspects including accuracy, completeness, relevance, consistency, reliability, and accessibility. See Section 1.5.4.

Data quality management enforces the established standards to ensure that data meets the relevant business definitions and rules of the data governance framework. The data incident management process should ensure that data problems and errors are identified, evaluated, resolved, and closed in a timely manner. Data should be safeguarded throughout its life cycle by appropriate system access and security management procedures.

Systems and procedures should be established to minimize the potential risk to data integrity, identify the residual risks, and apply the principles of ICH Q9 [10].

3.4 Human Factors in Data Integrity

Consideration of various human factors is considered critical for effective data integrity.

Cultural considerations can refer to a corporate culture (the model within which an organization operates) or to a local geographic culture (the moral and behavioral norm within a country or region).

Openness and a willingness to discuss difficult situations can support an environment where failing results are seen as a group problem needing to be resolved.

Management should help employees to achieve the openness around data integrity that is needed for compliance.

Data integrity issues often arise from genuine human error; however, regulators do not distinguish between human error and data falsification when assessing the impact of a data integrity failure.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded: 6/10/2017 11:34 AM

Personal gain or self-interest has been the motivator in several high profile fraud cases. The extent and impact of falsification can be magnified if collusion is involved, but geographic and corporate cultures can influence the degree to which collusion may be prevented.

Robust technical controls within all of the data generation, collection, processing or storage systems, coupled with effective data review processes, can reduce opportunities for fraud.

The main foundation for a high level of data integrity is the knowledge and understanding of what data integrity is, the importance it has for an organization, and the personal role each employee has in protecting it.

For further information see Appendix M3.

For individual use only. © Copyright ISPE 2017. All rights reserved.

3.5 Data Integrity Maturity Model

Regulated companies should focus on modifying their processes and systems to use appropriate available technical controls, and evaluate systems for gaps prior to use.

Where feasible, regulated companies should design record and data integrity into their processes before purchasing systems and technology. Purchased systems should be able to be configured to provide adequate data integrity.

The data integrity maturity model described in Appendix M2 is a simple representation of the regulated company. It is based on the status of essential elements of effective processes for data integrity.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

4 Data Life Cycle

4.1 Introduction

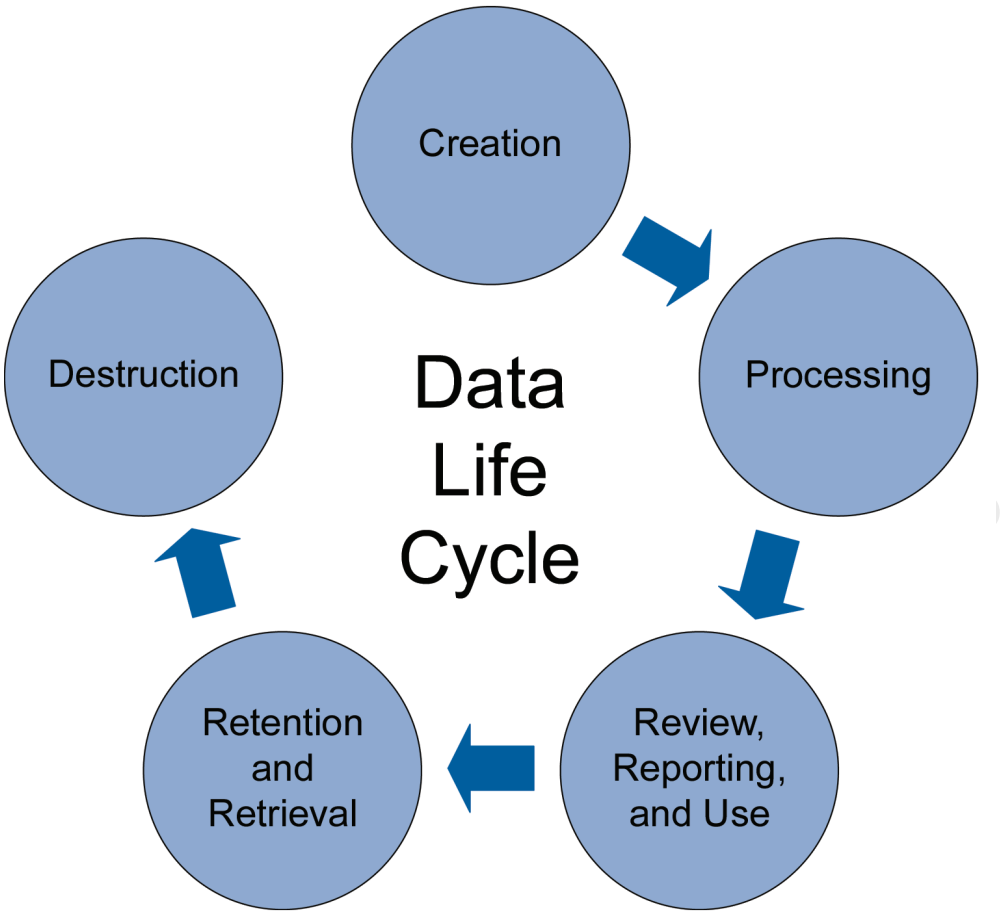
This section describes a generic data life cycle model suitable for all types of data and records. It also describes the activities and requirements for each phase in the data life cycle. Variations within the life cycle phases for different record types are also addressed.

Data integrity should be ensured throughout the data life cycle. Data integrity controls for data and records should ensure that they remain attributable, legible, contemporaneous, original, and accurate (ALCOA) throughout the data life cycle. In addition, data and records should be complete, consistent, enduring and available (ALCOA+). See Section 1.5.4.

The data life cycle includes all phases from initial creation of the data, through processing, use, retention and retrieval to eventual destruction, as shown in Figure 4.1. The data life cycle also supports instructions (e.g., specifications, procedures and templates) and records/reports (including data and results).

Different life cycle phases may need different controls, e.g., second person verification of data during creation or audit trail review during processing and/or use.

Figure 4.1: Data Life Cycle



For individual use only. © Copyright ISPE 2017. All rights reserved.

Each life cycle phase can have an impact on data integrity. Robust risk-based business processes should be defined and implemented and data flows should be understood. This understanding, and these risk-based business processes, should be used to identify, assess, mitigate, and communicate potential data integrity issues throughout the data life cycle.

A specific data life cycle should be defined, based on a thorough understanding of the supported business process. Quality risk management should be applied throughout the data life cycle.

GxP computerized systems supporting the data life cycle and business process should be validated for their intended use, including verification of compliance with regulatory requirements and expectations for data integrity. Regulated companies should ensure that their compliance activities include appropriate specification and verification of data integrity requirements and controls. Regulated companies should not rely only on supplier qualification packages [13].

For further details of verification activities see the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems* [17]. For further details on all aspects of system operation see *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [18].

Data associated with a product or process may cross various boundaries and interfaces throughout the data life cycle [13]. These boundaries may include transfer:

- Of data between systems
- Between a manual process and a computerized system
- To cloud-based applications and storage
- Across organizational boundaries, e.g., between production, QC and QA (internal boundaries)
- Between regulated companies and third parties, e.g., service providers (external boundaries)

Risks associated with such transfers should be considered and appropriate controls established to prevent loss or modification.

4.2 Data Creation

Data capture or recording should ensure that data of appropriate accuracy, completeness, content, and meaning is collected and retained for its intended use [8]. Data integrity may be compromised at the point of creation. If the original data is not reliable then its integrity cannot be ensured. Data creation should provide accurate data which is needed throughout the business process for decisions based on that data.

Data can be created either by entry of new data, captured by the system from an instrument, device, another system, or captured manually. Where data is created by an instrument or measuring system, the instrument should be adequately maintained and calibrated, and should have the range, resolution, linearity, and sensitivity to accurately measure and/or detect the sample attributes under evaluation.

Data should be captured and saved at the time of the activity (contemporaneously), and prior to proceeding to the next activity in the process. Where possible, automated data capture techniques should be applied to minimize the risk of data transcription error. Appropriately controlled and synchronized clocks should be available for recording timed events [8]. Time and date stamps used should be explicit within the context of their use and should be protected from unauthorized change.

For individual use only. © Copyright ISPE 2017. All rights reserved.

All data (even if it has been excluded) should be retained, and be available for review in a format that allows the validity of the decision to exclude the data to be confirmed [8]. If any data is excluded from GxP decision making processes or investigations (e.g., the product release process), there should be a valid, documented, scientific justification for its exclusion [9]. Data may be excluded only where it can be demonstrated through robust science that the data is anomalous or non-representative. This justification should be documented and considered during data review and reporting [8].

Where the capability of the electronic system permits dynamic storage, high resolution or dynamic (electronic) data should be collected in preference to low resolution or static (printed/manual) data [8]. Data should not be stored electronically in temporary memory in a manner that allows for manipulation, before being stored safely and securely.

Data should be attributable to a specific individual, where relevant. The need for verification of data entry, e.g., via second person verification or through technical means such as data validation or barcoding, should be considered based on specific requirements, intended use, and potential impact of data errors within the process.

Risks to data integrity will be influenced by the degree to which data can potentially be manipulated. Individuals with a direct interest in the data should not be granted system level privileges (e.g., permitting data deletion, database modification).

Data should be stored in the predefined location and format. Where the same information is recorded concurrently in more than one location or format, the process/data owner should define where the primary record is retained [1]. Data should be secured from modification by unauthorized persons and should be changed or deleted only in accordance with regulatory expectations and requirements. Any changes should be recorded in the audit trail.

4.3 Data Processing

During this phase, data is processed to obtain and present information in the required format. Processing should occur in accordance with defined and verified processes (e.g., specified and tested calculations and algorithms), and approved procedures.

Record/report type documents are typically processed prior to review and reporting. Process data should not be manipulated to achieve a more desirable end point. If data processing has been repeated, with iterative modification of processing parameters, this should be made apparent [8]. All data relating to iterative processing runs should be reviewed during routine data verification and stored for the duration of the regulatory retention period.

If data is reprocessed, written procedures should be established and followed. Each result should be retained for review, including all data relating to iterative processing runs. For most laboratory analyses, reprocessing data should not be needed on a regular basis. Sampling, testing, or processing should not be performed with the goal of achieving a specific result or to overcome an unacceptable result (e.g., testing different samples until the desired passing result is obtained; this practice is sometimes referred to as testing into compliance) [9].

The Standard for Life Science
Carlos J. Cabrer Valdez PE
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

The impact of data processing on product quality and patient safety will vary by product and business process. The rigor of the controls and verification required for the data processing step should be determined by a documented and justified risk assessment. Topics to consider include, where appropriate:

- Impact of data on product quality and decision making
- Requirements for independent second person verification by a qualified individual
- Opportunity for data modification or deletion
- Preventing original data from being overwritten or deleted

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Preventing data in displays and printouts from being obscured (e.g., by inappropriate annotation)
- Limiting processing to authorized personnel
- Securing processing parameters from unauthorized change
- Logging of parameter changes
- Reporting of data processing errors (either by the system or manually)
- Reconstruction of all data processing activities
- Ensuring traceability of user defined parameters
- Ability of user to influence what data is reported (e.g., user can select what data to print)
- Ability of user to determine presentation of data (e.g., adjusting scale/resolution of graphical reports)
- Use of calculations as validity checks
- Use of calculations for transformation of data
- Exclusion of data during processing should be justified and documented. Excluded data should be retained with the original data set and be available for subsequent review [8].

4.4 Data Review Reporting and Use

During this phase data is used for informed decision making. Data review, reporting, and use should be performed in accordance with defined and verified processes and approved procedures. Data review and reporting is typically concerned with record/report type documents.

4.4.1 Data Review

Data review (including second person review as required by regulation) should determine whether predefined specifications, targets, limits, or criteria have been met. The review should be based on a thorough process understanding (and where applicable system understanding) and impact on product quality and/or decision making, and outcomes and conclusion documented.

This Document is licensed to

The process for the review and approval of data should be described in a procedure.

Original records subject to review should be defined. Reviews should be based upon original data or a true copy (preserving content and meaning). Data review should include a review of relevant metadata and GxP data audit trails, where appropriate [8]. Audit trails are considered part of the history of associated records. Personnel responsible for the review of regulated records should review the audit trails that capture changes to critical data associated with the record. Audit trails that capture changes to critical data should be reviewed with each record and before final approval of the record [9].

All data should be considered, recognizing that data may be stored in different locations. This includes atypical, suspect, rejected, invalid, or deleted data, along with any justifications. Excluded data should be supported by a documented justification.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Routine data review should evaluate [8]:

- The integrity of an individual data set
- Compliance with established organizational and technical measures
- Any data risk indicators (e.g., data amendment, or orphan data)

Data review procedures should cover:

- Method for review
- Method for approval, e.g., by use of an electronic signature
- The meaning of review and approval signatures to ensure persons understand their responsibilities
- Requirements for review by quality assurance (e.g., under US GMPs, any data created as part of a CGMP record must be evaluated by the quality unit as part of release criteria) [9]
- Handling errors or omissions identified during data review
- Managing data corrections or clarifications
- Managing atypical, erroneous, or invalid results

Second person reviews should focus on the overall process from data creation to calculation of reportable results. Such reviews may cross system boundaries as well as the associated external records and may include verification of any calculations used.

Review by exception should be based on validated data processing routines that cannot be influenced by the user.

Periodic review or audit of data governance measures should assess effectiveness of established organizational and technical measures, and should also consider the possibility of unauthorized activity [8].

Where data reviews are conducted by a third party the regulated company should ensure respective roles and responsibilities are documented and agreed by both parties.

4.4.2 Audit Trail Review

This Document is licensed to
Carlos J. Cabrer
Validio, LLC
Downloaded on 6/10/18 11:34 AM

Regulated companies should establish a documented process for review of audit trails, including as a part of second person review. These reviews should form part of the routine data review/approval process and are usually performed by the operational area which has generated the data (e.g., clinical, laboratory, manufacturing).

The requirement for audit trail review, including the frequency and rigor and roles and responsibilities, should be based on a documented risk assessment taking into account the business process and criticality of the data, the complexity of the system and its intended use, and the potential impact on product quality and patient safety.

Audit trail reviews should be performed by an individual who has an understanding of the business process and the impact of the actions recorded. They are an effective means of verifying that changes are made by authorized users and for detecting potential data integrity issues.

For more information on review of audit trails, see Appendix M4.

For individual use only. © Copyright ISPE 2017. All rights reserved.

4.4.3 Data Reporting

Data reporting procedures should ensure the consistency and integrity of results. The procedures should:

- Define what data is to be included in the data set used for reporting the results, i.e., the complete data set
- Address report layout and formatting requirements
- Describe use of reports for GxP decisions
- Address report, review, and approval requirements
- Ensure all data is included in the dataset, unless there is documented justification for excluding it
- Address manual data entry
- Address handling and investigation of atypical results
- Address suspect, rejected, invalid, or deleted data
- Describe how corrective and preventative actions are established for invalid runs, failures, repeats, and other atypical data
- Consider controls to prevent and detect data manipulation
- Encourage problem identification and solving

Particular attention is required when users are able to influence the reporting of data, e.g., testing into compliance should be avoided.

Poorly designed or defined processes, test methods, and reports can create opportunities for data reporting errors, and the potential for erroneous decisions.

Summary reports are limited as they may not contain all data and there is a risk that data issues may not be included, and therefore, not reviewed. Where data summaries are used for reporting, there should be documented verification of these summaries in accordance with original data.

Trending and appropriate metrics can be used to identify and investigate potential data integrity issues.

This Document is licensed to
Patricia Shaw
Valrico, FL
IDnumber: 1568
Downloaded on: 6/19/19 11:34 AM

4.4.4 Data Distribution

Data should be accessed by, and distributed to, authorized individuals and other systems supporting the business process. Interfaces between business process systems should be designed and verified to report failures, prevent data loss, and enable recovery.

Version control should be applied to ensure that personnel have access to the appropriate and up to date versions required in order to perform regulated activities. Instruction type documents should have clear effective dates.

The need for formal confirmation of data receipt should be considered.

For individual use only. © Copyright ISPE 2017. All rights reserved.

4.5 Data Retention and Retrieval

4.5.1 General Requirements

During this phase, data should be retained securely. Data should be readily available through the defined retention period in accordance with defined and verified processes and approved procedures.

Applicable regulatory requirements, other laws and legislation, and internal regulated company policies should be met. This includes retention and privacy requirements. Regulated companies should be aware that legislation such as local laws may have specific requirements to be met (e.g., blood products have different retention periods in the US, Europe, and Japan). Legal admissibility of information stored electronically should also be considered.

Data, including all the original data and associated metadata required to maintain GxP content and meaning, should be defined and stored in a secure location that has adequate physical and electronic protection against deliberate or inadvertent alteration or loss throughout the retention period. Access should be limited to authorized persons and adequate environmental protection from damage should be provided (e.g., from water and fire).

Data, and relevant associated metadata, should be readily traceable and accessible throughout the retention period. The relationships between data and associated metadata should be preserved securely to support future queries or investigations, including reconstruction of GxP activities. Data and associated metadata may reside in separate locations and possibly on different media.

Retrieval of records and copies of records made (including those made for archival purposes), should preserve the content and meaning of the record, and continue to meet relevant GxP regulatory requirements.

Paper records may be retained electronically, e.g., by scanning, provided the copy is verified as a true copy, following an established validated process. Regulated companies may discard the original record once a verified true copy (preserving content and meaning) has been made, e.g., where the original record is not permanent.

Following changes to the system (hardware or software) the regulated company should verify that the retained data can still be accurately retrieved.

Changes to data should be amended only by authorized persons in accordance with an approved process. A record of all changes should be retained indicating when and how the original data was changed. There should be controls in place to ensure that previous versions of data are not inadvertently restored or otherwise made available.

Data retention and retrieval procedures should consider the following, where relevant:

- Address data synchronization where the system architecture involves storing data on multiple servers
- Disaster recovery, including backup and restore
- Durability of media used for storage
- Use of encryption to enhance security (dependent on criticality of data and risks to that data)
- Environmental controls

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For further details on operational processes and controls see *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [18].

Where a third party is involved in regulated data retention and retrieval activities, the regulated company should ensure that a documented assessment of the third party and the risks is undertaken. This should demonstrate that adequate controls are in place and residual risks are understood and accepted.

For individual use only. © Copyright ISPE 2017. All rights reserved.

A formal agreement should be established defining the respective roles and responsibilities and covering:

- Procedures to follow
- Physical location
- Applicable regulations and laws and their impact
- Monitoring
- Incident management
- Business continuity
- Backup
- Data destruction

The same retention and retrieval requirements apply irrespective of whether the data is electronic or paper based.

When a system is retired, or can no longer be supported, regulated companies should consider how regulated data will continue to be retained and retrieved throughout the remainder of the retention period, considering:

- Criticality of data
- Practicality of maintaining existing software (e.g., in a virtual environment)
- Options for migrating the data to another system or to an alternative file format, while retaining the original content and meaning
- Risk of retaining the information without metadata, e.g., retaining only reports written to PDF or paper

Regulated companies may choose to retain records in formats other than the original, provided content and meaning is preserved, and GxP regulations are met. The ability to retain records in a format that ensures the dynamic nature of the data throughout the retention period is not always possible or cost effective, due to the difficulty of migrating the data over time. Decisions should consider the balance between the need for long term accessibility and the level of ongoing retrieval functionality required (e.g., need for dynamic searching, trending, reprocessing). Original records can only be deleted if GxP regulations are fully satisfied and the content and meaning of the records are preserved, following a defined procedure including management authorization.

This Document is licensed to

Migration should be based on a defined process, including a documented risk assessment, and managed within the framework of a data migration plan and report. See *ISPE GAMP® 5* [3].

Carlos J. Cabrer
Validert, LLC
Downloaded on 6/10/2019 11:34 AM

When migrating data, regulated companies should make an informed risk-based decision regarding the migration of metadata, including the audit trail along with the data. This decision should be based upon business requirements and regulatory expectations. If the audit trail is integral to understanding the data, it should be maintained as part of the migrated data. A decision not to migrate an audit trail should be justified based on risk, and documented.

Where legacy systems are retained for data retention and retrieval, the regulated company should periodically verify that data can still be retrieved.

For individual use only. © Copyright ISPE 2017. All rights reserved.

4.5.2 Backup and Restore

Regular backups of all relevant data, including associated metadata required to maintain GxP content and meaning, should be performed in accordance with a documented process in order to allow recovery in the case of system failure, data corruption, or loss. The regulated company should ensure that the backup process is designed such that regulated data is not lost or corrupted.

Data backup should have controls commensurate with those controls for the original data to prevent unauthorized access, modification, or deletion. Backups should be held in a physically separate and secure location. The process and technology for restoring data should be based on the criticality of the data and the required restoration time.

The process for backup and the ability to restore data, should be verified before use and monitored periodically for accessibility, readability, and accuracy through the retention period.

Where relevant metadata is stored separately to the regulated data (e.g., in audit trails or separate files), it should be ensured that all required data is available and can be successfully restored.

4.5.3 Archiving

Archiving involves the long term, permanent retention of data and associated metadata for the purposes of review or investigation throughout the retention period, which may include the reconstruction of a process or activity [1].

Archiving should be performed in accordance with defined and verified processes and approved procedures, that meet the general requirements for retention and retrieval. See Section 4.5.1.

These procedures should consider where appropriate:

- Determination of storage media life expectancy
- Multiple copies
- Management of stored media
- Indexing of stored records
- Impact of system upgrade on stored records
- Impact of changing technology on stored records
- Ability to reprocess data where required

Archived data should be periodically checked for accessibility and readability.

For more information on archiving of records, see Appendix O1.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

4.6 Data Destruction

The data destruction phase involves ensuring that the correct original data is disposed of after the required retention period in accordance with a defined process and approved procedures. The procedure should consider:

- Retention requirements
- Method of disposal, ensuring deletion from all systems and physical locations
- Conditions of disposal
- Measures to prevent inadvertent disposal of data that is still required
- Documentation required to demonstrate timely disposal (for business reasons)
- Limiting disposal functionality to a restricted number of responsible individuals

Data disposal should account for all local legislative retention requirements and for all locations that reference the data.

Retention requirements may differ by jurisdiction, or there may be a litigation hold on some data in some countries/regions. There may also be conflict between applicable laws.

Data disposal should not occur without verification that the regulated record is not in a hold status to support litigation. Distributed copies should also be destroyed of when a record is disposed.

Data should not normally be retained beyond the defined retention period.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

5 Quality Risk Management

5.1 Introduction

Quality risk management is a systematic process for the assessment, control, communication, and review of risks. It is an iterative process used throughout the entire computerized system life cycle from concept to retirement, and throughout the data life cycle from creation to destruction. Risks to data and record integrity should be identified and managed along with other quality and safety risks by adopting a risk management approach based on an understanding of the process.

The evaluation of the risk to quality should be based on scientific knowledge and ultimately linked to the protection of the patient. The level of effort, formality, and documentation of the quality risk management process should be commensurate with the level of risk.

Some records and data may reside on more than one system during their life cycle, and quality risk management activities should start at the business process level, at a level higher than individual systems.

5.2 Process Risk Assessment

A process risk assessment (also known as business process risk assessment) is a non-system specific high level assessment at the business process or data flow, which may occur before systemspecific quality risk management activities. An equivalent risk assessment from a data flow (rather than business process flow) perspective may be performed, using the same approaches and techniques, and with the same benefits.

The process risk assessment is aimed at identifying key high level risks to patient safety, product quality and data integrity, and identifying the required controls to manage those risks. Typically, at this stage no assumptions are made about the nature or exact functionality and design of the computerized system(s) that will support the process.

The process risk assessment provides valuable input to subsequent quality risk management activities. Typical inputs to the process risk assessment include:

- Defined business process scope
- Process descriptions and/or diagrams
- Identified regulatory requirements for the proposed process scope
- Identified company quality requirements

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
[illegible]
Downloaded on: 6/19/19 11:34 AM

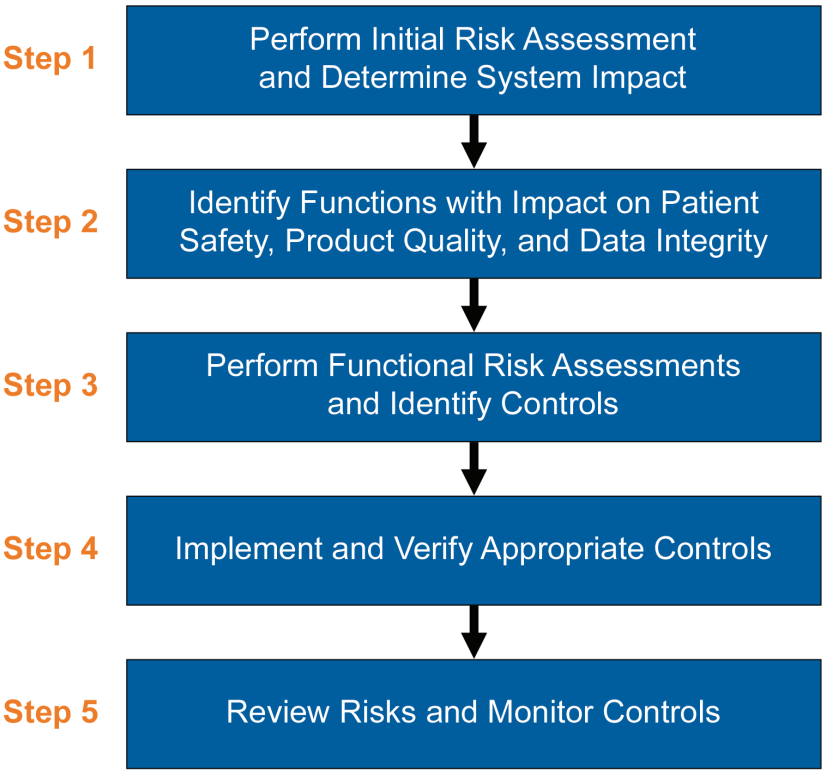
5.3 Quality Risk Management Approach

The activities required to manage the specific risks associated with records and data should form part of the normal individual GxP computerized system life cycle. Decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment [7].

ISPE GAMP® 5 [3] describes a five-step approach for quality risk management, based on ICH Q9 [10].

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 5.1: Quality Risk Management Approach



Some records may be stand alone, maintained on a file share, and may not be associated with any one specific computerized system. The risks associated with such records should be considered and addressed, typically as part of process (or data flow) risk assessment.

Step 1 – Perform Initial Risk Assessment and Determine System Impact

An initial risk assessment should be performed based on an understanding of business processes and process risk assessments, user requirements, regulatory requirements, and known functional areas. This should include initial identification of important data, records, and signatures.

Step 2 – Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity

This Document is licensed to
Carlos J. Cabrer
Valid to: [illegible]
ID number: 1568
Downloaded on: 6/10/2011 1:34 AM

Functions which have an impact on patient safety, product quality, and data integrity should be identified by building on information gathered previously, referring to relevant specifications, and taking into account project approach, system architecture, and categorization of system components.

Based on defined business processes, during development of user requirements and during subsequent functional, configuration, or design specifications, the associated data, records, and signatures should be defined and documented.

This activity typically begins in Step 1, and continues iteratively through the data life cycle. A data flow analysis is useful in supporting this activity and in determining the role of each item in regulated processes. The primary record should be identified. The emphasis should be on identifying data and records at the regulated process level, rather than physical database records, or table fields.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Step 3 – Perform Functional Risk Assessments and Identify Controls

Functions identified during Step 2 should be assessed by considering possible hazards, and how the potential harm arising from these hazards may be controlled. It may be necessary to perform a more detailed assessment that analyzes further the severity of harm, likelihood of occurrence, and probability of detection (See *ISPE GAMP® 5* [3] for an example detailed assessment process).

Potential hazards to data, records, and signature integrity should be specifically addressed as an integral part of these assessments. Required data integrity controls should be identified and documented. It is desirable to eliminate risk by modifying processes or system design, where possible. If risk cannot be eliminated, it should be reduced to an acceptable level by appropriate controls.

Controls may be behavioral, procedural, or technical in nature. Technical controls should be included in the relevant specifications (e.g., user requirements specifications or functional specifications), and identified procedures should be developed for the system. Verification of the installation and correct operation of technical controls (and some procedural controls) should occur during testing. Behavioral controls are general, i.e., not specific to a single system, and should be part of a wider data governance framework. See Appendix D3.

A suitable cross functional team should be involved in risk assessments, including the process owner, data owners, and other functions as necessary including QU, IT, and engineering.

Step 4 – Implement and Verify Appropriate Controls

The control measures identified in Step 3 should be implemented and verified to ensure that they have been successfully implemented. Controls should be traceable to the relevant identified risks. The verification activity should demonstrate that the controls are effective in performing the required risk reduction.

Step 5 – Review Risks and Monitor Controls

Regulated companies may have different mechanisms and programs in place to review and assess the effectiveness of data integrity controls. These include periodic review of system, user access reviews, IT security audits, data audits, and QA audits.

Periodic reviews may address only a subset of data integrity controls, as they are typically focused on validation and system based aspects and not organizational, data, and process level aspects.

5.4 Product and Process Context

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

Effective quality risk management depends on knowledge of the regulated product and process. Judgment should be driven by an overall risk assessment of the business or facility aimed at identifying the overall risks to product quality or public safety that may occur due to data integrity problems. Different facilities and products will have different risk profiles.

Product and process risk considerations include:

- Misinterpretation of product quality, safety, or efficacy
- Adulteration of product
- Release of adulterated or quarantined product
- Misbranding of product

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Inability to recall product
- Incorrect product quality or patient safety decisions, e.g., impact on preclinical or clinical safety results, Adverse Drug Reactions (ADR) and Adverse Events (AE).
- Incorrect submission to a regulatory agency

Risks of such outcomes, the existence of other mitigating controls, as well as the vulnerability of the data to loss or corruption, and the actual physical and technical environment, should be considered when identifying the appropriate and commensurate level of control.

Hazards and vulnerabilities should be identified and documented as part of the risk assessment process. Examples of hazards potentially impacting data integrity include:

- Data falsification due to storing data electronically in temporary memory in a manner that allows for manipulation
- Loss or corruption of data due to system interface errors
- Manual transcription or data entry errors
- Unauthorized approvals due to uncontrolled access
- Data corruption due to information security failures (e.g., firewall breaches or malware attacks)
- Processing failures due to software or configuration error
- Loss of data availability due to environmental problems or hardware failures

Effort should be focused on hazards that are specific to the process, type of data, use of data, or type of system, as this will help identify required controls beyond the basic controls, aimed at routine factors, that are typically already in place.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

6 Appendix M1 – Corporate Data Integrity Program

6.1 Introduction

Regulated companies should consider implementing a corporate data integrity program to identify, remediate, and manage potential risks to data integrity. This appendix is intended to provide regulated companies with a direction for creating a successful corporate data integrity program [19].

Regulated companies should ensure that they appropriately address record and data integrity and data governance. Organizational, procedural, and technical controls should also be considered as part of data governance. The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality assurance resource demands [1].

Key implementation considerations for a corporate data integrity program include development of a high-level strategy which:

- Includes a documented rationale
- Defines the executive sponsorship and governance process
- Focuses on management accountability
- Defines and implements tools for knowledge sharing
- Develops and provides the appropriate levels of training

The corporate data integrity program should address behavioral factors and drive a strategy that focuses on prevention, detection, and response.

Business processes, systems, equipment, and personnel continue to evolve and change. Corporate data integrity programs should include a plan for continuous improvement, which includes:

- Appropriate metrics to measure performance
- Program reporting to communicate progress
- Appropriate audit and assessment processes to identify issues and measure progress and ongoing compliance

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded on: 6/19/19 11:34 AM

6.2 Is a Corporate Data Integrity Program Required?

The MHRA GMP Data Integrity Definition and Guidance for Industry (March 2015) [1] discusses the need and importance of focusing on data integrity as part of a corporate program. It states that:

> *"Data Integrity is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality."*

The MHRA [1] goes on to state that:

> *"The data governance system should be integral to the pharmaceutical quality system ..."*

For individual use only. © Copyright ISPE 2017. All rights reserved.

These two statements reinforce the expectation that regulated companies should address data integrity and data governance in their QMS, because it is fundamental to ensuring product quality. The MHRA Guidance for Industry [1] further states that:

> *"The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality assurance resource demands."*

The emphasis is on designing and implementing a quality and data governance program that provides an acceptable state of control based on the risk to data integrity. Assessment activities can serve as a good basis for defining and establishing a corporate data integrity program strategy, as discussed in Section 6.4.

6.3 Indicators of Program Scope and Effort

In order to design and implement an appropriate corporate data integrity program, regulated companies should first understand their current state and acceptability of control based on risk to data integrity.

Data integrity and data governance should be an integral part of the QMS. Focusing on the organizational/procedural controls is an appropriate place to start.

Regulated companies should understand whether data integrity requirements are adequately addressed within the QMS.

Performing a review of the QMS versus data integrity requirements can identify where procedural controls may need to be addressed. Considerations include:

- Do adequate processes exist within the QMS to prevent, detect, report, and address data integrity failures?
- Are the ALCOA + requirements clearly addressed within the QMS?
- Are there adequately defined processes for generating and reviewing data?
- Are there adequate controls for the entire life cycle of data?

In a well-defined corporate QMS aligned with GxP regulations, most of these items should be addressed and traceable to the regulations applicable to the business processes; however, a more detailed gap assessment may be required to understand the state of data integrity controls in place at the local level. Organizational gaps are more likely to be identified as sites and local business areas define and execute their local procedures.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

The corporate and quality culture can impact the level of data integrity within a regulated company and should also be assessed and understood, e.g.:

- Is there appropriate knowledge and accountability for data integrity requirements and expectations at the operational level, as these are the personnel who typically generate and manage the data used to support product quality?

Management accountability, at all levels of the corporation, should play a key role in ensuring data integrity. Management should set an example and foster an environment that promotes and ensures good data integrity practices, including:

- Technical controls, which include equipment and computer systems, should be assessed to establish whether systems are adequately qualified and/or validated to ensure data integrity

For individual use only. © Copyright ISPE 2017. All rights reserved.

- System access and security should be defined and audit trails should be utilized to review, detect, report, and address data integrity issues
- Appropriate data life cycle management processes should ensure the integrity of the data throughout its required retention period
- A combination of technical and procedural controls should ensure segregation of duties to eliminate role conflicts that can raise concerns about data integrity, including:
  - Administrator access
  - Control and/ or elimination of shared accounts
  - Defined user roles with privileges assigned based on the user's roles and responsibilities

Organizational and technical controls should be implemented within the context of the product and business process. Understanding how these data integrity and QMS procedures and controls are executed and applied is considered a key indicator of the acceptability of the controls based on the risk to data integrity.

For further information on management roles and responsibilities. See Section 3.3.2.

6.3.1 Self-Assessment

A key QMS requirement is to have an auditing or self-assessment process to monitor adherence and compliance with the QMS and the regulatory requirements of the business.

A review of the self-assessment, internal audits, and third party audits reports and observations associated with these activities should provide a measure of the effectiveness of the data integrity controls. Reviews can help to:

- Identify data integrity issues
- Understand whether they are isolated, repeated, or part of a trend
- Understand whether there are any systemic corporate or quality culture issues

The self-assessment and audit processes should be designed to identify and address risks to data integrity and gaps in a timely manner. Self-assessment and audit processes should also be part of monitoring the overall success and effectiveness of the corporate data integrity program.

This Document is licensed to
Valrico, FL
Downloaded: 6/19/19 11:34 AM

6.3.2 Regulatory Inspection

Regulatory inspection findings can provide a measurement of the level of control of the risk to data integrity, especially if they were conducted by a regulatory agency which has implemented forensic data integrity inspection techniques.

Data integrity related observations issued for a given site are potential indicators of systemic issues that might exist at other sites within the regulated company. If it is found that similar issues exist at other sites within the regulated company, action plans addressing not addressing that issue in a timely manner could demonstrate a systemic issue and a potential corporate and quality culture issue.

For individual use only. © Copyright ISPE 2017. All rights reserved.

6.3.3 Effort and Resources

The level of effort and resources required should be considered when implementing a corporate data integrity program. The MHRA GMP Data Integrity Definition and Guidance for Industry (March 2015) [1] states that:

> *"The degree of effort and resource applied to the organisational and technical control of data lifecycle elements should be commensurate with its criticality in terms of impact to product quality attributes."*

These decisions depend on several factors:

1. The first factor is the outcome of gap assessments and audits of the organizational controls within the QMS. Significant gaps can require a greater effort to update the QMS with the appropriate controls to address those integrity risks. These updates may result in the creation of site and/or local procedures to functionally implement the controls and processes.

2. The second factor involves the outcome of the gap assessment and audits of the technical controls associated with equipment and computer systems. These could result in updates, reconfiguration, or even replacement of several systems, all of which should be qualified and/or validated. Depending on the extent of the changes to these systems, the amount of effort and resources will vary by project and/or system.

3. The third factor involves the gaps associated with business processes and execution of those processes. These are typically found by executing a detailed business process review and gap assessment with those individuals responsible for executing those processes. Business process changes may not be easy, especially when processes and approaches have been in place for a significant time. These types of changes can require both procedural changes and quality and business culture changes in order to implement them. The outcomes of these activities can serve as the basis for developing an initial data integrity strategy and defining the corporate data integrity program.

6.4 Implementation Considerations

A well-defined strategy can be the key to success of a corporate data integrity program. This high-level plan for executing the corporate data integrity program should define the approach, timeline, resource requirements, and rationale.

A strategy can:

- Serve as a mechanism to track progress for senior management
- Provide a documented rationale and plan to outline the program and actions during audits and inspections
- Demonstrate a commitment to identifying and addressing data integrity issues, and establishing a corporate governance process for overseeing these activities.
- Provide a mechanism to ensure multisite alignment of activities and a holistic approach to data integrity compliance

Corporate governance is considered critical to success. Executive sponsorship should be identified and established in order to obtain support for a corporate data integrity program.

This Document is licensed to
Valrico, FL
ID number: 1568
Downloaded: 6/6/2019 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

6.4.1 Sponsor

A sponsor is considered crucial to the overall success and will be required to:

- Set the direction
- Define the priorities
- Provide the resources
- Break down organizational barriers

The sponsor should help executives within a regulated company to be aware of the four key benefits that a corporate data integrity program can deliver including the:

1. Financial benefits
2. Reduction of risk
3. Regulatory benefits
4. Legal product liability impact

6.4.2 Management Accountability

Management accountability is considered critical to the success of a corporate data integrity program. When management leads by example, they demonstrate the core values of integrity in response to a failure. This can eliminate the fear of management retribution and foster an environment where employees are encouraged to identify and report data integrity issues. Management should provide the appropriate resources to ensure data integrity, including personnel, instruments and systems, and sound and understandable business processes. Management should acknowledge that some level of data integrity issues have and will occur.

Human factors contribute to data integrity issues, whether intentional or inadvertent. It is human nature to make mistakes and this should be recognized. Management should drive a strategy that focuses on prevention, detection, and response. However, to be successful, development of this strategy requires business process knowledge and ensuring those processes support data integrity requirements. Data integrity should be owned by the business and requires cross functional supervision and participation, including IT, Quality Unit, records management, etc.

6.4.3 Knowledge Sharing and Training

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/10 11:24 AM

Knowledge sharing and training are closely related. When a corporate data integrity program is rolled out, there are usually several questions and topics to address and share to help build a good data integrity foundation across the regulated company. These can include:

- What does data integrity mean and how does it apply to my day to day business activities?
- What role does equipment qualification and computerized system validation play in data integrity?
- How does data integrity relate to regulations such as 21 CFR Part 11 [2] and EU GMP Annex 11 [7]
- What are our roles and responsibilities versus those of the regulatory agencies?

For individual use only. © Copyright ISPE 2017. All rights reserved.

Making information readily available to all levels of an organization can be beneficial. Establishing a data integrity knowledge repository or knowledge base can provide historical and current information. Leveraging SMEs early in the process can provide a foundation of knowledge of data integrity to be established and used.

Data integrity should be an integral part of the business processes. This can provide a robust basis for implementing more focused training. Users of data should be formally trained to understand their:

- Role in maintaining data integrity
- Business processes and the information and the data they generate
- Responsibilities for identifying and escalating concerns regardless of the impact on delivery, quotas, or timelines

Quality and compliance roles should have advanced training and an understanding of data integrity requirements to ensure requirements are implemented within systems and processes, as well as support the business processes and business owners.

6.4.4 Behavioral Factors

Behaviors can promote and encourage the appropriate actions, or damage and discourage data integrity within a regulated company. For example:

- Damaging behavior – cost saving measures, which may require the sharing of passwords due to limited user license purchases
- Discouraging behavior – poorly conducted investigations that blame human error or end in no assignable cause

Three factors that support fraudulent practice are:

1. Pressure
2. Opportunity
3. Rationalization

Metrics that encourage any one of these factors can promote data integrity issues. For example, emphasis on speed versus accuracy and quality; this can force employees to cut corners and focus on the wrong things. Other behavioral factors include improvisation, impartiality, and falsification for profit.

Poorly chosen metrics can also undermine data integrity. See Section 3.3.4.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded on: 6/10/19 11:34 AM

6.5 Keys to Success

There is no single approach when it comes to implementing a corporate data integrity program; however, there are some elements that can increase the likelihood of success. Corporate data integrity program metrics should be defined and established to:

- Help to realize a positive return on investment. Whenever senior management invests time, money, and resources into a program, they expect there to be a return on that investment
- Measure the success of the corporate data integrity program and demonstrate progress against defined goals

For individual use only. © Copyright ISPE 2017. All rights reserved.

During the early stages of the corporate data integrity program, reporting of data integrity issues will increase with better awareness and improved detection, but may distort any metrics. An environment of open reporting should continue to be fostered, even if this distortion is considered as “bad news”. A reporting process can help to increase success.

The strategy for the corporate data integrity program should define the reporting expectations to senior management, area business leadership, the program team, as well as operational users. It can be an opportunity to share metrics and progress to date against the plan. It can also identify and communicate issues and provides a mechanism to agree on next steps.

Audit processes can be key to the success of a corporate data integrity program. Several types of audits should be performed, e.g.:

- Initial gap assessment or audit of nonconformance
- Periodic audit of long term data archives
- Supplier qualification audits
- Closeout gap assessment or full audit following program completion
- Ongoing internal quality audits of established data integrity controls to ensure continuing effectiveness and compliance

Audits can provide critical information to set a baseline and measure the success of implementation, as well as highlight possible gaps and possible corrections and additions to project scope. For the initial and closeout assessments, the use of an independent auditor should be considered, i.e., someone independent of the core team.

Robust review processes can be key to the success of a corporate data integrity program, including result review and periodic review processes. See Section 4.4, Appendix M4, and Appendix M5.

Review of individual results or sets of results prior to release should include the comparison of results against specification/limits/acceptance criteria. It should also include the evaluation of completeness and correctness of metadata. The review can provide a method to make a judgment about the accuracy and integrity of any manually entered values, as well as review any information associated with any decisions or actions taken.

Reviewers should assess and understand the impact that any manual adjustments or alterations to data or metadata might have on the results or product decision, as well as be aware of any changes to method versions used in creation of the result. Reviewers should also make an assessment of compliance to rigorous scientific practice and documented procedures. Increased result review rigor should be applied for manual adjustments and/or results that that are within, but close to, specification limits.

Carles J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

Audit trails should be reviewed. The MHRA GMP Data Integrity Definitions and Guidance for Industry (2015) [1] states that:

> *“Audit trail review should be part of the routine data review/ approval process, usually performed by the operational area which has generated the data (e.g. laboratory).”*

An audit trail can provide a method for assessing data integrity. Appropriate and accessible audit trails can provide a technical means of preventing and detecting data integrity issues, however:

- Audit trails may not be easily accessible and/or permanently associated with the result, making this review difficult to complete and the detection of data integrity issues difficult to achieve

For individual use only. © Copyright ISPE 2017. All rights reserved.

- The volume of results generated can present logical and resource challenges for review of associated audit trails and metadata

Regulated companies should consider planning for remediation or replacement of systems where audit trails are difficult to review.

6.5.1 Technology Controls

Technology controls can provide a method to review by exception. This approach applies a risk-based approach to data review, based on alerts to highlight a subset of results requiring additional review. For example, results and data that are within, but close to, the specification limit, and which have been:

1. Manually manipulated (i.e., integration of chromatograms)

2. Reprocessed

Technology controls can highlight situations where critical data has been manually entered or changed. A detailed review should be performed on a subset of the results/data.

Reviewers should understand that it is their responsibility to determine and document what the minimal level of result review is, and be able to provide a documented rationale for doing so during an audit or regulatory inspection.

These types of systems also require validation to verify and document the alert functionality.

6.5.2 Periodic Reviews

Computerized systems require periodic review to ensure they continue to operate in a manner consistent with their intended use and remain in a compliant and validated state consistent with that use. For further information see *ISPE GAMP® 5* [3].

From a data integrity perspective, periodic reviews should include the evaluation of any changes to system configuration that could impact data integrity. It should also focus on system administration activities and control, monitoring, and management of user accounts.

Other periodic review activities that should be addressed include checking that the:

- System validation records are current and reflect the intended use of the computerized system

- Change control process is functioning properly, to ensure that the risk to data integrity is being considered appropriately when changes are implemented.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

7 Appendix M2 – Data Integrity Maturity Model

This appendix describes an approach to assessing the maturity level of a regulated company in relation to data integrity. Maturity process areas are identified and maturity factors are described for aspects related to data integrity.

7.1 Maturity Model

Regulated companies should focus on modifying their processes and systems to use appropriate available technical controls, and evaluate systems for gaps prior to use.

Where feasible, regulated companies should design record and data integrity into their processes before purchasing systems and technology. Purchased systems should be able to be configured to provide adequate data integrity.

The data integrity maturity model[2] described is a simple representation of the regulated company. It is based on the status of key elements of processes needed for data integrity.

Regulated companies can use the data integrity maturity model to assess their current state of maturity, and understand actions and improvements required to reach the next maturity level.

The aim is to improve existing work practices, but not to define what those work practices should be for any given activity or regulated company. Maturity improvement activities should be performed to achieve improvement goals tied to quality, compliance, and business objectives, rather than a rating or level.

The maturity model may also be used as a rapid and efficient, but relatively detailed management indicator, enabling regulated companies to focus resources and effort effectively. This general approach is flexible and may be structured several ways, e.g., by geographical area, site, or department.

Figure 7.1 supports demonstrates a Red, Amber, and Green dashboard approach. See Section 3.3.4, which is at a higher level and more focused on key compliance risks.

This Document is licensed to

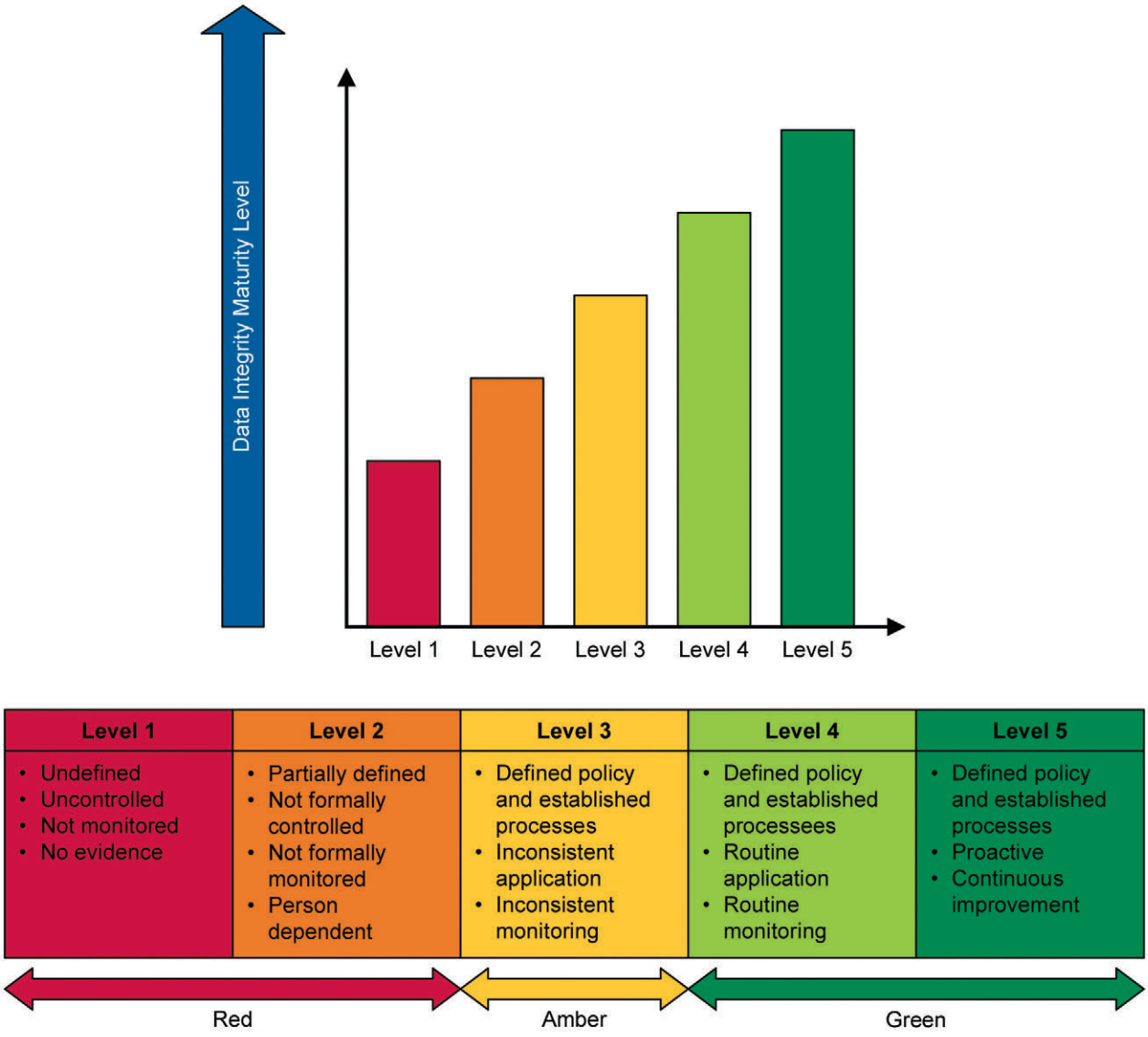
Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

[2] This model uses concepts and approaches similar to those of the Capability Maturity Model Integration (CMMI), but is not linked or affiliated.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 7.1: Data Integrity Maturity Model



Managing and reducing risk depends on the establishment of appropriate procedures and the application of appropriate behavioral, procedural, and technical controls.

Note: having a stated policy is not considered sufficient to reduce risk to an acceptable level.

Maturity levels are a continuum, rather than discrete levels or steps, so a regulated company may span more than one level for some areas. Regulated companies, or parts of regulated companies, may display characteristics of more than one maturity level.

Different sites, business areas, or departments within a regulated company may differ in data integrity maturity. For any assessment of maturity level, the scope should be well defined, to avoid confusion and inconsistent results.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/9/2017 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.1 can be used to help to determine a maturity level. The table describes the:

- Process areas that should be assessed
- Maturity factor that should be assessed for each area

Table 7.1: Maturity Factors

Process Area	Maturity Factors
Culture	
Data Integrity Understanding and Awareness	Awareness of the importance of data integrity and understanding of data integrity principles
Corporate Culture and Working Environment	A culture of willing and open reporting for errors, omissions, atypical results, and willing collaboration to achieve data integrity objectives
Quality Culture	An environment in which employees habitually follow quality standards, take quality focused actions, and consistently see others doing so
Governance and Organization	
Leadership	Objectives defined and communicated by executive management
Sponsorship	Executive management providing appropriate resources and support
Structure	Appropriate roles and reporting structures
Stakeholder Engagement	Engagement of business process owners, quality assurance, and key supporting technical groups (e.g., IT)
Data Ownership	Clear ownership of data and data related responsibilities
Policies and Standards	Defined polices and standards on data integrity
Procedures	Established procedures defining key activities and processes
Awareness and Training	Awareness and training on regulatory requirements and organizational polices and standards
Quality Management System	Established and effective QMS, focused on patient safety, product quality, and data integrity
Business Process Definition	Clear and accurate definitions of regulated business processes, covering all key GxP areas, including definition of data and data flows
Supplier and Service Provider Management	Assessment of suppliers and service providers against agreed standards, and setting up and monitoring of contracts and agreements to deliver those standards
Strategic Planning and Data Integrity Program	
Planning	Executive level strategic planning and programs for improving and/or maintaining data governance and data integrity
Communication	Communication and change management processes, supported by a suitable repository of information and resources.
Regulatory	
Awareness	Awareness of applicable regulatory requirements
Traceability	Traceability to applicable regulatory requirements from, e.g., quality manual, polices, or procedures

This Document is licensed to
Carlos I. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.1: Maturity Factors (continued)

Process Area	Maturity Factors
Regulatory (continued)	
Inspection Readiness	Preparation for inspection, including responsibilities and inspection readiness documentation
Regulatory Relationship and Communications	Effectiveness of communication with regulatory authorities and effectiveness of dealing with concerns and citations
Data Life Cycle	
Data Life Cycle Definition	Data life cycle(s) defined in standards and/or procedures
Quality Risk Management	Application of risk management (including justified and documented risk assessments) through the data life cycle
Data Management Processes and Tools	Established data management processes supported by appropriate tools
Master and Reference Data Management	Established processes to ensure the accuracy, consistency, and control of master and reference data
Data Incident and Problem Management	Established processes to deal with data incidents and problems, linked with change management and deviation management as appropriate
Access and Security Management	Establishing technical and procedural controls for access management and ensuring the security of regulated data and records
Archival and Retention	Establishing processes for ensuring accessibility, readability, and integrity of data in compliance with regulatory requirements including retention periods
Electronic Signatures	Effective application of electronic signatures to electronic records, where approval, verification, or other signing is required by applicable regulations
Audit Trail and Audit Trail Review	Usable and secure audit trails recording the creation, modification, or deletion of records and data, allowing effective audit trail review as part of normal business process, or during investigations or periodic review
Data Life Cycle Supporting Processes	
Data Auditing	Auditing against defined data quality standards, including appropriate techniques to identify data integrity failures
Self-inspection	Inspection against defined data quality standards, including appropriate techniques to identify data integrity failures
Metrics	Measuring the effectiveness of data governance and data integrity activities
Classification and Assessment	Data and system classification and compliance assessment activities
Computerized System Validation and Compliance	Established framework for achieving and maintaining validated and compliant computerized systems
Control Strategy	Proactive design and selection of controls aimed at avoiding failures and incidents, rather than depending on procedural controls aimed at detecting failure
IT Architecture	Appropriate IT architecture to support regulated business processes and data integrity
IT Infrastructure	Qualified and controlled IT infrastructure to support regulated computerized systems
IT Support	Documented service model defining responsibilities and the required level of support for regulated computerized systems

This Document is licensed to
Cassandra Schroer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/18 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

7.2 Data Integrity Maturity Level Characterization

Table 7.2 provides more detailed examples of possible, or typical, states related to maturity levels.

These examples are intended to be indicative only, and should be considered and interpreted within the specific context of individual regulated companies.

Table 7.2: Data Integrity Maturity Level Characterization

Maturity Area	Maturity Factors	Maturity Level Characterization				
		Level 1	Level 2	Level 3	Level 4	Level 5
Culture						
Data Integrity Understanding and Awareness	Awareness of the importance of data integrity and understanding of data integrity principles	Low awareness, limited to SMEs and specialists	General awareness of the topic, but not fully reflected in working practices	Principles reflected in working practices, but not consistently applied	Data integrity principles fully incorporated and applied in established processes and practices	Formal ongoing awareness program, proactively keeping abreast of industry developments
Corporate Culture and Working Environment	A culture of willing and open reporting for errors, omissions and atypical results, and willing collaboration to achieve data integrity objectives	Unwillingness or no motivation to report errors and atypical results	Data integrity problems may be reported but mitigation is either inadequate or ignored	Policies and procedures encourage openness, but not implemented in all cases. Mitigation generally limited to the specific instance	Full openness and collaboration achieved through such behavior being motivated by management behavior. Mitigation considers wider implication	Anticipating potential future data integrity weaknesses and applying appropriate controls
Quality Culture	An environment in which employees habitually follow quality standards, take quality focused actions, and consistently see others doing so	Low awareness and application of quality principles and standards. A culture of not reporting what management would rather not hear	Ad hoc quality. Activities performed, but relying on individual efforts	General application of some quality principles, but not fully ingrained or consistent	Quality considerations incorporated in normal working practice	Quality and continuous improvement incorporated in normal working practice
Governance and Organization						
Leadership	Objectives defined and communicated by executive management	Leadership silent or inconsistent on the need for data integrity. Other business priorities typically override	Leadership state need for DI, but do not lead by example	Objectives defined in policies and high level statements, but not always fully reflected in management priorities	Management actions and priorities fully reflect stated objectives	Data integrity aspects routinely addressed and improved as part of management review
Sponsorship	Executive management providing appropriate resources and support	Appropriate resources only made available in emergencies (e.g., critical citation)	Appropriate resources available in principle, but often not be available in practice due to other pressures	Appropriate resources available, but may be diverted or diluted due to other pressures	Required and planned resources are available and safeguarded due to ongoing commitment to data integrity	Management looking ahead to identify future resource needs, based on experience

This Document is licensed to
Carlos J. Cabrera
Verica, FL
Downloaded on: 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.2: Data Integrity Maturity Level Characterization (continued)

Maturity Area	Maturity Factors	Maturity Level Characterization				
		Level 1	Level 2	Level 3	Level 4	Level 5
Governance and Organization (continued)						
Structure	Appropriate roles and reporting structures	No consideration of specific data governance in roles and responsibilities	Data governance roles only recently established or in flux	Data governance roles established but not always effective	Data governance roles are well integrated into the management structures and systems	Management reviewing and adapting organizational structures based on experience
Stakeholder Engagement	Engagement of business process owners, quality assurance, and key supporting technical groups (e.g., IT)	Data integrity and governance seen as either an IT issue or a quality issue. No real process owner involvement	Ad hoc involvement of Ppocess owners and quality assurance. High person dependence	Process owners, and quality assurance typically involved, but not consistently	Process owners, quality assurance, and IT work together through the data and system life cycles	All stakeholders consistently work together to identify further cooperation opportunities, based on experience
Data Ownership	Clear ownership of data and data related responsibilities	Process, system, and data owners not defined	Process, system, and data owners identified in few areas	Process, system, and data owners typically defined in many, but not all cases, and responsibilities not always clear	Process, system, and data owners are well defined and documented	Process, system, and data owner responsibilities considered and clarified during management review
Policies and Standards	Defined polices and standards on data integrity	No established policies and standards for data integrity	Ad hoc policies and standards for data integrity in some cases	Polices and standards exist but not fully integrated into the QMS and business process	Policies and standards fully integrated into the QMS and fully reflected in business processes and practices	Policies and standards regularly reviewed and improved based on experience
Procedures	Established procedures defining key activities and processes	No established procedures for key data integrity related activities	Ad hoc procedures for data integrity in some cases	Some procedures and standards exist but not covering all data integrity related activities	Procedures for all key areas fully integrated into the QMS and reflecting established policies and standards	Procedures regularly reviewed and improved based on experience
Awareness and Training	Awareness and training on regulatory requirements and organizational polices and standards	No real awareness of regulatory requirements and company policy in this area	Some awareness of regulatory requirements and company policy, in pockets	General awareness of well-known regulations, and the existence of company policies	Comprehensive training program ensures an appropriate level of knowledge of specific regulatory and company requirements	Formal training needs analysis, taking into account regulatory developments. Training effectiveness assessment for ongoing improvement
Quality Management System	Established and effective QMS focused on patient safety, product quality, and data integrity	Few procedures in place focused on patient safety, product quality, and data integrity	Some procedures and quality control processes, but not consistently achieving quality goals	Established QMS, but compliance and data integrity activities are not fully effective	Established and effective QMS, consistently achieving data integrity goals in support of patient safety and product quality	QMS subject to regular management review and continuous improvement

This Document is licensed to
Carlos J. Cabrel
Valrico, FL
ID number: 1568
Downloaded: 2019-03-04 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.2: Data Integrity Maturity Level Characterization (continued)

Maturity Area	Maturity Factors	Maturity Level Characterization				
		Level 1	Level 2	Level 3	Level 4	Level 5
Governance and Organization (continued)						
Business Process Definition	Clear and accurate definitions of regulated business processes, covering all key GxP areas, including definition of data and data flows	Few business processes and associated data formally defined and documented	Some business processes and data formally defined and documented on an ad hoc basis, either by project or operational groups	Most business processes and data defined, but not consistently following conventions or standards, and not always complete and up to date	Business processes and data defined following established conventions and standards	Business processes and data defined and supported by appropriate tools, and consistently maintained
Supplier and Service Provider Management	Assessment of suppliers and service providers against agreed standards, and setting up and monitoring of contracts and agreements to deliver those standards	Many suppliers and providers with a potential impact on data integrity not assessed or managed	Some suppliers and providers with a potential impact on data integrity informally assessed	Established process for supplier management, but not applied consistently. Data integrity implications not always fully covered by assessments or agreements	Established process for supplier management, consistently applied, and including a data integrity risk review	Effectiveness of supplier management subject to regular management review based on metrics
Strategic Planning and Data Integrity Program						
Planning	Executive level strategic planning and programs for improving and/or maintaining data governance and data integrity	No planning for data integrity or data governance at executive level	Limited planning for data integrity or data governance, typically driven by emergencies	Specific corporate data integrity program or equivalent underway	Successful data integrity programs achieving stated objectives	Data integrity integral to ongoing organizational strategic planning
Communication	Communication and change management processes, supported by a suitable repository of information and resources	No communication and change management process for data integrity	Some informal and person dependent communication and change management.	Formal communication and change management for data integrity in place, but on a per-project or per-site basis, with ad hoc repositories	Communication and change management for data integrity integral to QMS, supported by tools and central repository	Communication and change management for data integrity subject to review and improvement, supported by defined metrics
Regulatory						
Awareness	Awareness of applicable regulatory requirements	No awareness of key regulatory requirements	Some awareness of detailed regulatory requirements, based on individual experience and effort	Formal regulatory awareness raising underway, including training on regulations and guidance	All staff aware of regulatory requirements affecting their work	Formal training needs analysis and action, taking into account regulatory and industry developments
Traceability	Traceability to applicable regulatory requirements from, e.g., quality manual, polices, or procedures	No traceability to regulations	Little traceability of policies and procedures to specific regulations	Traceability in place but limited to key regulatory requirements	Full traceability, e.g., from quality manual or policies, to specific regulatory requirements	Traceability effectively maintained and updated taking into account regulatory developments

This Document is licensed to
Carlos J. Cabrera
Valrico, FL
ID number: 1568

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.2: Data Integrity Maturity Level Characterization (continued)

Maturity Area	Maturity Factors	Maturity Level Characterization				
		Level 1	Level 2	Level 3	Level 4	Level 5
Regulatory (continued)						
Inspection Readiness	Preparation for inspection, including responsibilities, and inspection readiness documentation	No inspection readiness preparation	Limited inspection readiness preparation ad hoc and dependent on individual process and system owners	Inspection readiness activities in place, but inconsistent in level, content, and approach	Established process for inspection readiness covering all systems maintaining regulated data and records	Inspection readiness processes regularly reviewed and refined based on regulatory and industry developments
Regulatory Relationship and Communications	Effectiveness of communication with regulatory authorities, and effectiveness of dealing with concerns and citations	No communication except during inspections when specific citations are addressed	Ad hoc, informal communication as and when required, not following a defined procedure	Communication as and when required, following a defined procedure	Effective, consistent communication with regulatory bodies following a defined procedure	Clear communication lines to key regulatory bodies, with internal specialists following an established process. Concerns and citations are proactively managed.
Data Life Cycle						
Data Life Cycle Definition	Data life cycle(s) defined in standards and/or procedures	Data life cycles not defined	Some data life cycles defined on an ad hoc basis	Data life cycles generally defined following procedures. Not consistently applied.	Data life cycle defined in procedures, and applied consistently to all key regulated data and records	Data life cycles defined and maintained, supported by effective automated tools
Quality Risk Management	Application of risk management (including justified and documented risk assessments) through the data life cycle	No documented and justified assessment of risks to data integrity	Limited data integrity risk assessments performed on an ad hoc basis.	Data integrity considered in risk assessment procedures, but not performed to a consistent level	Data integrity risk management established as an integral part of the data life cycle and system life cycle	Quality Risk Management activities subject to continuous improvement.
Data Management Processes and Tools	Established data management processes supported by appropriate tools	No data management processes	Some data management processes defined by individual process owners	Data management procedures defined, but not always effectively implemented	Well established and effective data management processes	Well established common data management processes, maintained, updated, supported by appropriate automated tools
Master and Reference Data Management	Established processes to ensure the accuracy, consistency, and control of master and reference data	No master/ reference data management processes	Some master/ reference data management processes defined by individual process owners	Master/ reference data management procedures defined but not always effectively implemented	Well established and effective master/ reference data management processes	Well established common master/ reference data management processes, maintained, updated, supported by appropriate automated tools

This Document is licensed to
Carlos J. Cabrel
Valrico, FL
ID number: 1568
Downloaded on: 04/19/19 8:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.2: Data Integrity Maturity Level Characterization (continued)

Maturity Area	Maturity Factors	Maturity Level Characterization				
		Level 1	Level 2	Level 3	Level 4	Level 5
Data Life Cycle (continued)						
Data Incident and Problem Management	Established processes to deal with data incidents and problems, linked with change management and deviation management as appropriate	No formal data incident and data problem management process	Some data incident and data problem management processes defined by individual process/system owners	Data incidents and problems typically effectively dealt with as a part of normal system or operational incident management, but with limited consideration of wider data integrity implications	Established data incident and problem management process linked to CAPA and deviation management where necessary	Established data incident and problem management process, supported by tools and appropriate metrics, leading to process improvement
Access and Security Management	Establishing technical and procedural controls for access management and to ensure the security of regulated data and records	Lack of basic access control and security measures allowing unauthorized changes	Some controls, but group logins and shared accounts widespread. Password polices weak or not enforced	Established standards and procedures for security and access control, but not consistently applied	Established system for consistent access control and security management, including regular review of security breaches and incidents	Established integrated system for consistent access control and security management, supported by appropriate tools and metrics for continuous improvement
Archival and Retention	Establishing processes for ensuring accessibility, readability, and integrity of regulated data in compliance with regulatory requirements including retention periods	No consideration of long term archival and retention periods	No effective process for identifying and meeting regulatory retention requirements. Few archival arrangements in place	Retention policy and schedule defined covering some, but not all regulated records. Some systems with no formal archival process	Retention schedule includes all regulated records, and those policies supported by appropriate archival processes and tools	Archival and data retention policies and processes regularly reviewed against regulatory and technical developments
Electronic Signatures	Effective application of electronic signatures to electronic records, where approval, verification, or other signing is required by applicable regulations	No control of electronic signatures	Lack of clear policy on signature application, and lack of consistent technical support for e-signatures	Policies in place. Compliant e-signatures in place for some, but not all relevant systems	Compliant e-signatures in place for all relevant systems, supported by consistent technology where possible	Electronic signature policies and processes regularly reviewed against current best practice and technical developments
Audit Trail and Audit Trail Review	Usable and secure audit trails recording the creation, modification, or deletion of data and records, allowing effective review either as part of normal business process or during investigations	Lack of effective and compliant audit trails	Some limited use of audit trails. Often incomplete or not fit for purpose (e.g., in content and reviewability). Not typically reviewed as part of normal business process	Audit trail in place for most regulated systems, but with undefined and inconsistent use within business processes in some cases	Effective audit trail in place for all regulated systems, and use and review of audit trail included in established business processes	Audit trail policies and use regularly reviewed against regulatory and technical developments

This Document is licensed to Carlos J. Cabrer Varela, A ID number: 1568 Downloaded on: [illegible]

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.2: Data Integrity Maturity Level Characterization (continued)

Maturity Area	Maturity Factors	Maturity Level Characterization				
		Level 1	Level 2	Level 3	Level 4	Level 5
Data Life Cycle Supporting Processes (continued)						
Auditing	Auditing against defined data quality standards, including appropriate techniques to identify data integrity failures	No data quality or integrity audits performed	Some audits performed on an ad hoc and reactive basis, but no established process for data quality and integrity auditing	Data quality and integrity process defined, but audits not always effective and the level of follow up inconsistent	Effective data auditing fully integrated into wider audit process and schedule	Auditing process and schedule subject to review and improvement, based on audit results and trends
Self-inspection	Inspection against defined data quality standards, including appropriate techniques to identify data integrity failures	No data quality or integrity self-inspection performed	Some self-inspections performed on an ad hoc and reactive basis, but no established process for data quality and integrity auditing	Data quality and integrity process defined, but self-inspections not always effective and the level of follow-up inconsistent.	Effective data self-inspections fully integrated into wider business processes	Self-inspection process subject to review and improvement, based on results and trends
Metrics	Measuring the effectiveness of data governance and data integrity activities	No data related metrics captured	Limited metrics captured, on an ad hoc basis	Metrics captured for most key systems and datasets. Level, purpose, and use inconsistent	Metrics captured consistently, according to an established process	Metrics captured consistently, and fed into a continuous improvement process for data governance and integrity
Classification and Assessment	Data and system classification and compliance assessment activities	No data classification	Limited data classification, on an ad hoc basis. No formal process	Data classification performed (e.g., as a part of system compliance assessment), but limited in detail and scope	Established process for data classification, based on business process definitions and regulatory requirements	Classification process subject to review and improvement, based outcomes and trends
Computer System Validation and Compliance	Established framework for achieving and maintaining validated and compliant computerized systems	Systems supporting or maintaining regulated records and data are not validated	No formal process for computerized system validation. The extent of validation and evidence dependent on local individuals	Most systems supporting or maintaining regulated records and data are validated according to a defined process, but approach is not always consistent between systems and does not fully cover data integrity risks	Established process in place for ensuring that all systems supporting and maintaining regulated records and data are validated according to industry good practice, and fully compliant with regulations, including effective and documented management of data integrity risks	Computerized system validation policies and processes regularly reviewed against regulatory and industry developments

This Document is Licensed to
Carlos J. Herrera
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 7.2: Data Integrity Maturity Level Characterization (continued)

Maturity Area	Maturity Factors	Maturity Level Characterization				
		Level 1	Level 2	Level 3	Level 4	Level 5
Data Life Cycle Supporting Processes (continued)						
Control Strategy	Proactive design and selection of controls aimed at avoiding failures and incidents, rather than depending on procedural controls aimed at detecting failure	No consideration of potential causes of data integrity failures and relevant controls	Some application of controls, typically procedural approaches aimed at detecting failures	Technical and procedural controls applied, but dependent on individual project or system	Technical and procedural controls are applied in most cases, based on an established risk-based decision process	Integrity fully designed into processes before purchase of systems and technology, including appropriate controls
IT Architecture	Appropriate IT architecture to support regulated business processes and data integrity	No consideration of IT architecture strategy	IT architecture strategy and decisions not documented, and dependent on local SMEs	IT architecture considered, and generally supports data integrity and compliance, but is typically defined on a system by system basis	Established IT architecture policy and strategy, with full consideration on how this supports data integrity	IT architecture strategy regularly reviewed against industry and technical developments
IT Infrastructure	Qualified and controlled IT infrastructure to support regulated computerized systems	No infrastructure qualification performed	No established process for infrastructure qualification. Some performed, dependent on local SMEs.	Infrastructure generally qualified, according to an established process, but is often a document driven approach, sometimes applied inconsistently	Established risk-based infrastructure qualification process, ensuring that current good IT practice is applied, supported by tools and technology	Infrastructure approach regularly reviewed against industry and technical developments.
IT Support	Documented service model defining responsibilities and the required level of support for regulated computerized systems	No consideration of what support is required with no individual responsible	No defined model. Support dependent on experienced individuals	Service level model is established per system, but with evidence of inconsistent application, measurement and reporting	Risk-based service level model consistently applied across systems, with evidence of measurement and reporting	Service level model regularly reviewed and refined based on performance against targets, specific concerns and trends

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

8 Appendix M3 – Human Factors

8.1 Introduction

Consideration of various human factors is considered critical for effective data integrity. Consideration should be given to:

- Understanding and mitigating the impact of corporate and local cultures
- Understanding the classification and underlying root cause of incidents (from minor lapses to fraud)
- Implementing mechanisms to minimize human error rates
- Reducing motivation, pressures, and opportunities for data falsification and fraud
- Promoting impartiality in quality related decision making
- Applying effective behavioral controls – influencing behaviors and attitudes

8.2 Corporate and Local Cultures

Cultural considerations can refer to a corporate culture, i.e., the model within which an organization operates, or to a local geographic culture, i.e., the moral and behavioral norm within a country or region.

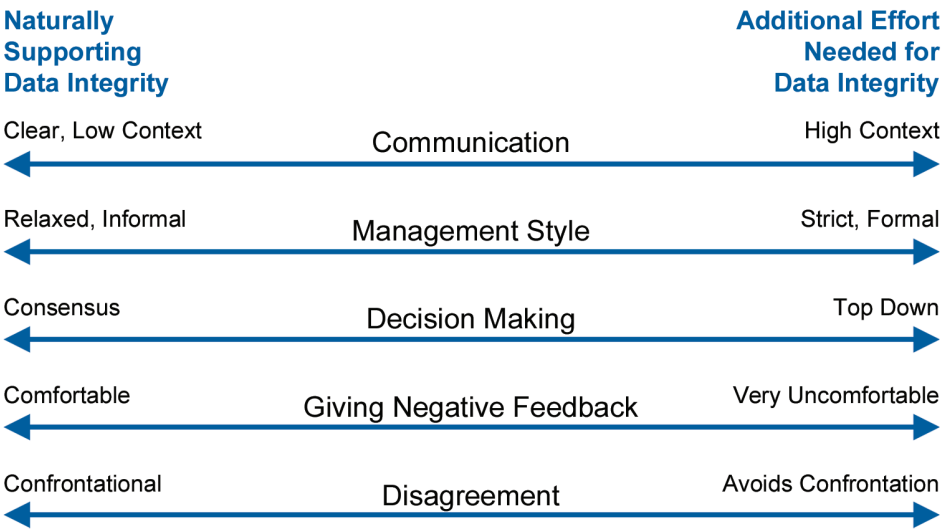
8.2.1 Corporate Culture

Corporate culture can vary widely from a family owned private company to a publicly traded corporation; however, from a regulatory perspective, the expectation for data integrity and product quality is the same.

8.2.2 Local Geographic Culture

Geographic culture can have a significant impact on site operations. One system of classification for cultures works on a scale of key behavioral attributes (Meyer, 2014) [20].

Figure 8.1: Effects of Different Cultural Types



For individual use only. © Copyright ISPE 2017. All rights reserved.

Openness and a willingness to discuss difficult situations can support an environment where failing results are seen as a group problem to be resolved, with clearly documented corrective actions that mitigate the manufacturing or other root cause.

Management should help employees to achieve the openness around data integrity that is needed for compliance; significant additional effort will be needed within the cultural types possessing behavioral norms that are naturally less inclined to openness, e.g., those with highly formal management structures combined with an aversion to negative feedback and confrontation.

8.2.3 Cultural Differences

Differences in corporate culture can lead to difficulties in working. For example, suppliers should allow sufficient time for an extended approval process for a customer that is a regulated company.

Working across different geographic cultures can create issues and misunderstandings, e.g., cultures may vary in the way they communicate:

- US, Canadian, and Australian cultures: instinctively based around low-context communication, where the key message is laid out simplistically, assuming very few shared reference points
- China and Japan: using high-context communication that relies on implicit knowledge to fill in the context between the verbal or written phrases and may be based more on body language and linguistic nuance than on clear statements

High-context communication across different nationalities may:

- Give rise to significant misunderstandings during collaborations
- Make written communication more prone to misinterpretation

8.3 Classification of Incidents

Figure 8.2 provides a useful classification of incidents affecting data integrity [21]. The approach taken to mitigate different types of incidents should consider changes to governance, management systems, and behaviors. If there have been multiple incidents, then root cause investigation should be performed in addition to taking specific actions for individual incidents.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 8.2: Classification of Incidents

Slips and Lapses	Mistakes	Situational Violation	Routine Violation	Optimizing Violation	Intentionally Misleading
Slips and momentary lapses of concentration can be treated as one-off incidents if there is no pattern. **Example:** Jumping over and forgetting to complete a single manual data-cell entry concerning supplementary information in a batch record spreadsheet.	***Mistakes*** are often associated with areas of insufficient control or too much complexity. **Example:** Excessively long reference codes that when hand-typed lead to errors.	***Situational violations*** occur when an individual reacts in an inappropriate manner to an unexpected situation. **Example:** In a rush to get crashed systems up and running again after a storm an operator deletes a record of analytical sample run that was corrupted by an electrical surge.	***Routine violations*** involved repeated inappropriate practices that became the norm and are often based on a premise that they were inconsequential. **Example:** In effective change control leads to modification of an analytical method that was appropriate for one product but not for another product sharing the same method.	***Optimizing violations*** concerned ways of working apparently introduced to avoid a control and/or evade triggering associated additional workload. **Example:** Change system configuration to hide sampling errors and thereby avoid raising deviations.	***Intentional misleading*** actions cover unauthorized manipulation of data and fraud. **Example:** Inserting "pass" values into a laboratory database when individual test results were out of registered specification.

8.4 Human Error

Data integrity issues often arise from genuine human error, however regulators do not distinguish between human error and data falsification when assessing the impact of a data integrity failure. Any data integrity failure can potentially impact patient safety and/or product quality and, therefore, efforts should be made to minimize human error.

Human error may be indicative of failures in systems and processes within a regulated company [22]. The root cause of failures may be a combination of failures involving several personnel and across several processes. When transparent, open investigations are performed to determine the true root cause of failures and followed up with effective solutions, the incidence of human error can be reduced.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

Monitoring of human error rates can provide an indicator of the regulated company's error culture. Consistently high incidences of error changing little over time could show that mistakes are accepted as inevitable, with no effort made to improve working practices.

Effective mechanisms to reduce human error rates include:

1. Using personnel less: humans are considered naturally poor at manual data entry and, therefore, this should be avoided by implementing direct interfacing of equipment and automated transfer of data.

2. Using personnel only for their strengths: humans are considered highly effective at monitoring multiple systems simultaneously; however, it would require a complex computerized system to achieve the same monitoring function.

3. Limit the opportunity for human error, e.g., by using drop down lists in place of free text entry so that searching for a specific product name will not fail because of a spelling error.

For individual use only. © Copyright ISPE 2017. All rights reserved.

8.5 Data Falsification and Fraud

8.5.1 Falsification for Profit

Personal gain or self-interest has been the motivator in several high-profile fraud cases. Commonplace fraudulent activities include:

- Unofficial testing to see if a sample will pass before running the "official" sample for the batch record
- Concealing, destroying, or overwriting original data and samples
- Re-naming or misrepresenting results from a passing batch in support of other batches
- Manually manipulating chromatography integrations to alter the result.

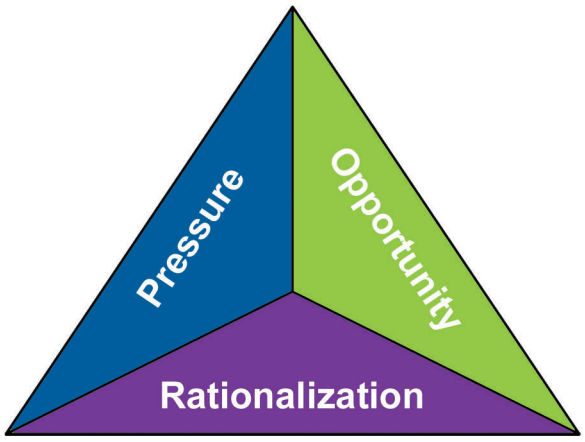
Administrative and technical controls can be used to reduce the opportunities for falsification.

The extent and impact of falsification can be magnified if collusion is involved. Geographic and corporate cultures can influence the degree to which collusion may be prevented; strongly hierarchical cultures may be more susceptible to collusion as these cultures inherently discourage any disagreement with authority figures.

8.5.2 Reducing Fraud

A framework for understanding how an individual comes to commit fraud is the Fraud Triangle [23]:

Figure 8.3: Fraud Triangle



Opportunity potentially comes from:

- Weak system controls
- No restriction on data deletion
- Accessible hard drive
- Using paper records for complex data (potentially missing key dynamic data)
- Lack of effective review processes

t is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

- No audit trail review
- Approval based on reviewing the paper report only

Robust technical controls within all of the data generation, collection, processing, or storage systems, coupled with effective data review processes can, therefore, reduce the opportunities for fraud.
Pressure can be managed and mitigated by ensuring that workplace targets are achievable with the equipment and resources that have been provided, and that any metrics monitored focus on data integrity and overall product quality rather than throughput or pass rates.

A corporate culture of openness and honesty at all levels, with management appreciation and other employee incentives for highlighting quality issues and concerns, is considered essential to prevent any rationalization that falsifying data can ever be in either the individual's or company's best interests.

8.6 Impartiality

The WHO Annex 5: Guidance on Good Data and Record Management Practices [12] states that:

> *"Elements of effective management governance should include: … assurance that personnel are not subject to commercial, political, financial and other organizational pressures or incentives that may adversely affect the quality and integrity of their work;"*

For example, a QC laboratory supervisor should report through the independent Quality Assurance department.

8.7 Behavioral Controls

The interaction of soft skills needed to guide people's behavior and responses should be considered as a way to assist supporting data integrity.

8.7.1 Understanding Effective Controls

Effective data integrity controls include those that:

- Do not solely rely on people's actions
- Are built in
- Are easy to comply with
- Are well communicated and understood
- Management will support and enforce
- Have backups/contingencies
- Make errors/failures clearly visible
- Fail over to a safety condition
- Focus on resolving problems rather than taking punitive action

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

8.7.2 Corporate Data Integrity Training Program

A corporate data integrity training program should address behavioral factors and drive a strategy that focuses on reducing the risk to data integrity. Training can assist in providing personnel with the:

- Knowledge and understanding of what data integrity is
- Importance data integrity has for a regulated company
- Personal role each employee has in relation to data integrity

Data integrity training should be implemented at all levels of the corporation in order to have a positive effect on a regulated company's quality culture. Management should set an example and foster an environment that promotes and ensures a "speak up"/"quality first" culture.

Training should also include practices that support good data governance. For example, establishment of multisite standards for management of supporting data (metadata) that allows analytics that span the entire regulated company.

A corporate data integrity training program should be both general and specific. It should target the correct audiences and should consider the specific scale of the regulated company.

In a large regulated company, high level training for all employees might be at a foundational level, but the content and focus of additional training may vary significantly for different functions, e.g., the consequences of a data integrity issue will differ significantly for a line operator compared to the operations director. This training approach might be ineffective, however, for a small regulated company where both the foundational and detailed training might be more effectively rolled out simultaneously.

At the operator level, data integrity should be inherent within the process and should not be compromised to meet delivery timelines.

Users of data should be formally trained to understand their role in maintaining the integrity of the data they handle. They are normally responsible for highlighting and escalating any concerns about data and quality irrespective of the impact on production quota or deadlines. Training provided to personnel creating or using regulated data users of data should ensure:

- Understanding of data integrity
- Understanding of data life cycles
- Emphasize good data management
- Emphasize good documentation practices

Data stewards or personnel with QA responsibilities should be given additional training to allow a deeper understanding of technical expectations and requirements, inspection and auditing techniques, and process governance

It is a regulatory expectation that the data life cycle is understood throughout the regulated company's processes and systems. Personnel in roles that own processes and systems should be aware of their role and responsibility in maintaining data integrity, e.g.:

- Understanding how and where data is used, and its impact on product quality and patient safety

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded on: 6/10/10 11:24 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Knowing what other review processes and data stewards are involved in the data life cycle, particularly those downstream of the system

- Indepth knowledge of the system functionality with potential impact on data integrity, and how to detect such activity

Training on the general principles of data integrity could be complemented by more detailed, contextual training appropriate for data stewards who have a direct role in data handling. The specific training provided to such persons (including quality and compliance personnel) must extend past the general requirements and definitions of data integrity. This role-based training should focus on critical thinking, auditing techniques, and could include specific use cases related to the roles. For example, data integrity training for laboratory auditors and process owners might include a comprehensive review of US FDA warning letters that describe data integrity observations in laboratory settings, and practical exercises around examining audit trails. See Appendix M4.

8.7.3 Improvisation

Improvisation is the ability to work around a lack of people, absent, or damaged equipment, and even lack of training, to “get the job done, somehow”. Improvisation can be widespread where insufficient or inappropriate resources are commonplace. SOPs or other controls may not be followed within a culture of improvisation.

The integrity of any data produced by improvisation should be considered as questionable.

Improvisation as a working practice should be discouraged. Management should remove the drivers for improvisation by:

- Providing sufficient competent people to complete assigned tasks (e.g., overworked personnel may feel pressured to maximize yield or productivity at the expense of data integrity)

- Providing sound, reliable equipment and instrumentation for the production and quality personnel to achieve the expected throughput (e.g., outdated equipment may not provide the technical controls for data integrity nor produce accurate data. Frequent equipment downtime can increase pressure on personnel to seek alternative ways keep up with their workload)

- Maintaining the facilities and operating environment in a fit state for their intended purpose (e.g., lack of physical security and poor IT infrastructure can jeopardize data integrity, e.g., by allowing unauthorized access to a server room, or by losing data from a local hard drive in a laboratory)

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

9 Appendix M4 – Data Audit Trail and Audit Trail Review

9.1 Introduction

This appendix describes a risk-based approach to data audit trails and audit trail review for GxP regulated computerized systems. It places audit trails in the wider context of information security, and suggests a practical approach for audit trails and audit trail review within that wider framework. It outlines the current regulatory requirements for audit trails, as defined in EU GMP Annex 11 [7], 21 CFR Part 11 [2], and associated guidance.

Audit trails should be specified, implemented, and controlled. Audit trails can be useful in supporting routine inprocess reviews of critical electronic records, and as investigative tools. For example, in chromatography systems audit trails can show changes to methods associated with reprocessed results, therefore, helping a reviewer to identify instances of testing (or processing) into compliance.

Reviews should be performed of audit trail content that has direct impact on reported values that will be used for product or patient decisions. General routine, historical, retrospective, non-targeted reviews of audit trail content should be avoided and can use significant resources and may not discover atypical data.

Examining audit trails for a specific set of records as part of an inprocess review, or during an investigation where data integrity has been determined to be uncertain can help to determine the integrity of the records in question.

There are three main types of data audit trail review:

1. Review of data audit trails as part of normal operational data review and verification
2. Review of audit trails for a specific data set during an investigation (e.g., of deviations or data discrepancies)
3. Review and verification of effective audit trail functionality (e.g., verification of audit trail configuration as part of periodic review)

Holistic and risk management based decisions on the need for audit trails and the review of audit trails should be based upon:

- A detailed understanding of the process supported by the computerized system
- Applicable GxP requirements
- The risk to patient safety, product quality, and data integrity

Data audit trails normally record the creation, modification, or deletion of records and data.

Technical system logs normally record various system, configuration, and operational events.

Technical system logs should not be regarded as equivalent to data audit trails. This distinction is consistent with existing regulations and normal IT good practice and terminology.

Where systems lack appropriate audit trails, alternative arrangements to verify the accuracy of data should be implemented, e.g., administrative procedures, secondary checks, and controls.

Technical system logs may be helpful, e.g., in case of investigations or in the absence of true audit trails.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

9.2 Regulatory Background

The MHRA GMP Data Integrity Definitions and Guidance for Industry (2015) [1], states that:

> *"Where computerised systems are used to capture, process, report or store raw data electronically, system design should always provide for the retention of full audit trails to show all changes to the data while retaining previous and original data. It should be possible to associate all changes to data with the persons making those changes, and changes should be time stamped and a reason given. Users should not have the ability to amend or switch off the audit trail.*
>
> *The relevance of data retained in audit trails should be considered by the company to permit robust data review/verification. The items included in audit trail should be those of relevance to permit reconstruction of the process or activity. It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.), and may be achieved by review of designed and validated system reports.*
>
> *Audit trail review should be part of the routine data review/approval process, usually performed by the operational area which has generated the data (e.g. laboratory). There should be evidence available to confirm that review of the relevant audit trails have taken place. When designing a system for review of audit trails, this may be limited to those with GMP relevance (e.g. relating to data creation, processing, modification and deletion etc). Audit trails may be reviewed as a list of relevant data, or by a validated 'exception reporting' process. QA should also review a sample of relevant audit trails, raw data and metadata as part of self inspection to ensure on-going compliance with the data governance policy/procedures."*

US FDA 21 CFR Part 11 [2], in Section 11.10 (e), requires:

> *"Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying."*

Note: this requirement specifically covers operator entries and actions that create, modify, or delete regulated electronic records, but not all activities performed by users, and not all system actions.

In the FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application [16], FDA clarifies their expectations and interpretation:

> *"We recommend that you base your decision on whether to apply audit trails, or other appropriate measures, on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on product quality and safety and record integrity. We suggest that you apply appropriate controls based on such an assessment. Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operation."*

The guidance clarifies that when applying time stamps (such as in audit trails), they should be implemented with a clear understanding of the time zone reference used. In such instances, system documentation should explain time zone references as well as zone acronyms or other naming conventions.

The guidance also notes that audit trails may be just one among various physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the records, within the context of a wider information security management framework.

This Document is Licensed to
Carlos J. Cabrer
Valkaria, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

EU GMP Annex 11, as revised in 2011, [7] includes the following clause (with a focus on GMP relevant data changes or deletions):

> *"Audit Trails*
> *Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed."*

EU GMP Annex 11[7] also requires electronic systems to record the identity of the person creating an electronic record along with the date and time. This is required even when there is no audit trail. EU GMP Annex 11 [7] requires that risk management is applied throughout the life cycle of a computerized system, which supports a review by exception approach provided that the audit trail of the application supports identification of changed records easily and that this function has been validated.

Some technical and system logs may be used in support of compliance and investigations, especially in the absence of true audit trails; however, these are not intended to be audit trails in the sense that 21 CFR Part 11 [2] and EU GMP Annex 11 [7] require and considering them as such may increase compliance risk.

9.3 Application and Use of Audit Trails

GxP regulations require traceability of creation, modification, or deletion of regulated records and data.

In a traditional paper based system, GxP requirements would typically be implemented as follows:

- If a user recognizes that a specific data entry is wrong, they strike out the wrong data in a way that it is still readable and put the correct value next to it with their initials, the date, and in some cases the reason

For further information see the applicable requirements for good documentation practice in EU GMP Chapter 4 [6].

In an electronic system, an audit trail is designed to provide equivalent traceability.

The need for, and the type and extent of, audit trails should be based on a documented and justified risk assessment. Specific GxP requirements requiring audit trails may also apply. An audit trail is particularly appropriate when users create, modify, or delete records and data during normal operation [16]. The audit trail should record the:

1. Initial values at creation
2. Modifications and deletions
3. Reason(s) for such modification or deletion

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/19 11:24 AM

Decisions on which items to include in the data audit trail, if configuration is available, should be based on risk assessment and specific GxP requirements.

Including unnecessary information should be avoided and can increase, rather than decrease, compliance risk.

With the exception of entering a reason for a change, audit trails should be automated, i.e. all audit trail functions should be executed without user intervention, and secure. Audit trails should be secure from unauthorized change.

An electronic data audit trail is useful for records and data. Other methods, e.g., change control records, may be appropriate for lower impact records and data.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Audit trail information on process operations may form part of the electronic record and should be reviewed during the approval process of the electronic record. In such cases a separate audit trail may not be required.

Records (e.g., instructions and summary reports) typically contain a history embedded in the document itself. A separate audit trail intended to be the equivalent of a document change history log is not normally required.

Audit trail information should include the following:

- The identity of the person performing the action
- In the case of a change or deletion, the detail of the change or deletion, and a record of the original entry
- The reason for any GxP change or deletion
- The time and date when the action was performed

Logical controls should be established for the management of audit trails, including limitations to the ability to deactivate, change, or modify the function of the audit trails. Procedural controls may also be needed. Controls should cover:

- Initial verification of audit trail functionality and subsequent verification during change management
- Management, monitoring, and periodic verification of audit trail configuration according to established procedures
- Preventing configuration of audit trails by persons with normal user privileges or approval responsibility
- Preventing turning off of audit trails (except for well-documented purposes related to maintaining or upgrading the system, during which time normal user access should be prevented)
- Where an audit trail is deemed necessary, but the system is incapable of creating an audit trail, other measures (e.g., a log book) should be implemented. As this is not automated and independent of the operator, it should be regarded as a less desirable option and regulated companies should consider alternative solutions.
- Ensuring that system clocks used for time stamps are accurate and secure
- Effective segregation of duties and related role based security, (e.g., system administrator privileges should be restricted to individuals without a conflict of interest regarding the data)
- Ensuring that any change to audit trail configuration or settings is documented and justified, and captured in automatic system logs, where possible
- Periodic checks that audit trails remain enabled and effective
- Established and effective procedures for system use, administration, and change management

Audit trails should be regarded as only one element in a wider framework of controls, processes, and procedures aimed at an acceptable level of record and data integrity.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

9.4 Audit Trail Review

There are three main types of audit trail review:

1. Review of data audit trails as part of normal operational data review and verification, second person verification and approval, usually performed by the operational area which has generated the data (e.g., a laboratory), i.e., using the audit trail routinely.

2. A tool to be used for investigation (e.g., of deviations or data discrepancies) as and when required, i.e., using the audit trail as and when needed.

3. Review of audit trail functionality (as part of normal periodic review or audit) to check that they remain enabled and effective, i.e., checking the audit trail.

Most audit trail reviews are of the first type, i.e., reviews conducted as part of normal operational data review. They may form part of a second person review (e.g., as required by 21 CFR Part 211.194 (a)(8) [24] for laboratory systems). Such reviews should not focus only on audit trails to the exclusion of other records, which may be especially important in hybrid situations. The review should cover the overall process from record generation to calculation of reportable results, which may cross system boundaries as well as the associated external records, and may cover several records and audit trails.

The objective of reviewing audit trails is to identify potential issues that may result in loss of data integrity. Issues may include:

- Erroneous data entry
- Modifications by unauthorized persons
- Data not entered contemporaneously
- Falsification of data

The review should be performed within the context of the business process, to be effective in identifying such problems.

9.5 Technical Aspects and System Design

Properly specified, implemented, and controlled audit trails are useful in supporting routine inprocess reviews, and as investigative tools, but current electronic audit trail solutions vary in degree of effort required to access and interpret them. Some common challenges with audit trail solutions include:

- Audit trails may require specialist tools to access them and are not readily available to system users
- System logs may need to be translated from technical data to business information
- Audit trails may be very extensive and identifying specific required information is difficult
- Audit trails may contain much information that is irrelevant from the perspective of the main objective of seeking to ensure data integrity

For enhanced usability, if available, systems should be configured to allow the search, sorting, and filtering of audit trail data. It should be recognized, however, that applications may not support this.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Regulated companies implementing and using the purchased systems should consider specific details of the available audit trail that may not be under their control.

Solutions may technically provide the required information, but it may be difficult and costly to support inprocess or periodic review of audit trail information. Regulated companies should encourage and support suppliers to develop useful audit trail functionality and provide effective data analysis tools.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

10 Appendix M5 – Data Auditing and Periodic Review

10.1 Introduction

Software applications can provide an audit trail, but only a human can decide whether an integration parameter change (noted in the audit trail) is scientifically valid; therefore, review processes remain in the human domain.

Review processes can be discrete or continuous, one off, or repeated and scheduled or unscheduled.

10.2 Auditing for Data Integrity

Auditing for data integrity goes beyond the typical internal quality auditing necessary for an effective quality system. Types of audits required in an effective data integrity program include:

- Initial gap assessment or audit where a regulated company is/is not complying with data integrity control requirements and best practices
- Ongoing internal quality audits of established data integrity controls to ensure continuing effectiveness and compliance
- Periodic audits of long term data archives to verify the data deterioration and media migration controls are being followed and are effective
- Supplier qualification audits for suppliers creating, modifying, reviewing, analyzing, transmitting, storing, and/or archiving data on behalf of a regulated company
- Closeout gap assessment or full audit following (or close to) completion of data integrity program implementation

Examples of data integrity auditing exercises could include:

1. Conducting a mock inspection of a specific data handling process, where the entire data life cycle would need to be explained as if it was being presented to a regulatory inspector. This can highlight any confusion about where the data resides and how it passes from one system to another, and may identify areas of weakness.
2. Picking a single result and tracing it back through to the raw data, including any laboratory notebook entries. Verifying the data integrity and audit trail at each step, and demonstrating that all raw data, paper or electronic, is readily retrievable and fully support the final result and is consistent with any summary data filed with the regulatory agencies as part of a drug master file or new drug application.
3. Repeating example 2 above in the opposite direction to verify that all data has been processed and reported, and to confirm that there is no orphan data which could be indicative of trial injections or other malpractices.

Further proactive data audit activities could be based on the regulators own guidance, e.g., US FDA Compliance Policy Guide Manual 7346.832 on Pre-Approval Inspections (FDA, 2010) [25] suggests that inspectors should:

- Review data on finished product stability, dissolution, content uniformity, and API impurity
- Determine if data was not submitted to the application that should have been

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1368
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Look for invalidated Out of Specification (OOS) results and assess whether it was correct to invalidate them
- Seek out inconsistencies in manufacturing documents (e.g., identification of actual equipment used).

10.3 Periodic Review

During a system's periodic review, the following could be evaluated within the system audit trail as part of monitoring human behavior and the effectiveness of the technical controls:

- Any changes to system configuration that could impact data integrity controls. Such changes should have been completed in accordance with the applicable change control procedure.
- Rationale for any deletion of data. If data was deleted as part of an archiving process, verify that the archived data is still accessible.
- Account disabling due to successive failed logons - look for repeat offenders and any timing patterns that indicate attempts at unauthorized access.

Such a review process may be practical only in a system where the audit trail can be filtered for review purposes. See Appendix M4.

Personnel records and system administrator logs can be reviewed for ongoing assurance of data integrity by:

- Checking the active user account list to ensure that only current personnel retain access to the system
- Confirming via the training records that all active personnel are adequately trained to operate the system
- Ensuring that system/database backups are happening as per the defined schedule, with the integrity of the backup being verified, and trial restoration of the system periodically occurring in a documented manner
- Ensuring that personnel are not given improper authority (e.g., enhanced access) for brief periods of time to perform improper activities

Other periodic review activities involve the review of:

- SOPs
- System records
- SOP records
- Change control
- Validation documentation
- System performance

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

These activities support ongoing compliance but are out of scope of this guide. For further information on periodic review and SOPs see the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [18].

For individual use only. © Copyright ISPE 2017. All rights reserved.

10.4 Other Reviews

Record reviews and audit trail review are covered in Section 4.4.

10.5 Documenting Review Processes

Within regulated companies, there should be documented evidence when an action was completed and by whom. Data integrity audits and system periodic reviews should be documented in their respective formal reports.

Reviewing audit trail entries associated with results (i.e., data audit trail) may be governed by a “Review of GxP Data SOP”, and documented by a statement similar to:

“By approving this report, I certify that I have reviewed the data, metadata, manually entered values, and audit trail records associated with this data, in accordance with Review SOP XXX.”

This statement could be included in the signature process for a record, and be visible on the printed and displayed report.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

11 Appendix M6 – Inspection Readiness

This appendix provides guidance on inspection readiness specifically for the integrity of records and data.

11.1 General Procedures

Regulated companies should:

- Consider record and data integrity within the context of broader inspection readiness programs
- Establish and maintain policies and procedures that ensure a constant state of inspection readiness
- Have robust established procedures for all aspects of the system life cycle
- Be prepared for regulatory inspections:
    1. On the management of record and data integrity to verify the adequacy of controls
    2. Using a forensic type approach which challenge the data integrity of specific records

11.1.1 Special Requests

Copies of electronic records should be available on request during a regulatory inspection.

Copies of electronic records may be provided as:

1. Printed copies of electronic records:
    - Printed copies should be suitably marked and signed as authorized copies of an electronic record.
    - Where paper copies do not represent complete copies of an electronic record, someone in the regulated area should be prepared to have a discussion with the regulatory inspector(s) to clarify this.
2. Electronic copies of electronic records:
    - The media on which it will be stored should be agreed with the regulatory inspector(s)
    - The media should be labeled as an authorized copy
    - The media should be scanned to ensure that there are no viruses and that it is an accurate and complete copy of the requested record

Regulated companies should also consider whether an electronic copy of an electronic record should be password controlled so the record remains secure.

Regulatory authorities have the same rights to access electronic records as they do for paper records.

It is not necessary to keep the superseded legacy computerized systems as long as content and meaning of a record is preserved.

The regulated company should create and retain a second copy of records and data provided to the regulatory authority, in case they need to refer to it in the future.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Regulatory inspectors may want to take photographs of equipment and facilities. Where there are restrictions on taking photographs due to safety issues in areas with potentially explosive processes, then this should be explained at the beginning of the inspection.

If photographs are taken by electronic means (e.g., digital camera or smart phone), the regulated company should try to obtain copies of the photographs taken by the regulatory inspector or take their own comparable photographs. Photographs should be retained, in case the regulated company needs to refer to them in the future.

11.1.2 Legal

Regulators may share information and may be aware of data integrity issues before an inspection occurs. Details of what has been reported to other regulatory authorities may be requested during a regulatory inspection.

Legal should be engaged to confirm which information may be shared within any restrictions imposed by other regulatory authorities.

Regulated companies should consider whether to obtain agreement that records and data are treated as confidential business information and not used for any purpose outside the jurisdiction of the regulatory authority, without prior written consent of the regulated company.

11.1.3 Access to Computer Systems

Regulatory inspectors may request direct access to computer systems to view records or workflows. Inspectors should not be granted access that allows them to manipulate data, apply electronic authorizations or approvals, or otherwise administer workflows. Regulatory inspectors could be given read only access; however, it is typically more efficient to provide trained and authorized personnel to access the computerized system and for the inspector to watch.

All system interactions and data queries should be performed in accordance with established SOPs.

Regulatory inspectors should understand the context of data retrieved when running data queries.

Regulated companies should keep copies of records and data provided for inspection, along with the database queries and routines used to collect them. A record of the name of the preparer and reviewer of the data collected should be maintained. Consideration should be given to how to protect this information from modification.

11.2 Key Information for Regulatory Inspections

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
IP Address: 156.
Downloaded on 6/10/19 11:24 AM

Regulated companies should be able to demonstrate that the systems they use are fit for their intended purpose. The regulated company should be able to readily identify personnel responsible for systems and associated data, i.e., the process owner, system owner, and data steward.

Personnel may be based centrally at an off-site location rather than at the point of inspection.

Quality agreements should be established to define roles, responsibilities, and contact information where local teams rely on central organizations or third parties.

For global information systems and interconnected systems, control of records and data should be demonstrable; system interfaces should also be considered.

For individual use only. © Copyright ISPE 2017. All rights reserved.

11.2.1 Process Owners and System Owners

The process owner and system owner are normally accountable for responding to system specific questions during regulatory inspections.

Process owners and system owners should be:

- Knowledgeable about the documentation supporting the implementation, control, maintenance, use, and history of the system
- Able to discuss any technical and procedural controls implemented to support the integrity of the creation, processing, and reporting of records and data
- Able to share the information about the requirements and testing of the data integrity relating to technical and procedural controls. A documented version history of the system can be created to assist in sharing such information.
- Able to discuss the key computer system documents including:
  - Validation Plan
  - Requirements:
    - > Data integrity controls
    - > System security controls
  - Validation report
  - Change control records

11.2.2 Process Owners

The process owner should be knowledgeable about and able to explain:

- The business processes supported by the system
- Data flows
- Any business SOPs supporting the process
- System security controls
- The validation documentation supporting the validation and use of the system
- System record integrity including how the:
  - Use SOP governs the timely recording of data
  - Audit trail is enabled and operating
  - Records are approved/signed only by authorized users
  - Approvals are enforced at specific points in the business process

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Audit trail review (in accordance with risk) is integrated into the business process
- Records and data:
  - > Can be changed only by authorized users
  - > Are restricted from change at required points in the life cycle

11.2.3 System Owners

The system owner should be able to explain:

- IT procedures used to support the system
- The change control process
- Change controls and associated documentation

11.2.4 Monitoring

There should be robust monitoring of the system, business, and IT support procedures to ensure that the processes are adequate and are being followed. Areas that should be routinely reviewed as part of monitoring to ensure inspection readiness includes:

- Access control:
  - access SOPs are in place and being followed
  - Available user roles are documented and managed by change control
  - Documentation supporting that only authorized and trained people have system access
  - Evidence that access is periodically reviewed (by automated checks where available)
  - Segregation of duties enforced
  - Generic accounts are not used for data modification
  - Back door changes requiring IT tools and skills are authorized, verified, and documented
  - Historic access records
- Backup and disaster recovery:
  - Documented and verified procedures for backup, restore, disaster recovery, and record retention
  - Documented evidence that records and data are periodically backed up
  - Records retention policies are clearly defined and followed
  - Records and data can only be accessed by authorized users (network and system)
  - Archived records are secure and accessible for the retention period

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Record and data maintenance

11.2.5 Personnel Preparedness, Training Records, and Procedures

Personnel using or supporting the system should be prepared for regulatory inspections, as well as the process owner and system owner. There should be robust processes in place to ensure that all individuals have current resumes, job descriptions, and training records.

Where there are procedures for management review of training records, there should be documented evidence supporting the review. Training should ensure that personnel using or supporting computer systems understand which SOPs govern their roles. Personnel should also be able to communicate clearly their roles and responsibilities with respect to a system.

Workflows, equipment, and facilities should assure data integrity. The provision of appropriate training and supportive oversight should also assure data integrity. Process and data flows can be used in risk assessments to identify where additional controls might be warranted.

11.2.6 Internal Data Integrity Investigations

Quality Units may need to perform data integrity investigations including, e.g.:

- Deviations with incident summaries
- Root cause analysis
- CAPAs

Trends across multiple data integrity incidents should be analyzed. Global CAPAs should be followed where there are wider organizational implications.

A risk assessment should form part of the investigation. It should consider risk to data and the consequences to safety, efficacy, and quality of medicinal products.

Regulatory inspectors may be interested in both human factors and any contributory supervision and leadership factors associated with the incidents subject to the inspection.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

12 Appendix M7 – Integrating Data Integrity into Existing Records Management Processes

12.1 Introduction

Records management is a long-established discipline. Organizations such as the Association of Record Managers and Administrators (ARMA) [26] are dedicated to this topic, and have developed standards in association with bodies such as the American National Standards Institute (ANSI) [27].

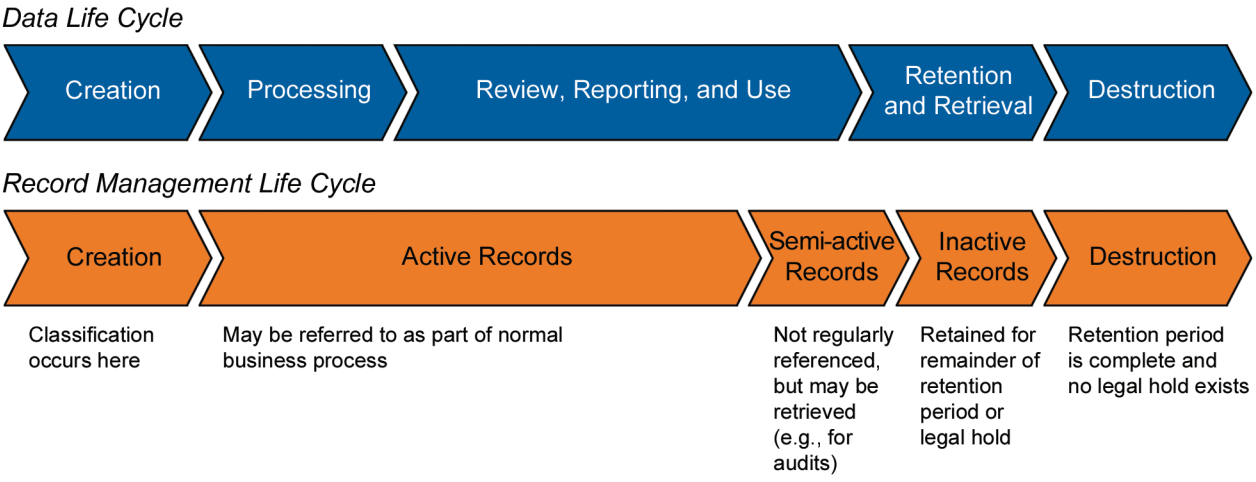
Large companies typically have departments that are specifically dedicated to records management. The scope of records management is larger than GxP data; it encompasses all of the records generated by a regulated company, including financial, legal, administrative, personnel, etc. The principles and standards for records management are considered compatible with data integrity.

Records management has its own established vocabulary, including a defined life cycle (see Figure 12.1).

Records managers should not be expected to replace or modify established standards, terminology, and processes based on convention or additional guidance relating to a relatively small subset of the records they control, i.e., GxP regulated records.

The records life cycle does, however, map to the data life cycle discussed in this guide (see Section 4) without risk to data integrity. Data owners and Quality Unit personnel should understand this mapping and how the regulated company's records processes meet expectations for the corresponding phases. For example, they should understand whether the records management group fulfills the formal role of archivist. Record managers typically apply a record life cycle that translates to paper, as well.

Figure 12.1: Mapping of Record Life Cycle to Data Life Cycle



Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

12.2 Record Creation

Records should be classified (e.g., as GxP, data privacy sensitivity) in order to understand which laws and regulations apply to their management.

12.3 Active Records

Active records are routinely subject to retrieval for business purposes. Electronically, they will reside in the active database. Paper records should be readily retrievable in a short time. For global information systems, this might involve replication to local sources in distributed systems.

Records may need to be reprocessed. This typically would occur during the active phase, although it could happen in the semi-active, or possibly in the inactive phase (possibly in response to an audit request). Change control processes should be followed if the record is to be updated. This may affect the retention period.

Typically, reprocessing would require the availability of the system originally used to analyze the data. The likelihood of such a need should be a consideration for system retirement planning.

12.4 Semi-active Records

These records can continue to be referenced for business purposes, although rarely. For example, they may be needed to support a regulatory inspection. Electronically, they may reside in a near-line archive with limited access. Expectations for the retrieval of semi-active records needs to be clearly defined. For global information systems, near-line archives can be local, although it is probably better to do this globally in order to minimize the number of copies of the record being managed.

Regulated companies may prefer to limit themselves to active and inactive, rather than use a semi-active stage in their life cycle.

12.5 Inactive Records

Most archived records fall into this category. These records are unlikely to be retrieved, but are being held to conform to retention policy. For global information systems, it is recommended that one archive should be managed globally, which will make the eventual destruction of a record simpler.

12.5.1 Destruction

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

This stage of the record life cycle is effectively the same as for the data life cycle.

For individual use only. © Copyright ISPE 2017. All rights reserved.

13 Appendix D1 – User Requirements

13.1 Introduction

This appendix provides specific guidance on establishing and defining data integrity requirements for new and existing GxP regulated computerized systems. This appendix supports *ISPE GAMP® 5* [3], which provides general guidance on the contents and production of a URS.

URSs should describe the required functions of the computerized system and be based on a documented risk assessment. URSs should be linked to the defined business process workflows and regulatory requirements governing the data and records in the system.

GxP requirements and data should be identified and documented to support appropriate quality risk management throughout the system life cycle. Requirements should be unambiguous and testable.

13.2 Business Process

User requirements should accurately reflect business process and data workflows, in order to establish a computerized system which meets its intended use. Business process understanding and regulatory assessment should drive the system validation from the initial user requirements to its functional and design requirements through qualification, procedural controls, system release and continued use. A consistent and complete URS should be produced to help ensure successful validation and compliance.

Business processes and associated data should be documented, e.g., through definition of business processes and/or data workflows, to ensure that a system adequately addresses all data integrity concerns necessary to meet regulatory requirements and expectations. For further information on defining business process flows and data flow diagrams, see Appendix D2.

Figure 13.1 provides an example of a change management enterprise system business process workflow and shows how potential user requirements may be derived from it.

Laying out the business process workflow can assist the stakeholders in identifying and agreeing the roles, records, signature requirements, system functionality, etc., necessary to support the system for its intended use.

Potential failures can also be assessed and remediated prior to selecting, designing, or establishing the system; therefore, saving resources, time, and money. In this example the business process workflow is broken into user requirements that further clarify how the system is intended to be used.

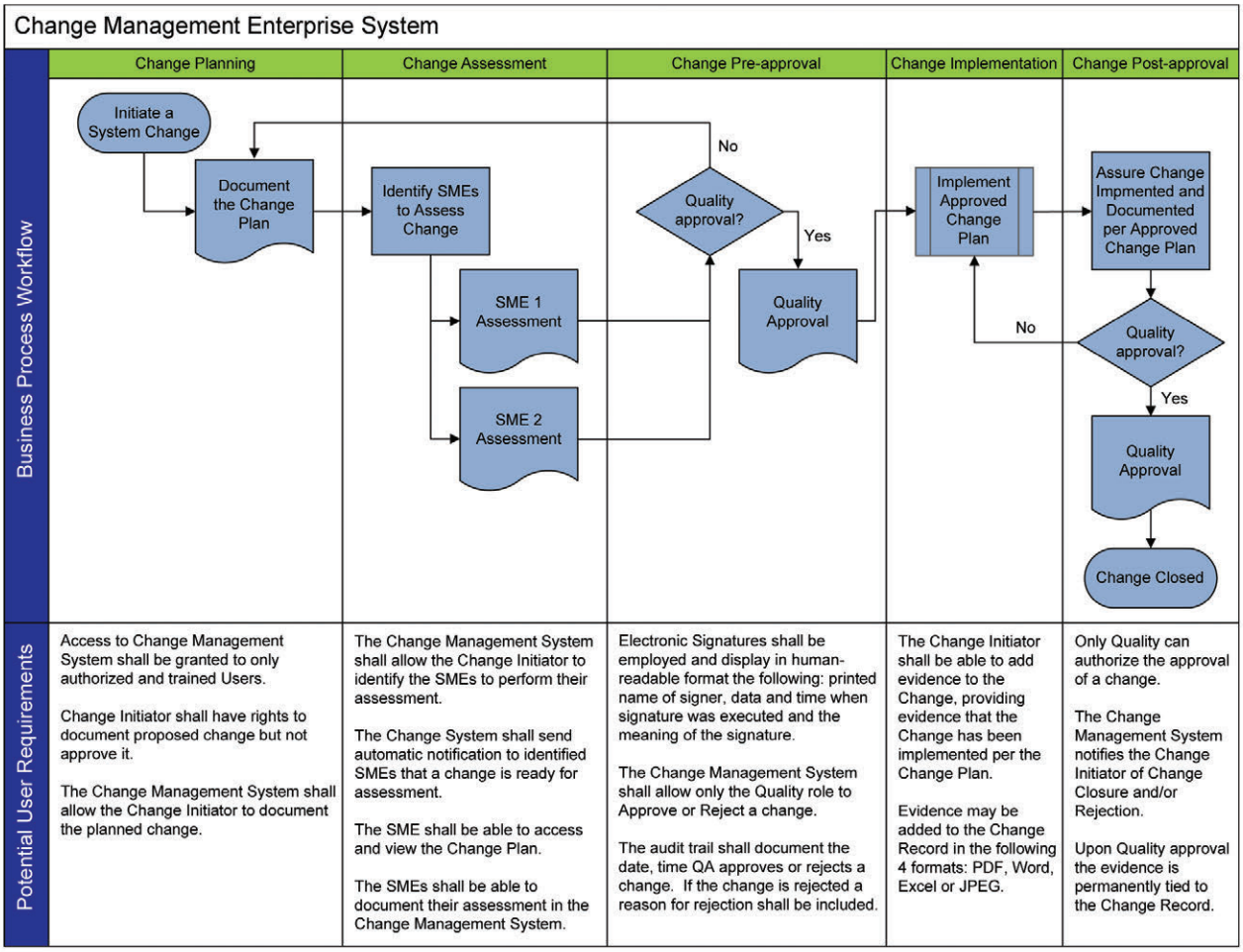
This document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 13.1: Potential User Requirements derived from a Business Process Workflow



13.3 General Data Integrity Requirements

General data integrity related requirements and expectations may be addressed by processes or procedures that are part of standard computerized system validation, operation, and compliance (e.g., backups, ensuring individuals understand the accountability for their electronic signatures) or business processes and may not be included in a URS.

Note: The text in the following tables should not be copied and included verbatim into a URS. Content should be converted into specific and testable requirements, taking into account the context and use of the system.

Regulations and business rules governing a process should be considered, and relevant requirements should be documented in the URS.

This Document is licensed to
Carlos A Cabrera
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

13.3.1 Technical Requirements

#	Requirement
1	The system should employ logical controls to restrict access to authorized persons. The extent of security controls depends on the criticality of the computerized system. The system should use authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand [2]. The system should have access controls to ensure that personnel have access only to functionality that is appropriate for their job role, and that actions are attributable to a specific individual.
2	Suitable control methods for preventing unauthorized physical access to the system should be employed e.g., computer hardware, communications equipment, peripheral components and electronic storage media. Controls may include the use of keys, pass cards, personal codes with passwords, biometrics, or restricted access to specific computer equipment (e.g., data storage areas, interfaces, computers, server rooms). Creation, change, and cancellation of access authorizations should be recorded.
3	The system should ensure that the accuracy, completeness, content, and meaning of data is retained throughout the data life cycle. Original records and true copies should preserve the integrity (accuracy, completeness, content, and meaning) of the record.
4	The system should be able to generate accurate and complete copies of GxP electronic records in both human readable and electronic form suitable for inspection, review, and copying by the agency [2].
5	Access to the system should be via individual login credentials made up of a unique combination of user id and password. Pass through technologies such as single sign on that leverage earlier user authentication are acceptable.
6	The system should provide a mechanism to archive complete and accurate records, including relevant metadata, from the system. The records should continue to be protected from deliberate or inadvertent loss, damage and/or alteration for the retention period. Security controls should be in place to ensure the data integrity of the record throughout the retention period, and validated where appropriate.
7	The computer system should provide a process for regular backups of all data including relevant metadata. **Note:** The URS should include details as to the frequency of backup, the nature of the backup (full/incremental), and the length of time the backups are retained. The integrity and accuracy of backup data, and the ability to restore the data, should be checked during validation and monitored periodically [7].
8	The system should provide a mechanism to enforce data retention requirements, including data ownership, data holds (regulatory holds), and destruction of data. Stored data should be verified for restorability, accessibility, readability and accuracy throughout the retention period [7].
9	Where appropriate, operational system checks should enforce permitted sequencing of GxP steps and events, and should disallow non-permitted sequencing of GxP steps and events [2].
10	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks [7].

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

#	Requirement
11	The system should perform an accuracy check on manually entered data.
12	The system should provide a secure, computer generated, time stamped audit trail to independently record the date and time of entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information [2]. The system should record the identity of operators entering or confirming critical data. Any modification to an entry of critical data should be recorded with the reason for the change.
13	The system should provide audit trails that are available and convertible to a human readable form [7].
14	The system should enable review of audit trails that capture changes to critical data, e.g., as part of the review of their associated records.
15	The computer system should ensure that electronic signatures, including the human readable display or format, captured by the system include [2]: 1. Printed name of the signer 2. Date and time when signature executed 3. Meaning associated with the signature
16	Electronic signatures and handwritten signatures executed to electronic records should be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means [2].
17	The system should use at least two distinct identification components such as an identification code and password to ensure that electronic signatures can only be used by their genuine owners [2]. The system should support that the human readable form of an electronic signature for display or print out should be unique to an individual.
18	The computer system should ensure that when an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual [2].
19	The computer system should ensure that when an individual executes one or more signings not performed during a single, continuous period of controlled access, each signing shall be executed using all of the electronic signature components [2].

13.3.2 Procedural Requirements

#	Requirement
1	All personnel should have appropriate qualifications, level of access, and defined responsibilities to carry out their assigned duties [7].
2	Evidence should be available to demonstrate that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks [2].
3	GxP electronic records created, processed, stored, or reported should be identified. The system should be able to generate accurate and complete copies of GxP electronic records in both human readable and electronic form suitable for inspection, review, and copying [2].
4	Procedures should be established to check stored data for accessibility, durability, and accuracy.

This Document is licensed to
Carlos J. Cabrer
Valrico, US
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

#	Requirement
5	Validation documentation and reports should cover the relevant steps of the life cycle and should include operational change control records (if applicable) and reports on any deviations observed during the validation process [7]. Regulated companies should be able to justify their standards, protocols, acceptance criteria, procedures, and records based on their risk assessment [7].
6	Computerized system configuration settings should be defined, tested as part of computer system validation, and protected from unauthorized access. They should be managed under change control.
7	Procedures should be established for an additional check on the accuracy of the record when critical data are being entered manually [7].
8	Procedures should be established to ensure that only authorized personnel can amend entered data.
9	Audit trail information should be retained for a period at least as long as that required for the subject electronic records and should be available for regulatory review and copying [2].
10	Based upon risk, procedures should be established to review audit trails with each critical record, and before final approval of the record.
11	System access records should be periodically reviewed based upon the criticality of the process supported by the computerized system.
12	System administrator access should be restricted to the minimum number of personnel possible, taking account of the size and nature of the regulated company. Personnel with system administrator access should log in under unique logins that allow actions in the audit trail(s) to be attributed to a specific individual. The generic system administrator account should not be available for use [8].
13	Critical changes with data integrity implications (e.g., system access changes, configuration changes, data movement, data deletion etc.) performed under system administrator access should be visible to, and approved within, the quality system.
14	Business areas should ensure individuals understand that they are accountable and responsible for actions initiated under their electronic signatures [2], and that electronic signature components should not be made known to others.
15	Procedures should be established to ensure that electronic signatures have the same impact as handwritten signatures. The consequences of misuse or falsification should be documented.
16	A procedure should be established to ensure that the identity of the individual is verified prior to the assignment of their electronic signature [2], or any element of an electronic signature (such as the user ID).
17	Procedures should be established to ensure that electronic signatures are unique to one individual and not reused or reassigned [2].
18	Procedures should be established to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password [2].
19	Processes should be established to ensure that the attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals [2].
20	A procedure should be in place to ensure that the linkage of handwritten signatures to electronic records is maintained throughout the retention period.
21	Procedures should be established to perform periodic testing of devices that bear or generate the confidential component of an electronic signature to ensure that they function properly and have not been altered in an unauthorized manner [2].

This Document is licensed to
Valrico, FL
Downloaded on: 4/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

#	Requirement
22	Password aging procedures should ensure that identification code and password issuances are periodically checked, recalled, or revised [2].
23	Password expiry procedures should be established.
24	Procedures should ensure that the ability to apply electronic signatures is withdrawn for individuals whose responsibilities change, without the loss of information relating to signatures already executed.
25	Loss management procedures should be established to electronically deactivate lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls [2].
26	Procedures should cover the method of delegating signature responsibilities (e.g., periods of absence, holidays).

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

14 Appendix D2 – Process Mapping and Interfaces

14.1 Introduction

Process workflow and dataflow diagrams are visual tools to show relationships of a business activity, including the creation and/or movement of data through a business activity and/or relationships between entities (interfaces). Visual tools permit whole systems/processes to be analyzed in ways that would otherwise be difficult to achieve with text alone.

It can be difficult to understand a process adequately without process workflows and relationship diagrams, including data flow diagrams across infrastructure, especially when enterprise level systems are involved.

Two commonplace tools used are:

1. Business process flowcharts, which identify:
    - Business activities and decision points
2. Data flow diagrams, which identify:
    - The creation, movement, use, and archiving of data throughout a process

Both the business process flowchart and dataflow diagram may be implemented in layers, with Level 1 giving the most abstract “high level” view and Levels 2, 3 etc., giving progressively more details about the process or data under consideration.

14.2 Process Flowcharts

Process flowcharts illustrate the discrete steps of a business process; the “process” view of activities.

This includes actions, decision points, and subprocesses.

Figure 14.1 provides an example[3] of a hypothetical Level 1 flowchart of a supporting IT infrastructure process, granting a user access to a business computer system. This flowchart provides the steps and relationships between steps that people in the business would perform.

This Document is licensed to

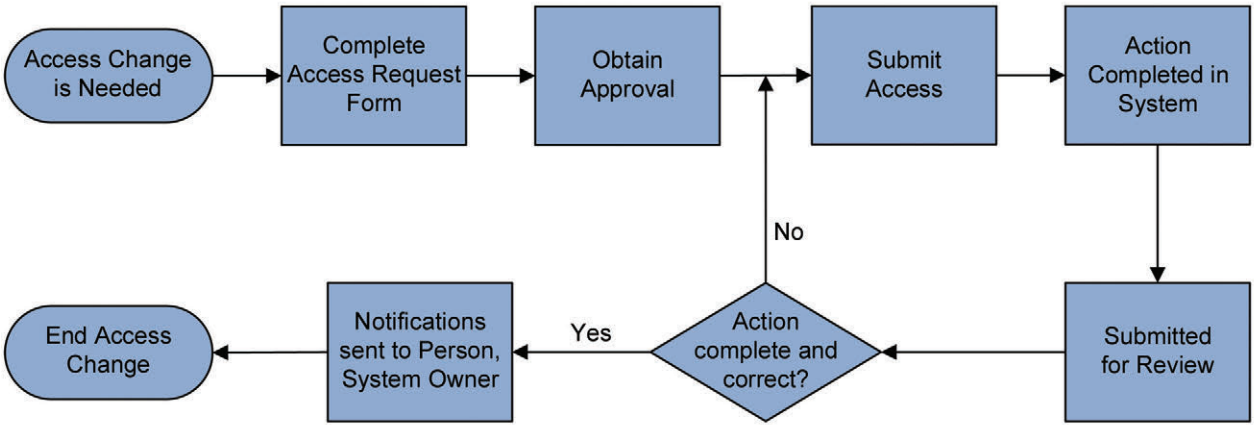
Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

[3] This example was chosen as a simple illustration only, and is not intended to suggest that the process shown is a GxP regulated business process.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 14.1: Example IT Infrastructure Process: Granting Access to a Computer System



Note: In this first flowchart user roles, locations, or details are not specified.

This flowchart can be extended by using lanes (also called swim lanes) that add an additional dimension to the flowchart, such as the role that should perform the action, or the location.

Another approach, shown in Figure 14.2, is to create a table that provides details to explain each step of the flowchart in greater detail. For example, each action is numbered, and corresponding numbers in a table can provide details such as the:

- Location (where)
- Responsible person/role (who)
- Proper time to perform the action (when)
- Output(s) of the action

Flowchart/table combinations can help in understanding a process, and allow users to associate useful metadata with specific points. Risk management can also be applied at these points to form the basis of a risk-based control strategy.

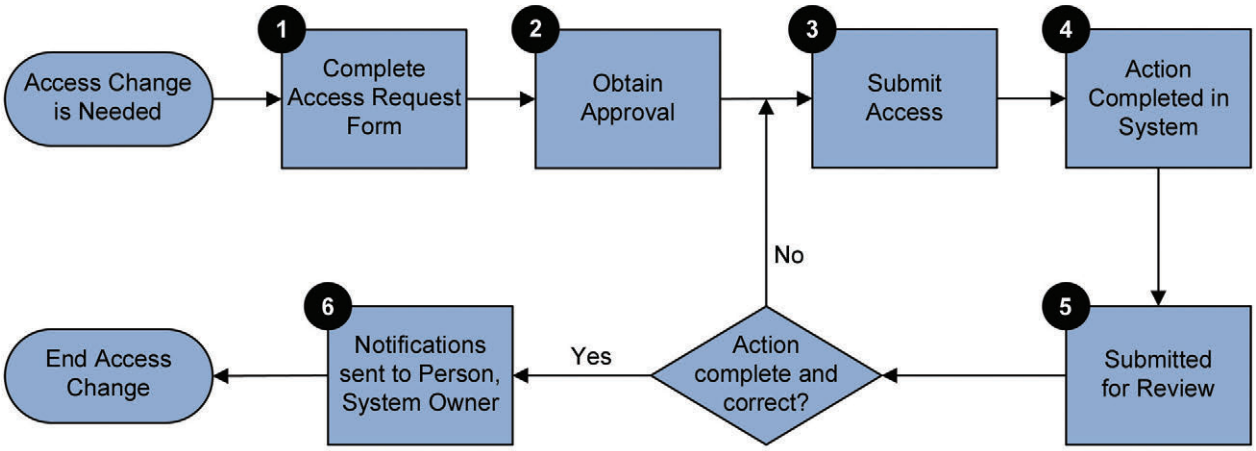
This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 14.2: Example Process Flowchart (with additional details, linked by step numbers)



	1	2	3	4	5	6
Who	Line Supervisor	System Owner Training Leader	Access Website	System Administrator	System Owner or SME	Access Website
When	Upon User Request	Once User Completes Form	After Owner Approves	Within 24 hours of Receipt	Immediately after Execution	After Request is Verified
Where	Access Website	Access Website	(Email Message)	Requested System	Requested System	(Email Message)

For large and/or complex systems it may be more efficient to flowchart the process in several levels. For example:

- Level 1 flowchart shows the entire system as a single box, showing its interfaces to other large systems.
- Level 2 flowchart shows interfaces between the system and one or several other systems, in greater detail, e.g., the interface with the financial system and its associated product library with standard costs.

Process flowcharts detailed in this multiple level format can be used to provide information at the level needed by a specific audience, e.g.:

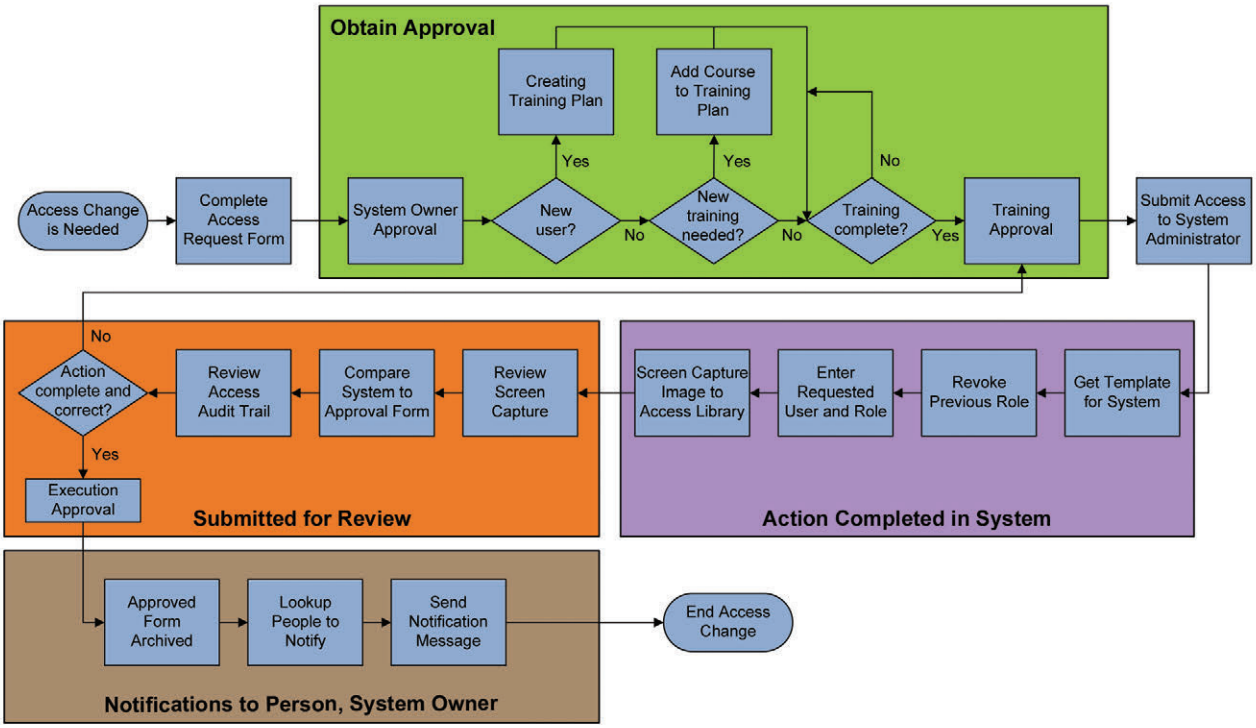
- Level 1: intended for senior executive
- Level 2: intended for system support personnel

Levels can be added, as needed, e.g., if Level 2 does not have sufficient detail for system understanding, another layer of depth may be necessary (e.g., Level 3). The goal should be to create the minimum number of levels needed to define requirements, identify decision points and risks, and support the system in operation.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
IDnumber:1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 14.3: Example Process Flowchart (taken to a greater level of detail)



14.3 Data Flow Diagrams

Data flow diagrams should graphically illustrate the creation, use, and movement of data elements throughout a business process: the “data” view of activities. Data flow diagrams should display data elements (fields, tables, or databases) that are impacted at each step. Data flow diagrams should also use images similar to those in process flowcharts to illustrate actions and decisions.

For simple systems, a hybrid may be created that combines both process and data in a single flow diagram.

For systems of moderate complexity, a business process flowchart may be created, along with an identical data flow diagram re-labelled with data rather than process activities. This approach can allow support personnel to see both process and data views in parallel, to help process understanding.

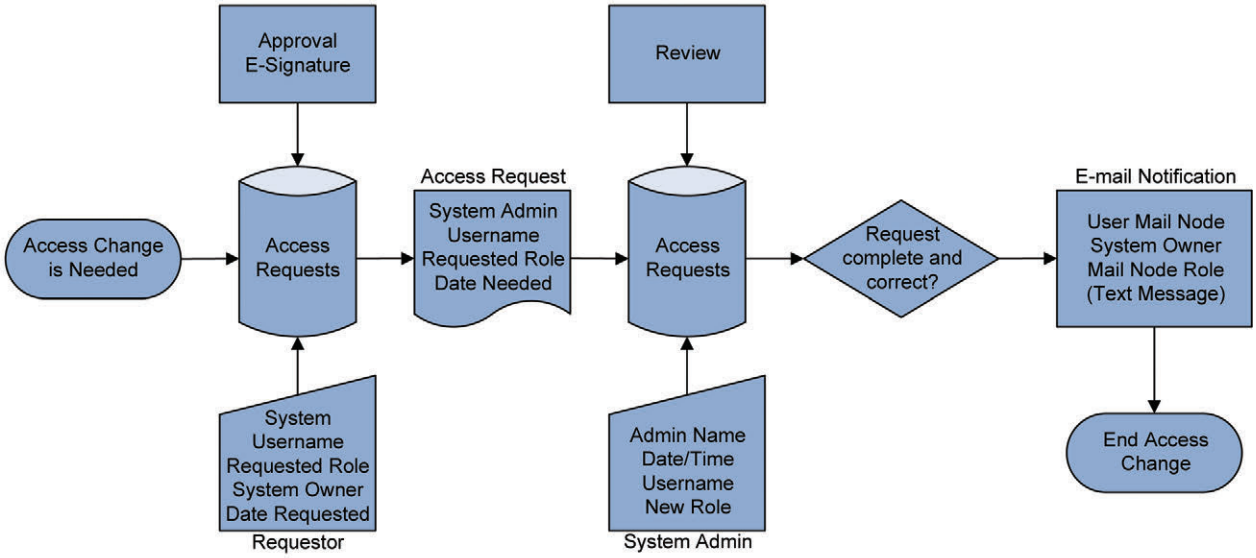
This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

Data flow diagrams can be useful for identifying:

- Data impacted by activities
- Data elements required by regulations
- Data that can be reprocessed or modified (therefore requiring an audit trail)
- Data that is necessary for correct decisions

For individual use only. © Copyright ISPE 2017. All rights reserved.

Figure 14.4: Example Data Flow Diagram for Granting Access to a Computer System



Advantages of data flow diagrams:

- Better than text for understanding relationships between steps (data process, etc.)
- Show decision points
- Illustrate inputs and outputs for each step
- Illustrate links between different processes or systems

14.4 How Much Is Needed?

As the system size, complexity, and support level increases, the greater the need to document in increasing detail. In practice, personnel performing a routine process daily/weekly are usually able to identify inherent risks to data integrity and decision points when given a business process flowchart; consequently, a process flowchart can be sufficient.

In contrast, e.g., an electronic batch system with connections to inventory, planning, financials, control, and historian systems can require several process flowcharts. It may need a process flowchart for each listed connection, and two levels of flowcharts for each process, and, possibly, more levels for some areas.

Process charting should be sufficient to assist personnel in:

- Accomplishing process definition and understanding
- Identifying data integrity risks
- Identifying critical decision points
- Risk identification

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

15 Appendix D3 – Risk Control Measures for Records, Data, and Electronic Signatures

15.1 Introduction

This appendix discusses principles and controls for records and data and the application of electronic signatures. It describes various control measures that can be used to manage identified risks.

The control measures should be aimed at eliminating or reducing the probability of occurrence of the harm, reducing the severity of harm, or increasing the probability of detection. The rigor and extent of controls will depend upon the identified risks to records and data.

For further information on controls for paper records and hybrid situations. See Appendix O2.

15.2 Record and Data Controls

Controls may be applied at different levels including, e.g.:

- Organizational
- Infrastructure
- System
- Database
- Record
- Field

Controls may be behavioral, procedural, or technical in nature. This appendix describes procedural and technical controls that can reduce risks to an acceptable level. For further information on behavioral controls. See Section 3.4 and Appendix M3.

A combination of procedural and technical controls may be necessary to adequately manage identified risks. The selected controls should be implemented, verified, and documented. Controls may be implemented at the system level (e.g., audit trail).

The implementation of procedural controls should be considered at a corporate, site, or department level, as appropriate, to minimize unnecessary duplication of procedures.

This document is licensed to
Sybil Stiller
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:38 AM

15.3 Electronic Signature Controls

A regulated signature is a signature required by a GxP regulation. Regulated signatures include signatures that document that specific events/actions occurred in accordance with a GxP regulation (e.g., approval, review, or verification of a regulated record).

A regulated electronic signature is a regulated signature applied electronically, and intended to be the equivalent of a handwritten signature required by a GxP regulation.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Within the US regulatory framework, the electronic signature requirements of 21 CFR Part 11 [2] apply to electronic signatures that are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules. Signatures are not automatically Part 11 signatures because they are executed in a regulated system. See FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application (Section 2: Definition of Part 11 Records) [16].

Electronic signatures should be distinguished from identification events:

- An electronic signature can be regarded as a specific event in the life cycle of a record. A record can be verified, reviewed, or approved, and the status of the record changed (e.g., from draft to final, or unapproved to approved) by the application of an electronic signature.

- Identification events (that may also be required by regulations) are those events where the requirement is only for the identification of an individual performing a particular activity. For example, this may be achieved by the logging of an event by a validated computerized system.

Electronic signatures may be implemented by a unique user ID and password combination. Other uses of user IDs and password, such as logging on to a system, acknowledgement of alarms, or identification of individuals are not electronic signatures.

Regulated companies should define when electronic signatures are required in regard to their own processes and circumstances, along with their interpretation of GxP regulations. Where signatures are applied electronically, appropriate electronic signature controls should be applied.

The following should be clear for each electronic signature:

- The identity of the signer

- The date and time when the signature was executed

- The meaning of the signature (such as verification, review, or approval)

This information should be clear to any reader or user of the record, e.g., included as part of a human readable form of the signed record, and should be permanently linked to the record, such that it cannot be removed, altered, or copied by ordinary means.

The following implementation options may be considered when deciding upon a suitable approach to ensuring compliant electronic signatures. The appropriate level of control will depend upon the level of impact and vulnerability:

This Document is licensed to
Carlos J. Cabrer
Valid to: [illegible]
ID number: 1568
Downloaded on [illegible]

- Method for ensuring uniqueness of electronic signature components, including prohibition of reallocation of user IDs

- Prevention of deletion of electronic signature related information after the electronic signature is applied

- Biometrics – *"a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable."* (21 CFR Part 11) [2]).

- Digital Signature – *"an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified".* (21 CFR Part 11 [2]).

- Technical or procedural approaches to ensure the integrity of the link between electronic signature and record (especially if handwritten signatures are applied to electronic records).

For individual use only. © Copyright ISPE 2017. All rights reserved.

- Method of display or print of signed records
- Procedure for delegation of electronic signature responsibilities (e.g., covering holidays or periods of absence)
- Options for entry of all or some components of multiple component electronic signatures

15.4 Implementation of Record and Data Controls

Controls may be implemented in different ways and with differing degrees of rigor. Table 15.1 shows how various types of controls can be implemented.

Table 15.1: Possible Implementation of Controls

Control	Implementation Considerations and Options
Security and Access Management	• Physical security • Formal access authorization • Confirming identity of new user before granting access • Unique user identification • Providing defined profiles for individual users or groups • Clear separation of server administration, application administration, and user roles and responsibilities • Limiting write, update, or delete access (e.g., to key users) • Enforced password changing • Enforced minimum password length and format • Idle time logout (inactivity logout or timeout) • Management of lost or compromised passwords • Group access (sharing of access accounts) • Proactive monitoring for attempted breaches • Automated measures on attempted unauthorized access (e.g., lock account, notify management) • Limiting and controlling use of superuser accounts • Testing and renewal of identity devices or tokens • Access revocation: - Access rights change and removal process - HR monitoring of staff changes • Periodic access rights review
Backup and Restore	• Frequency of backups • Auto or manual processes • Backup verification • Backup media • Storage conditions • Storage location(s) including remote storage locations • Media management (e.g., labeling, storage, rotation, refresh) • High availability system architecture • Mirroring and redundancy • Periodic restore verification

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 15.1: Possible Implementation of Controls (continued)

Control	Implementation Considerations and Options
Disaster Recovery and Business Continuity	• Service level agreements • Formal contracts for restoration of service • High availability system architecture • Assessment of possible failure modes • Defined allowable time of outage • Recovery mechanisms (e.g., hot standby, procedural) • Documented testing of the disaster recovery and business continuity plan • Defined recovery point objective and recovery point time for different systems • Documented procedures for business continuity and number of personnel trained in these procedures

Audit Trail	• Which events are audit trailed (record creation, modification, deletion)
	• Reason configurable/predefined or free text
	• Purpose, e.g.:
	  - As a part of normal business data verification
	  - For auditing of authorized or unauthorized changes to data
	• Type (automatic, manual, combination)
	• Date and time stamped
	• Identification of time zone
	• Amount of information retained (who/what/when)
	• Access control and security of the audit trail
	• Ability to change the audit trail
	• Retention of the audit trail
	• Backup and restore of the audit trail
	• Procedures for managing the audit trail
	• Retention of previous versions of data

Copying and Retention Controls	• Format of copy (e.g., common portable electronic, paper)
	• Reference to original on copy
	• Relationship with original (e.g., exact copy, summary)
	• Search, sort, and trend capabilities
	• Process for producing copies (time required, access levels)
	• Checksums
	• Retention periods
	• Definition of what is being retained
	• Retention of associated data (e.g., audit trails, configuration information)
	• Indexing and searching to aid retrieval
	• Capacity limits
	• Automatic or requiring human intervention
	• Ability to reprocess data
	• Formal disposal procedure
	• Periodically testing ability to retrieve records throughout retention period
	• Media maintenance procedures throughout retention period:
	  - Ability to read physical media
	  - Dependence on original version of software application
	  - Dependence on original version of operating system
	  - Dependence on original configuration of hardware

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 15.1: Possible Implementation of Controls (continued)

Control	Implementation Considerations and Options
Software Controls	• Functional controls based on business rules and GxP requirements • User identity checks • Interfaces: - Checksums and other verification of data transfer - Standard network protocols for data transfer • Automatic functionality to reduce human error, e.g.: - Use of barcodes or other electronic data reading functionality - Sequence enforcement - Creation of predefined text and lists • Measurement redundancy in critical applications • Data entry checking • Error handling • Alarms • Notification of software failure • Prompting for confirmation of action • Monitoring tools (e.g., event logs)
Hardware Controls	• Mirrored or RAID drives • UPS • Contingency in sizing of hardware • Network monitoring (could be also software control) • Virtualization management
Policies and Procedures	• Formality of policies and procedures • Extent of QA involvement • Formality and roles involved in authorization • Formality and roles involved in review • Formality and roles involved in approval • Internal audit processes to confirm adherence to procedures
Training and Experience	• Importance of data integrity principles • Training and experience of users • Training and experience of developers of systems (both regulated companies and suppliers) • Significance of electronic signatures in terms of individual responsibility • Consequence of falsification • Use of electronic signatures

This Document is licensed to
Carles J. Cabrer
Validaat S.L.
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

Many of the controls identified in Table 15.1 are technical in nature and will form part of the functionality of a supplied system. Suppliers should be aware that these controls may be typical requirements for systems supplied to regulated companies. Suppliers should be prepared for assessments, including auditing, to ascertain that technical controls have been implemented appropriately, as regulated companies have ultimate responsibility for the system in use.

Suppliers should provide documentation that defines which electronic records and signatures a system can maintain. The controls available to help manage electronic records and signatures should also be described; regulated companies can use this information during the risk management process.

Where it is not possible to implement specific technical controls, e.g., lack of availability in the automated system, the use of alternative technical or procedural controls should be considered. The use of several procedural controls may produce sufficient collaborative information to support evidence for the control of electronic records.

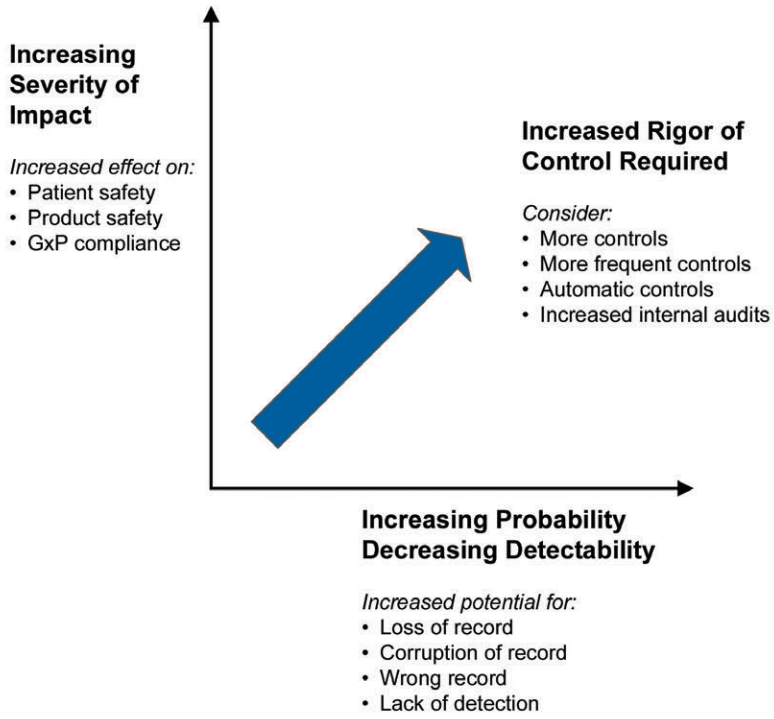
For individual use only. © Copyright ISPE 2017. All rights reserved.

Suppliers may provide administrative features and utilities which can make the implementation of procedural controls more efficient, consistent, and secure. For example, the inclusion of a system workflow to route lists of authorized users to process owners on a periodic basis for review.

15.5 Rigor of Controls

The rigor with which the controls are applied should consider both the impact of the electronic record and the risks identified. As the impact and risk increase, more rigorous controls are required, as shown in Figure 15.1.

Figure 15.1: Rigor of Required Controls



For electronic records, regulated companies should consider the need for:

- Authenticity
- Integrity
- Accuracy
- Reliability
- Confidentiality (where appropriate)

A combination of technical and procedural controls may be needed to achieve an adequate level of protection.

For systems containing multiple types of records, two approaches are:

1. Apply controls to all records appropriate to the highest identified risk
2. Apply controls to individual record types appropriate to the identified risk for each type

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

16 Appendix D4 – Data Integrity Concerns Related to System Architecture

This appendix addresses different architectures and approaches to managing data integrity issues that relate to each.

The architecture of applications will impact the controls that are appropriate to ensure data integrity. Architectures that should be considered range from the C:\ drive on a PC that collects or processes GxP data to SaaS applications for which the data owner may not know where a particular record resides.

Architecture choices can have direct and obvious data integrity impact; others will have more subtle and indirect impact.

16.1 Data Resides on a Local Hard Disk

This may be the simplest architecture, but these systems can have the greatest vulnerability because of the lack of built in controls. This may be particularly problematic for laboratory instrument control systems which have not been designed in regard to data integrity. This is likely the case with older instruments.

Where applications do not provide adequate protection, Operating System (OS) level controls should be implemented where possible. In cases where an application does have sufficient protection, OS level controls should be established to ensure that the application level controls cannot be avoided by accessing the data directly through the OS. The following should be considered:

- **Attributability:** Login should be required to ensure that a record created on the system is attributable to the person who created it. If this is not possible, consideration should be given to upgrading or replacing the system. A logbook may be kept, but this may be ineffective.
- **Audit trails:** Elements that may make audit trails less trustworthy include:
  - Improper control of the system clock
  - Controlled data access at the operating system level
  - Lack of attributability
- **Segregation of duties:** OS level access to data should be limited to IT. Laboratory analysts should not have administrator rights on instrument controllers or data systems.
- **Protection from hazards:** In cases where storage media are exposed to unusual risk (e.g., potential vulnerability of laboratory or manufacturing systems to spills or other hazards) measures should be considered that could minimize such exposure, e.g., placing the systems in a safer area or in an enclosure.
- **Backup:** Locally stored records should be protected. Data should be accumulated to a managed network drive instead of a local hard disk. An alternative is an automated backup process where local files are automatically copied periodically to a managed network drive. A properly executed manual backup may also be used.

  Note: backup media should be suitably protected and should be stored in a remote location.
- **Archive:** Archiving may be a simple process, if the PC application includes an archive function. If the PC application does not include an archive function, it may be difficult to manually move all data and associated metadata to archive media. Archive media should have a level of protection similar to back-up media.

This Document is licensed to
Sabah Sabah
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

- **Disaster recovery:** There should be specific plans to deal with system loss. Stating that a new PC will be obtained may not be acceptable, as a PC with the correct configuration may not be available.

- **Data accessibility:** Local user ability to access individual files on the system, restoring deleted files, renaming files, etc.

16.2 Internally Managed Central Database

These systems are either server based applications or PC based applications where all data management occurs outside the PC. The key to this is that such architecture should be among the easiest to properly manage to ensure integrity of data. Data integrity protection should address:

- **Attributability:** Based on login. In this architecture, it can be harder to justify a paper based control such as a logbook.

- **Segregation of duties:** Administrative rights should be limited to IT professionals. It may be preferable to assign some limited administrative functions, such as approval of user rights, to the business. There should be no potential conflict of interest.

- **Backup:** In general, this will be handled through enterprise processes owned by IT. There should be a standard periodicity to take incremental and full backups. Backup media should be stored securely (usually offsite). Media may be recycled according to a standard practice, e.g., only the four most recent copies are retained, with the fifth iteration being overwritten onto the media used for the first.

However, the business process owner should ensure that such an enterprise process is compatible with the actual business process. For example, if an application is only used in January to compile annual summaries, the process described would not work. If the data became corrupted between February and August, the next time the database is opened in January the corruption would be found, but the corruption would have been propagated to all existing backup copies.

- **Archive:** Archives should be managed in alignment with the data life cycle. This includes the destruction of all archive copies, including backups, when the records reach the end of their retention period.

  Note: The retention of backups in lieu of a true archive is not recommended. It can make record destruction problematic, as it is very difficult to selectively remove expired records. Restoring a backup to access archived records could have significant business impact.

- This should include testing, since there are likely to be dependencies on other enterprise owned assets. Disaster recovery planning should follow a well-defined risk-based process, so that systems with major patient safety or business impact are appropriately scheduled in case of a wide-ranging disaster.

This Document is Licensed to
Carlos J. Cabrer
Valrico, FL
ID Number: 1568
Downloaded: 6/19/19 11:34 AM

16.3 Internally Managed Distributed Data

Distributed systems require the same protection as centralized systems. Added complications could occur based on two architecture subtypes.

16.3.1 Locally Unique Data Accessible Globally

Local databases may be used to achieve desired performance of the system at multiple sites. This generally does not involve managing local record copies at sites other than the one at which the records were generated. A small subset may have local copies that were saved in accordance with local business practice. For example, manufacturing records for products made offshore may be copied locally to support a regulatory compliance expectation.

For individual use only. © Copyright ISPE 2017. All rights reserved.

The local databases should be managed similarly to the centralized system described above. Complication may occur regarding treatment of data that is required to be retained in other jurisdictions. For global information systems, regulated company processes should account for the use of information at other sites when making decisions related to archive management and data destruction.

16.3.2 Data Replicated Globally

The issues described for centralized systems apply and should be appropriately addressed for data replicated globally. For replicated data when records are scheduled for destruction, all copies of the record should be destroyed. This should account for all locally archived copies in addition to copies in the active database. Failure to do so could expose the regulated company to legal discovery liabilities.

The second complication with centrally stored records is that retention policies need to recognize the potentially differing requirements based on the applicable jurisdictions. For example, some blood product records need to be retained for ten years in the United States, whereas the same records need to be retained for thirty years in Europe and Japan. Therefore, knowledge of where the product has been distributed is key in determining the timing of the steps in the data life cycle.

The same considerations described above apply to any centrally managed archive.

16.4 Outsourced Managed Services

While this section concentrates on cloud based solutions, considerations described may also be applicable to any outsourced or externally managed infrastructure and/or applications. As part of an outsourcing process regulated companies need to:

- Understand and accept which aspects of control are being delegated to a provider
- Assess and accept the controls implemented by the provider
- Contractually define the level and frequency of reporting
- Agree the need for supplier support during regulatory inspections, depending on the architecture and services provided

If any of the above are not satisfactory, the decision to outsource should be revisited.

For additional further information on cloud based solutions in a GxP environment, see the *Pharmaceutical Engineering* magazine articles by David Stokes “Compliant Cloud Computing – Managing the Risks” [28] and the ISPE GAMP® Cloud Computing Special Interest Group (SIG) “Cloud Computing in a GxP Environment: The Promise, the Reality and the Path to Clarity” [29].

In general, the evaluation process, the controls, and the complexity of contractual and service level agreements should increase in line with the amount of control the regulated company is transferring to the cloud provider. From lowest to highest this is IaaS → PaaS → SaaS. Each type of solution should have the controls discussed for the lower level solution(s) in addition to those discussed at that level.

Regulated companies may consider cloud solutions for GxP processes that have not been specifically developed for the GxP world. When evaluating such a supplier, the regulated company should not expect to see the same processes that would be found in a supplier whose primary customer is the pharmaceutical industry. Documentation may be less formal; management approval may not be required in as many places, etc. The emphasis should be on evaluating the state of control over the high-risk processes. The regulated company should look for “GxP-compatible processes.”

For individual use only. © Copyright ISPE 2017. All rights reserved.

The regulated company should consider whether there are reasonable and appropriate controls that ensure data integrity.

16.4.1 Internally Managed with Cloud Storage (Infrastructure as a Service (IaaS))

The requirements for these systems are the same as for internally managed centralized systems, except that some of the tasks of managing the data will fall to external personnel. The following should be accounted for in assessing the risks related to this architecture:

- Data management processes at the cloud provider need to be assessed to make sure that the regulated company is satisfied that the provider's controls are adequate. If there are some countries where the regulated company does not want data stored, this needs to be contractually agreed.

- Depending on the level of access and the type and format of the information being processed or stored in the cloud the regulated company may decide that the data should be encrypted.

- Some cloud providers may have internal policies that give administrative rights to dozens or hundreds of staff, believing that they need to have the internal flexibility to assign any employee to work on any contract. While this is probably not necessary, a regulated company is unlikely to be able to convince a cloud supplier to change that model. The regulated company should assess whether this can be acceptable, possibly with additional compensating controls.

- Supplier change control processes should be evaluated to ensure that proper and timely notification is given for changes that may impact data integrity.

- Disaster recovery processes should be assessed to ensure that they will restore data access in a time frame acceptable to the regulated company. This should include a mutually agreeable Recovery Time Objective (RTO, or how quickly service is restored), and this should be included in the SLA. Recovery Point Objective (RPO), or how much data can be lost since the last backup, is the responsibility of the customer (the regulated company), as they are managing the database on the supplier equipment. However, if data backup is contracted to the supplier, this can affect the ability to meet the RPO.

- Before entering into an arrangement with a cloud service there should be an agreed and well-defined process for disengagement. This should address timing, including both advanced notice of intent to sever the relationship and the time allowed to do it, supplier and regulated company responsibilities, and cost. Disengagement should also include the removal of data from provider owned equipment, and if applicable backup media.

16.4.2 Internally Managed Application with Cloud Based Platform

This Document is licensed to

Solutions involving a Platform as a Service (PaaS) supplier should include consideration of all of the above plus:

- Change control will have wider impact, as it will extend beyond hardware and operating systems and into layered software. When entering into an agreement with a PaaS supplier, it should be clarified what the supplier's policy is related to support of older software versions. For example, if the provider's policy is to support only the current and one older version of a database it may drive more upgrades than the regulated company desires, and such upgrades may require data migrations with all the associated data integrity risks.

- Disaster recovery responsibilities will move more toward the supplier. In addition to RTO, the supplier will probably be charged with meeting the RPO requirements as well; therefore, RPO should be covered in the SLA.

For individual use only. © Copyright ISPE 2017. All rights reserved.

- In addition, staff at the provider may now be directly managing data, e.g., as a database administrator (DBA). It should be understood and documented what the DBA can do. For example, is the DBA allowed to make direct data changes, and if so what controls are in place for that? DBA access to confidential data may also make encryption advisable. The impact of a supplier policy of wide granting of administrative rights has greater potential data integrity impact if it applies to DBA access, as well as to hardware support.

- Suppliers may have multiple data centers and will distribute load in order to balance the demand. This could entail placing data in one country and manipulating the platform from another. If either of these are unacceptable to the regulated company restrictions need to be contractually negotiated.

16.4.3 Software as a Service (SaaS)

Every issue noted above applies to SaaS systems, but aside from decisions related to record retention virtually all of the data management activities are carried out by the supplier. It should be recognized that the regulated company remains accountable for the integrity of the data, regardless of the fact that it is being managed by a service provider. This means that the contract and SLA should be written to ensure mutually agreeable controls are in place. Some of these controls will have direct data integrity impact, and others indirect. Specific points that should be addressed include:

- Some SaaS providers execute non-optional changes periodically. For the most part, this is not likely to have a negative impact, but for GxP applications there needs to be sufficient prior notification to allow testing, and defined processes at the regulated company for dealing with the impact of both successful and unsuccessful testing.

- It may be that the supplier wants to use customer data to test software changes. Such testing should only be allowed with the express permission of the regulated company. Some precautions like deidentification or masking of confidential data may be advisable.

- A provider may have internal processes for incident management that delay reporting of serious issues to customers pending preliminary investigation. Depending on the application, this might be unacceptable to the regulated company. This needs to be outlined in the SLA.

- Similarly, a SaaS provider may be reluctant to activate disaster recovery processes because of the marketing fallout of a declared disaster. As a result, they may allow themselves a few hours to troubleshoot before declaring a disaster, and this may impact data collection and processing during this early stage of a disaster. It is incumbent upon the customer (regulated company) to examine and understand the provider's disaster recovery procedures.

- As with PaaS, the SaaS supplier may want to move or archive data at other locations, and they may not even know where at the time of engagement. The SLA should address whether this can be allowed, or at least timely notification of such actions.

When evaluating a SaaS supplier regulated company auditors are unlikely to find software development practices that are aligned with traditional GxP expectations. For example, many SaaS suppliers use some form of Agile development process, and some interpretations of the Agile manifesto avoid documentation in favor of rapid results. Evaluation should concentrate on the state of control of the software development process, focusing on compensating controls and any documentation that is eventually produced. An Agile SDLC that allows for quality and documentation to be defined and used, as required, can be used to support validation. Companies would not employ Agile methodologies if they could not produce reliable software when used properly – "GxP compatible" processes should be the goal.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Some concerns may require a degree of compromise on the part of a SaaS supplier and there may need to be some investment in documentation and process changes. This may entail resistance from the supplier. However, the life sciences industry is among the most heavily regulated and any technology company desiring to enter this arena needs to be aware of this. The regulated company should be prepared to assist the supplier develop acceptable processes.

A prospective customer needs to consider the risks of engaging a SaaS supplier with no experience of regulated company clients. While flexibility in the form of accepting GxP compatible processes is important, the willingness to walk away if the circumstances are not right should always remain on the table. A risk management approach should always be applied to the selection process.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

17 Appendix D5 – Data Integrity for End-User Applications

17.1 Introduction

End user applications are small applications that are typically created outside of traditional software development environments. They may be developed by the people who will use them and can range in complexity from users simply clicking a series of buttons to being able to modify and execute code directly.

End user applications may be repeatedly created based on stored templates.

Examples include:

- Spreadsheets (the most frequent type)
- Small databases (regularly PC-based)
- Statistical programs (e.g., developed on a SAS® platform)
- Computer programs (e.g., developed in Visual Basic)

The decision to use end user applications for GxP processes should be risk-based. The use of end user applications is considered as having an increased risk to data integrity. For example, there have been numerous US FDA warning letters regarding the use of spreadsheets to manage GxP records.[4]

End user applications may have weaknesses in the attribution of actions. For example, by default a spreadsheet records the identity of the creator and of the last person to modify it, but users who have modified it in the interim are not tracked. Similar issues may also apply to the use of statistical programs or other similar applications.

End user applications usually need extra controls in order to satisfy regulatory expectations. Appropriate controls should be implemented to mitigate risks to an acceptable level.

End user applications and the data they generate should be stored in a secure manner. This can include the use of operating system controls, e.g., read/create/modify/delete access restrictions and auditing OS level audit trails (if available).

This Document is licensed to
Carlos D. Brown
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 10:34 AM

17.2 Data Integrity for Spreadsheets

Spreadsheets are useful tools that are attractive for a variety of uses related to regulated activities. It is the flexibility that makes a spreadsheet a high-risk form of electronic record from a data integrity standpoint, particularly if the spreadsheet is not carefully controlled.

Limits should be set related to the manner in which spreadsheets are used and managed. *ISPE GAMP® 5* [3] provides a discussion of the various types of uses of spreadsheets and validation implications. There is also guidance available from regulators, e.g., US FDA Field Science and Laboratories: Laboratory Manual Volume 3 – Laboratory Operations, Applications and Programs: Section 4.5 – Development and Validation of Spreadsheets for Calculation of Data [30]; or DFS/ORA Laboratory Information Bulletin No.4317, Spreadsheet Design and Validation for the Multi-User Application for the Chemistry Laboratory Part 1 (2004) [31].

[4] US FDA warning letters can be viewed on the agency website: www.fda.gov.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Spreadsheets do not support audit trails. There may be add-on tools available to do so, but they are not commonly used. If a regulated company chooses to depend on an add-on tool, a thorough analysis of the capabilities and limitations of the add-on should be performed, as many of the controls described below may be required.

17.2.1 Spreadsheets that are Simple Documents

The easiest class of spreadsheets to manage are static tables. These should be controlled in the same way as word processing documents and their control can be managed within an Electronic Document Management System (EDMS). EDMSs are designed to apply controls to documents that ensure that storage, access, versioning support compliance, and legal requirements.

Where an EDMS is not available, the primary challenge is control of the storage of documents. Control issues are similar to those for other electronic files. Saving the final version as a PDF can help to ensure a document is more difficult to edit. Digital signature tools can be used as needed.

17.2.2 Spreadsheets that are Templates

A frequent role for spreadsheets is for the repetitive usage of calculation algorithms. Any integrity issues related to the template can spread to every record that is generated based upon that template; therefore, the integrity issues can have significant potential impact.

It should be ensured that algorithms in templates are appropriate; however, it is not necessary to verify that a spreadsheet performs arithmetic accurately. Templates should be independently verified and approved, prior to providing them for use. Templates should be stored in a manner restricting the ability to alter them to a very small number of people. Typically, this will be a combination of measures such as:

- Storage of the template in a directory that appropriately restricts write, edit, and delete access
- Users should only be able to copy the template to a separate, protected directory with limited access
- Password protection of all cells in the template, except for those where data is entered so that the algorithms cannot be edited by during use
- Restriction of the ability to edit documents created using the template
- Traceability to the creator/editor of records created based on a template
- Where feasible, once records created from a template are finalized they should be stored in an immutable format, e.g., PDF
- Spreadsheets based on templates that support GxP decisions should be saved in a secure manner that prevents unauthorized and/or undetectable changes to the recorded data throughout the required retention period

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

17.2.3 Single Use Spreadsheets

Spreadsheets may be used to analyze a unique problem, such as investigating an out of specification result or evaluating a manufacturing trend.

Single use spreadsheets should be managed in a similar way to spreadsheets that are simple documents. The main difference is the integrity of the calculations. Calculations should be verified as appropriate, but checking arithmetic is not considered necessary. Capturing a view of the calculations can provide a long-term record that the calculations are the correct.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Available spreadsheet programs may include tools that allow cell contents to be displayed and subsequently printed to paper or saved to PDF.

If a spreadsheet of this type needs to be left open for additional data entry, it should be set up so that revision of the spreadsheet will require versioning. One mechanism would be to disallow saving over the existing version. Administrative procedures defining protections are recommended.

Depending on the risks related to the record, the data and calculations may need to be independently reviewed by a second individual.

17.2.4 Spreadsheets as Databases

Spreadsheets should not be used as databases from a data integrity viewpoint.[5] In addition, audit trails for the individual cell contents are not available, so that it is not possible to recreate changes without examining every single version. Control of change tracking is generally not sufficient to meet GxP regulatory expectations, even if it can be enabled.

Where a desktop database is required, acceptable control of data integrity may be more achievable by using a real database engine. Platforms other than a desktop or handheld device are recommended for controlling data integrity.

Note: Just accessing a database using such a device is a more easily manageable risk.

17.3 Data Integrity for PC Databases

17.3.1 User Developed and Managed Tools

Aspects of a purely local database that require protection are the same as those required for a server based database, but they can be more difficult to administer. For example, segregation of duties is not possible if the user of the database is also the developer and owner. For this reason, the routine use of such tools for GxP processes is not recommended.

When a user developed and managed tool is developed for a specific problem, e.g., supporting an investigation, single use applications would be expected. Short term IT projects may not need to be executed under a formal SDLC with built-in data integrity protections. Data integrity concerns should nonetheless be considered.

Once the investigation is completed, the database should be locked and securely stored.

17.3.2 Centrally Managed PC Databases

This Document is licensed to
[illegible]
Valrico, FL
[illegible]er: 1568
Downloaded on: 6/19/19 11:34 AM

Where a regulated company decides to use a PC database, an IT group should manage the tool in the same fashion as a server based database. This effectively makes the tool a server based database on a different database engine and operating system. Segregation of duties, access controls, backup, and archiving can be managed appropriately.

However, some PC based database engines may not be able to manage issues such as audit trails and role based security in a way that would be expected by regulators.

Choosing to use a tool such as a PC database, should be based on a formal risk assessment.

[5] The main reason for this is that every time data is added to the database, a completely new version of the database is effectively created.

For individual use only. © Copyright ISPE 2017. All rights reserved.

17.4 Data Integrity for Statistical Tools

User developed statistical tools may be used in the same way as a PC databases and have the same data integrity concerns. Single use tools supporting investigations should be locked and controlled following completion of the investigation.

User developed statistical tools may be used repetitively, e.g., to analyze tablet weight distribution for a batch of finished product. Template controls should be similar to those for spreadsheet templates:

- The template should be stored in a controlled location, with limited access
- Authorized users should only be able to copy the template to a different directory where it can be used. The code should be inaccessible to users in this location; users should only be able to add and process data.
- Once the result of the analysis has been obtained, it should be protected against unauthorized change
- The result of the analysis should be traceable to the user who generated it
- If there are tools to remove or hide statistical outliers from the data set, it may be appropriate to control how and by whom that functionality can be used.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

18 Appendix O1 – Retention, Archiving, and Migration

18.1 Introduction

This appendix describes approaches to managing records in order to comply with GxP regulations in regard to record retention and data integrity. The focus is on issues relating to the choices a regulated company may want to make, including consideration of issues related to migrating electronic records to non-processable formats.

Note: this appendix does not discuss the definition of the retention period for various types of electronic records, which is based on the relevant GxP regulations and company policy. In addition, it is not intended to be a complete guide to GxP compliant data migration or archiving practices.

18.2 Retention Options

The approach to data retention should be based on regulatory and legal requirements, as well as an assessment of the risk associated with the data format, physical media, and anticipated future use of the data. Data management activities (including security, and disaster recovery) should also be considered.

The terms “record retention” and “archiving” describe separate issues. Typically, archiving involves removing an electronic record from the system that produced it, e.g., a production database. Archiving is also an approach to meeting electronic record retention requirements. The selected approach to electronic record retention should meet relevant GxP regulations:[6]

- Near-line solutions: these can archive electronic records invisibly to users. For example, older electronic records may be moved to another database but the electronic records remain accessible through the main application. Near-line solutions have the advantage of rapid access.

- Off-line solutions: these involve archiving electronic records on different media (e.g., optical disk or magnetic tape). Typically, this will involve more effort to retrieve archived electronic records. Off-line solutions usually trade rapid access for less costly storage solutions.

Use of non-electronic media such as microfilm, microfiche, and paper, or a standard electronic file format, such as PDF, SGML, or XML should also meet relevant GxP regulations. Electronic record content and meaning should be preserved. Metadata should be considered and may be a critical component of the content and meaning of an electronic record.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

18.3 Protection of Records

For on-line electronic records, logical and physical security measures, including backup, should be applied.

System upgrades may require data migration. Data migration plans should ensure the integrity of the electronic records in the database, as well as electronic records that have been archived.

[6] 21 CFR Part 58.190 [32] requires that the results of preclinical studies be archived (and under the control of an archivist) at the completion of the study. In such cases, if the records are to be retained on-line in a production database, measures need to be taken to protect them from alteration in order to comply with this predicate rule.

For individual use only. © Copyright ISPE 2017. All rights reserved.

For archived electronic records, additional considerations include:

- Exercise of the media
- Refresh of the media
- Storage conditions

Media should be used in accordance with its specifications. When refreshing the media, the typical approach is to use new media of the same type, although this is not required. Any change in the media should be evaluated for potential risk. Magnetic media is prone to degradation over time, so the lifetime of magnetic media can vary. Alternative media (e.g., optical) can provide increased durability.

Archived electronic records may need to be technically refreshed and/or converted it to a new format that is compatible with an upgraded production system, e.g., to support new versions of layered software such as a database engine upgrade.

Considerations for technically refreshing electronic records include:

- Validation activities
- Floating point issues
- Rounding versus truncating

When systems are retired, electronic records may still be within their retention period. Rendering software may be developed to provide access to these electronic records as an alternative to retaining a costly software license. Limitations of the rendering software in regard to processing of the records should be understood. A formal risk assessment associated with the system retirement and rendering software development should be undertaken.

18.4 Record Aging and Risk

For some records the associated risks are not constant throughout the record life cycle. This can impact the measures and controls required to safely, effectively, and economically manage the records. For example, data migration planning should include an evaluation of the risks to the records.

Data migration may be required several times for electronic records with a long retention period. Data migration can be difficult and expensive. If the risk related to the electronic records is low, migration of the records to a medium with a longer lifespan (e.g., paper, PDF, flat file) may be appropriate. For global information systems, the risk assessment should consider risks related to all sites and jurisdictions with an interest in the data.

Whenever a decision is made to convert electronic records to a less processable format (e.g., from dynamic to static) a risk assessment should be performed and documented. The risk assessment should consider applicable risks for all jurisdictions and for prospective uses of the information. For example, clinical data relating to a mature product that is being phased out of production might be a candidate for conversion to another format. However, if the product is planned for introduction to a new country, or is being considered for a new therapeutic indication, it may be more appropriate to migrate the electronic records and keep them processable.

This Document is licensed to
Carlos L Cabrer
Vanrico, FL
Downloaded on: 6/19/19 11:34 AM

18.5 Archival

Archival is a solution for the retention of records that are no longer actively used, but need to be retained for business, legal, or regulatory reasons. Not all records will be archived, e.g., those with short retention periods.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Reasons for archiving records include:

- Freeing storage space (this can apply to disk space for electronic records (or to file cabinets for paper records))
- Protection of the records
- Computer system performance, which may degrade when the database becomes too large

Archiving electronic records involves moving the records into an archive and then deleting the records from the active database. The archive is intended as a long-term storage solution (years).

Archived electronic records should be removed from an active database otherwise there can be a risk that a change is made to the record in the active database after it has been archived. This can cause differences between the record in the active database and in the archive and this will raise questions regarding the integrity of the archive.

18.5.1 Backup

Backup of electronic records involves generating a copy of the records.

The purpose of a backup is to provide a copy that allows restoration of the database in case of loss or corruption. The retention of backups should be relatively short term (e.g., weeks or months).

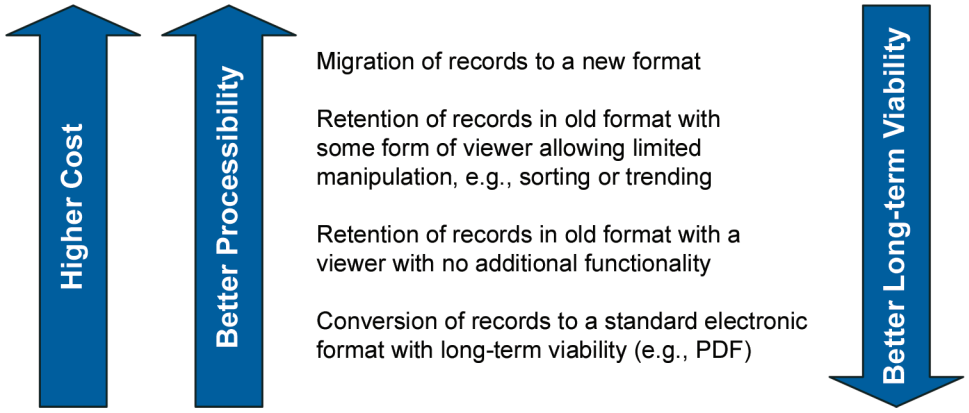
Backups should not be used in place archives. It is inefficient to manage years of backups, and it can be difficult to recover individual records should the need arise.

18.6 Hybrid Situations and Archives

Regulated companies may choose to retain electronic records in formats other than the original record format. The content and meaning of the original electronic record should be preserved and GxP regulations should be met.

It may not be considered necessary to retain electronic records in a processable format throughout the entire retention period. The likelihood that a record may need to be reprocessed may reduce significantly as that record ages. A point may be reached where a decision should be made on the risk/benefits of maintaining an electronic record in a processable format. See Figure 18.1.

Figure 18.1: Risk/Benefit Considerations for Data Conversion



For individual use only. © Copyright ISPE 2017. All rights reserved.

Regulated companies should evaluate whether retaining electronic records in a processable form is worth the expense of doing so. If the result of the evaluation is a decision to compromise or remove the ability to reprocess, a documented risk assessment supporting the decision, should be performed. The risk assessment should include the reasoning behind the choice of which metadata needs to be migrated to the new format.

The primary consideration should be the effect of a change in electronic record format on risk to patient safety. Other considerations may include:

- The ability to demonstrate record integrity in the new format
- The likelihood that changes to the record would be necessary after conversion
- Future use of the record, including potential need to:
    - Sort
    - Trend
    - Otherwise manipulate the record
- The difficulty and expense to do the any of the described manipulations, if necessary
- Availability of the electronic record to regulators
- Regulated company risk tolerance related to a potential regulatory request

Lower cost and simpler technical options, e.g., paper, may be adequate solutions, depending on the impact on the record (e.g., the criticality of metadata for understanding the record) and the requirements for processing. Where an assessment has determined that the audit trail needed to be retained, and if there is any metadata that is needed to support electronic record integrity, the metadata should remain part of the electronic record. Metadata may include:

- Date of edit of the electronic record
- Identity of the editor
- Previous values

The original version of an electronic record may be deleted if the content and meaning of the original record is preserved and archived, and GxP regulations are met. Where migration or transformation is not required to keep the electronic record in a processable format, archival of the electronic record may be the lowest risk approach.

18.7 Audit Trail Considerations

Carlos J. Cabrer
Valrico, FL

Audit trails should be considered part of records. Data migration activities should retain audit trial information. A record of the changes to an electronic record prior the conversion of its format should be preserved, if possible. This should occur even if the electronic record is converted to PDF or paper.

A decision not to migrate an audit trail should be justified, based on risk, and should be documented. For example:

- If the audit trail is integral to understanding or ensuring the integrity of the record, it should be part of the migrated record, e.g., changing a GLP or GMP laboratory test result based on reintegration of a chromatogram.

For individual use only. © Copyright ISPE 2017. All rights reserved.

- If the audit trail is not required by GxP regulation and the data was used only for unregulated purposes, e.g., statistical process optimization within validated parameters, or for workflow tracking; therefore, it has low GxP impact.

18.8 Alternative Systems

Electronic records may be collected and managed on different systems. For example, it may be appropriate to utilize superior data management capabilities (e.g., audit trailing, consolidated backup) in a higher-level system, rather than trying to build those capabilities into several laboratory instruments (i.e., the originating systems).

If uses and manipulations of an electronic record are intended to be in the higher-level system:

- The content and meaning of the electronic record should be preserved
- Manipulation of the original raw data file through the originating system should be prevented

Systems may allow the original data file from the laboratory instrument to be retained and managed in the higher-level system.

This can be advantageous because it can allow:

- Greater control of the data offered in the higher-level system
- Restoring of the data to the originating system for reprocessing while retaining the original data file

Systems may use proprietary data formats. The content and meaning of the electronic record may not be preserved when these formats are converted to new formats. In some cases, it may be possible to manage data files through the higher-level system; however, the electronic records may be only viewable in the originating system. An assessment should be performed to determine whether processability is critical. The need for this may decrease as the record ages.

The content and meaning of migrated records should be preserved. This typically involves either validating the conversion or verifying the accuracy of the new version.

Regulated companies should understand the risks, as well as benefits, of a solution that places records in an alternative system. EU GMP Chapter 6, Section 6.9 [33] states:

> *"Some kinds of data (e.g. test results, yields, environmental controls) should be recorded in a manner permitting trend evaluation."*

This Document is licensed to
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

If a regulated company interprets this as requiring the ability to reprocess the data, transferal to a higher-level system may not be appropriate. If transferal to a higher-level system is considered, that system should be able to support reprocessing data or exporting data back to the originating system.

Regulated companies should consider potential future needs for manipulating records, when evaluating the risk of performing anticipated analyses without the ability to reprocess data. The risks and costs associated with validating or verifying data migration should also be considered.

For individual use only. © Copyright ISPE 2017. All rights reserved.

18.9 Converting Electronic to Alternative Format or Alternative Media Hybrids

Regulated companies may decide to retain records in a format other than electronic (e.g., paper, microfilm/microfiche), or in an alternative standard electronic format like PDF.[7]

18.9.1 Considerations for Conversion

The primary driver for any decision to convert electronic records to other formats should be business need.

Appropriate points for considering conversion include:

- Creation of the record
- The point at which a record is to be archived
- At system upgrade, especially if electronic record conversion is needed
- At system replacement when contemplating data migration to the new system
- At system retirement, especially if electronic record conversion or development of rendering software is needed
- The point at which a media refresh is needed

For example, for drug product distribution records, the speed of response is critical for dealing with recall situations. A regulated company may decide that distribution records are not well suited for immediate conversion to a non-processable format, as the ability to search and access the distribution records quickly is usually suited to a computerized system. The risk would be substantially lower, however, after the expiration of a lot of drug product, so conversion to paper at that point might be justified.

18.9.2 Changing Repositories without Altering Format

There are risks associated with moving electronic records from one repository to another, e.g., for archiving. Risks may include:

- Media degradation
- Accidental loss
- Failure to retain software capable of viewing the records

Methods such as checksum verification help to ensure that migration of an electronic record is complete.

18.9.3 Risk Assessment for Conversion

Decisions to convert electronic records to an alternative media, format, or repository should be justified. The risk assessment should demonstrate that there is no unacceptable risk to data integrity, product quality, and patient safety.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded on: 6/19/19 11:34 AM

[7] While PDF is an electronic format, and does offer some possibility to manage records using audit trails and digital signature, it is considered an alternative format because conversion to PDF generally sacrifices the ability to process the data. However, PDF carries the advantage of being able to execute searches within documents (if not scanned), and depending on how the files are stored, also may offer searchability on the documents themselves. This should be considered when selecting to what format to convert records.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Where appropriate, the risk assessment process should be based on groups of related records:

- For a small to moderate sized system (e.g., a chromatography data system), it may be possible to evaluate all of the records as a single group.
- For larger more complex systems (e.g., an ERP), several groups of records should be evaluated independently.

When considering conversion of regulated records to another format, risks, and requirements should be considered for higher impact records. See Table 18.1.

For low impact records the approach to archiving should follow good IT practices. For higher impact records, risks and requirements such as those in Table 18.2 should be evaluated.

Risk assessments should consider the way in which electronic records are accessed and used. Regulated companies should consider potential effects (see Tables 18.1 and 18.2) in the context of each unique set of electronic records. For example, if accuracy and completeness of records in a drug safety database could be compromised by conversion, and the converted record could then be interpreted incorrectly, there could be significant risk to patient safety, based on erroneous medical conclusions. The same occurrence to records in a training database would have a less severe impact.

Table 18.1: Risk Factors for Conversion of Electronic Records to an Alternative Format

Risk Factors and Requirements	Considerations	Potential Effects
Conversion may change the accuracy and completeness of the record in a manner that would affect the interpretation of the data	If the converted record is considered the original data, the possibility of changing the interpretation of the data would be unacceptable	Interpretation of the converted record leads to a different conclusion than before conversion
Users may have to execute a rapid search of the data across records	If rapid retrieval is necessary, e.g., to support a product recall, conversion may be in appropriate, as cross record searching is far easier using database technology	• Unable to rapidly search • Inadequate/incomplete searches
Users may have to execute large or frequent searches on the records	Frequent or large searches introduce increased probability that the searches will be incomplete	• Spend inordinate resources on searches • Inadequate/incomplete searches • Unable to execute effective search
Users may have to search the records based on a wide range of keys	Most filing systems for non-electronic records have limited searchable keys	• Spend inordinate resources on searches • Inadequate/incomplete searches • Unable to execute effective search
Retention of original record after conversion to an alternative format	Why retain the original? How will it be kept consistent with the converted copy?	• Inconsistency of records • Confusion/inaccuracy
Record may have to be modified after it is converted to an alternative format	Changes may be harder to execute and to track in the alternative format	• Audit trail inadequate • External audit trail may be required

This Document is licensed to
Carlos A. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 7/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 18.1: Risk Factors for Conversion of Electronic Records to an Alternative Format (continued)

Risk Factors and Requirements	Considerations	Potential Effects
Employees who need it do not have ready access to the electronic record in the new format in order to perform their job responsibilities	If they are expected to use the alternative format electronic record, it needs to be accessible. This can be problematic due to geographic or technical factors (e.g., no access to a required reader).	• Inefficiency • Actions taken based on insufficient data
An audit trail needs to be retained as part of the electronic record in the alternative format	• Is the electronic record history retained in the audit trail critical to the value of the record? • Is the audit trail integral to electronic record integrity? • Is an audit trail required by a GxP regulation? • An audit trail in an alternative format may double (or worse) the size of each record. (This may in fact be a driver for moving records from the database to archive.)	• Audit trail inadequately shows subsequent changes, with potential reduction in record integrity • Size of archive may become unwieldy if audit trail retention is handled ineffectively • Large database size may lead to performance problems
An electronic signature is associated with the electronic record	• Is evidence of the approval still in the new version? • Is the alternative format adequate evidence of authenticity? • Is the link between electronic signature and electronic record preserved?	• Evidence of timely approval is compromised or lost • Hybrid manifestation of electronic signature loses legal meaning/weight • Linkage of electronic record with signature is broken

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

Table 18.2: Risk Factors for Transfer of Electronic Records to Alternative Media (archiving)

Risk Factors and Requirements	Considerations	Potential Effects
Users may have to execute a rapid search of the data across records	If rapid retrieval is necessary, e.g., to support a product recall, search capabilities on the new media may be limited and restoration of the records to a searchable platform may cause delay	Unable to rapidly search. This may be partially mitigated by development of emergency procedures to eliminate delays that are purely administrative in nature.
Users may have to execute large, complex, or frequent searches	Search capabilities on the new media may be limited. Frequent restoration of archived data would be resource intensive and expensive.	Spend inordinate resources on searches
Retention of original electronic record after conversion to an alternative media	• Why retain the original? • How will it be kept consistent with the converted copy?	Inconsistency of records
Record may have to be modified after it is committed to alternative media	Changes may be harder to execute and to track on the new media	• Required changes not executed or not executed in a timely fashion • Audit trail inadequate
An audit trail needs to be retained as part of the record	• Is the electronic record history retained in the audit trail critical to the value of the record? • Is the audit trail integral to electronic record integrity? • Is an audit trail required by GxP regulation? • Depending on architecture of the audit trail, changes after commitment to different media may multiply electronic record size several-fold.	Size of archive may become unwieldy if audit trail retention is handled ineffectively

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

19 Appendix O2 – Paper Records and Hybrid Situations

19.1 Paper Records

19.1.1 Introduction

The management of paper based records should support data integrity. The management system for paper records should be designed to meet regulatory requirements and should be an integral part of the QMS. Paper records should be controlled and managed according to the principles of ALCOA+. See Section 1.5.4.

In this appendix, the term "document" is used to reflect common usage for paper, and is aligned in approach and terminology with Eudralex: Rules Governing Medicinal Products in the European Union; Volume 4 Good Manufacturing Practice – Chapter 4: Documentation [6], where it states under "Principles" that *"there are two primary types of documentation used to manage and record GMP compliance: instructions (directions, requirements) and records/reports."*

The management of paper records is well established and well described in applicable regulations and regulatory guidance. This appendix provides a high-level overview of such expectations, but is intended to be neither prescriptive nor exhaustive. The relevant applicable regulations and guidance should be consulted when defining and designing a management system for paper records.

19.1.2 Overview

Procedures should be established for:

- Creation review and approval for use of documents and procedures (including instructions, records, and templates)
- Management of copies of documents for routine use, ensuring copies of documents and forms are issued and reconciled for use in a controlled and traceable manner
- Completion of paper based documents, including identification of individuals, data entry formats, and how amendments are recorded
- Routine review of completed documents for accuracy, authenticity and completeness
- Filing, retrieval, retention, archive, and disposal of documents

Detailed specific requirements depend on the nature of the document, and any applicable specific regulatory requirements.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

19.1.3 Management

An index of all documents (including template documents) should be maintained. All documents should be uniquely identifiable (including a version number) and should be checked, approved, signed, and dated, as appropriate [13].

Documents should be protected from unauthorized or inadvertent changes. The reproduction of document copies should not allow any error to be introduced through the reproduction process [6]. Different versions of templates should be maintained using change control.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Updated versions should be distributed in a timely manner. Procedures should ensure that only the current approved version is available for use [13]. Procedures should cover the generation and management of controlled copies.

Documents should be stored in an appropriately secure location in a traceable and accessible manner for the required retention period. Documents should be protected from damage, destruction, or unauthorized alteration [13].

Obsolete documents should be archived for the required retention period and access to them restricted.

Any issued and unused circulated copies of superseded documents should be withdrawn and destroyed [13]. Documents that have exceeded their retention period should also be destroyed, taking into account all applicable local and international laws and any ongoing litigation.

19.1.4 Use

Document design should make clear what data is to be recorded [13], and provide sufficient space for manual data entries.

The use of uncontrolled documents and the use of temporary recording practices should be prohibited [13], e.g., recording data on note paper prior to transferring it to the official record, such as a laboratory notebook or batch record.

Handwritten entries should be:

- Contemporaneous
- Made by the person who executed the task
- Clearly attributable to the individual
- Indelible
- Clear
- Legible

Unused, blank fields within documents should be marked as such (e.g., Not Applicable or N/A), dated and signed [13]. Date formats should be consistent, clear and unambiguous.

Corrections should be made in such a way as:

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568

- Not to obscure the original value (e.g., struck through with a single line)
- Indelible
- Dated

The person making the correction identified (e.g., by initial). Where appropriate, the reason for the alteration should be recorded.

Downloaded on: 6/19/19 11:34 AM

A process for review and/or verification of records as required by the applicable regulations should be established. The recording of such reviews and/or verifications should be follow good documentation practices.

For individual use only. © Copyright ISPE 2017. All rights reserved.

19.2 Hybrid Situations

19.2.1 Introduction

Paper and electronic record and signature components can coexist (i.e., a hybrid situation) as long as wider GxP requirements are met and the content and meaning of those records are preserved [16].

A formal risk assessment should be performed to ensure that suitable controls are in place and that all required data is retained. This Guide encourages a move away from hybrid situations wherever practical.

Where other options are available, hybrid situations should be avoided, as the long-term integrity of data and the link between hybrid components, e.g., paper signatures and electronic records, can be difficult to ensure.

Procedural controls may be needed to ensure the long-term integrity of data and to maintain links between hybrid components.

The presence of interfaces between paper based processes and electronic records and data processes increases the risk to data integrity. Regulated companies should plan to replace systems requiring hybrid situations.

19.2.2 Controls for Managing Hybrid Situations

Regulated companies should define and document which hybrid component is the primary record.

Suitable controls should be established and verified. These may include SOPs that define the process of controlling the signed paper record, and for making modifications to the paper and electronic records, if needed. Procedures should prevent the use of incorrect or out of date versions of records.

Examples include:

- **Procedure for signing paper copies:** procedures should define the creation, review, and approval of the paper record, including attached printouts of electronic records. Procedures should describe the link between the electronic record and the signed paper copy. The signed paper copy should be defined as the primary record.
- **Procedure for data retention/data integrity:** describing how data is managed and retained including:
  - Retention period requirements
  - Legibility for the required period
  - Retention of date and time stamps
  - Retention of data about the user who created the record (user ID)
  - Retention of associated metadata needed to preserve GxP content and meaning
  - Changes recorded using change control and audit trail
- **Access control:** this may be physical access control to the document control center for paper records.
- **Change control:** changes managed on paper with change SOP.
- **Audit trail:** no electronic audit trail is available; therefore, a paper audit trail could be maintained in the record, or maintained separately and linked by reference to the record.

This Document is licensed to
Carlos J. Cabrer
Valdez, PE
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

- **Transfer of data from old systems:** old systems may have retained data overwritten every time the system is used or after a period of time. Data for long term storage of the record should be stored by printing out and signing. Formal risk assessments should be used to determine what forms the complete record for transfer; this may include metadata.

Paper records which include attached electronic data may be retained as paper or by scanning into a separate electronic system for long term storage. These records require the same controls as described in this section, plus additional controls to be applied to the electronic storage system.

If a record in electronic format is used to support regulated activities or decisions, then a printed copy cannot be considered as the primary record. If only the paper copy is used, it may be possible to consider it as the primary record. In such cases, it may be possible to delete the electronic record.

Note: this reasoning does not apply to all records. While it may be acceptable for a validation report, it may not be appropriate for records where metadata is crucial to the integrity and meaning of the record, e.g., for chromatography, or for spreadsheets that manipulate data such as performing calculations.

19.2.3 Practical Difficulties with Hybrid Situations

Examples provided in this section of the appendix illustrate some practical difficulties with establishing and maintaining hybrid situations.

Chromatography Data

Usual practice has been to print out the chromatogram and approve it by applying signatures to the paper record and attaching the printout to the batch record. This does not capture all the required raw data to enable the sample to be rerun. Additional information related to the analytical method including setup, solvent gradient, base line noise suppression information, etc., should be retained.

The quantity and complexity of the raw data means that the data needs to be retained in the original computer system to ensure that samples can be reprocessed and compared. It cannot be managed on paper.

The management of chromatography data should be defined in a formal procedure that should include the ability to reprocess samples and compare all raw data. The scope of reprocessing includes reintegration of chromatograms. Resetting parameters describing changes are part of normal operation and should be recorded and controlled by change control and audit trail (manual intervention/integration) describing the retention of all raw data.

Risk assessment should look at the risks related to reprocessing samples and comparing the raw data. Any change of format and media should also be subject to risk assessment, as the data may be transferred to another system for long term storage.

This Document is licensed to
Carlos J. Cabrer
Varian, Inc.
Downloaded on: 6/10/19 11:24 AM

Spreadsheets

Recording production and laboratory data and calculating results is frequently performed using a spreadsheet. The spreadsheet can be used to record the data and can be configured to manipulate the data to obtain a result. These results can be printed out, reviewed, signed, and dated. The printout is retained in the paper batch record or laboratory record; therefore, the paper printout should be regarded as the primary record.

The spreadsheet should be regarded as the original data and adequately protected, unless the data has been stored separately and securely.

Spreadsheet records and calculations using templates should be verified and controlled as described in *ISPE GAMP® 5* [3].

For individual use only. © Copyright ISPE 2017. All rights reserved.

The use of spreadsheets should be described in a formal procedure and the risks related to managing and retaining these records should be formally assessed.

Production Equipment

Production equipment may collect electronic data which is printed out for subsequent review and approval as part of a paper batch record.

It may not be possible to record confirmation of key processing steps or record the management of primary data or fixed data. Changes may need to be recorded separately on the batch record system, e.g., changes made to:

- Machine settings
- Set points
- Processing instructions
- Warning/action alarms

A formal risk assessment should consider risks related to managing the retained data, including any changes to primary data.

The data may be transferred to another system for long term storage. Any change of format and media should also be subject to risk assessment.

Systems may retain information in a fixed size buffer, and information may be overwritten, once it becomes older information, or once the buffer is full. Critical data in such systems should be transferred to another system or to paper records to prevent its loss.

Older equipment may provide only physical access control or limited logical access, e.g., only one ID and password for all users. A formal risk assessment should consider risks related to unauthorized access/changes. Additional physical controls, procedures, and training may be required.

19.3 Use of Forms to Enforce Procedures

In primarily paper based or hybrid situations, the use of forms should be considered to capture data, and to ensure that all data required for each step of the process is recorded. Forms should include references to the data, standards, or SOPs that they support, to enable linkage to associated electronic records, and to assist with archiving.

Forms can be retained on paper or scanned into an electronic system for long term storage. Any change of format and media should be subject to formal risk assessment.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

20 Appendix G1 – References

1. MHRA GMP Data Integrity Definitions and Guidance for Industry, Revision 1.1, March 2015, www.gov.uk/government/publications/good-manufacturing-practice-data-integrity-definitions.

2. 21 CFR Part 11 – Electronic Records; Electronic Signatures, Code of Federal Regulations, US Food and Drug Administration (FDA), www.fda.gov.

3. *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems,* International Society for Pharmaceutical Engineering (ISPE), Fifth Edition, February 2008, www.ispe.org.

4. ISPE GAMP® guidance documents, International Society for Pharmaceutical Engineering (ISPE), http://www.ispe.org/publications-guidance-documents/series.

5. US Code of Federal Regulations (CFRs), https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR.

6. EudraLex Volume 4 – Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use, Chapter 4: Documentation, January 2011, http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

7. EudraLex Volume 4 – Guidelines for Good Manufacturing Practices for Medicinal Products for Human and Veterinary Use, Annex 11: Computerized Systems, June 2011, http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

8. MHRA GxP Data Integrity Definitions and Guidance for Industry, Draft version for consultation, July 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538871/MHRA_GxP_data_integrity_consultation.pdf.

9. FDA Draft Guidance for Industry: Data Integrity and Compliance with CGMP, April 2016, US Food and Drug Administration (FDA), www.fda.gov.

10. International Council for Harmonisation (ICH), ICH Harmonised Tripartite Guideline, *Quality Risk Management – Q9,* Step 4, 9 November 2005, www.ich.org.

11. International Council for Harmonisation (ICH), ICH Harmonised Tripartite Guideline, *Pharmaceutical Quality System – Q10,* Step 4, 4 June 2008, www.ich.org.

12. WHO Technical Report Series, No. 996, Annex 5: Guidance on Good Data and Record Management Practices, World Health Organization (WHO), 2016, http://apps.who.int/medicinedocs/en/d/Js22402en/.

13. PIC/S Draft Guidance: PI 041-1 (Draft 2) Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments, August 2016, Pharmaceutical Inspection Co-operation Scheme (PIC/S), https://www.picscheme.org/.

14. ISPEAK Blog Post, "Data Integrity, Critical Thinking & MHRA 2017, Oh My!" 21 October 2016, http://blog.ispe.org/critical-thinking-data-integrity-mhra.

15. MHRA Out Of Specification Investigations Guidance, August 2013, https://www.gov.uk/government/publications/out-of-specification-investigations.

16. FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application, August 2003, US Food and Drug Administration (FDA), www.fda.gov.

This Document is licensed to
Carlos J. Cabrer
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

17. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems,* International Society for Pharmaceutical Engineering (ISPE), Second Edition, December 2012, www.ispe.org.

18. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems,* International Society for Pharmaceutical Engineering (ISPE), First Edition, January 2010, www.ispe.org.

19. *ISPE GAMP® Concept Paper: Considerations for a Corporate Data Integrity Program,* International Society for Pharmaceutical Engineering (ISPE), March 2016, www.ispe.org.

20. Meyer, Erin, *The Culture Map,* Publisher: PublicAffairs, 2014, http://www.publicaffairsbooks.com/book/hardcover/the-culture-map/9781610392501.

21. Wingate, Guy, "Data Integrity: Management Factors and Effective Leadership," ISPE UK Annual Meeting presentation, 10 November 2016.

22. McAuley, Gerry, "Optimizing Human Performance," *BioPharm International,* July 2014, Volume 27, Issue 7.

23. Cressey, Donald R., *Other People's Money: A Study in the Social Psychology of Embezzlement,* Publisher: Patterson Smith, 1953.

24. 21 CFR Part 211 – Current Good Manufacturing Practice for Finished Pharmaceuticals, Code of Federal Regulations, US Food and Drug Administration (FDA), www.fda.gov.

25. US FDA Compliance Program Guidance Manual 7346.832: Pre-Approval Inspections, 2010, US Food and Drug Administration (FDA), www.fda.gov.

26. Association of Record Managers and Administrators (ARMA), www.arma.org.

27. American National Standards Institute (ANSI), www.ansi.org.

28. Stokes, David, "Compliant Cloud Computing – Managing the Risks," *Pharmaceutical Engineering,* July/August 2013, www.ispe.org.

29. ISPE GAMP® Cloud Computing Special Interest Group (SIG), "Cloud Computing in a GxP Environment: The Promise, the Reality and the Path to Clarity," *Pharmaceutical Engineering,* January/February 2014, www.ispe.org.

30. US FDA Field Science and Laboratories: Laboratory Manual, Volume III – Laboratory Operations, Applications and Programs, Section 4.5 – Development and Validation of Spreadsheets for Calculation of Data, https://www.fda.gov/ScienceResearch/FieldScience/LaboratoryManual.

31. DFS/ORA Laboratory Information Bulletin No. 4317, Spreadsheet Design and Validation for the Multi-User Application for the Chemistry Laboratory – Part I, 2004, Division of Field Science (DFS)/Office of Regulatory Affairs (ORA), US Food and Drug Administration (FDA), www.fda.gov.

32. 21 CFR Part 58.190 – Good Laboratory Practice (GLP) for Nonclinical Laboratory Studies; Storage and Retrieval of Records and Data, Code of Federal Regulations, US Food and Drug Administration (FDA), www.fda.gov.

33. EudraLex Volume 4 – Guidelines for Good Manufacturing Practices for Medicinal Products for Human and Veterinary Use, Chapter 6: Quality Control, October 2014, http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

For individual use only. © Copyright ISPE 2017. All rights reserved.

34. ISO/IEC Guide 51:2014 Safety Aspects -- Guidelines for their Inclusion in Standards, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

35. NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011, National Institute of Standards and Technology (NIST), www.nist.gov.

36. ISPE Glossary of Pharmaceutical and Biotechnology Terminology, www.ispe.org.

37. 21 CFR Part 58 – Good Laboratory Practice (GLP) for Nonclinical Laboratory Studies, Code of Federal Regulations, US Food and Drug Administration (FDA), www.fda.gov.

38. ISO Guide 73:2002 Risk Management – Vocabulary – Guidelines for Use in Standards, International Standards Organization (ISO), www.iso.org.

39. FDA Guidance for Industry: Electronic Source Data in Clinical Investigations, September 2013, US Food and Drug Administration (FDA), www.fda.gov.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

21 Appendix G2 – Glossary

21.1 Acronyms and Abbreviations

ADR	Adverse Drug Reaction
AE	Adverse Event
ALCOA	Attributable, Legible, Contemporaneous, Original, Accurate
ALCOA+	ALCOA, with the addition of Complete, Consistent, Enduring, Available
ANSI	American National Standards Institute (US)
API	Active Pharmaceutical Ingredient
AQL	Acceptable Quality Limit or Acceptance Quality Level
ARMA	Association of Record Managers and Administrators (US)
CAPA	Corrective and Preventive Action
CDO	Chief Data Officer
CEO	Chief Executive Officer
CDS	Chromatography Data System
CGMP	Current Good Manufacturing Practice
CFR	Code of Federal Regulations
CMMI	Capability Maturity Model Integration
DBA	Data Base Administrator
DS	Design Specification
EDMS	Electronic Document Management System
ERP	Enterprise Resource Planning
EU	European Union
FAQ	Frequently Asked Questions
FDA	Food & Drug Administration (US)
FS	Functional Specification
GAMP®	Good Automated Manufacturing Practice
GC	Gas Chromatography

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

GCP	Good Clinical Practice
GDP	Good Distribution Practice
GDocP	Good Documentation Practice
GEP	Good Engineering Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GPvP	Good Pharmacovigilance Practice
GVP	Good Pharmacovigilance Practices
GxP	Good "x" Practice
HR	Human Resources
IaaS	Infrastructure as a Service
ICH	International Council for Harmonisation
IT	Information Technology
JPEG	Joint Photographic Experts Group
KPI	Key Performance Indicator
LC	Liquid Chromatography
LIMS	Laboratory Information Management System
MES	Manufacturing Execution System
MHRA	Medicines and Healthcare Products Regulatory Agency (United Kingdom)
OS	Operating System
OOS	Out of Specification
PaaS	Platform as a Service
PC	Personal Computer
PDF	Portable Document Format
PIC/S	Pharmaceutical Inspection Convention and Pharmaceutical Inspection Cooperation Scheme
QA	Quality Assurance
QC	Quality Control

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
ID number: 1568
Downloaded on: 6/10/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

QMS	Quality Management System
QRM	Quality Risk Management
RAID	Redundant Array of Independent Disks
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SDS	Software Design Specification
SGML	Standard Generalized Markup Language
SLA	Service Level Agreement
SME	Subject Matter Expert
SOP	Standard Operating Procedure
UAT	User Acceptance Test
UPS	Uninterruptible Power Supply
URS	User Requirements Specification
WHO	World Health Organization
XML	eXtensible Markup Language

21.2 Definitions

Atypical / Aberrant / Anomalous Result (MHRA Out Of Specification Investigations Guidance [15])

This Document is licensed to

Results that are still within specification but are unexpected, questionable, irregular, deviant or abnormal. Examples would be chromatograms that show unexpected peaks, unexpected results for stability test point, etc.

Carlos J. Cabrer
Valrico, FL

Biometrics (US FDA, 21 CFR Part 11 [2])

A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

Critical Thinking

Downloaded on: 6/19/19 11:34 AM

A systematic, rational, and disciplined process of evaluating information from a variety of perspectives to yield a balanced and well-reasoned answer.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Data Governance (MHRA, 2015 [1])

The sum total of arrangements to ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data life cycle.

Data Integrity (MHRA, 2015 [1])

The extent to which all data are complete, consistent and accurate throughout the data life cycle.

Data Owner

The person ultimately responsible for the integrity and compliance of specific data at various stages of the data life cycle in accordance with applicable policies and SOPs. The Data Owner may also be the Process Owner.

Data Steward

A person with specific tactical coordination and implementation responsibilities for data integrity, responsible for carrying out data usage, management and security policies as determined by wider data governance initiatives, such as acting as a liaison between the IT department and the business. They are typically members of the operational unit or department creating, maintaining, or using the data, for example personnel on the shop floor or in the laboratories who actually generate, manage, and handle the data.

Detectability (ICH Q9 [10])

The ability to discover or determine the existence, presence, or fact of a hazard.

Digital Signature (US FDA, 21 CFR Part 11 [2])

An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Electronic Record (US FDA, 21 CFR Part 11 [2])

Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature (US FDA, 21 CFR Part 11 [2])

A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

GxP Regulated Computerized System (*ISPE GAMP® 5* [3])

Computerized systems that are subject to GxP regulations. The regulated company must ensure that such systems comply with the appropriate regulations.

This Document is Licensed to
Carlos J. Cabrer
Varico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

GxP Regulation

The underlying international pharmaceutical requirements, such as those set forth in the US FD&C Act, US PHS Act, FDA regulations, EU Directives and guidelines, Japanese regulations, or other applicable national legislation or regulations under which a company operates. These include but are not limited to:

- Good Manufacturing Practice (GMP) (pharmaceutical, including Active Pharmaceutical Ingredient (API), veterinary, and blood)
- Good Clinical Practice (GCP)
- Good Laboratory Practice (GLP)
- Good Distribution Practice (GDP)
- Good Pharmacovigilance Practice (GVP, also known as GPvP)

Harm (ICH Q9 [10])

Damage to health, including the damage that can occur from loss of product quality or availability.

Hazard (ISO/IEC Guide 51 [34])

The potential source of harm

Hybrid Situation

A situation where paper and electronic record and signature components co-exist.

Infrastructure as a Service (IaaS) (NIST Special Publication 800-145 [35])

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components e.g. host firewalls.

Likelihood of Occurrence

This Document is licensed to
Carlos J. Cabrer
Valtech Inc
Downloaded on: 6/19/19 11:34 AM

The probability of a hazard occurring and causing harm.

Metadata (MHRA, 2016 [8])

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. It also permits data to be attributable to an individual (or if automatically generated, to the original data source).

Out of Specification (OOS) (ISPE Glossary [36])

An examination, measurement, or test result that does not comply with pre-established criteria.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Platform as a Service (PaaS) (NIST Special Publication 800-145 [35])

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment

Primary Record (MHRA, 2015 [1])

The record which takes primacy in cases where data that are collected and retained concurrently by more than one method fail to concur.

Probability of Detection

The probability that a fault will be detected before harm occurs.

Process Owner (*ISPE GAMP® 5* [3])

The person ultimately responsible for the business process or processes being managed.

Quality Risk Management (QRM) (ICH Q9 [10])

A systematic process for the assessment, control, communication and review of risks to the quality of the drug (medicinal) product across the product lifecycle.

Raw Data

1. Any laboratory worksheets, records, memoranda, notes, or exact copies thereof, that are the result of original observations and activities of a nonclinical laboratory study and are necessary for the reconstruction and evaluation of the report of that study. In the event that exact transcripts of raw data have been prepared (e.g., tapes which have been transcribed verbatim, dated, and verified accurate by signature), the exact copy or exact transcript may be substituted for the original source as raw data. Raw data may include photographs, microfilm or microfiche copies, computer printouts, magnetic media, including dictated observations, and recorded data from automated instruments. (US FDA, 21 CFR Part 58, Subpart A--General Provisions, Sec. 58.3 [37])

2. All original nonclinical laboratory study records and documentation or exact copies that maintain the original intent and meaning and are made according to the person's certified copy procedures. Raw data includes any laboratory worksheets, correspondence, notes, and other documentation (regardless of capture medium) that are the result of original observations and activities of a nonclinical laboratory study and are necessary for the reconstruction and evaluation of the report of that study. Raw data also includes the signed and dated pathology report. (US FDA, 21 CFR Part 58, Subpart A--General Provisions, Sec. 58.3 Definitions – Proposed Amendment in Federal Register, 81 FR 58341, 22 November 2016 [37])

Document Creator
Valrico, FL
ID number: 1568
Downloaded on: 6/19/19 11:34 AM

Regulated Data

Information used for a regulated purpose or to support a regulated process.

Regulated Record

A collection of regulated data (and any metadata necessary to provide meaning and context) with a specific GxP purpose, content, and meaning, and required by GxP regulations. Records include instructions as well as data and reports.

For individual use only. © Copyright ISPE 2017. All rights reserved.

Regression Testing

Testing geared toward demonstrating that a change has not affected a system or part of a system that it was not intended to affect.

Risk (ISO/IEC Guide 51 [34])

The combination of the probability of occurrence of harm and the severity of that harm.

Risk Assessment (ICH Q9 [10])

A systematic process of organizing information to support a risk decision to be made within a risk management process. It consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.

Risk Control (ISO Guide 73 [38])

Actions implementing risk management decisions.

Risk Identification (ICH Q9 [10])

The systematic use of information to identify potential source of harm (hazards) referring to the risk question or problem description.

Software as a Service (SaaS) (NIST Special Publication 800-145 [35])

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user- specific application configuration settings.

Service Level Agreement (SLA)

An agreement between an IT service provider and a customer. The SLA describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple services or multiple customers.

Severity (ICH Q9 [10])

A measure of the possible consequences of a hazard.

Source Data (FDA Guidance for Industry: Electronic Source Data in Clinical Investigations [39])

All information in original records and certified copies of original records of clinical findings, observations, or other activities (in a clinical investigation) used for the reconstruction and evaluation of the trial. Source data are contained in source documents (original records or certified copies).

System Owner (*ISPE GAMP® 5* [3])

The person ultimately responsible for the availability, and support and maintenance, of a system and for the security of the data residing on that system.

This Document is licensed to
Carlos J. Cabrer
Valrico, FL
Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

This Document is licensed to

Carlos J. Cabrer
Valrico, FL
ID number: 1568

Downloaded on: 6/19/19 11:34 AM

For individual use only. © Copyright ISPE 2017. All rights reserved.

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

www.ISPE.org