GAMP Good Practice Guide:

A Risk-Based Approach to Compliant Electronic Records and Signatures

ISPE
Engineering Pharmaceutical Innovation

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Preface to the GAMP Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures

The appropriate management of electronic records and signatures is of current concern to both the regulated life science industry and its regulators. This *GAMP Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures* provides timely and much needed guidance on meeting current regulatory expectations for compliant electronic records and signatures, which include the need for record integrity, security, and availability throughout the required retention period.

It describes how a risk management approach may be used to ensure the compliance of regulated electronic records and signatures, through the application of appropriate controls commensurate with the impact of records and signatures and the identified risks. The Guide covers:

- New automated systems
- Existing automated systems
- Those systems that have already been subject to electronic record and signature assessments

This Guide is intended as a supplement to the *GAMP Guide for Validation of Automated Systems (GAMP 4)*. It has been designed so that it may be used in conjunction with guidance provided in GAMP 4 and other ISPE publications.

Disclaimer:
This Guide is meant to assist pharmaceutical manufacturing companies in managing systems which use and maintain regulated electronic records and signatures. The GAMP Forum 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 (including the GAMP Forum), or the officers, directors, employees, members, or agents of each of them, 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 2005.

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.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Acknowledgements

This document was an international collaboration, produced by the GAMP Europe and GAMP Americas Steering Committees, under the overall direction of Guy Wingate (GSK), Chair of the GAMP Council. The document was coordinated on their behalf by Tony Margetts (Margetts Associates) and Colin Jones (Conformity Ltd.).

GAMP Americas Steering Committee

Rory Budihandojo	Schering-Plough Corp.
Tom Burrus	GlaxoSmithKline
Paul D'Eramo	Johnson & Johnson
Bob Herr	Covance
Jim John	CimQuest Inc.
Klaus Kraus	Amgen Inc.
Kevin Martin	CimQuest Inc.
Barbara Mullendore	Watson Pharmaceuticals Inc.
Arthur 'Randy' Perez	Novartis Pharmaceuticals Corp.
Mike Rutherford	Eli Lilly & Co.
Lorrie Schuessler	GlaxoSmithKline
Mike Wyrick	Washington Group International

GAMP Europe Steering Committee

Sam Brooks	Novartis Consumer Health SA
Mark Cherry	AstraZeneca
Chris Clark	Napp Pharmaceuticals Ltd.
Peter Coady	Pfizer
Mark Foss	Boehringer Ingelheim
Heinrich Hambloch	GITP
Hartmut Hensel	Hochschule Harz
Niels Holger Hansen	Novo Nordisk A/S
Paige Kane	Wyeth Medica Ireland
Scott Lewis	Eli Lilly & Co. Ltd.
Tony Margetts	Margetts Associates
Chris Reid	Integrity Solutions Ltd.
Peter Robertson	AstraZeneca
Kate Samways	KAS Associates Ltd.
David Selby	Selby Hope International Ltd.
Rob Stephenson	Pfizer Global Mfg.
Anthony J. Trill	UK MHRA
Guy Wingate	GlaxoSmithKline
Sion Wyn	Conformity Ltd.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

In addition to members of the above committees, the GAMP Council would like to thank the following for contributing material or coordinating reviews:

Anders Bredesen	YIT Building Systems AS
John Farrell	Synapse Partnership
Kathy Gniecko	Hoffmann-La Roche Inc.
Jerry Hare	GlaxoSmithKline
Madeleine Kennedy	Eli Lilly & Co.
Gale Robinson	CimQuest Inc.
Paul Seelig	Merck (retired)
Nader Shafiei	Aventis
Leonard Smyth	Invensys Validation Technologies
Gail Utnage	GlaxoSmithKline
Wendy Westlund	GlaxoSmithKline
Frank Woods	GlaxoSmithKline

The GAMP Council also would like to thank the following groups for providing and reviewing material:

- GAMP Americas coordinated by Arthur 'Randy' Perez
- GAMP Europe coordinated by Chris Clark
- GAMP Japan coordinated by Makato Koyazaki (Shimadzu Corp.), Yuichi Watanabe (Banyu Pharmaceutical Co. Ltd.), and Bunpei Matoba (IBM Business Consulting Services)
- GAMP Nordic coordinated by Niels Holger Hansen
- GAMP DACH coordinated by Peter Bosshard (F. Hoffmann La-Roche AG)
- GAMP European Suppliers Group coordinated by Chris Reid

The GAMP Council would like to thank PhRMA for their review and valuable comments on this GAMP Good Practice Guide. The commenting process was coordinated by Madeleine Kennedy, Ph.D.

The GAMP Council would like to thank the following regulators for their review:

Regulatory Reviewers

Karl-Heinz Menges	RPDA (Germany)
George Smith	FDA (US)
Robert Tollefsen	FDA (US)
Anthony J. Trill	MHRA (UK)

The GAMP Council would like to thank all those involved in the worldwide review of this Guide during 2004. To view this list please go to www.ispe.org/gamp/.

The GAMP Editorial Team on behalf of ISPE was Gail Evans, Colin Jones, Tony Margetts, Arthur 'Randy' Perez and Sion Wyn.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table of Contents

1 Introduction 6
1.1 Overview 6
1.2 Purpose 6
1.3 Scope 7
1.4 Benefits 8
1.5 Objectives 8
1.6 Structure of this Guide 9
1.7 Key Concepts 9
1.8 Current Regulatory Situation 11

2 Risk Management Process 11
2.1 Overview of Process 11
2.1.1 Current Risk Management Practices 11
2.1.2 Managing Risks to Electronic Records 12
2.1.3 Risk Management Based on the Impact of Records 14
2.2 Step 1: Identify Regulated Electronic Records and Signatures 15
2.3 Step 2: Assess Impact of Electronic Records 16
2.4 Step 3: Assess Risks to Electronic Records Based on Impact 20
2.4.1 Approach for Records Identified as Low Impact 20
2.4.2 Approach for Records Identified as Medium Impact 20
2.4.3 Approach for Records Identified as High Impact 21
2.4.4 Hazards 21
2.5 Step 4: Implement Controls to Manage Identified Risks 23
2.6 Step 5: Monitor Effectiveness of Controls 23
2.7 Points to Consider 24

3 Applying the Risk Management Process 25
3.1 Corporate Level Activities 28
3.2 Applying the Process to New Systems 30
3.3 Applying the Process to Existing Systems 31
3.4 Systems Previously Assessed Against 21 CFR Part 11 32

4 Controls 34
4.1 Record Controls 34
4.1.1 Implementation of Controls 34
4.1.2 Rigor of Controls 39
4.2 Signature Controls 39
4.3 Managing Hybrid Records 41
4.4 User/Supplier Responsibilities 42
4.4.1 Procedural Requirements (responsibility of user) 42
4.4.2 Technical Requirements (largely the responsibility of supplier) 43

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table of Appendices

Appendix 1 **Validation**

Appendix 2 **Audit Trail and Data Security**

Appendix 3 **Record Retention, Archiving, and Migration**

Appendix 4 **Copies of Records**

Appendix 5 **21 CFR Part 11 Legacy Systems**

Appendix 6 **Examples of Records and Signatures Required by GxP Regulations**

Appendix 7 **Case Studies**

Appendix 8 **Copy of GAMP 4, Appendix M3**

Appendix 9 **Example Template Form for Risk Assessment and Identification of Controls**

Appendix 10 **Form for Previously Assessed 21 CFR Part 11 Systems**

Appendix 11 **Current Regulatory Situation**

Appendix 12 **Glossary**

Appendix 13 **References**

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

1 Introduction

1.1 Overview

The increased use of information technology and computer systems in all aspects of business is leading to the automation of more and more processes. Key decisions and actions are routinely being taken using automated systems, with regulated records being generated electronically. Increasingly, confirmation and approval of these actions and decisions is also being provided electronically.

As a result, the appropriate management of electronic records and signatures is a very important topic for the life science industries.

This Guide has been developed by the GAMP Forum, a technical subcommittee of ISPE, to provide timely and much needed guidance in this area. It supplements the existing *GAMP 4, GAMP Guide for Validation of Automated Systems* (see Appendix 13, reference 1).

Good Automated Manufacturing Practice (GAMP) guidance aims to achieve validated and compliant automated systems meeting all current life science regulatory expectations, by building upon existing industry good practice in an efficient and effective manner.

1.2 Purpose

This Guide provides comprehensive new guidance on meeting current regulatory expectations for compliant electronic records and signatures, which includes the need for record integrity, security, and availability throughout the required retention period. This is achieved by well-documented, validated systems, and the application of appropriate operational controls.

The main drivers for this Guide are:

1. An increasing emphasis on the assessment and management of risk within the regulated environment

2. The need to consider and comply with all applicable international regulations

3. Recent regulatory activity and guidance, such as FDA guidance on 21 CFR Part 11 Scope and Application (see Appendix 13, reference 3).

This Guide supersedes previous guidance published jointly by ISPE and PDA, Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures (see Appendix 13, reference 2).

The guidance is intended primarily for regulated companies, but will also be useful for suppliers of systems, products, or services in this area.

The intended audience for this Guide includes:

- Quality assurance (QA) and computer validation professionals responsible for defining and managing validation practices in regulated life science industries

- IT personnel, including IT compliance, who manage and support these systems

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

- Business owners, data owners, and system users
- System developers, engineers and suppliers

Some familiarity with GAMP and current international regulations is assumed.

1.3 Scope

This Guide addresses compliance with international regulations and guidelines for electronic records and signatures covering automated systems used within the regulated life science industries including pharmaceutical, biological, and medical devices. While not specifically targeted as such, this Guide may also be useful in other regulated areas such as cosmetics and food. Specific guidance is given for:

- New automated systems
- Existing automated systems
- Those systems that have already been subject to electronic record and signature assessments

Current international GxP life science requirements related to electronic records and signatures have been taken into account, and the following publications have been specifically considered:

- US Codes of Federal Regulations (CFRs) covering GCP, GLP, GMP, and medical devices
- US CFR regulation 21 CFR Part 11, and associated guidance documents
- Relevant sections of EU regulations
- PIC/S (Pharmaceutical Inspection Convention/Pharmaceutical Inspection Co-operation Scheme) Guidance
- Proposed Japan MHLW (Ministry of Health, Labour and Welfare) guidelines
- European Medicines Agency (EMEA) guidance
- World Health Organization (WHO) guidelines
- International Conference on Harmonization (ICH) guidelines
- International Society of Blood Transfusion (ISBT) guidelines
- Relevant ISO documents, such as ISO 14971 Medical devices - Application of risk management to medical devices and ISO 17799:2000 Information technology - Code of practice for information security management

This Guide covers electronic records, electronic signatures, handwritten signatures captured electronically, and handwritten signatures applied to electronic records. The Risk Management approach described applies to records generally. While paper, electronic and hybrid situations are considered, the detailed activities described are focused on the electronic aspects.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

This Guide provides a method for managing risk to electronic records and signatures. Organizations may already have established risk management activities, including the use of methods such as HAZOP, CHAZOP, FMEA, FMECA, FTA, and HACCP. While the Guide may encourage organizations to perform new activities, it 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.

While not within the scope of this Guide, it is recognized that aspects such as business criticality, health and safety, and environmental requirements may require specific assessment and control. Legal admissibility of information stored electronically should also be considered.

Note that this Guide provides one method of managing risk. It is not intended to imply that this is the only acceptable method of managing risks associated with regulated electronic records, or that companies not using the process will be failing to comply with regulations. Other methods or techniques giving documented evidence of adequate record control, ensuring appropriate record security and integrity, may also be acceptable.

1.4 Benefits

This GAMP Good Practice Guide applies a risk management approach to the identification, management, and control of electronic records and signatures in a regulated GxP context. This allows the implementation of technical and procedural controls appropriate to the impact of records, and to the risks to those records. As a result, a simple and pragmatic approach is described that can be applied to any automated system required to meet international regulations.

The approach allows measures aimed at a high degree of integrity, availability, and confidentiality (where required) to be established for records that have a high potential impact on product quality or patient safety, while permitting a less rigorous approach for records of lower impact, or those with lower levels of associated risk.

This overall philosophy is intended to encourage innovation and technological advances while avoiding unacceptable risk to product quality, patient safety, and public health.

1.5 Objectives

Risk management practices for electronic record and signature controls must protect public health. In order to be effective, however, risk management practices must also be practical and efficient. To this end the GAMP Council defined the following guiding principles for this Guide:

- Provide a consistent risk management approach to electronic records and signatures to address what are now similar expectations from international agencies.
- Adopt the philosophy of managing risk by defining minimum acceptable requirements to address electronic records and signatures. Any additional controls should be justified on the basis of tangible business benefit.
- Ensure the risk management approach to electronic records and signatures is simple and effective. The effort required to assess and manage risk must not outweigh the benefit of its application.
- Facilitate ready and meaningful access to international regulations identifying regulated records and signatures. It is important to focus on records and signatures with significant potential impact on product quality or patient safety.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

- Ensure the new risk management approach to achieving compliant electronic records and signatures recognizes the need to minimize transition issues with any existing programs of remediation work.

- Emphasize the benefits, and encourage the use of technology, rather than introduce discouraging barriers.

The GAMP Council believes that the guidance developed has met these criteria. A single approach to risk management for electronic records and signatures is described that should be acceptable in all main regulated markets. The approach permits the adoption of electronic record and signature controls appropriate to the market supported.

1.6 Structure of this Guide

This Guide consists of a Main Body and a set of supporting Appendices.

Following the introductory and background material, the Main Body describes a process for managing risks to electronic records and signatures. It then explains how the process should be applied to existing and new systems, and provides particular guidance for those organizations who have already undertaken remediation programs to comply with 21 CFR Part 11. Finally, the Main Body considers the various controls that may be used to manage identified risks.

The Appendices cover a range of common issues of concern, as well as reference and supporting materials. These include:

- Validation

- Audit trail and data security

- Record retention and archiving

- Copies of records

- Legacy systems

- Examples of records required by GxP regulations

- Examples of signatures required by GxP regulations

- Case studies

- Template forms to support the processes described

- Current regulatory situation

1.7 Key Concepts

The term *GxP regulation* refers to the underlying international life science requirements such as those set forth in the US FD&C Act, US PHS Act, FDA regulations, EU Directives, Japanese MHLW regulations, or other applicable national legislation or regulations under which a company operates.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

A *regulated record* is one required to be maintained or submitted by GxP regulations. A regulated record may be held in different formats, for example, electronic, paper, or both.

Electronic record refers to records required by GxP regulations such as clinical study reports, training records, or batch records when maintained in electronic format. Where emphasis is needed in order to avoid possible misunderstanding, the term *regulated electronic record* is used. Regulated electronic records include Part 11 records as defined by FDA. Appendix 6 of this Guide provides examples of records required by GxP regulations.

Note that some records are required to support regulated activities, despite them not being explicitly specified in the regulations. For example, monitoring records are not required by all regulations. However, monitoring is a regulated activity and reports are relied upon for performing this regulated activity.

A *regulated signature* is a signature required by a GxP regulation. The terms *signature* and *signed* are defined as *"The record of the individual who performed a particular action or review. This record can be initials, full handwritten signature, personal seal, or authenticated and secure electronic signature."* (ICH Guideline Q7A, (see Appendix 13, reference 12)). Appendix 6 of this Guide provides an interpretation with examples of signatures and identifications required by GxP regulations.

Company is used in this Guide to refer to the regulated entity (such as company, partnership, corporation, or association). It is synonymous with the term "firm", as used by the FDA, and "User Company" as used in *GAMP 4* (see Appendix 13, reference 1).

Impact is a measure of the possible consequences of loss or corruption of a record.

The following terms used in this Guide are taken from ISO 14971 Medical Devices - Application of risk management to medical devices (see Appendix 13, reference 4) except where specified:

- **Harm:** physical injury or damage to the health of people, or damage to property or the environment
- **Hazard:** potential source of harm
- **Risk:** combination of the probability of occurrence of harm and the severity of that harm
- **Risk assessment:** overall process comprising a risk analysis and a risk evaluation:
  - **Risk analysis:** systematic use of available information to identify hazards and to estimate the risk
  - **Risk evaluation:** judgment, on the basis of risk analysis, of whether a risk which is acceptable has been achieved in a given context (ISO 14971 definition modified by GAMP)
- **Risk control:** process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels
- **Risk management:** systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, and controlling risk
- **Severity:** measure of the possible consequences of a hazard

Appendix 12 (Glossary) of this Guide contains further definitions and acronyms.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

1.8 Current Regulatory Situation

Since the effective date of 21 CFR Part 11 in August 1997, there has been much discussion and debate among regulated life science companies, their regulators, and suppliers regarding the effective implementation of compliant electronic records and signatures.

Recent regulatory developments in Europe, Japan, and the US will fundamentally alter the way industry approaches this subject.

The US FDA are currently (at time of printing) re-examining 21 CFR Part 11 and may propose changes to the regulation as a result. FDA's most recent thinking on 21 CFR Part 11 is reflected in the guidance document on the scope and application of 21 CFR Part 11 (see Appendix 13, reference 3), published on 3 September 2003. The guidance describes how FDA intends to interpret the scope of 21 CFR Part 11 narrowly, and intends to exercise enforcement discretion with respect to certain 21 CFR Part 11 requirements during the re-examination period. The guidance also describes the current FDA thinking on key topics in this area, such as validation, audit trails, record copying, and record retention, and describes the role of justified and documented risk assessment in selecting appropriate controls.

Similarly, European, Japanese, and other international regulators and agencies have been active in this area (see Appendix 13, references 5, 9, 11).

2 Risk Management Process

2.1 Overview of Process

2.1.1 Current Risk Management Practices

Risk management is an integral element of good project management practice. Initial risk assessments are carried out during project start-up phases, when project scope is being defined, initial requirements and plans are being drafted, project sponsors are being identified, and budgetary approval is being sought. Risks to the overall project that might affect the capability to meet objectives, timescales, cost, quality, and safety are identified and considered. Following assessment, risks are then prioritized, monitored, and managed on an on-going basis as the project proceeds. Depending upon criticality and nature, some projects schedule further detailed risk assessments (e.g., hazard and operability studies, threats and controls studies, or failure mode and effect analysis) as functionality and design is developed.

Risks to product quality and patient safety are particularly important for life science industries. These risks have typically been assessed at the system level and the following topics considered:

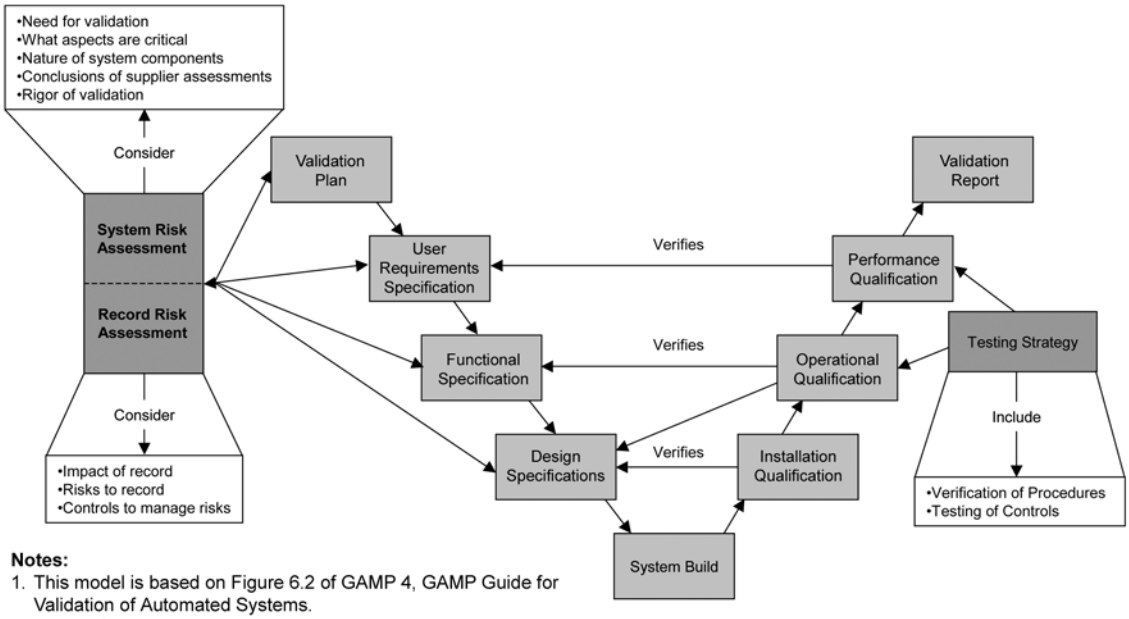
- Need for validation based upon the processes being managed and supported
- Criticality of the system based upon functionality and operation
- Nature of system components (e.g., custom software, configurable software packages, standard software packages)
- Outcomes and conclusions of supplier assessments
- Rigor of validation based upon system criticality and vulnerability

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

These activities may be incorporated within a typical validation process as shown in Figure 2.1. While the approaches to system level assessments vary from company to company, the guidance provided in Appendix M3 of *GAMP 4, GAMP Guide for Validation of Automated Systems* (see Appendix 13, reference 1) describes one approach. See also IEEE 1540 Standard for Software Lifecycle Processes - Risk Management (see Appendix 13, reference 13) for further guidance on this topic. In all cases, the conclusions of these assessments influence the validation strategy for the system.

To date the assessment and management of risks specific to electronic records and signatures have not typically formed part of this process. Figure 2.1 shows how these activities may be added to the typical validation process. It should be noted that this Guide does not intend or imply that any existing methods such as HAZOP, CHAZOP, FMEA, FMECA, FTA, and HACCP already used by organizations should be discarded, but rather that they continue to be used as appropriate within the context of the overall risk management process described.

Figure 2.1: Risk Management as part of the Validation Process



Notes:
1. This model is based on Figure 6.2 of GAMP 4, GAMP Guide for Validation of Automated Systems.
2. The URS may be developed before the Validation Plan, or in parallel.
3. Controls should also be considered during design reviews and code reviews, where applicable.

2.1.2 Managing Risks to Electronic Records

Managing risks to electronic records and signatures involves the following activities:

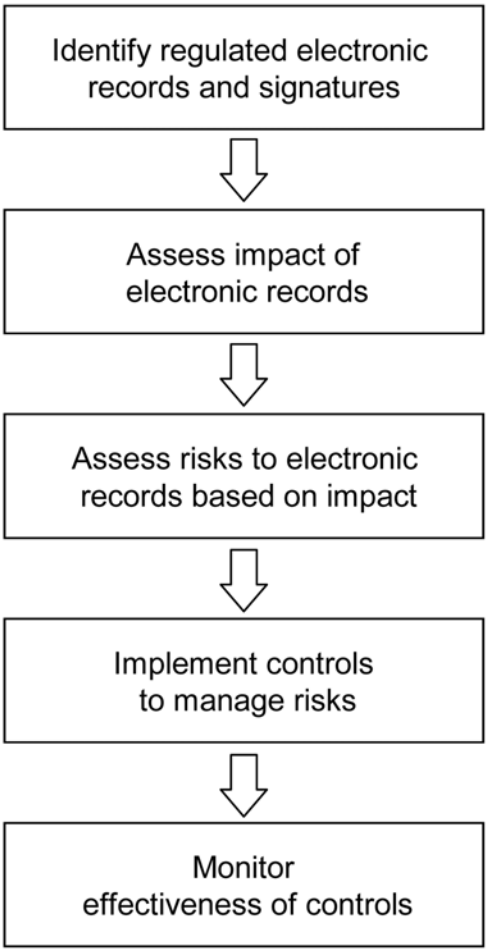
- Identifying which regulated electronic records are maintained in the system and where signatures are applied to those records, based on an analysis of the processes, and the applicable regulations.
- Assessing the impact of the electronic records on product quality or patient safety.
- Assessing the risks to the electronic records using a scaleable approach based on the impact of the records.
- Implementing controls to manage the identified risks, and verifying that the controls have been successfully implemented.
- Monitoring the effectiveness of controls during operation.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

The objective of these activities is to reduce risks to product quality or patient safety to an acceptable level and to comply fully with GxP regulations. These activities are shown as a series of steps in Figure 2.2:

Figure 2.2: Managing Risks to Electronic Records



Where appropriate, during development of User Requirements and then Functional Specifications, business processes should be defined and the associated electronic records and signatures identified. The impact of the electronic records can then be established, risks assessed, and controls identified. More detailed assessments may be performed as the life cycle progresses and more information becomes available.

Similar records (e.g., training records) may be grouped by type, so that a consistent risk management approach can be applied to all records of that type either within individual projects or across the organization.

Controls may be technical or procedural in nature. Technical controls should be included in the relevant specification and identified procedures should be developed for the system.

Verification of the installation and correct operation of controls occurs during qualification.

It is recommended that the activities to manage specific risks associated with regulated electronic records and signatures be incorporated into the company's overall quality and project management system, and validation planning strategy.

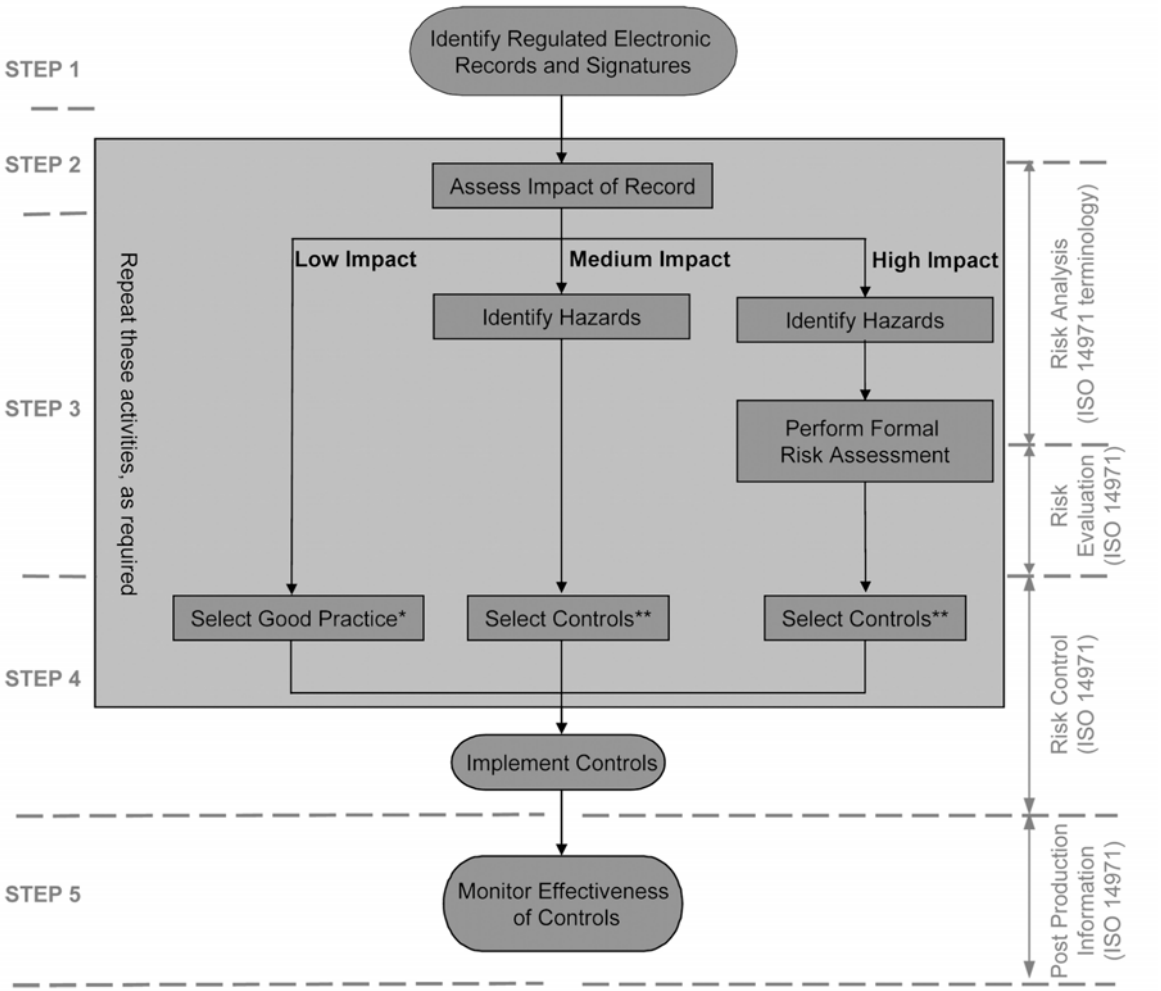
Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

2.1.3 Risk Management Based on the Impact of Records

This Guide describes a risk management process based on the impact of the record, or type of record, on product quality or patient safety.

Depending upon the impact, a suitable risk management approach is taken, as shown in Figure 2.3. The purpose of this approach is to allow selection of appropriate controls while ensuring that the effort to assess and manage risk does not outweigh the benefit of its application.

Figure 2.3: Risk Management Approach based on Record Impact



* Good Practice covers Good IT Practice and Good Engineering Practice, such as backup and restore, and security management.
**In addition to Good Practice.

Subsequent sections provide more detailed guidance on each of the steps shown in Figure 2.3:

Step 1: Identify regulated electronic records and signatures

Step 2: Assess impact of electronic records

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Step 3: Assess risks to electronic records based on impact

Step 4: Implement controls to manage identified risks

Step 5: Monitor effectiveness of controls during operation

A suitable cross-functional team, made up of individuals representing QA, system owner and users, IT, and engineering, as appropriate, should perform these activities. The team should include the electronic record or data owners, where these have been defined.

2.2 Step 1: Identify Regulated Electronic Records and Signatures

Each regulated record or record type in the system should be identified and documented. A data flow analysis is useful in supporting this activity and in determining the role of each record in regulated processes. The emphasis should be on identifying records required by regulations such as clinical study reports, training records, or batch records, rather than physical database records, or table fields. Some electronic records may be created and maintained on one system and electronic copies transferred and used by other systems. Companies should ensure that the approach taken with these copies makes maximum use of existing assessments in order to avoid unnecessary repetition.

Each signature or signature type (e.g., preclinical study approval) should also be identified. Whether or not the signed record is used for regulatory purposes should be decided and the conclusion documented.

Appendix 6 gives examples of records and signatures required by GxP regulations.

It should be noted that many systems, such as typical microprocessor or PLC controlled manufacturing equipment or laboratory equipment, do not generate or hold any regulated electronic records. Such determinations should be documented and no further analysis is required.

Other systems do not maintain electronic records required by GxP regulations although data relating to regulated records is processed. An example might be a measurement device or system capturing data to be passed on to another system, where it is later incorporated into a regulated record. Again, such determinations should be documented and no further analysis is required.

Some systems generate large amounts of intermediate data which is used to generate the regulated records upon which quality decisions are based. Only those records required to meet GxP regulations, or submitted to regulators, should be identified as regulated electronic records and not all data captured, generated, or held by such systems. For example, a validated system measures two million capsule weights for a single batch. The system generates a curve showing that batch weight distribution falls within validated norms. The individual data points would not be considered as regulated records.

Some systems are used to generate a record which is subsequently printed out, and it is the printed paper copy that is retained and used as the regulated record. It may be that the electronic record is only being used as a transitional phase in the creation of the paper record. A documented determination should be made of whether the electronic or paper record (or both) will be relied upon to perform regulated activities.

Software code, internal system configurations, and technical parameters are not regulated electronic records as described in this Guide. These are controlled by validation, change control, and configuration management.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

2.3 Step 2: Assess Impact of Electronic Records

Impact assessment allows the selection of the appropriate approach to risk management for an identified record or record type. The conclusions of the impact assessment should be documented.

Impact should not be determined solely by the requirement for a record in a GxP regulation, but by an assessment of the potential impact of the record on patient safety or product quality. Regulated electronic records should be classified as one of High, Medium, or Low. While there is a continuous scale of impact, the following provides an indication:

- **High impact** records typically have a direct impact on product quality or patient safety, such as batch release or adverse event records.

- **Medium impact** records typically have an indirect impact on product quality or patient safety. These records are used as supporting evidence of compliance, such as validation documentation or training records.

- **Low impact** records typically have negligible impact on product quality or patient safety. Such records may be used to support regulated activities, but are not key evidence of compliance. For example, calibration scheduling records are typically low impact; the key records being the standards defining the required frequency and the records showing calibration has been performed in accordance with those standards.

Examples of record types specifically identified in GxP regulations with an indication of their typical impact are given in Table 2.1. It is important to note that this list of records is for guidance only. It is not intended to be definite or an all-inclusive list of possible record types. Companies should make a documented judgment of the impact of records or types of records based on their own processes and circumstances.

This judgment should be driven by an overall risk assessment of the business or facility aimed at identifying the overall undesirable outcomes that may occur independently of whether electronic records are involved. These can then be assessed against the primary, and related, risks to product quality or public safety. Different facilities and products will have very different profiles in this respect.

For example, a medical device company making tongue depressors is likely to focus on issues associated with direct contamination and failures of sterility, while an oncology drug manufacturer would typically focus on potency, stability, composition, and lab assay.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 2.1: Typical Impact of Records by Record Type

H: High Impact
M: Medium Impact
L: Low Impact

Type of Record	Typical Impact	Considerations
Training/personnel record, job descriptions, incl. roles and responsibilities of QA	**M**	While required by some GxP regulations these records do not have direct impact on product quality or patient safety.
QA Audits and Investigations (including Deviations)	**M-H**	QA investigations are often used for internal control, but if the record is used in a study report or for a product release decision then the impact is higher.
Equipment cleaning records	**M-H**	Cleaning records may impact product quality or patient safety (for example risk of cross-contamination). The impact will depend upon materials & products concerned and detectability.
Calibration records	**M-H**	Calibration records may impact product quality or patient safety (for example risk of incorrectly processed products). The impact will depend upon materials & products concerned and detectability.
Planning documents	**L**	Documents such as cleaning, calibration, or maintenance schedules may be requested by inspectors as a sign of compliance with GxP requirements, when considered as part of a quality system. While the absence of such plans may increase the risk of companies not having the required results available for inspection the key records are the results of executing such plans. Management information, such as project plans would have low impact.
Validation documentation	**M**	E.g., Validation Plan, Specifications, Traceability Matrix, Qualification Protocols and Results, Validation Reports.
Financial Disclosure by Clinical Investigators	**M**	Required by GxP regulations.
Inspection Records	**M**	Records of inspections of laboratories or facilities.
Review and approval of reports	**M**	Records which show that reports have been reviewed by knowledgeable responsible persons.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 2.1: Typical Impact of Records by Record Type (continued)

H: High Impact
M: Medium Impact
L: Low Impact

Type of Record	Typical Impact	Considerations
Monitoring records	**L-M-H**	This encompasses many types of record.Impact will vary depending on the criticality of parameters being monitored. For example, microbiological and environmental performance of a sterile area may be high impact. Another example may be monitoring records from clinical trials studies. Secondary packaging and warehousing areas may be medium impact depending on the product, while building management records of office environments would have negligible impact. Management information such as progress of validation, progress of internal audits or other internal investigations would have low impact.
SOPs	**L-M**	SOPs used in electronic form constitute electronic records. The impact of SOPs will depend on the nature of the SOP or set of SOPs concerned. For example, a set of SOPs that are used to govern the validation of automated systems should not be considered as critical as SOPs that are used to govern QC operations including final batch release.
Material and finished product specifications	**M-H**	These are the specifications used to release product. Material can range from finished product to shipping boxes.
Distribution records	**H**	These affect product recall and product return.
Clinical and Non-clinical studies	**M-H**	Indicate the methods and content of the study to be carried out and include: non-clinical study protocols, clinical study protocols, Institutional Review Board (IRB) documentation
Clinical and Non-clinical study report	**H**	Contains patient safety data.
Informed consent documentation	**M**	Required for clinical trials.
Investigational New Drug applications (INDs)	**H**	An IND is a compilation of documentation. These records contain patient safety data and information about process and product specifications.
Disposition of investigational drug	**H**	Affects the ability to recall investigational product.
New Drug Applications (NDAs)	**H**	An NDA is a compilation of documentation. These records contain patient safety data and information about process and product specifications.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 2.1: Typical Impact of Records by Record Type (continued)

H: High Impact
M: Medium Impact
L: Low Impact

Type of Record	Typical Impact	Considerations
Adverse Events (AEs) and Adverse Drug Reactions (ADRs)	**H**	Contains patient safety data.
Bioequivalency Study Reports	**H**	Contains patient safety data.
QC Analysis results	**M-H**	High if used for final product release decisions.
Batch records	**H**	These records document production and product quality.
Component, drug product container, closure, and labeling records	**H**	These records enable component traceability and batch recall.
Patient information leaflets	**H**	Contains information such as usage instructions and contraindications
Master production and control records	**H**	Contain specifications on which release decisions are based.
Complaint files	**H**	These are an important measure of product quality.

Not all records are specifically identified in GxP regulations. Some are maintained in order to provide evidence of GxP compliance or GxP decision making. A standard approach should be adopted to determine the impact of records, using a checklist of questions, such as the following:

- Can corruption or loss of the record lead to misinterpretation of product quality, safety, or efficacy?
- Can corruption or loss of the record cause the product to be adulterated or result in the release of adulterated or quarantined product?
- Can corruption or loss of the record cause the product to be misbranded?
- Can corruption or loss of the record affect the ability to recall product?
- Can corruption or loss of the record affect product quality or patient safety decisions?
- Does the record have an impact on patient safety decisions? (E.g., impact on pre-clinical or clinical safety results, impact on Adverse Drug Reactions (ADR) and Adverse Events (AE)).
- Is the record required by, or submitted to, a regulatory agency and could it relate to decisions on product quality or patient safety?

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Impact classification will vary from case to case depending on factors such as the nature of the product, and company procedures and processes. The initial tendency of organizations may be to define the majority of records in the high impact group rather than in the low to middle groups. However, with improved understanding over time the interpretation of degrees of risk associated with records may start to decrease.

Typically, most regulated electronic records across an organization will be used within an overall management process with independent safeguards against failure (e.g., final QC testing and QA release of product). Therefore, while electronic records such as QA release decisions will be high impact, the majority of electronic records across the organization should have medium impact on product quality or patient safety. Classifying records as high when they are more realistically medium may lead to unnecessary work and controls which are not justified by the risks to product quality or patient safety.

It may also be appropriate to consider records associated with rules or regulations other than GxP regulations when identifying record types. These may include records relating to the handling of controlled substances or occupational health and safety. Issues of legal admissibility should also be considered (for an example, see Appendix 13, reference 14).

2.4 Step 3: Assess Risks to Electronic Records Based on Impact

Following the identification of electronic records and their impact, the next step is to select the appropriate risk management approach.

The risk management approach depends upon the impact, becoming increasingly more rigorous with greater impact.

2.4.1 Approach for Records Identified as Low Impact

Systems maintaining these records and any associated signatures should be subjected to standard validation practices supported by infrastructure qualification, project management, and operational controls. Such controls will involve good IT or engineering practice such as backup and restore, and security management.

For further information on these and related good practice topics see *GAMP 4* (see Appendix 13, reference 1).

2.4.2 Approach for Records Identified as Medium Impact

In addition to implementation of good practice, potential hazards to medium impact records and any associated signatures should be identified and appropriate controls should be designed and implemented to counter these threats (see Section 4 of this Guide).

This analysis should be documented and companies may decide to include the results of the analysis in an existing specification or in a standalone document. The use of a list of generic hazards should be considered. An example template form for recording an assessment of generic hazards and the implementation of appropriate controls is provided in Appendix 9 of this Guide.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

2.4.3 Approach for Records Identified as High Impact

In addition to implementation of good practice, high impact records and any associated signatures should be subjected to more formal risk assessment as part of the overall risk management approach.

Potential hazards should be identified and the associated risks assessed. The following aspects should be considered during the assessment:

- Severity of the consequence
- Probability of occurrence
- Likelihood of detection prior to harm occurring

Hazards to high impact records should be formally identified and analyzed by a cross-functional team, including QA. Consideration should also be given to performing a more rigorous assessment, such as that provided by Appendix M3, Guideline for Risk Assessment of *GAMP 4, GAMP Guide for Validation of Automated Systems* (see Appendix 13, reference 1).

For ease of reference, Appendix M3 of *GAMP 4, GAMP Guide for Validation of Automated Systems* is reproduced in Appendix 8 of this Guide.

2.4.4 Hazards

The approach for medium and high impact records involves the evaluation of hazards during specification and design.

Potential hazards to records and associated signatures may be classified as *human-related, computer-related, or physical/environmental.*

Table 2.2 provides some examples of potential hazards to records and signatures. Note that the focus here is on hazards to the record rather than to the system. These examples are not intended to be definitive or all-inclusive.

There are several well established techniques for identifying hazards including HAZOP, CHAZOP, FMEA, FMECA, FTA, and HACCP (see Appendix 13, reference 8 for further details).

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 2.2: Examples of Hazards to Records and Signatures

Hazard	Consequence
Human-related (accidental or deliberate)	
Human error (includes errors of judgment and errors in carrying out required actions)	• Wrong record/signature displayed • Accidental corrupted record/signature • Invalid contents of record/signature • Incorrect copy of record
Change error	Invalid contents of record
Unauthorized change	Invalid contents of record/signature
Undetectable change	Invalid contents of record/signature
Wrong access rights	• Wrong record/signature displayed • Invalid contents of record/signature
Computer-related	
Hardware undersized	Loss or corruption of record(s) or signature(s)
Hardware loss (e.g., disk crash)	Loss or corruption of record(s) or signature(s)
Data loss (e.g., backup failure)	Loss or corruption of record(s) or signature(s)
Software terminates	Loss or corruption of record(s) or signature(s)
Wrong version of software	Loss or corruption of record(s) or signature(s)
Multiple versions of software	Loss or corruption of record(s) or signature(s)
Software lost or deleted	Loss or corruption of record(s) or signature(s)
Software failure**	• Invalid contents of record/signature • Wrong record/signature displayed • Accidental corrupted record/signature
Printer error or failure	Incorrect copy of record/signature
Physical/Environmental	
Power surge	Loss or corruption of record(s) or signature(s)
Power failure	Loss or corruption of record(s) or signature(s)
Fire and/or smoke	Loss or corruption of record(s) or signature(s)
Environment problem	Loss or corruption of record(s) or signature(s)
Theft of hardware/software	Loss of record(s) or signature(s)
** Includes incorrect manifestation and incorrect link to the appropriate record	

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

2.5 Step 4: Implement Controls to Manage Identified Risks

The company should identify risk control measures that are appropriate for reducing risks to an acceptable level. Risk control involves eliminating or managing the hazard and may be achieved by one or more of the following:

- Modifying the process
- Modifying the system design
- Applying technical controls
- Applying procedural controls

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 selected control measures should be documented and justified with reference to the identified risks, and implemented and verified. The rigor and extent of controls will depend upon the impact of the electronic record and identified risks.

The company should consider any residual risks to records that remain after the risk control measures are applied. If these risks are not acceptable, further risk control measures should be considered and applied. The risk control measures may also introduce new hazards. If so, risks associated with these new hazards should be assessed.

Finally, the company should satisfy themselves that risks from all identified hazards have been evaluated. This judgment should be documented.

There should be traceability between the identified hazards and the implemented and verified control measures.

The range of electronic record controls that may be applied is discussed in detail in Section 4. For further guidance on physical, logical, and procedural security measures see ISO 17799 (see Appendix 13, reference 14).

2.6 Step 5: Monitor Effectiveness of Controls

During periodic review of systems, or at other defined points, the company should review the risks to records. It should be verified that controls established during system development and validation are still effective, and corrective action taken if deficiencies are found. The company should also consider:

- If previously unrecognized hazards are present
- If the estimated risk associated with a hazard is no longer acceptable
- If the original assessment is otherwise invalidated (e.g., following changes to applicable regulations or change of system use)

Where necessary, the results of the evaluation should be fed back into the risk management process, and a review of the appropriate steps for the affected records should be considered. If there is a potential that the residual risk or its acceptability has changed, the impact on previously implemented risk control measures should be considered, and results of the evaluation documented. It should be noted that some changes may justify relaxation of existing controls.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

2.7 Points to Consider

Organizations applying the risk management approach as described in this Guide should consider the following potential pitfalls.

Organizational Assumptions

Some organizations may assume that carrying out risk assessments will lead to less validation, others may see this as more work, and others may believe that the existence of risk assessments will guarantee inspection success.

Organizations may implement the risk management approach described in this Guide without considering how this integrates with their existing project management methodologies, which may include risk management techniques.

This may lead to friction between project groups, validation groups, and QA.

The risk based approach is a powerful tool for allocating priority and focusing effort. However, the process must be thought about carefully before being implemented by organizations, in particular:

- Emphasis should be to encourage innovation and technological advances without leading to over-engineered solutions that adversely impact the productivity of the process and without providing added benefit to patient health.
- Management may see record risk assessment as an extra overhead with no benefit. Organizations should ensure that the methodology is introduced in a way that demonstrates the benefits of the approach.
- The approach is not a one-off activity but an ongoing process throughout the system life cycle (as an integral part of change control).
- Presentation during regulatory inspections of the risk based approach, and outputs such as assessment results and implementation of controls based on justified conclusions, should be considered in advance.

Incorrect Assessment

The result of the impact and risk assessments could be either too high, or too low, leading to inappropriate, ineffective, or inconsistent conclusions. Possible reasons for this could be:

- Lack of adequate knowledge of either the system or the business process
- Lack of knowledge or understanding of the applicable regulations
- The participants do not understand the assessment process
- Too much focus on how the business process may fail, rather than on how the record may be affected throughout the process
- Constraints, such as timelines, resources
- Lack of clear guidance or interpretation within the company
- Failure to establish separation of authorities

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

It is therefore essential to ensure that the participants in the assessment bring with them the required project knowledge, business process knowledge, operational experience, and training.

Inappropriate use of controls

The controls implemented to address risks identified during the assessment may be either too rigorous or insufficient. The balance of technical and procedural controls may be inappropriate, leading to extra costs and difficulties either during project development or during operation.

Again, it is essential to ensure that the participants determining the controls have the necessary project knowledge, business process knowledge, operational experience, and training. Organizations should ensure there are adequate policies, procedures, and standards in place to support the required controls.

3 Applying the Risk Management Process

This section explains how the risk management process described in Section 2 may be applied to:

- New systems (including systems where implementation is not yet complete)
- Existing systems (either un-assessed or previously assessed)

Regulated companies may be at different stages in their response to 21 CFR Part 11, and electronic record and signature regulations in general. Section 3.4 considers the implications of the risk management process on existing systems that have already been assessed against 21 CFR Part 11, and offers guidance on how to deal with these systems.

Applying the risk management process involves initial activities that should be carried out at the company or department level, followed by other activities that should be performed at the individual system level. These activities are described in detail in subsequent sections and are summarized in Table 3.1.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 3.1: Summary of Activities Required to Apply Risk Management Process

Corporate Level Activities		
Stage	**Activity**	**Comments**
1	Agree Objectives	Ensure objectives agreed by senior management
2	Create an interpretation of GxP regulations for ER&S (that subset of regulations that apply to the company)	Interpretation should be risk based and should consider new and existing systems. In many cases this will involve updating existing interpretation.
3	If not already done, the company should certify to FDA, in writing, that they regard electronic signatures as legally binding equivalents of traditional handwritten signatures (if appropriate)	Important for new companies or companies implementing new systems who may not have used electronic signatures previously.
	Communicate interpretation to all	Provide clarity on identity and location of electronic record and signatures Emphasize importance of ensuring integrity of electronic record and signatures Describe how new interpretation affects new and existing systems

For New Systems		
Stage	**Activity**	**Comments**
1	Educate project team	Provide understanding of company policies interpreting GxP regulations
2	Determine whether ER&S regulations apply	If they do apply, ensure that an accurate and up-to-date user requirements specification is available, and that all requirements including ER&S are communicated to the supplier
3	Assess system	Identify and assess records required by GxP regulations, and determine required technical and procedural controls based on risk. Supplier assessments may include technical assessment of proposed system versus agreed ER&S requirements
4	Implement controls - Update Validation Plan - Execute the plan - Produce reports	Identify those activities and procedures required to ensure compliance - this may involve updating the appropriate specifications Implement, test and document required technical and procedural controls
5	Monitor effectiveness of controls during operation	Implement periodic review and evaluation procedures

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

For Unassessed Existing Systems		
Stage	**Activity**	**Comments**
1	Establish and educate project team to assess existing systems	Educate to provide understanding of company policies interpreting GxP regulations
2	Establish list of systems For each system, determine whether ER&S regulations apply	If in scope need to carry out an assessment of compliance with GxP regulations and company procedures
3	Assess in scope systems	Identify and assess records required by GxP regulations, and determine required technical and procedural controls based on risk
4	Carry out remediation - Develop Remediation Plans - Execute the plan - Produce reports	Identify those activities and procedures required to ensure compliance. Prioritize remediation of systems based on risk Implement, test, and document required technical and procedural controls
5	Monitor effectiveness of controls during operation	Implement periodic review and evaluation procedures

For Systems Previously Assessed Against 21 CFR Part 11		
Stage	**Activity**	**Comments**
1	Determine company approach to previously assessed systems in light of current regulations	Can either: - Continue with existing remediation plans - Carry out full reassessment of each system - Consider specific points in the latest FDA guidance, e.g., audit trails
2	If required, based on company approach, establish and educate project team to carry out assessment Establish list of systems to reassess	Educate to provide understanding of company policies interpreting GxP regulations
3	Carry out assessment	Reassess required technical and procedural controls based on risk
4	Carry out remediation - Reconsider existing Remediation Plans in light of assessment - Execute the plan - Produce reports	Identify changes to activities and procedures required to ensure compliance Prioritize remediation of systems based on risk Implement, test, and document required technical and procedural controls
5	Monitor effectiveness of controls during operation	Implement periodic review and evaluation procedures

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

3.1 Corporate Level Activities

The initial stages are applicable to all regulated companies, regardless of previous work performed toward compliance with ER&S regulations. These should be completed before carrying out any system assessments.

Stage 1: Agree Objectives

A set of new, or revised, objectives should be agreed by senior management, based on the approach described in this Guide. A clear policy should exist, and the implications for company plans, activities, and organization at the global, regional, functional, and site level should be considered.

The objectives may include:

- To understand the applicable regulations
- To gain management commitment for resources and budgets
- To educate users in their responsibilities
- To ensure each new system is compliant when operational, or to establish controls and action plans to address any non-compliance
- To bring existing systems into compliance in the most cost-effective way taking into account work already completed or in progress
- To use a risk-based approach aimed at achieving compliance, while delivering business benefits
- To maximize compliance within existing constraints
- To set up an appropriate Information Security Management System (ISMS)

Stage 2: Agree An Interpretation

This is a documented interpretation of what the electronic record and signature regulations mean for the company, based on the approach described in this Guide. This should include representation from GCP, GLP, GMP, and GDP areas as appropriate so that a common approach is developed. This interpretation should then be communicated across the organization to ensure a common understanding.

Key points to consider as part of the interpretation are:

- Risk management
- Security management
- Backup and restore
- Disaster recovery
- Documentation standards

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

- Change control
- Training
- Validation
- Audit trail
- Record retention
- Copies of records
- Legacy systems
- Hybrid systems
- Use of electronic signatures
- Classification of record types (e.g., confidential, registered, private)

The interpretation should take into account all applicable regulations and guidance (e.g., 21 CFR Part 11, EU regulations, MHLW regulations, and PIC/S guidance) and this Guide.

Based on this interpretation, company standards, procedures, and guidelines should be written or revised if necessary.

The next stages will depend on whether the system under review is new or existing, and whether assessment, planning, or remediation activities are already underway. The management approaches for new and existing systems are described in subsequent sections.

Stage 3: Communicate To Everyone

Everyone involved should understand the implications of ER&S compliance, and the company policy. Commitment should be sought to resolve non-compliance in line with policy.

If the company intends to use electronic signatures, and has not already done so, the company should certify to FDA, in writing, that they regard electronic signatures as the legally binding equivalent of traditional handwritten signatures. This may not have been previously done if the company is new, or a company did not previously supply the US market, or if a company has not previously implemented a policy of allowing electronic signatures.

While this requirement can cause confusion the process is not complicated. An organization simply needs to notify the FDA that they intend to use electronic signatures as part of their regulated activities. It is not necessary to notify FDA about each employee who will use an electronic signature.

Note that as of the publication date there are no similar certification requirements for other regulatory authorities.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

3.2 Applying the Process to New Systems

The following stages should be incorporated into the project life cycle for new systems:

Stage 1: Educate Team

Educate project teams in the new company approach, ensuring an understanding of how compliance and benefits are to be achieved, and a commitment to resolve any non-compliance.

Stage 2: Determine Whether ER&S Regulations Apply

If they do apply, ensure the User Requirements Specification contains requirements for electronic records and signatures that meet current company policies and standards. An initial identification of which electronic records and signatures will exist within the system should be included in the URS. Use of the system to generate regulated paper records should also be covered by the URS to avoid any ambiguity. Examples of systems where GxP regulations may apply are given in Appendix 7 of this Guide.

Stage 3: Assess System

Identify and assess records required by GxP regulations, by using the risk management process provided in Section 2. The assessment should consider:

- The business processes that create and update records
- The purpose of any electronic signatures
- Which records are being signed
- Any data supporting the electronic records or signatures

Appropriate technological and procedural controls should be selected using guidance provided in Section 4.

Where an external supplier is involved, an assessment of the proposed technology's compliance with customer requirements for electronic records and signatures should be performed. This may form part of the supplier audit, which should be carried out prior to contract placement.

Stage 4: Implement Controls

- Document and justify decisions
- Update Validation Plan
- Create or update system specifications
- Apply technical and procedural controls
- Test technical controls and verify procedural controls
- Produce Validation Report

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Stage 5: Monitor Effectiveness of Controls During Operation

Key points to consider to ensure continuing compliance during operation are given in Section 2.6.

3.3 Applying the Process to Existing Systems

The following stages should be followed for existing systems that have not already been assessed. See Section 3.4 of this Guide for further information related to previously assessed systems.

Stage 1: Establish and Educate Team

Establish and educate project teams in the new company approach, ensuring an understanding of how compliance and benefits are to be achieved, and a commitment to resolve any non-compliance.

Stage 2: Determine Whether ER&S Regulations Apply

Using a master list of systems, determine which systems are in scope. This can be achieved by considering whether each system maintains an electronic record or captures electronic signatures. Examples are given in Appendix 7 of this Guide.

Stage 3: Assess In Scope Systems

Identify and assess records required by GxP regulations, by using the risk management process provided in Section 2. The assessment should consider:

- The business processes that create and update records
- The purpose of any electronic signatures
- Which records are being signed
- Any data supporting the electronic records or signatures

Where issues are identified, possible remediation should be considered and appropriate technological and procedural controls should be selected using guidance provided in Section 4. The next stage involves implementing the selected controls.

Stage 4: Carry Out Remediation

- Document and justify decisions
- Develop Remediation Plan: this should be prioritized against other systems based on risk to product quality or patient safety. The extent of non-compliance and useful life of system (when system is expected to be retired) should also be taken into account.
- Apply technical and procedural controls.
- Test technical controls and verify procedural controls
- Produce Remediation Report

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Stage 5: Monitor Effectiveness of Controls During Operation

Key points to consider to ensure continuing compliance during operation are given in Section 2.6.

3.4 Systems Previously Assessed Against 21 CFR Part 11

The following stages can be followed for existing systems that have previously been assessed against 21 CFR Part 11 requirements.

Stage 1: Determine Company Approach

Current regulatory expectations give an opportunity for companies to:

- Re-think their initial or current approach
- Apply risk based management
- Achieve compliance more cost effectively

Most regulated companies have already undertaken programs in response to 21 CFR Part 11 and electronic records and signatures in general, though how far advanced these programs are will vary.

The following options exist for systems that have already been assessed:

- Continue with existing remediation plans
- Carry out a full reassessment of each system or group of system(s)
- Consider the impact of specific points raised in the FDA guidance on existing remediation plans for each system or group of system(s)

While all the above options are valid, continuing with existing remediation plans may result in the implementation of unnecessary controls, but carrying out a full reassessment of the records in each system using the detailed risk assessment process described in this Guide will be prohibitively expensive for many. One approach might be to complete the work on systems where remediation is underway but to re-assess the systems for which remediation has not yet started.

Evaluating the continuing applicability of 21 CFR Part 11 based on the specific points raised in the FDA guidance may be another practical way of dealing with previously assessed systems.

Companies should make a documented interpretation of what the new 21 CFR Part 11 guidance means to them in the context of their business. They should consider in particular:

- Validation
- Audit trail
- Record retention
- Copies of records
- Legacy systems

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

These points are considered fully in Appendices 1 to 5.

All other 21 CFR Part 11 controls not under enforcement discretion as per the guidance are still required for existing systems, unless those systems are legacy systems.

Stage 2: Establish and Educate Team

If a reassessment is to be carried out, establish project teams and educate in the new company approach, ensuring an understanding of how compliance and benefits are to be achieved, and a commitment to resolve any non-compliance.

The list of systems to be reassessed should be defined.

Stage 3: Carry Out Assessment

If the company approach is to carry out a full reassessment, then the process given in Section 3.3 should be followed.

However, if a reassessment of the continuing applicability of 21 CFR Part 11 based on the specific points raised in the FDA guidance is required, this may be documented using the example form provided in Appendix 10 of this Guide. This form documents whether 21 CFR Part 11 still applies, based on the narrow scope and definition of legacy system provided by the FDA guidance. The form also documents the reassessment of existing remediation plans with regard to specific 21 CFR Part 11 expectations, namely:

- Meeting predicate rules
- An assessment of risk
- The potential of the system to affect product quality or patient safety
- Record integrity

The form can be applied to individual systems or to groups of systems, as appropriate.

Stage 4: Carry Out Remediation

- Changes to existing remediation plans, activities, and procedures should be identified.
- These should be prioritized against other systems based on risk to product quality or patient safety. The extent of non-compliance and useful life of system (when system is expected to be retired) should also be taken into account.
- Apply technical and procedural controls. Note: procedural controls should already be in place.
- Test technical controls and verify procedural controls
- Produce Remediation Report

Stage 5: Monitor Effectiveness of Controls During Operation

Key points to consider to ensure continuing compliance during operation are given in Section 2.6.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

4 Controls

This section discusses various risk control measures that can be used to manage risks, as identified by the process described in Section 2 of this guide. 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 impact of the electronic record and identified risks.

4.1 Record Controls

Procedural and technical controls available to reduce risks to an acceptable level include:

- Security management
- Backup and restore
- Disaster recovery and business continuity
- Change control
- Validation
- Audit trail
- Record copying controls
- Record retention controls
- Software controls
- Hardware controls
- Policies and procedures
- Training and experience

A combination of these controls may be necessary to adequately manage the risk. The selected measures should be implemented and documented. Many of these controls will 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.

4.1.1 Implementation of Controls

Controls may be implemented in different ways and with differing degrees of rigor. Table 4.1 shows how various types of controls may be implemented.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 4.1: Possible Implementation of Record Controls

Control	Possible Implementation
Security Management	• Physical access security • Formal access authorization • Confirming identity of new user before granting access • Unique user identification • Different user-id/password combinations for logon and signatures • Providing defined profiles for individual users or groups • Clear separation of server administration, application administration and user roles and responsibilities • Limiting Write, Update, Delete access (e.g., to key users) • Enforced password changing • Enforced minimum password length and format • Idle time logout • 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) • Use of super-user accounts • Changing user rights • Revoking access from users without losing record of their historical use • Testing and renewal of identity devices or tokens • Amount of documentation retained
Backup and Restore	• Formality of process • Documented testing of process • Frequency • Redundancy (e.g., number of tapes in cycle) • Auto or manual processes • Backup verification • Backup media • Storage conditions • Storage location(s) including remote storage locations • Media refresh • High availability system architecture if required • periodic testing throughout retention time • Amount of documentation retained
Disaster Recovery and Business Continuity (No IT service available)	• Service level agreements • Formal contracts for restoration of service • Defined allowable time of outage • Recovery mechanisms (e.g., hot standby, procedural) • Documented testing of the plan • Definition of defined recovery point • Documented procedures for business continuity and number of personnel trained in these procedures

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 4.1: Possible Implementation of Record Controls (continued)

Control	Possible Implementation
Change Control	• Extent of QA involvement (e.g., Procedural authorization vs. individual approval vs. audit verification) • Defined roles and responsibilities for change assessment, authorization, review and approval • Formality and roles involved in authorization • Formality and roles involved in different types of review (which can include design review/risk assessment) • Formality and roles involved in approval • Amount of testing carried out • Formality of go live process after upgrade • Amount of documentary evidence retained
Validation	• Extent of QA involvement • Formality of process with defined roles and responsibilities • Degree of specification • Degree of review • Nature, scope & degree of testing, including controls implemented in support of electronic records and signatures • Roles involved in review • Roles involved in approval • Amount of documentary evidence retained
Audit Trail	• 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 • Purpose: e.g., for auditing of planned authorized changes to data or for detecting unauthorized change (fraud attempts)
Record Copying Controls (see also retention below)	• Format of copy (common portable electronic, paper) • Reference to original on copy • Relationship with original (e.g., exact copy, summary) • Preservation of meaning and content • Search, sort, and trend capabilities • Process for producing copies (time required, access levels) • The method for controlling the exact copy, e.g., use of cyclic redundancy check (CRC-32) or message digest (MD5)

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 4.1: Possible Implementation of Record Controls (continued)

Control	Possible Implementation
Record Retention Controls	• Retention periods • Definition of what is being retained • Retention of associated data (e.g., audit trails, configuration information) • Capacity limits • Automatic or requiring human intervention • Ability to reprocess data • Involvement of QA • Formal disposal procedure • Periodically test 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
Software Controls	• User identity checks • Checksums and other verification of data transfer • Standard network protocols for data transfer • Automatic functionality to reduce human error, e.g., - use of barcodes - sequence enforcement • Measurement redundancy in critical applications • Data entry checking • Error handling • Alarms • Notification of software failure • Audit trail (treated separately, see above) • Prompting for confirmation of action • Monitoring tools (e.g., event logs)
Hardware Controls	• Mirrored or RAID drives • UPS • Stress testing • Contingency in sizing of hardware • Network monitoring (could be also software control)

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Table 4.1: Possible Implementation of Record Controls (continued)

Control	Possible Implementation
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 Policies and Procedures to cover topics such as the following where appropriate: • Validation • Risk management • System documentation management • Change management • Taking copies of electronic records • Backup and restore • Access management • Audit trail management • Signature management • Usage of electronic signature • Operation of automated software controls • Record retention periods • Significance of electronic signatures in terms of individual responsibility • Consequence of falsification • Data archiving and deletion • Application archiving
Training and Experience	• Training and experience of users of systems containing electronic records • Training and experience of developers of systems (both pharmaceutical organizations and suppliers) • Amount of documentation retained • Significance of electronic signatures in terms of individual responsibility • Consequence of falsification • Usage of electronic signature

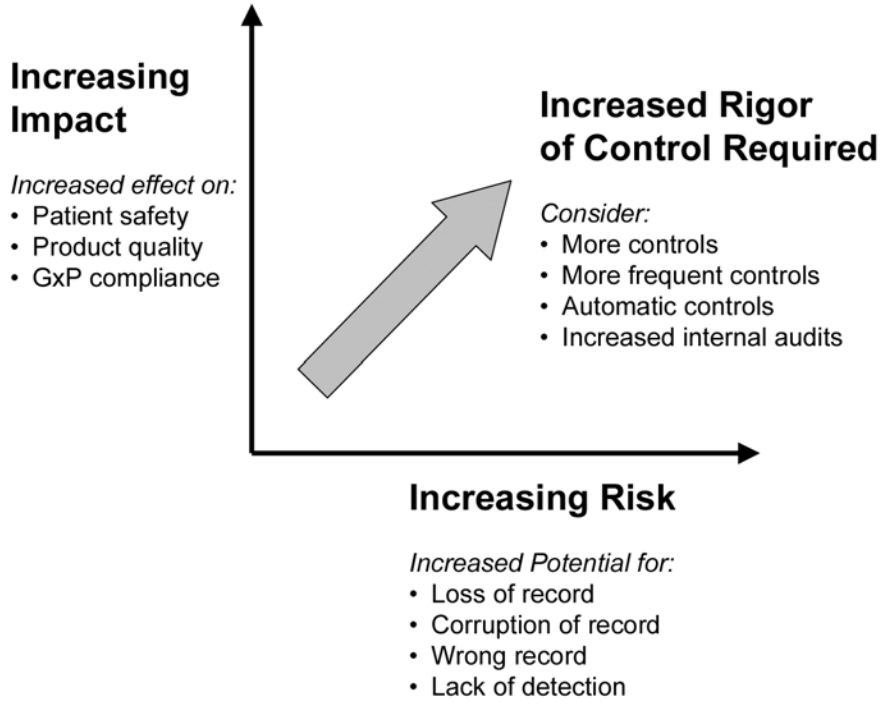
Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

4.1.2 Rigor of Controls

The rigor with which the controls are applied should take into account both the impact of the record and the risks identified. As the impact and risk increase then more rigorous control is required, as shown in Figure 4.1.

Figure 4.1: Relationship between Impact, Risk, and Rigor of Controls



Companies should take into account the need for authenticity, integrity, accuracy, reliability, and where appropriate the confidentiality of the electronic records.

A combination of several technical and procedural controls may be required to achieve an adequate level of protection. For further information see National Institute of Standards and Technology (NIST) Engineering Principles for IT Security <SP 800-27> (see Appendix 13, reference 15).

For systems containing multiple types of records, there are two approaches to applying the controls.

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

4.2 Signature Controls

Electronic signatures should be applied where a record is required to be signed by a GxP regulation and the record is maintained in electronic format. Electronic signatures are defined in 21 CFR Part 11 as “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.”

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Companies should define when signatures are required in light of their own processes and circumstances. Examples of GxP regulations for electronic signatures and identifications are provided in Appendix 6 of this Guide.

21 CFR Part 11 provides clear instruction on the information associated with a signing that needs to form part of a signed electronic record:

- The printed name of the signer
- Date and time when the signature was executed
- Meaning (such as review, approval, responsibility, or authorship) associated with the signature

This information must be included as part of any human readable form of the signed record (e.g., displayed on the screen or a printout of the record). Note that the information need not be physically stored in the same file but must be linked in a way that ensures it cannot be removed, altered, or copied by ordinary means.

The European Union has also provided requirements regarding the use of Advanced Electronic Signatures (EU Directive 1999/93/EC 13 Dec 1999, see Appendix 13, reference 11). EU advanced e-signatures security certificates are based on a secure 'signature creation device' (i.e., the signature creation data can practically occur only once; their secrecy is reasonably assured; the signature generation cannot, with reasonable assurance, be derived; the signature is protected against forgery using currently available technology; and can be reliably protected by the legitimate signatory against the use of others). The EU advanced e-signature has the following characteristics:

- It is uniquely linked to the signatory
- It is capable of identifying the signatory
- It is created using means that the signatory can maintain under their sole control
- It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

Only authorized certification organizations are allowed to administer this type of electronic signature.

It is possible to meet the requirements of the controls required for both markets if systems are designed with forethought. The intent is to ensure that electronic signatures are equivalent to handwritten signatures and are legally binding.

The integrity of the electronic signature is vital. Companies should ensure that if individuals use the same electronic signature on both regulated and unregulated systems, that the controls on the unregulated systems are sufficient so as not to potentially compromise the use of the electronic signature on the regulated system.

The following signature controls should be considered when deciding upon a suitable approach to ensuring compliant signatures. The appropriate controls will depend upon the impact of, and risks to, the signed electronic record in question.

- Method for ensuring uniqueness of signature, including prohibition of reallocation
- Prevention of deletion of signature related information after the signature is applied
- Biometric methods

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

- Information recorded on signing (e.g., name, date and time, meaning of signature)
- Integrity of link between signature and record
- Method of display or print of signed records
- Procedure for delegation of signature responsibilities (e.g., holidays, periods of absence)
- Entry of all or some components of multiple component signatures
- Storage of password used in the act of signing (e.g., not in signed record)
- Use of certified providers of electronic signatures

4.3 Managing Hybrid Records

Hybrid records are commonly found in automated systems. Examples include:

- Records that are maintained electronically and handwritten signatures applied
- An electronic representation of a signed paper record and both are maintained

Existing technology may not allow the use of electronic signatures with electronic records in a particular system. An example could be the release of a manufacturing batch that has been compiled using electronically created records with no facility for electronic signature. These batch records would typically be identified as high impact and the risk assessment would likely highlight the issue of establishing and maintaining the link between the electronic and signed paper copies (since maintaining records synchronized in a hybrid system carries a significant risk). Companies should decide and document which is the regulated record (may be both).

Suitable controls should be established and verified. These may include standard operating procedures that define the process of controlling the signed paper record, and for making modifications to the paper and electronic records if required. The procedure should provide a process that prevents incorrect or out of date versions of records from being used.

Another example is a master batch record maintained in electronic form which is used to generate a blank paper batch record (including manufacturing instructions) which is completed manually. The original printout of the master batch record is signed on paper by head of manufacturing and QA. Subsequent printouts (i.e., working copies) are signed by QA to confirm that this is a true copy of the master batch record. In this case the electronic version of the signed paper master batch record is used to produce copies of the master batch record. Companies should have controls established to ensure that the electronic record used for printing is the same as the approved paper record.

A third example is a paper record, scanned into an electronic system and stored in PDF format. The assessment and resulting controls would be dependent upon the usage of the record.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

4.4 User/Supplier Responsibilities

4.4.1 Procedural Requirements (responsibility of user)

The following list defines procedural requirements to support the use of compliant electronic record and signature systems. The procedures implemented should be commensurate with the identified risk:

1. Systems should be validated according to defined procedures.

2. Systems, records, and documentation should be developed according to defined procedures and should be managed under change control procedures.

3. Provision of data to external parties should be formally managed.

4. When copies of records with any associated audit trails and signatures are created for regulatory inspection, there should be controls to ensure legal compliance and that confidentiality is maintained.

5. Retention periods, and responsibilities for complying with these periods, should be documented. Document management procedures should ensure that handwritten signatures linked to electronic records are maintained for the same retention period.

6. Backup and recovery, and archive and retrieval of data should be formally documented.

7. Procedures should define how access to systems is limited to authorized individuals.

8. Evidence should be available to demonstrate that persons who develop, maintain, or use electronic record and signature systems have the education, training, and experience to perform their assigned tasks. There should be training records and a procedure that addresses this requirement. Refer to local SOPs for Staff and Training Records.

9. Unsuccessful attempts to access the system should be monitored - this is a system control and may not be possible on some systems.

10. There should be a system of self-inspection to demonstrate compliance with the procedures and controls.

The following procedural requirements relate to systems that utilize electronic signatures:

1. The significance of electronic signatures, in terms of individual responsibility, and the consequences of misuse or falsification should be documented. Procedures should be established to ensure individuals understand they are accountable and responsible for actions initiated under their electronic signatures, and that electronic signatures must not be made known to others. Particular attention is needed when electronic signature components are used on multiple systems, or for other activities such as logging into a system, to ensure that the integrity of the signature components is not compromised.

2. Security procedures should be established that ensure electronic signatures are unique to an individual. The user id should never be reassigned to another individual.

3. Procedures should be established to verify the identity of an individual before the assignment of their electronic signature, or any component of an electronic signature (such as the user ID).

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

4. Security procedures should ensure that the ability to apply electronic signatures is withdrawn for individuals whose responsibilities change and make the original assignment no longer applicable, without the loss of information relating to signatures already executed.

5. There should be initial and, where applicable, 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.

6. Procedures should be established to manage signature loss (e.g., token, password), and periodic changing where applicable (e.g., passwords).

7. Procedures should cover the delegation of signature responsibilities (e.g., holidays, periods of absence).

4.4.2 Technical Requirements (largely the responsibility of supplier)

Many of the controls identified in Table 4.1 in Section 4.1.1, and signature controls identified in Section 4.2, are technical in nature and will form part of the functionality of the supplied system. Suppliers of such systems should be aware that these controls will likely be standard requirements for systems supplied to the regulated life science industries, consistent with their applicability as shown in Table 4.1. Suppliers are liable to assessment, including audit, to ascertain that technical controls have been implemented appropriately, since user companies have ultimate responsibility for the system in use.

Suppliers should provide documentation that defines which electronic records and signatures a system is capable of maintaining. The controls available to help manage these records and any associated signatures should also be described. The user can then use this information during the risk management process.

It may not be possible to implement certain technical controls due to the required functionality not being currently available in the automated system. If it is determined that including the required technical control would not be practical, then the use of alternative technical controls, or failing that procedural controls, should be considered for acceptability by the user. The use of multiple procedural controls may together produce sufficient collaborative information to support the evidence of record control.

Suppliers may also provide administrative features and utilities in their applications and systems to make the user implementation of procedural controls more efficient, consistent, and secure. An example of this would be the inclusion of a system workflow to route lists of authorized users to the System Owners on a periodic basis for review.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Appendices

Appendix 1 Validation

Appendix 2 Audit Trail and Data Security

Appendix 3 Record Retention, Archiving, and Migration

Appendix 4 Copies of Records

Appendix 5 21 CFR Part 11 Legacy Systems

Appendix 6 Examples of Records and Signatures Required by GxP Regulations

Appendix 7 Case Studies

Appendix 8 Copy of GAMP 4, Appendix M3

Appendix 9 Example Template Form for Risk Assessment and Identification of Controls

Appendix 10 Form for Previously Assessed 21 CFR Part 11 Systems

Appendix 11 Current Regulatory Situation

Appendix 12 Glossary

Appendix 13 References

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Appendix 1
Validation

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

1 Introduction

The regulated company should have established policies and procedures for the validation of systems, including those that generate or maintain regulated electronic records and signatures. Security and integrity of regulated records should be considered when planning validation activities.

Factors to be taken into account should include:

- GxP regulatory requirements for validation
- Potential impact and risk to product quality or patient safety
- Complexity, system size, and degree of standardization or novelty
- Nature and source of software and hardware components

2 Examples of Relevant GxP Regulations

21 CFR Part 820 Quality System Regulation, Subpart G, §820.70 Production and process controls:

"(i) Automated processes. When computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software for its intended use according to an established protocol...These validation activities and results shall be documented."

21 CFR Part 211, Subpart D, §211.68 Automatic, mechanical, and electronic equipment:

"(a) Automatic, mechanical, or electronic equipment or other types of equipment, including computers, or related systems that will perform a function satisfactorily, may be used in the manufacture, processing, packing, and holding of a drug product. If such equipment is so used, it shall be routinely calibrated, inspected, or checked according to a written program designed to assure proper performance. Written records of those calibration checks and inspections shall be maintained."

EU GMP, Annex 11, Computerised Systems, Paragraph 2, Validation:

"The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether the validation is to be prospective or retrospective and whether or not novel elements are incorporated. Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and modifying."

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Annex 15, Section 1, Principle:

"Significant changes to the facilities, the equipment and the processes, which may affect the quality of the product, should be validated. A risk assessment approach should be used to determine the extent and scope of validation."

Annex 18, Ref 5.40:

"GMP related computerised systems should be validated. The depth and scope of validation depends on the diversity, complexity and criticality of the computerised application."

3 Validation of Electronic Records and Signatures

Controls for regulated electronic records and associated signatures should be validated. This should happen as part of the overall validation strategy for the system, following a process such as that described in *GAMP 4* (Appendix 13, reference 1). Relevant material may also be found in:

General Principles of Software Validation; Final Guidance for Industry and FDA Staff (Appendix 13, reference 6)

Good Practices for Computerised Systems in Regulated 'GxP' Environments (Appendix 13, reference 5)

"Guideline on Control of Computerized Systems in Drug Manufacturing" (Appendix 13, reference 7)

Trial Management, Data Handling and Record Keeping (Appendix 13, reference 16)

The Good Laboratory Practice Regulations, Statutory Instrument 1999 No. 3106 - Part X, Section 1(e) (Appendix 13, reference 17)

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Compliant Electronic Records and Signatures 2005