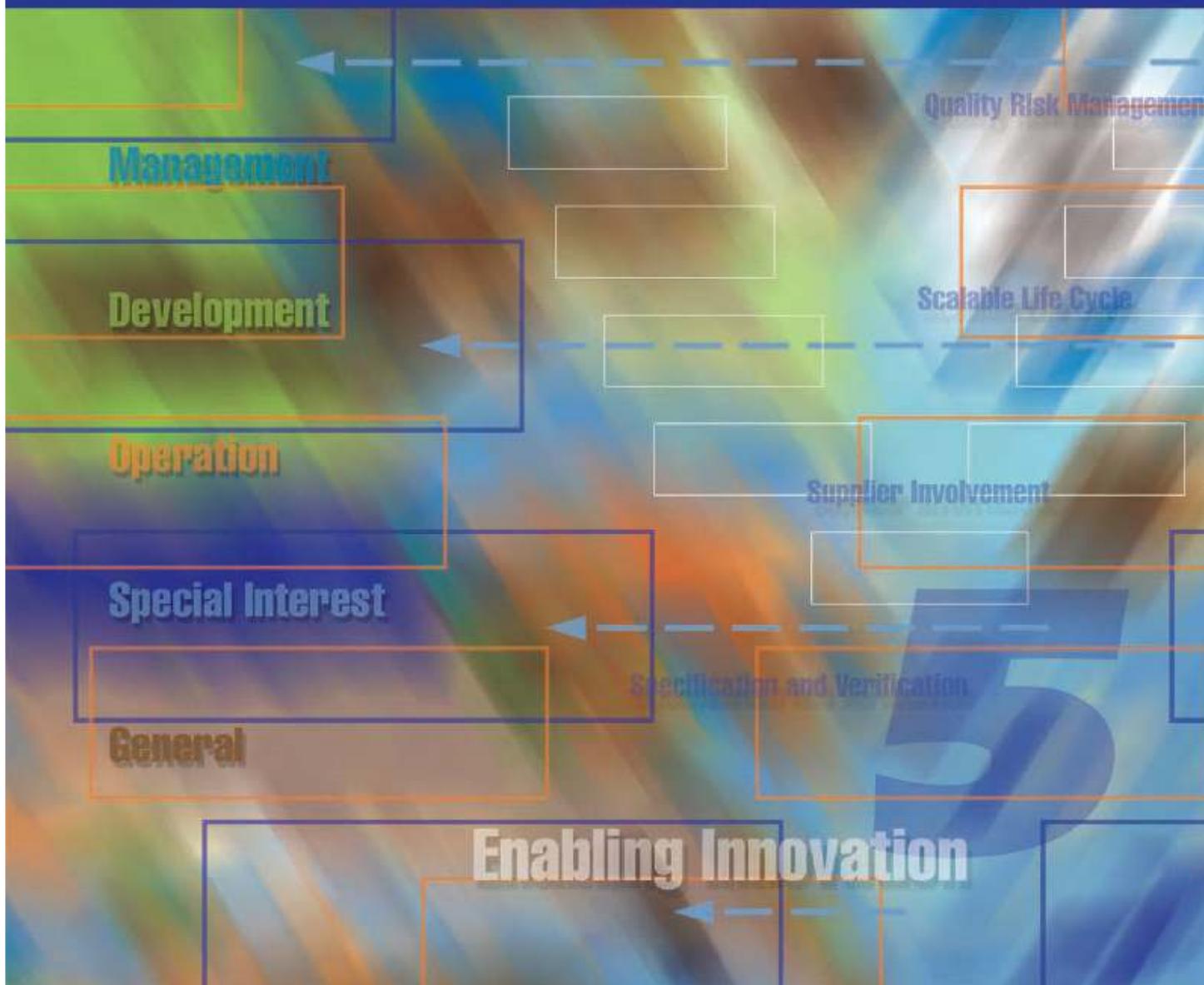




GAMP 5

A Risk-Based Approach to Compliant GxP Computerized Systems





GAMP 5

A Risk-Based Approach to Compliant GxP Computerized Systems

Disclaimer:

This Guide is meant to assist pharmaceutical manufacturing companies in managing GxP Regulated systems. ISPE cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability

In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, 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 2008. All rights reserved.

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

All trademarks used are acknowledged.

ISBN 1-931879-61-3

Foreword

Changing Environment – Regulatory and Industry Initiatives

The pharmaceutical industry is responding to the challenge of significantly improving the way drug development and manufacturing is managed.

New concepts are being developed and applied, including science based risk management approaches, a focus on product and process understanding, and the application of Quality by Design concepts.

Many of these ideas are defined and described in the FDA 21st Century Initiative, new ICH documents such as Q8 Pharmaceutical Development, Q9 Quality Risk Management, and Q10 Pharmaceutical Quality System, ISPE's Product Quality Lifecycle Implementation (PQLI) initiative, and various supporting industry consensus standards, such as the *ASTM E2500 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment*.

As these new ideas and ways of working are being established, the industry will for some time be in a period of transition.

GAMP® guidance must evolve to meet the needs of the changing environment, and integrate fully with ISPE initiatives such as PQLI, and the revision of the ISPE Baseline® Guide on Commissioning and Qualification. There is both a need and an opportunity to make activities related to all types of computerized systems efficient, effective, and focused on patient safety.

New and Innovative Approaches

Where a computer system is regarded as one component of a wider manufacturing process or system, particularly in an integrated Quality by Design environment, specific and separate computerized system validation may not be necessary. This environment requires both complete product and process understanding and that the critical process parameters can be accurately and reliably predicted and controlled over the design space. In such a case, the fitness for intended use of the computer system within the process may be adequately demonstrated by documented engineering or project activities together with subsequent Process Validation or continuous quality verification of the overall process or system. The same principle applies to the adoption of Process Analytical Technology (PAT).

These innovative approaches are available and useable now if the appropriate pre-requisites are met. While acknowledging that not all regulated companies will be in a position to, or will choose to, fully embrace the new approaches immediately, this Guide is intended to encourage the adoption of such approaches and in no way to be a barrier.

Improving Quality Practice

During the period of transition, the industry continues to need practical guidance based on current good practice – giving practitioners the tools to do the job today, while building a bridge to new approaches. This Guide aims to describe current good practice in order to satisfy the needs of the majority of practitioners involved with computerized systems, while also enabling new and innovative approaches, e.g., for process systems in a Quality by Design environment. These innovative approaches and the application of principles to specific system types will be explored in detail in subsequent documents.

In the meantime, key aspects supportive of ISPE PQLI and ASTM E2500 are addressed immediately to make current activities as effective and efficient as possible. These include:

- focusing on aspects critical to the patient
- avoiding duplication of activities (e.g., by fully integrating engineering and computer system activities so that they are performed only once)
- leveraging supplier activities to the maximum possible extent, while still ensuring fitness for intended use
- clarifying the roles of Subject Matter Experts and Quality Assurance
- scaling all life cycle activities and associated documentation according to risk, complexity, and novelty
- acknowledging that traditional linear or waterfall development models are not the most appropriate in all cases

These are reflected in the Key Concepts upon which this Guide is based, and in the detailed content of this Guide.

This Guide is deliberately flexible with regard to terminology – focusing on value-added activities and avoiding unnecessary activities is the main intent, and different regulated companies and suppliers may choose to use a wide range of different terms. In line with the principles of ASTM 2500, this Guide adopts specification and verification as overall terms describing specific life cycle activities, but does not discard the general life cycle validation framework to reflect current industry practice for companies that decide to maintain these practices rather than applying the new concepts.

Further details may be found in Appendix S1 Alignment with ASTM E2500.

Extended Scope and Application

Coupled with these initiatives in development and manufacturing, a wide and ever-increasing range of local and global networked computerized systems are being used throughout the product life cycle. Many of these are fundamental to GxP activities.

Accuracy and integrity of records and data is essential throughout the product life cycle, from research and development through pre-clinical studies, clinical trials, production and quality control to marketing. The *GAMP Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures* provides further guidance on this topic, and should be read in conjunction with this Guide.

Achieving compliance and fitness for intended use for all GxP regulated systems in a pragmatic and efficient manner is essential.

This Guide aims to address the need to safeguard public health, product quality, and data integrity while at the same time enabling innovation and technological advance.

Dr. Guy Wingate, Chair GAMP COP Council
Dr. Arthur (Randy) Perez, Chair GAMP Americas Steering Committee
Peter Robertson, Chair GAMP Europe Steering Committee

Acknowledgements

GAMP® 5 was produced by a task team led by Guy Wingate (GSK). The members of the task team revised existing material, and contributed and reviewed new material.

Task Team

Guy Wingate	GlaxoSmithKline (Task Team Leader and Chair of GAMP COP Council)
Anders Bredesen	YIT Building Systems AS (Chair of GAMP Nordic)
Sam Brooks	Novartis Consumer Health
Jay Buffi	Pfizer Inc.
Winnie Cappucci	Bayer Healthcare
Mark Cherry	AstraZeneca
Chris Clark	Napp Pharmaceuticals Ltd.
Gail Evans	ISPE
Heinrich Hambloch	GITP (Chair of GAMP DACH)
Colin Jones	Conformity Ltd.
Paige Kane	Wyeth Biotech (Vice Chair of GAMP Americas)
Tony Margetts	Margetts Associates (Chair of GAMP Editorial Review Board)
Arthur (Randy) Perez	Novartis Pharmaceuticals Corp. (Chair of GAMP Americas)
Peter Robertson	AstraZeneca (Chair of GAMP Europe)
Kate Samways	KAS Associates Ltd.
David Selby	Selby Hope International Ltd. (Vice Chair of GAMP Europe)
Sion Wyn	Conformity Ltd.

This work was overseen and supported by the ISPE/GAMP COP Committees:

GAMP COP Council

Guy Wingate	GlaxoSmithKline (Chair)
Anders Bredesen	YIT Building Systems AS (Chair of GAMP Nordic)
Rory Budihandojo	Boehringer-Ingelheim Chemicals
Chris Clark	Napp Pharmaceuticals Ltd.
Paul D'Eramo	Johnson & Johnson
Niels Holger Hansen	Novo Nordisk A/S
Paige Kane	Wyeth Biotech (Vice Chair of GAMP Americas)
Makoto Koyazaki	Shimadzu Corp.
Tony Margetts	Margetts Associates
Kenichi Ogihara	Nomura Research Institute Ltd. (Chair of GAMP Japan)
Arthur (Randy) Perez	Novartis Pharmaceuticals Corp. (Chair of GAMP Americas)
Peter Robertson	AstraZeneca (Chair of GAMP Europe)
David Selby	Selby Hope International Ltd. (Vice Chair of GAMP Europe)
Anthony Trill	MHRA (UK)
Sion Wyn	Conformity Ltd.

GAMP Americas Steering Committee

Arthur (Randy) Perez	Novartis Pharmaceuticals Corp. (Chair)
Paige Kane	Wyeth Biotech (Vice Chair)
Jerry Anderson	Elan Pharmaceuticals
Rory Budihandojo	Boehringer-Ingelheim Chemicals
Jay Buffi	Pfizer Inc.
Waunetka Clark	Abbott Laboratories
Winnie Cappucci	Bayer Healthcare
Marcelo Decanio	Boehringer-Ingelheim (GAMP Brazil Chair)

Paul D'Eramo	Johnson & Johnson
Gloria Hall	ISPE
Bob Herr	Pfizer Animal Health
Jim John	Altus Automation
Klaus Krause	Allergan Inc.
Jose Matos-Perez	Bristol-Myers Squibb (GAMP Puerto Rico Chair)
Kevin Martin	CimQuest-Vantage LLC
Barbara Nollau	Abbott Laboratories
Mike Rutherford	Eli Lilly and Co.
Robert D. Tollefson	ORA/ORO FDA (USA)
Lorrie Vuolo-Schuessler	GlaxoSmithKline
Michael Wyrick	Best Practices Consulting Services

GAMP Europe Steering Committee

Peter Robertson	AstraZeneca (Chair)
David Selby	Selby Hope International Ltd. (Vice Chair)
Carlo Bestetti	Convalida (Co-Chair of GAMP Italia)
Anders Bredesen	YIT Building Systems AS (Chair of GAMP Nordic)
Sam Brooks	Novartis Consumer Health SA
Mark Cherry	AstraZeneca
Chris Clark	Napp Pharmaceuticals Ltd.
Peter Coady	Pfizer Global R&D
Sandro De Caris	Decaris (Co-Chair of GAMP Italia)
Mark Foss	Boehringer Ingelheim Ltd.
Heinrich Hambloch	GITP (Co-Chair of GAMP DACH)
Niels Holger Hansen	Novo Nordisk A/S
Hartmut Hensel	Hochschule Harz (Co-Chair of GAMP DACH)
Scott Lewis	Eli Lilly and Co. Ltd.
Tony Margetts	Margetts Associates
Chris Reid	Integrity Solutions
Yves Samson	Kereon AG (Chair of GAMP Francophone)
Kate Samways	KAS Associates Ltd.
Rob Stephenson	Pfizer Global Manufacturing
Anthony Trill	MHRA (UK)
Guy Wingate	GlaxoSmithKline (Chair of GAMP Council)
Sion Wyn	Conformity Ltd.

GAMP Japan Steering Committee

Kenichi Ogiara	Nomura Research Institute Ltd. (Chair)
Yuichi Fujita	Toyo Engineering Corp. (Vice Chair)
Hiroaki Aikawa	Kajima Corp.
Masayuki Akutagawa	Yamatake Corp.
Rika Naito	Nomura Research Institute Ltd.
Takayuki Sugimoto	Eisai Co. Ltd.

The GAMP COP wish to thank the following individuals for their valuable contributions to GAMP 5, contributing to groups producing new materials, revising existing materials and reviewing material.

Greg Adcock	Watson Pharmaceuticals Inc.
Jerry Anderson	Elan Pharmaceuticals
Carlos A. Bruzos	Andrx
Joseph DeSpautz	Rockwell Automation Life Sciences
David Diaz	ISO Group

Karen Donaldson	Pfizer Inc.
Luis Gonzalez	Paciv
Hasse Greiner	Novo Nordisk A/S
Justin Iovino	Bearing Point Inc.
Paul Irving	Aptitude UK Ltd.
Ed Kanczewski	Process & Compliance Management
Flavio Kawakami	Doctor Bit Informatica Ltda
Jamie Kiguchi	Amgen Inc.
Ken Kovacs	Rockwell Automation
Allan Pfitzenmaier	Vectech Pharma Consultants Inc.
Greg Ruklic	Wyeth Biotech
Jens Seest	Novo Nordisk A/S
Siri Segalstad	Segalstad Consulting AS
Brian Stowe	Stowe & Associates
Anders Vidstrup	Novo Nordisk A/S
Guy Wakefield	Mi-Services Group Inc.
Greg Warth	MedImmune Inc.

Regulatory Input and Review

ISPE wish to thank the various regulatory authorities around the world who provided valuable discussion, advice and review comments. Contributing regulatory authorities included US FDA, UK MHRA, AFSSaPS (France), and Regierungspräsidium Darmstadt (Germany).

Particular thanks go to the following individuals for their review and comment:

Karl-Heinz Menges, Regierungspräsidium Darmstadt GMP-inspectorate (Germany)
John Murray, Office of Compliance, CDRH FDA (USA)
George Smith, Division of Manufacturing and Product Quality, CDER FDA (USA)
Robert D. Tollesen, Division of Field Investigations, ORA/ORO FDA (USA)
Anthony Trill, MHRA (UK)

Editorial

The GAMP Editorial Review Board created additional material, made major revisions to existing material and edited the complete document having reviewed all contributions.

Tony Margetts, Margetts Associates (Chair of GAMP Editorial Review Board)
Winnie Cappucci, Bayer Healthcare
Gail Evans, ISPE
Colin Jones, Conformity Ltd.
Arthur 'Randy' Perez, Novartis Pharmaceuticals Corporation (Chair of GAMP Americas)
Sion Wyn, Conformity Ltd.

Thanks to the following who assisted greatly in ensuring alignment with ASTM E2500 and PQLI:

Bruce Davis, AstraZeneca
Gert Moelgaard, NNE Pharmaplan
David Petko, Auxilium Pharmaceuticals, Inc.
Sabra Seyer, Pfizer

The GAMP Council would like to thank all those involved in the worldwide review of this Guide during 2007.

The Editor of GAMP 5 on behalf of ISPE was Sion Wyn.

Table of Contents

1	Introduction	11
1.1	Rationale for GAMP 5	11
1.2	New and Revised Material	13
1.3	Purpose	14
1.4	Scope	14
1.5	Business Benefits	15
1.6	Structure	16
2	Key Concepts	19
2.1	Key Concepts	19
2.2	Key Terms	21
3	Life Cycle Approach	25
3.1	Computerized System Life Cycle	25
3.2	Specification and Verification	27
3.3	Computerized System Validation Framework	27
4	Life Cycle Phases	29
4.1	Concept	29
4.2	Project	29
4.3	Operation	39
4.4	Retirement	46
5	Quality Risk Management.....	47
5.1	Overview	47
5.2	Science Based Quality Risk Management	48
5.3	Quality Risk Management Process	49
6	Regulated Company Activities	53
6.1	Governance for Achieving Compliance	53
6.2	System Specific Activities	56
7	Supplier Activities	65
7.1	Supplier Products, Applications, and Services	65
7.2	Supplier Good Practices	66
7.3	Quality Management System	67
7.4	Requirements	68
7.5	Supplier Quality Planning	69
7.6	Sub-Supplier Assessments	69
7.7	Specifications	70
7.8	Design Reviews	70
7.9	Software Production/Configuration	70
7.10	Testing	71
7.11	Commercial Release	71
7.12	User Documentation and Training	71
7.13	System Support and Maintenance During Operation	72
7.14	System Replacement and Retirement	72

8 Efficiency Improvements	73
8.1 Establishing Verifiable and Objective User Requirements	73
8.2 Use of Risk-Based Decisions	74
8.3 Leveraging Supplier Input	74
8.4 Leveraging Existing Documentation	75
8.5 Efficient Testing Practice	75
8.6 Well Managed Handover	77
8.7 Efficient Change Management	77
8.8 Anticipating Data Archiving and Migration Needs	78
Appendices	81
Index	347

1 Introduction

GAMP[®] guidance aims to achieve computerized systems that are fit for intended use and meet current regulatory requirements, by building upon existing industry good practice in an efficient and effective manner.

GAMP provides practical guidance that:

- facilitates the interpretation of regulatory requirements
- establishes a common language and terminology
- promotes a system life cycle approach based on good practice
- clarifies roles and responsibility

It is not a prescriptive method or a standard, but rather provides pragmatic guidance, approaches, and tools for the practitioner.

When applied with expertise and good judgment, this Guide offers a robust, cost effective approach.

The approach described in this document is designed to be compatible with a wide range of other models, methods, and schemes including:

- quality systems standards, such as those of the Institute of Electrical and Electronics Engineers (IEEE), and certification schemes, such as the International Organization for Standardization (ISO) 9000 Series
- schemes for assessing and improving organization capability and maturity, such as Capability Maturity Model Integration[®] (CMMI)
- software process models, such as the various spiral models, or ISO 12207
- software development methods, such as Rapid Application Development (RAD), Agile, Rational Unified Process[®] (RUP), or Extreme Programming (XP)
- approaches to IT service management, such as the IT Infrastructure Library[®] (ITIL)

Where possible, terminology is harmonized with standard international sources such as International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) and ISO.

This Guide aims to be fully compatible with the approach described in the *American Society for Testing and Materials (ASTM) E2500 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment*.

GAMP is an ISPE Community of Practice. For further information see www.ispe.org.

1.1 Rationale for GAMP 5

This revision of GAMP has been significantly updated to align with the concepts and terminology of recent regulatory and industry developments including:

- ICH Guidance Q8, Q9, and the forthcoming Q10: setting out expectations for the application of science- and risk-based approaches to drug development and manufacture supported by pharmaceutical quality systems

- Product Quality Lifecycle Implementation (PQLI): an initiative launched by ISPE to help industry to implement ICH guidance
- US Food and Drug Administration (FDA) current Good Manufacturing Practices (cGMPs) for the 21st Century Initiative and associated guidance: promoting science based risk management
- Pharmaceutical Inspection Cooperation Scheme (PIC/S) Guidance on Good Practices for Computerised Systems in Regulated GxP Environments: clarifying regulatory expectations
- Emerging industry standards such as those produced by the ASTM E55 Committee¹ promoting process understanding, control, and capability for drug development and manufacture

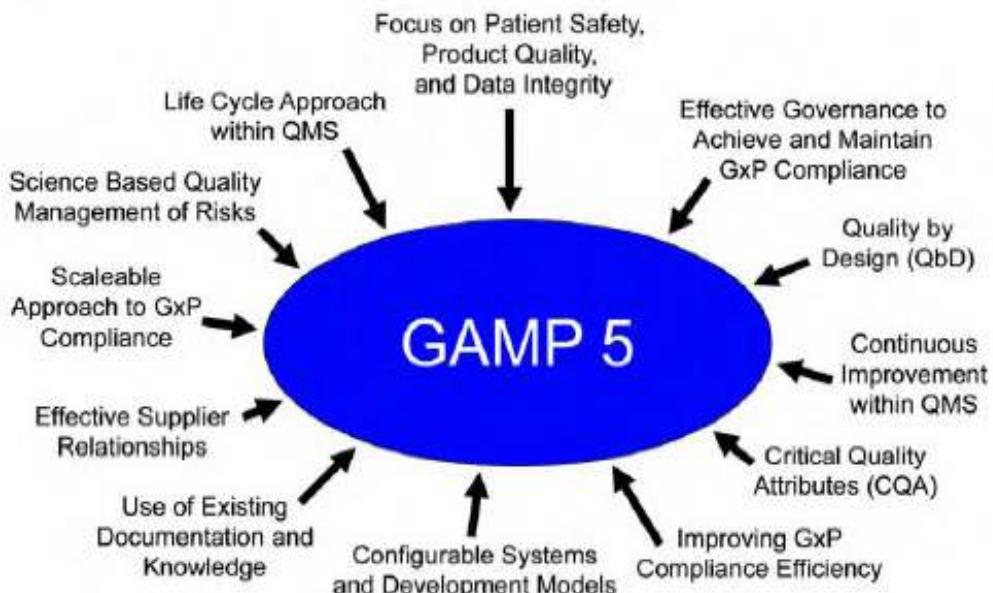
These regulatory and industry developments focus attention on patient safety, product quality, and data integrity. This is a key driver for this Guide.

In addition to this, there is the need to:

- avoid duplication of activities (e.g., by fully integrating engineering and computer system activities so that they are only performed once)
- leverage supplier activities to the maximum possible extent, while still ensuring fitness for intended use
- scale all life cycle activities and associated documentation according to risk, complexity, and novelty
- recognize that most computerized systems are now based on configurable packages, many of them networked
- acknowledge that traditional linear or waterfall development models are not the most appropriate in all cases

These regulatory and industry developments and expectations lead to the drivers shown in Figure 1.1.

Figure 1.1: Drivers for GAMP 5



¹ Including, but not limited to, ASTM E2500 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment.

1.2 New and Revised Material

Particular emphasis is given in this Guide on providing a cost effective approach to compliance and demonstrating fitness for intended use. To support this, new and updated guidance is given on:

- a complete system life cycle approach as part of a Quality Management System (QMS), from concept to retirement
- a scaleable approach to achieve and maintain GxP compliance driven by novelty, complexity, risk to patient safety, product quality, and data integrity
- clarifying the role of the Quality Unit, and introducing the roles of process owner, system owner, and Subject Matter Experts (SMEs)
- in the GMP environment, stressing the importance of clear requirements based on a thorough understanding of the science and of the Critical Quality Attributes (CQAs) of the development and manufacturing process and drug products, to facilitate the adoption of a Quality by Design (QbD) approach
- the leveraging of supplier documentation and knowledge, wherever possible, to avoid unnecessary duplication
- improving efficiency by promoting practical and effective interpretation of GAMP guidance
- maximizing use of documentation from activities, such as development and commissioning, as verification evidence
- the importance of effective governance to achieve and maintain compliance
- identifying opportunities for process and system improvements based on periodic review, root-cause analysis, and Corrective and Preventive Action (CAPA)

New information is provided in specific appendices on the following topics of special interest to industry:

- alignment with ASTM E2500
- organizational change
- outsourcing
- electronic batch recording
- end user applications, such as spreadsheets and small databases
- patch management

In summary, this Guide has been updated to address the changing environment, while still satisfying international GxP regulatory expectations, current at time of publication. This Guide represents industry good practice at time of publication and remains compatible with the principles presented in GAMP 4. The scope has been widened to include related industries and their suppliers, including biotechnology and systems used in medical device manufacturing (excluding software embedded within the medical devices).

1.3 Purpose

The purpose of this Guide is to provide a cost effective framework of good practice to ensure that computerized systems are fit for intended use and compliant with applicable regulations. The framework aims to safeguard patient safety, product quality, and data integrity, while also delivering business benefit. This Guide also provides suppliers to the life science industry with guidance on the development and maintenance of systems by following good practice.

Patient safety is affected by the integrity of critical records, data, and decisions, as well as those aspects affecting physical attributes of the product. The phrase 'patient safety, product quality, and data integrity' is used throughout this document to underline this point.

This Guide is intended for use by **regulated companies, suppliers, and regulators**. Suppliers include providers of software, hardware, equipment, system integration services, and IT support services, both internal and external to the regulated company.

This Guide has been designed for use by a wide range of disciplines and responsibilities, including:

- management
- quality unit
- research
- development
- manufacture
- laboratory
- engineering
- IT
- support staff
- all associated suppliers

GAMP documents are guides and not standards. It is the responsibility of regulated companies to establish policies and procedures to meet applicable regulatory requirements. Consequently, it is inappropriate for suppliers or products to claim that they are GAMP certified, approved, or compliant.

1.4 Scope

This Guide applies to computerized systems used in regulated activities covered by:

- Good Manufacturing Practice (GMP) (pharmaceutical, including Active Pharmaceutical Ingredient (API), veterinary, and blood)
- Good Clinical Practice (GCP)
- Good Laboratory Practice (GLP)

- Good Distribution Practice (GDP)
- Medical Device Regulations (with the exception of software embedded within medical devices)

These are collectively known as GxP regulations (see Section 2 of this Guide for full definition).

This Guide provides an approach that is suitable for all types of computerized systems, focusing on those based on standard and configurable products, but equally applicable to custom (bespoke) applications.

The principles described can be applied to a wide range of computerized systems. Detailed application of these principles to specific system types (e.g., IT, infrastructure, process control systems, and analytical laboratory systems) is described in supporting GAMP Good Practice Guides (see Appendix G1).

Not all the activities defined in this Guide will apply to every system. The scaleable approach enables regulated companies to select the appropriate system life cycle activities.

This Guide is also consistent with other regulatory demands such as Sarbanes-Oxley (SOX).² However, the use of this Guide does not guarantee compliance with, or replace, these regulatory demands.

It is recognized that there are acceptable methods other than those described in this Guide. The Guide is not intended to place any constraints on innovation and development of new concepts and technologies.

1.4.1 Supplier Aspects

The computerized system life cycle described in this Guide for a regulated company should not be confused with the need for a defined approach or method for software development, which is typically the responsibility of the supplier.

This Guide defines activities and responsibilities expected of the supplier in the provision of products and services. These activities perform an important role in supporting regulated company activities. The supplier may be a third party or an internal group of the regulated company.

This Guide uses various diagrams to represent the system life cycle. These diagrams often present relationships in a linear representation. This is not intended to constrain the choice of development methods and models. Suppliers should use the most appropriate methods and models, which may include RAD or prototyping techniques.

Modern systems may have a complex supply chain involving multiple suppliers. This Guide aims to meet the needs of each group.

1.5 Business Benefits

There are major business benefits in having a defined process that delivers systems that are fit for intended use, on time, and within budget. Systems that are well defined and specified are easier to support and maintain, resulting in less downtime and lower maintenance costs.

Specific benefits to both regulated companies and suppliers include:

- reduction of cost and time taken to achieve and maintain compliance
- early defect identification and resolution leading to reduced impact on cost and schedule
- cost effective operation and maintenance

² The US Sarbanes-Oxley law, specifically Section 404, mandates control of computer systems that generate financial records. Many of the good practice principles and electronic records management controls are relevant to compliance with this law.

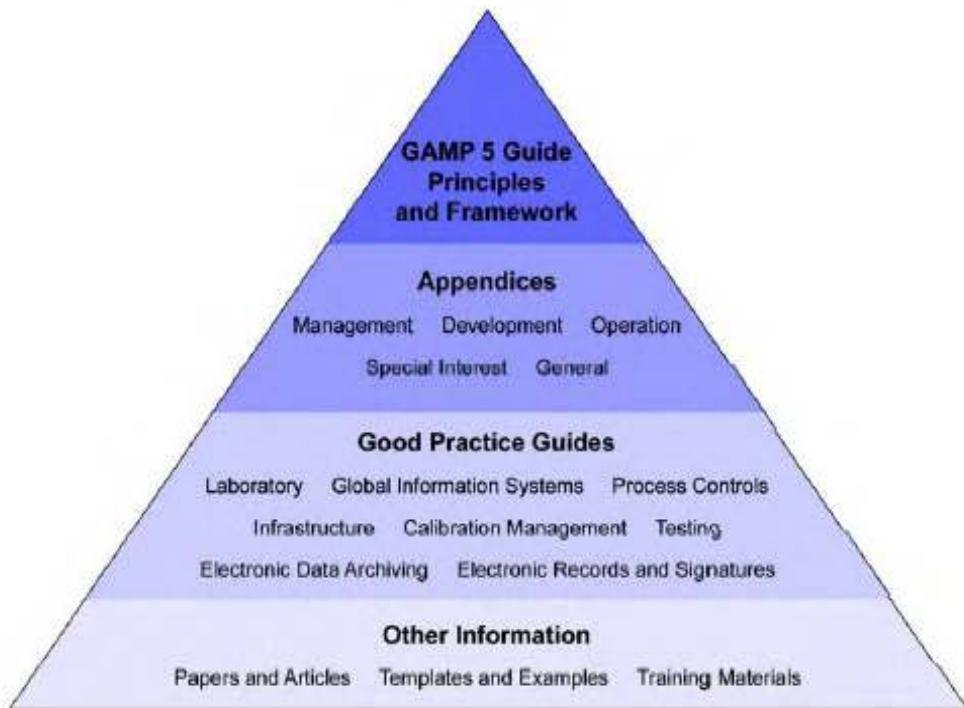
- effective change management and continuous improvement
- enabling of innovation and adoption of new technology
- providing frameworks for user/supplier co-operation
- assisting suppliers to produce required documentation
- promotion of common system life cycle, language, and terminology
- providing practical guidelines and examples
- promoting pragmatic interpretation of regulations

1.6 Structure

1.6.1 Overview of GAMP Documentation Structure

This Guide forms part of a family of documents that together provide a powerful and comprehensive body of knowledge covering all aspects of computerized systems good practice and compliance.

Figure 1.2: GAMP Documentation Structure



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

The Main Body provides principles and a life cycle framework applicable to GxP regulated computerized systems.

Practical guidance on a wide range of specific topics, such as planning, specification, risk management, testing, operation, and change management is provided in the supporting appendices. A new set of appendices is also provided in this Guide to cover topics of special interest, such as outsourcing and end user applications.

Separate GAMP Good Practice Guides (GPGs) cover the application of these general principles and framework to specific types of systems and platforms. Other GAMP GPGs provide detailed approaches to specific activities and topics. A summary of the purpose and scope of each GAMP GPG is given in Appendix G1.

It is intended that GPGs will be updated, where necessary, to align with the key concepts described in this Guide. New GPGs also are being developed.

Further details are available on ISPE Web site.

1.6.2 *GAMP 5 Main Body Structure*

The Main Body introduction covers the purpose, scope, benefits, and structure of this Guide. Subsequent sections of the Main Body cover the topics:

- key concepts
- life cycle approach
- life cycle phases:
 - concept
 - project
 - operation
 - retirement
- science based quality risk management
- regulated company activities:
 - governance for achieving compliance
 - system specific activities
- supplier activities
- efficiency improvements

The key concepts (see Section 2 of this Guide) are the five concepts, based on innovative industry thinking, current at the time of publication, that underpin the rest of the document.

The computerized system life cycle encompasses all activities from initial concept, and understanding the requirements, through development, release, and operational use, to system retirement. Section 3 of this Guide describes these activities and how they are related.

Section 4 describes the project life cycle phase in more detail, including:

- planning

- specification, configuration, and coding
- verification
- reporting and release

The key supporting processes of risk management, change and configuration management, design review, traceability, and document management are also introduced.

Quality risk management is a systematic approach for the assessment, control, communication, and review of risks to patient safety, product quality, and data integrity. It is an iterative process applied throughout the entire system life cycle. Section 5 of this Guide describes this approach, and how these activities should be based on good science and product and process understanding.

Ensuring compliance and fitness for purpose is the responsibility of the regulated company. Effective and consistent **regulated company activities** for individual systems requires a defined organizational and governance framework, covering aspects such as policies, responsibilities, management, and continuous improvement. Governance and system specific regulated company activities are covered in Section 6 of this Guide.

While the responsibility for compliance lies with the regulated company, the supplier has a key role to play. An overview of typical **supplier activities** is given in Section 7 of this Guide.

This Guide provides a flexible framework for achieving compliant computerized systems that are fit for intended use, but the full benefits can be obtained only if the framework is applied effectively in the context of a particular organization. Section 8 covers key topics leading to **efficiency improvements**.

2 Key Concepts

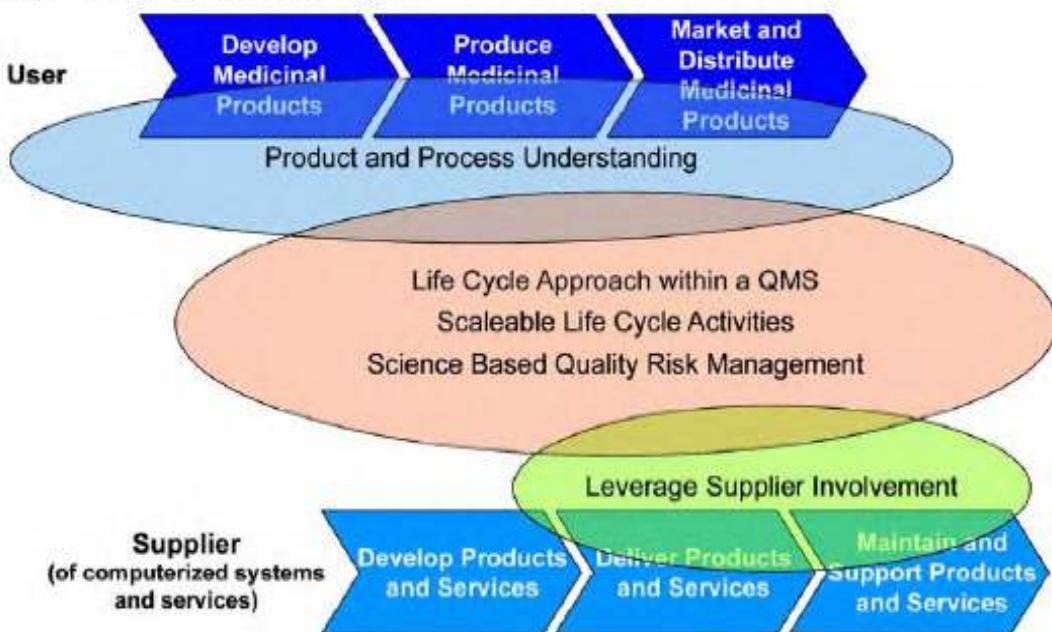
2.1 Key Concepts

Five key concepts are applied throughout this Guide:

1. product and process understanding
2. life cycle approach within a QMS
3. scaleable life cycle activities
4. science based quality risk management
5. leveraging supplier involvement

The relationship between these concepts is shown in Figure 2.1.

Figure 2.1: Key Concepts of this Guide



2.1.1 Product and Process Understanding

An understanding of the supported process is fundamental to determining system requirements. Product and process understanding is the basis for making science- and risk-based decisions to ensure that the system is fit for its intended use.

Efforts to ensure fitness for intended use should focus on those aspects that are critical to patient safety, product quality, and data integrity. These critical aspects should be identified, specified, and verified.

Systems within the scope of this Guide support a wide range of processes, including clinical trials, toxicological studies, API production, formulated product production, warehousing, distribution, and pharmacovigilance.

For some manufacturing systems, process requirements depend on a thorough understanding of product characteristics. For these systems, identification of Critical Quality Attributes (CQAs) and related Critical Process Parameters (CPPs) enable process control requirements to be defined.

Specification of requirements should be focused on critical aspects. The extent and detail of requirement specification should be commensurate with associated risk, complexity, and novelty of the system.

Incomplete process understanding hinders effective and efficient compliance and achievement of business benefit.

2.1.2 Life Cycle Approach within a QMS

Adopting a complete computerized system life cycle entails defining activities in a systematic way from system conception to retirement. This enables management control and a consistent approach across systems.

The life cycle should form an intrinsic part of the company's QMS, which should be maintained up to date as new ways of working are developed.

As experience is gained in system use, the QMS should enable continuous process and system improvements based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures. Identified improvements and corrective actions should follow change management.

A suitable life cycle, properly applied, enables the assurance of quality and fitness for intended use, and achieving and maintaining compliance with regulatory requirements. A well managed and understood life cycle facilitates adoption of a QbD approach.

The life cycle approach is fundamental to this Guide and embodies each of the other key concepts. The life cycle is structured into phases and activities, as described in Section 3 of this Guide.

2.1.3 Scalable Life Cycle Activities

Life cycle activities should be scaled according to:

- system impact on patient safety, product quality, and data integrity (Risk Assessment)
- system complexity and novelty (architecture and categorization of system components)
- outcome of supplier assessment (supplier capability)

Business impact also may influence the scaling of life cycle activities.

The strategy should be clearly defined in a plan and follow established and approved policies and procedures.

2.1.4 Science Based Quality Risk Management

Quality Risk Management is a systematic process for the assessment, control, communication, and review of risks.

Application of Quality Risk Management enables effort to be focused on critical aspects of a computerized system in a controlled and justified manner.

Quality Risk Management should be based on clear process understanding and potential impact on patient safety, product quality, and data integrity. For systems controlling or monitoring CPPs, these should be traceable to CQAs, and ultimately back to the relevant regulatory submissions for manufacturing systems.

Qualitative or quantitative techniques may be used to identify and manage risks. Controls are developed to reduce risks to an acceptable level. Implemented controls are monitored during operation to ensure ongoing effectiveness.

A practical risk management process is introduced and described in Section 5 of this Guide.

2.1.5 Leveraging Supplier Involvement

Regulated companies should seek to maximize supplier involvement throughout the system life cycle in order to leverage knowledge, experience, and documentation, subject to satisfactory supplier assessment.

For example, the supplier may assist with requirements gathering, risk assessments, the creation of functional and other specifications, system configuration, testing, support, and maintenance.

Planning should determine how best to use supplier documentation, including existing test documentation, to avoid wasted effort and duplication. Justification for the use of supplier documentation should be provided by the satisfactory outcome of supplier assessments, which may include supplier audits.

Documentation should be assessed for suitability, accuracy, and completeness. There should be flexibility regarding acceptable format, structure, and documentation practices.

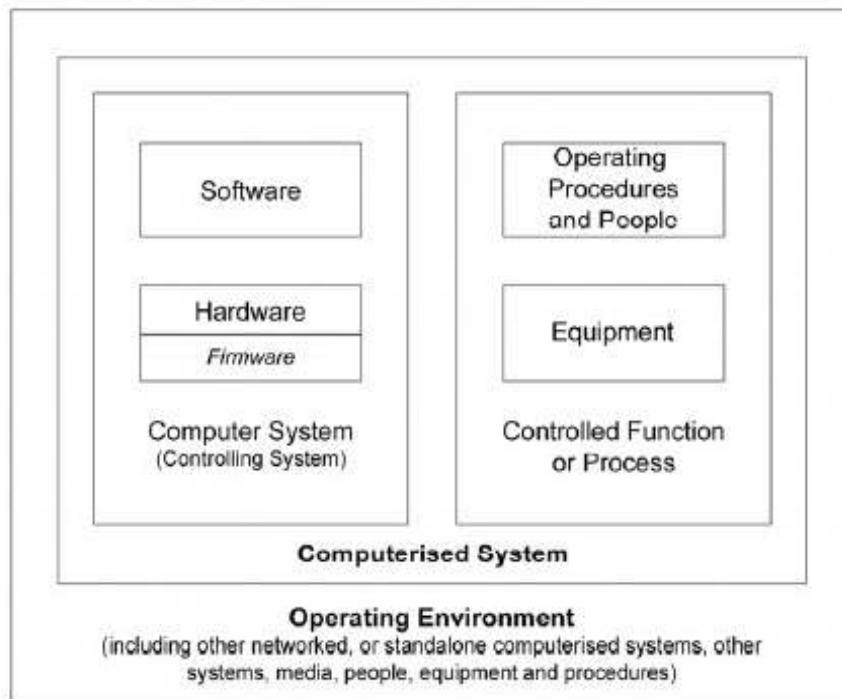
Supplier assessment is described in Section 6 of this Guide.

2.2 Key Terms

Computerized System

A computerized system consists of the hardware, software, and network components, together with the controlled functions and associated documentation (see also the *GAMP Good Practice Guide: IT Infrastructure Control and Compliance* for further details on network components).

Figure 2.2: Computerised System – from PIC/S Guidance



PIC/S Good Practices for Computerised Systems in Regulated 'GxP' Environments' (PI 011).

This term covers a broad range of systems, including:

- clinical trials data management
- manufacturing resource planning
- laboratory information management
- automated manufacturing equipment
- automated laboratory equipment
- process control and process analysis
- manufacturing execution
- building management
- warehousing and distribution
- blood processing management
- adverse event reporting (vigilance)
- document management

Computerized System Validation

Achieving and maintaining compliance with applicable GxP regulations and fitness for intended use by:

- the adoption of principles, approaches, and life cycle activities within the framework of validation plans and reports
- the application of appropriate operational controls throughout the life of the system

GxP Compliance

Meeting all applicable pharmaceutical and associated life-science regulatory requirements.

GxP Regulated Computerized System

Computerized systems that are subject to GxP regulations. The regulated company must ensure that such systems comply with the appropriate regulations.

GxP Regulation

The underlying international pharmaceutical requirements, such as those set forth in the US FD&C Act, US PHS Act, FDA regulations, EU Directives, Japanese regulations, or other applicable national legislation or regulations under which a company operates.

These include but are not limited to (further descriptions provided in Glossary):

- GMP

- GCP
- GLP
- GDP
- Good Quality Practice (GQP)
- Good Pharmacovigilance Practice
- Medical Device Regulations
- Prescription Drug Marketing Act (PDMA)

Process Owner

The person ultimately responsible for the business process or processes being managed. This person is usually the head of the functional unit or department using that system, although the role should be based on specific knowledge of the process rather than position in the organization. The process owner is responsible for ensuring that the computerized system and its operation is in compliance and fit for intended use in accordance with applicable Standard Operating Procedures (SOPs) throughout its useful life. Responsibility for control of system access should be agreed between process and system owner. In some cases, the process owner also may be the system owner. (Note: Ownership of the data held on a system should be defined and typically belongs to the process owner).

(cf. System Owner)

Quality Management System (QMS)

Management system to direct and control an organization with regard to quality. (ISO).

(This is equivalent to Quality System as defined in ICH Q9.)

Subject Matter Expert (SME)

Those individuals with specific expertise in a particular area or field. SMEs should take the lead role in the verification of computerized systems. SME responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results. (ASTM E2500)

System Owner

The person ultimately responsible for the availability, support and maintenance of a system, and for the security of the data residing on that system. This person is usually the head of the department responsible for system support and maintenance although the role should be based on specific knowledge of the system rather than position in the organization. The system owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable SOPs. Responsibility for control of system access should be agreed between process and system owner. In some cases, the system owner also may be the process owner.

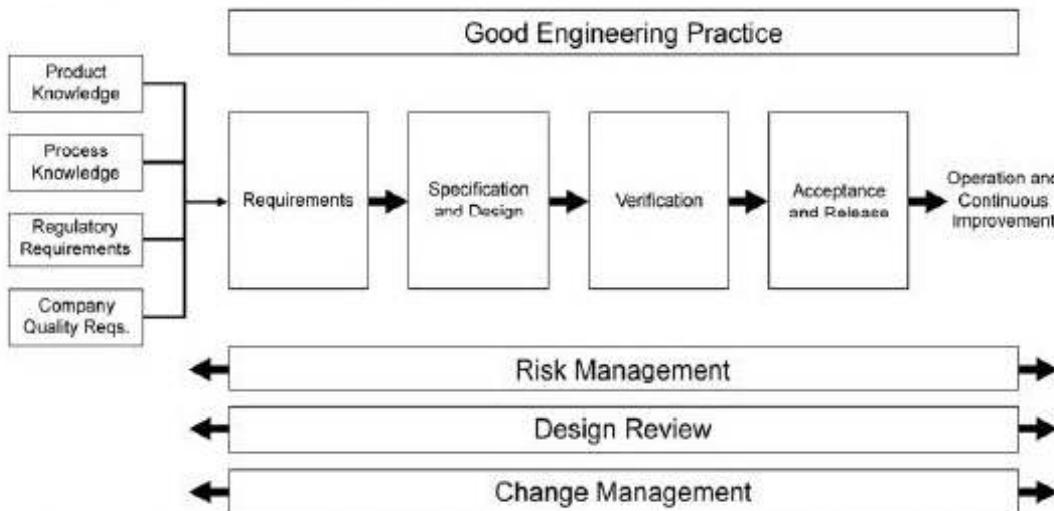
(cf. Process Owner)

3 Life Cycle Approach

Compliance with regulatory requirements and fitness for intended use may be achieved by adopting a life cycle approach following good practice as defined in this Guide.

A life cycle approach entails defining and performing activities in a systematic way from conception, understanding the requirements, through development, release, and operational use, to system retirement. Figure 3.1 shows a general specification, design, and verification process described in ASTM E2500.

Figure 3.1: The Specification, Design, and Verification Process



Reprinted with permission from *ASTM E2500-07 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment*, copyright ASTM International, 100 Barr Harbor Dr., West Conshohocken, PA 19428. A copy of the complete standard may be obtained from ASTM at www.astm.org.

This section of the Guide introduces the computerized system life cycle, a general approach to specification and verification, and a framework for computerized system validation.

3.1 Computerized System Life Cycle

The computerized system life cycle encompasses all activities from initial concept to retirement.

The life cycle for any system consists of four major phases:

- concept
- project
- operation
- retirement

During the concept phase, the regulated company considers opportunities to automate one or more business processes based upon business need and benefits. Typically, at this phase, initial requirements will be developed and potential solutions considered. From an initial understanding of scope, costs, and benefits, a decision is made on whether to proceed to the project phase.

The project phase involves planning, supplier assessment and selection, various levels of specification, configuration (or coding for custom applications), and verification leading to acceptance and release for operation. Risk Management is applied to identify risks and to remove or reduce them to an acceptable level.

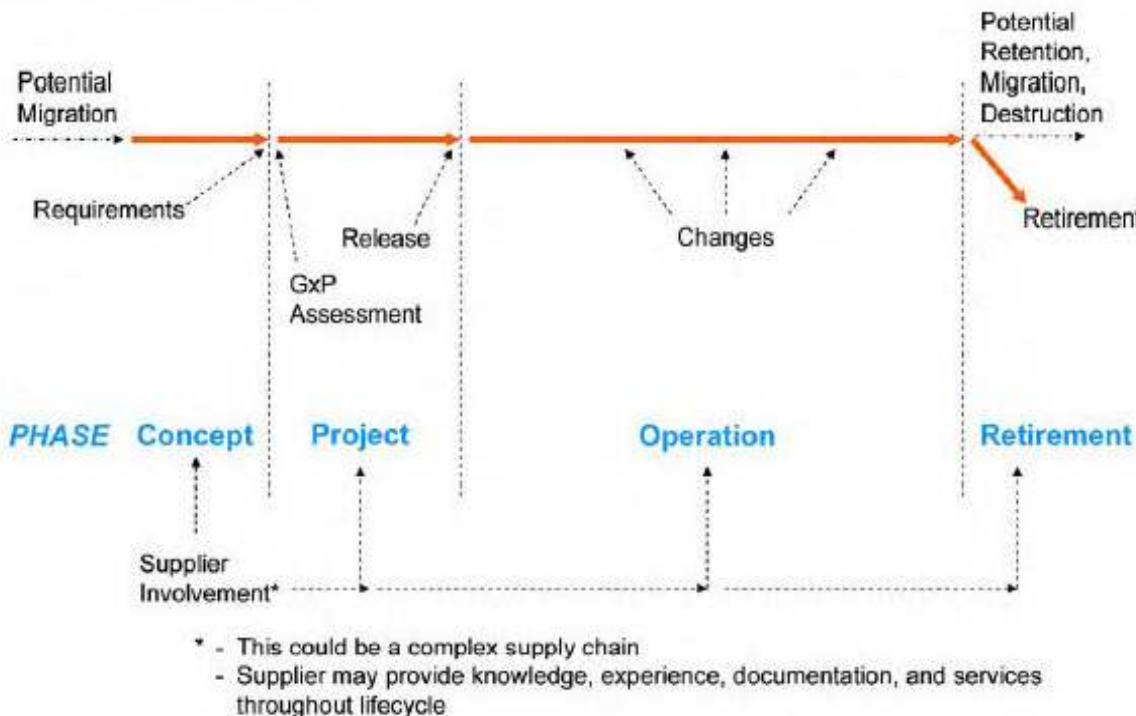
System operation, typically, is the longest phase and is managed by the use of defined, up to date, operational procedures applied by personnel who have appropriate training, education, and experience. Maintaining control (including security), fitness for intended use, and compliance are key aspects. The management of changes of different impact, scope, and complexity is an important activity during this phase.

The final phase is the ultimate retirement of the system. It involves decisions about data retention, migration, or destruction, and the management of these processes.

Suppliers of products and services should be involved as appropriate throughout the life cycle. It may be appropriate to delegate many of the described activities to suppliers, subject to satisfactory supplier assessment and control measures.

These life cycle phases are shown in Figure 3.2.

Figure 3.2: Life Cycle Phases



An inventory of computerized systems should be maintained. Further details are given in Section 6 of this Guide. A GxP assessment should be performed at the beginning of the project stage to determine whether a system is GxP regulated, and if so, which specific regulations apply, and to which parts of the system they are applicable. This should be performed as part of the initial system risk assessment (Step 1 as described in Section 5 of this Guide). For similar systems, it may be appropriate to base the GxP assessment on the results of a previous assessment provided the regulated company has an appropriate established procedure.

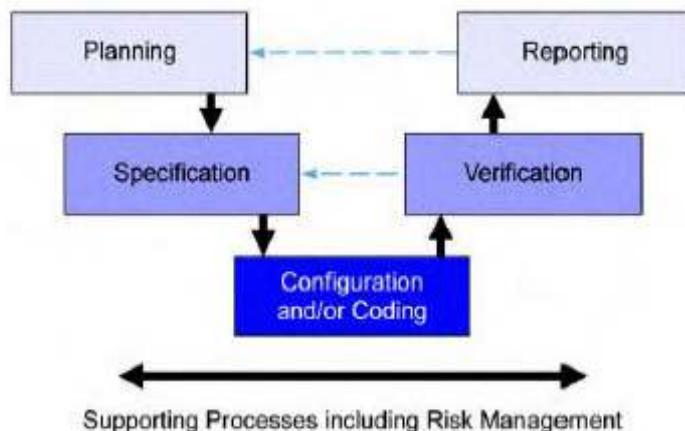
The computerized system life cycle described in this section should not be confused with the need for a defined approach or method for software development by the supplier. Section 7 of this Guide discusses supplier activities in more detail.

3.2 Specification and Verification

Figure 3.3 shows a general approach for achieving computerized system compliance and fitness for intended use within the system life cycle.

As shown, the specification activities have equivalent verification steps to determine whether the specification has been met. A hierarchy of specifications may be required for larger systems, while specifications may be combined for smaller, simpler, systems or systems classed as low risk. Specifications should be addressed by appropriate verification steps.

Figure 3.3: A General Approach for Achieving Compliance and Fitness for Intended Use



The application of this general approach will vary widely depending on the risk, complexity, and novelty of the system. Specific examples showing typical activities for different types of systems are provided in Section 4 of this Guide.

While this section provides a suggested approach for activities performed by a regulated company, it is recognized that other models and approaches are equally acceptable.

3.3 Computerized System Validation Framework

Traditionally GAMP has advocated a computerized system validation framework to achieve and maintain GxP compliance throughout the computerized system life cycle.

This framework is based on system specific validation plans and reports and the application of appropriate operational controls. Validation plans and reports provide a disciplined and consistent approach to meeting regulatory requirements, leading to appropriate documentation at the right level. Such documents are valuable both in preparing for, and during, regulatory inspections.

This framework is still applicable for the majority of computerized systems. This Guide has built on these principles by clarifying the scalability of the approach, and the central role of Quality Risk Management, to effectively and efficiently cover the very wide range of systems in scope.

Where a computer system is regarded as one component of a wider manufacturing process or system, particularly in an integrated QbD environment, specific and separate computerized system validation may not be necessary. This environment requires both complete product and process understanding and that the critical process parameters can be accurately and reliably predicted and controlled over the design space. In such a case, the fitness for intended use of the computer system within the process may be adequately demonstrated by documented engineering or project activities together with subsequent Process Validation or continuous quality verification of the overall process or system. The same principle applies to the adoption of Process Analytical Technology (PAT).

For automated manufacturing equipment, separate computer system validation should be avoided. Computer system specification and verification should be part of an integrated engineering approach to ensure compliance and fitness for intended use of the complete automated equipment.

This framework is described in Appendix M1 and Appendix M7.

4 Life Cycle Phases

This section further describes the phases of the Computerized System Life Cycle introduced in Section 3 of this Guide.

4.1 Concept

Activities in this phase will depend on company approaches to initiating and justifying project commencement. Generally, these activities are outside the scope of GAMP. However, gaining management commitment to provide appropriate resources is an important pre-project activity.

4.2 Project

This section describes the following project stages in more detail:

- planning
- specification, configuration, and coding
- verification
- reporting and release

The key supporting processes of risk management, change and configuration management, design review, traceability, and document management also are described in this section.

Figure 4.1 shows how these project stages and supporting processes form part of the computerized system life cycle. The stages are equally applicable to the project phase and to subsequent changes during operation.

This is a simplified general model that describes a staged approach to the project phase. For example, it covers both configuration and coding, which are required only for certain types of system. Specific examples of how to use this staged approach for typical types of system are given in Section 4.2.6 of this Guide.

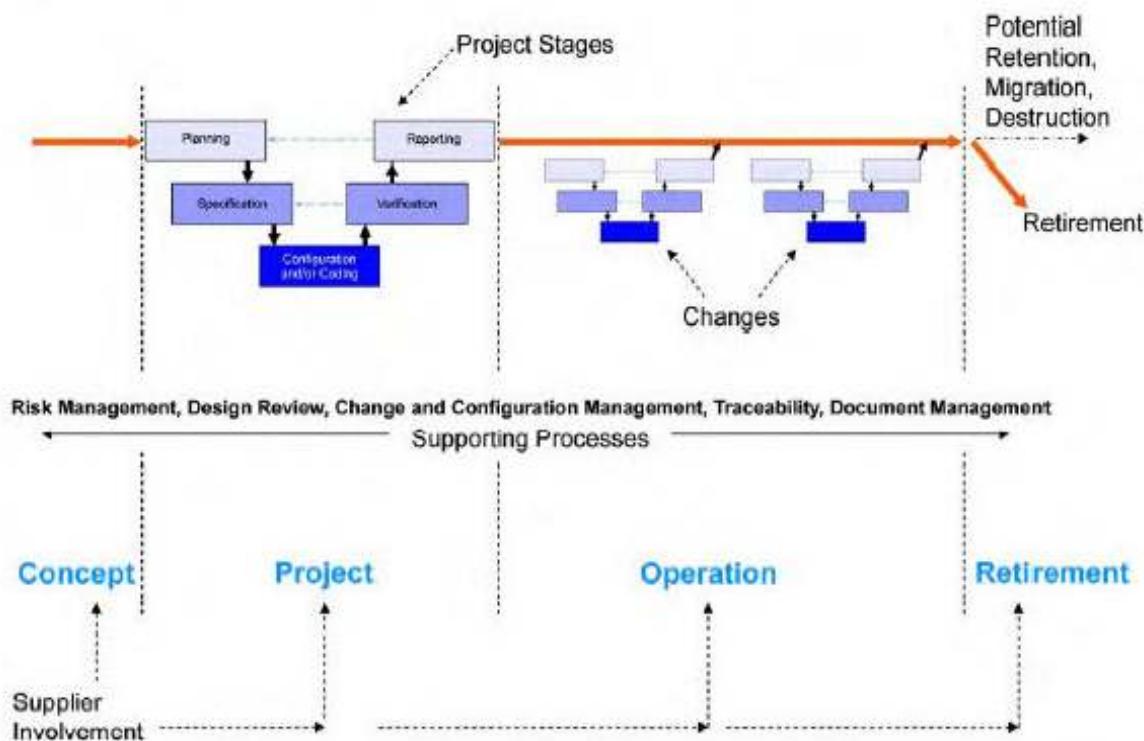
Each project stage typically involves multiple activities; planning for example may involve:

- preparing project plans
- developing requirements
- carrying out supplier assessments
- defining extent and formality of verification activities

While the project phase is made up of generally sequential stages, detailed activities often will be performed in parallel or with some overlap. For example, verification activities may occur through several stages.

The deliverables produced during the execution of these stages provide the documentary evidence that the system is fit for its intended use. Some of these may be used by the regulated company during regulatory inspections to provide justification of the suitability of the system.

Figure 4.1: Project Stages and Supporting Processes within the Life Cycle



4.2.1 Planning

Planning should cover all required activities, responsibilities, procedures, and timelines.

Activities should be scaled according to:

- system impact on patient safety, product quality, and data integrity (risk assessment)
- system complexity and novelty (architecture and categorization of system components)
- outcome of supplier assessment (supplier capability)

For further details on computerized system validation planning, see Appendix M1. In some cases, specific computerized system validation plans may not be required as described in Section 3.3 of this Guide.

A clear and complete understanding of user requirements is needed in order to facilitate effective planning. Initial requirements are often developed during the concept phase, and completion of user requirements gathering typically occurs during the planning stage.

The extent and detail of requirements gathering and specification should be sufficient to support risk assessment, further specification and development of the system, and verification. Comparison of available solutions may result in refinement of the requirements.

The approach should be based on product and process understanding, and relevant regulatory requirements. Where appropriate, e.g., for process control systems, requirements should be traceable to relevant CPPs.

User requirements are the responsibility of the user community and should be maintained and controlled.

See Appendix D1 for further details on User Requirements Specifications.

4.2.2 Specification, Configuration, and Coding

The role of specifications is to enable systems to be developed, verified, and maintained. The number and level of detail of the specifications will vary depending upon the type of system and its intended use. For example, software design specifications are not expected from the regulated company for non-configured products.

Specifications may be available from the supplier. Before use, the regulated company should ensure that they are adequate to support subsequent activities, including risk assessment, further specification and development of the system, and verification as appropriate.

The requirements for configuration and coding activities depend on the type of system (see Section 4.2.6 of this Guide for typical examples).

Any required configuration should be performed in accordance with a controlled and repeatable process. Any required software coding should be performed in accordance with defined standards. The need for code reviews should be addressed as part of risk management.

Configuration management is an intrinsic and vital aspect of controlled configuration and coding.

Figure 4.1 shows specification as a separate project stage from configuration and coding. However, specification activities may be distinct from, or tightly coupled with, configuration and coding activities depending on the software development method being adopted.

Specifications should be maintained and controlled. See Appendix D2 and Appendix D3 for further details on specification, configuration, and design. See Appendix D4 for further details on the management, development, and review of software.

4.2.3 Verification

Verification confirms that specifications have been met. This may involve multiple stages of reviews and testing depending on the type of system, the development method applied, and its use.

While verification is shown as a single box on Figure 4.1, verification activities occur throughout the project stages. For example, design reviews should verify specifications during the specification stage. See Section 4.2.5 of this Guide for further details on design reviews.

Terminology used to cover verification activities is described in Section 4.2.6.4 of this Guide.

Testing computerized systems is a fundamental verification activity. Testing is concerned with identifying defects so that they can be corrected, as well as demonstrating that the system meets requirements.

Testing often is performed at several levels depending on the risk, complexity, and novelty. One level of testing may be appropriate for simple and low risk systems. There is a range of different types of testing possible, including:

- normal case (positive)
- invalid case (negative)
- repeatability
- performance

- volume/load
- regression
- structural testing

Tests may be defined in one or more test specifications, to cover hardware, software, configuration, and acceptance.

An appropriate test strategy should be developed based on the risk, complexity, and novelty. Supplier documentation should be assessed and used if suitable. The strategy should define which types of testing are required and the number and purpose of test specifications. The test strategy should be reviewed and approved by appropriate SMEs.

See Appendix D5 for further details on testing and development of an appropriate test strategy.

4.2.4 Reporting and Release

The system should be accepted for use in the operating environment and released into that environment in accordance with a controlled and documented process. Acceptance and release of the system for use in GxP regulated activities should require the approval of the process owner, system owner, and quality unit representatives.

At the conclusion of the project, a computerized system validation report should be produced summarizing the activities performed, any deviations from the plan, any outstanding and corrective actions, and providing a statement of fitness for intended use of the system. See Appendix M7 for further details.

In some cases, specific computerized system validation reports may not be required as described in Section 3.3 of this Guide.

Well managed system handover from the project team to the process owner, system owner, and operational users is a pre-requisite for effectively maintaining compliance of the system during operation. See Appendix O1 and Section 8.6 of this Guide for further details on system handover.

4.2.5 Supporting Processes

4.2.5.1 Risk Management

An appropriate risk management process should be established.

See Section 5 of this Guide and Appendix M3 for further details on Risk Management.

4.2.5.2 Change and Configuration Management

Appropriate configuration management processes should be established such that a computerized system and all its constituent components can be identified and defined at any point.

Change management procedures also should be established. The point at which change management is introduced should be defined. Appropriate change processes should be applied to both project and operational phases.

Any involvement of the supplier in these processes should be defined and agreed.

See Appendix M8 for further details on project change and configuration management.

4.2.5.3 Design Review

At suitable stages during the life cycle, planned and systematic design reviews of specifications, design, and development should be performed. This design review process should evaluate deliverables to ensure that they satisfy the specified requirements. Corrective actions should be defined and progressed.

The rigor of the design review process and the extent of documentation should be based on risk, complexity, and novelty.

See Appendix M5 for further details on design reviews.

4.2.5.4 Traceability

Traceability is a process for ensuring that:

- requirements are addressed and traceable to the appropriate functional and design elements in the specifications
- requirements can be traced to the appropriate verification

As well as demonstrating coverage of design and verification, traceability can greatly assist the assessment and management of change.

Traceability should be focused on aspects critical to patient safety, product quality, and data integrity.

See Appendix M5 for further guidance on traceability.

4.2.5.5 Document Management

Management of documentation includes preparation, review, approval, issue, change, withdrawal, and storage. See Appendix M9 for further details on document management.

4.2.6 Practical Examples

This section shows how the general approach may be applied in a scaleable manner to three common types of system, using categorization of software. Categorization assists in selecting appropriate life cycle activities and documentation, as described in Appendix M4.

These examples are only intended to be indicative and for illustration purposes only. Actual approaches for specific systems should be based on the results of supplier assessments and risk assessments, in addition to categorization of system components, as described in Appendices M2, M3, and M4.

Terminology used in these examples is discussed in Section 4.2.6.4 of this Guide.

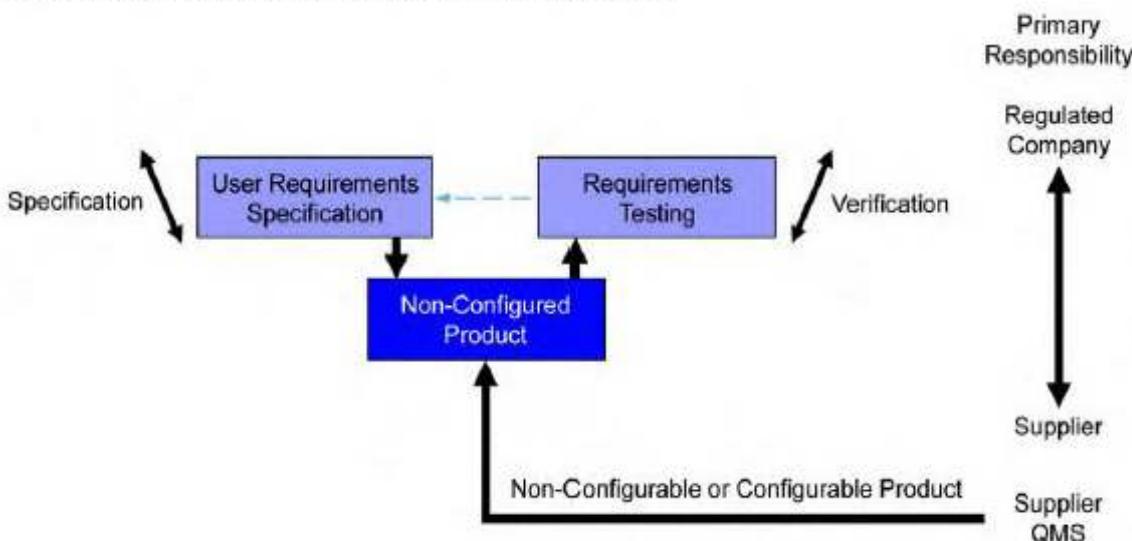
4.2.6.1 Example of a Non-Configured Product

Many computerized systems comprise commercially available software products running on standard hardware components.

Software products which are used off-the-shelf (i.e., which are either not configurable for a specific business process or where the default configuration is used) are typically classified as GAMP Category 3.

In such cases, and based on satisfactory supplier and risk assessments, a simple approach consisting of one level of specification and verification is typically applicable.

Figure 4.2: Approach for a Non-Configured Product (Category 3)



Testing typically covers:

- correct installation
- tests that demonstrate fitness for intended use and allow acceptance of the system against requirements
- any further tests as a result of risk and supplier assessments

Regulated companies typically perform the required specification and verification. While the system is not configured for a business process, there may be some limited configuration such as of run-time parameters or printer setup.

Supplier activities typically include supply of the product, and provision of documentation, training, and support and maintenance.

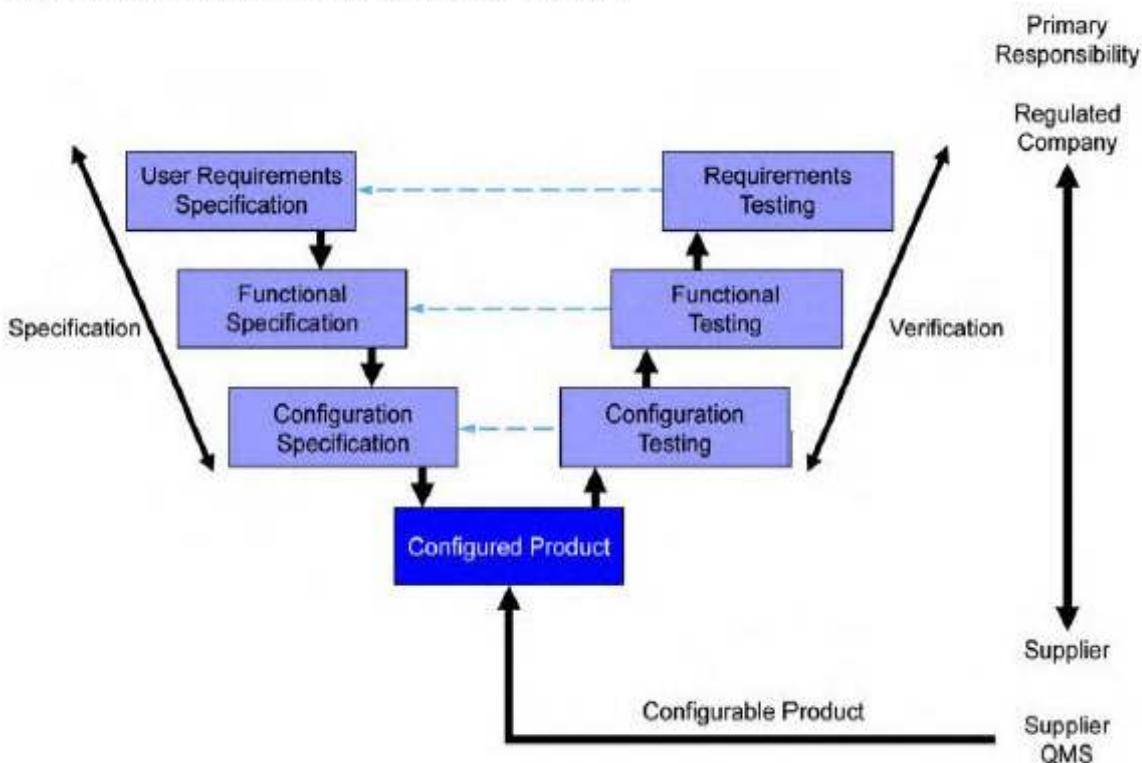
4.2.6.2 Example of a Configured Product

A common type of computerized system involves the configuration of commercially available software products running on standard hardware components.

Software products which are configured for a specific business process are typically classified as GAMP Category 4.

In such cases, and based on satisfactory supplier and risk assessments, the following approach consisting of three levels of specification and verification is typical. The number of documents required to cover these three levels will depend on the complexity and impact of the system. For example, for small or low risk systems the functional and configuration specifications may be combined into one document.

Figure 4.3: Approach for a Configured Product (Category 4)



Testing typically covers:

- correct installation
- configuration of the system
- functionality that supports the specific business process based on risk and supplier assessments (this is an area where supplier documentation may be leveraged, see Section 8.3 of this Guide)
- tests that demonstrate fitness for intended use and allow acceptance of the system against requirements
- any further tests as a result of risk and supplier assessments

Regulated companies should decide upon the required levels of specification and verification, and many of the project phase activities and documents may be delegated. Since the system is configured for a business process, testing should be focused on this configuration.

Supplier activities typically include:

- supply of the product
- production of specifications and test specifications on behalf of the regulated company
- support during configuration and testing
- user documentation

- training
- support and maintenance activities

The supply of the product and configuration may be performed by different suppliers.

Note that more complex configured systems may involve product customizations (changes to supplier delivered software) and new custom software, such as for interfaces.

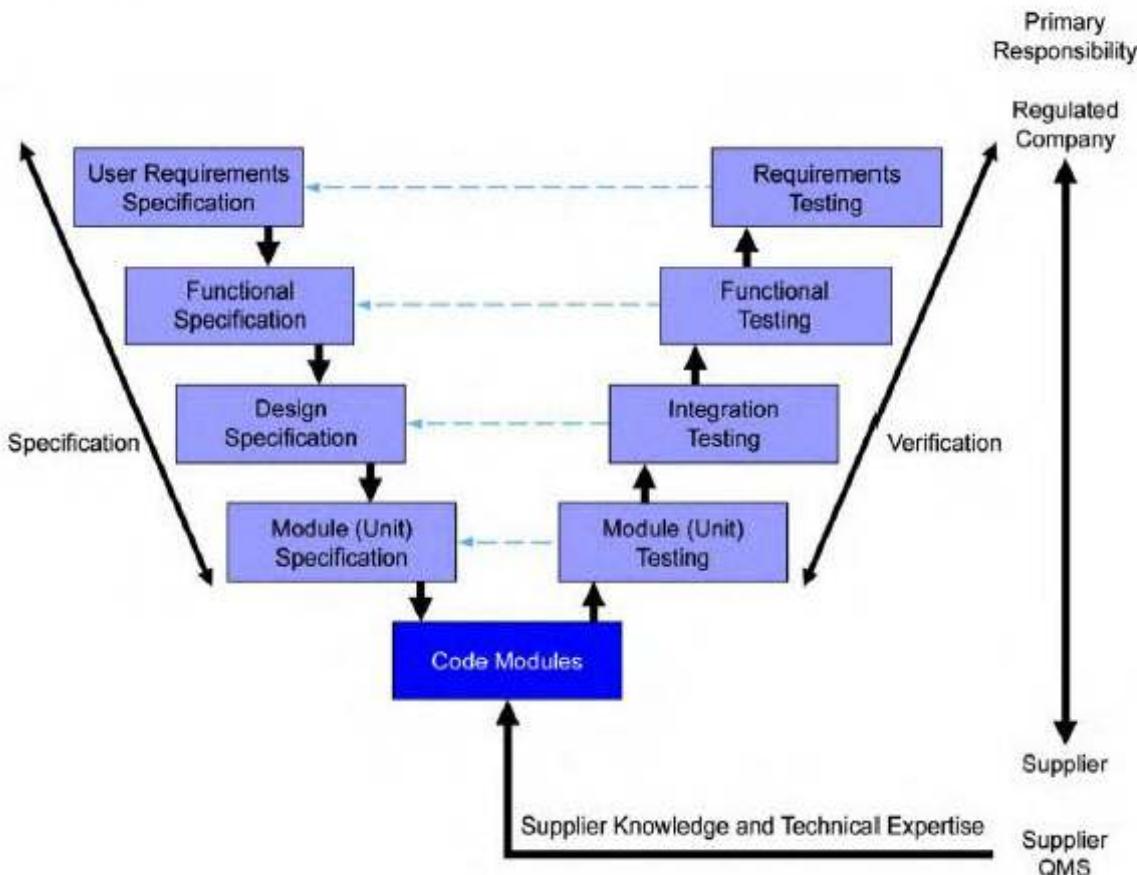
4.2.6.3 Example of a Custom Application

Some computerized systems are developed to meet individual user requirements, where no commercially available solution is suitable.

Such systems are becoming less common as companies use more standard products. The software developed for such systems is classified as GAMP Category 5.

In such cases, and based on satisfactory supplier and risk assessments, the following approach consisting of four main levels of specification and verification is typical. The number of documents required to cover these levels will depend on the complexity and impact of the system. For example, for a small system the design specifications may be combined into one document.

Figure 4.4: Approach for a Custom Application (Category 5)



Testing typically covers:

- correct installation
- functionality and design
- tests that demonstrate fitness for intended use and allow acceptance of the system against requirements
- any further tests as a result of risk assessments and supplier assessments

Regulated companies should decide upon the required levels of specification and verification, and many of the project phase activities and documents may be delegated. Since the system is new, rigorous testing should be performed at both functional and design levels.

Supplier activities typically include production of specifications and test specifications on behalf of the regulated company, development of new software, testing, user documentation, training, and support and maintenance activities.

Complex systems may require a further hierarchy of specifications covering hardware design specifications and configuration specifications.

4.2.6.4 Terminology

The specific terminology used to describe life cycle activities and deliverables varies from company to company and from system type to system type. There are a number of reasons for this, including:

- regulated companies having different approaches
- difference in emphasis of GLP, GCP, GMP, and medical devices
- difference in emphasis of various regulatory agencies
- different international or local standards being followed
- different types of computerized systems (e.g., IT, manufacturing, and laboratory systems)
- suppliers using a range of different development models and approaches

This Guide aims to be flexible, and does not intend to prescribe any one set of terms to the exclusion of others.

The terms used to describe verification activity in particular is a much debated area. This section describes how qualification terminology, as traditionally used, relates to the activities described in this Guide. This will assist readers who use this terminology with the application of this Guide.

Whatever terminology is used for verification activity, the overriding requirement is that the regulated company can demonstrate that the system is compliant and fit for intended use.

Table 4.1: Relationship between Traditional Qualification Terminology and GAMP 5 Activities

Traditional Term	Description	GAMP 5 Verification Activity
Design Qualification (DQ)	Documented verification that the proposed design of facilities, systems, and equipment is suitable for the intended purpose.	Design review (See Section 4.2.5 of this Guide for further details)
Installation Qualification (IQ)	Documented verification that a system is installed according to written and pre-approved specifications.	Checking, testing, or other verification to demonstrate correct: <ul style="list-style-type: none">• installation of software and hardware• configuration of software and hardware (See Appendix D5 for details)
Operational Qualification (OQ)	Documented verification that a system operates according to written and pre-approved specifications throughout specified operating ranges.	Testing or other verification of the system against specifications to demonstrate correct operation of functionality that supports the specific business process throughout all specified operating ranges. (See Appendix D5 for details)
Performance Qualification (PQ)	Documented verification that a system is capable of performing the activities of the processes it is required to perform, according to written and pre-approved specifications, within the scope of the business process and operating environment.	Testing or other verification of the system to demonstrate fitness for intended use and to allow acceptance of the system against specified requirements. (See Appendix D5 for details)

Note: The use of qualification terminology in relation to computerized systems and the relationship between OQ and PQ in particular, varies from company to company. The above comparisons provide a general interpretation only and are not intended to be prescriptive.

Regulated companies should decide on a verification approach appropriate to a specific system. Testing activities should be selected based on the risk, complexity, and novelty of the system as described in Section 4.2.3 of this Guide.

The examples in Section 4.2.6 of this Guide illustrate the typical different levels of testing applied to different categories of system, such as:

- module testing
- integration testing
- configuration testing
- functional testing
- requirements testing

Table 4.1 lists various GAMP verification activities. There is no one-to-one relationship between the levels of testing and the GAMP verification activities, for example:

- For a typical Category 3 system, testing of both installation and configuration are covered by requirements testing.

- For a typical Category 3 system, tests are executed to demonstrate fitness for intended use and to allow acceptance of the system against user requirements. There is typically no need for further testing to demonstrate correct operation of standard functionality of the product.
- For a typical Category 4 system, while testing of configuration is covered by configuration testing, testing of installation may occur at any of the testing levels depending on the project.
- For a typical Category 5 system, correct operation of functionality that supports the specific business process may be covered by module testing, integration testing and functional testing, and may be supplemented by pre-delivery testing.

The relationship between the required verification and the different levels of testing, particularly for GAMP Category 4 and GAMP Category 5 systems, may be complex. The verification or test strategy for a particular system should ensure that the required verification activities are adequately covered.

Acceptance of the system by the regulated company as being fit for release for operational use includes satisfactory completion of an agreed set of verification activities. For some systems, this may occur in stages including the leveraging, wherever possible, of testing or other acceptance activities performed prior to, and after, delivery. Commonly used terms within such a process include Factory Acceptance Testing, Site Acceptance Testing, and System Acceptance Testing. Verification activities should not be duplicated unnecessarily.

Whichever terms are used, the verification strategy should clearly define which activities should be satisfactorily completed to allow acceptance of the system for release into operational use by the regulated company.

See Appendix D5 for further guidance on aspects of testing.

4.3 Operation

This section provides comprehensive guidance on system operation. Not all of these activities will be directly relevant to all systems. The approach and required activities should be selected and scaled according to the nature, risk, and complexity of the system in question.

As part of preparing for final acceptance and formal handover for live operation, the regulated company should ensure that appropriate operational processes, procedures, and plans have been implemented, and are supported by appropriate training. These procedures and plans may involve the supplier in support and maintenance activities.

Once the system has been accepted and released for use, there is a need to maintain compliance and fitness for intended use throughout its operational life. This is achieved by the use of up to date documented procedures and training that cover use, maintenance, and management.

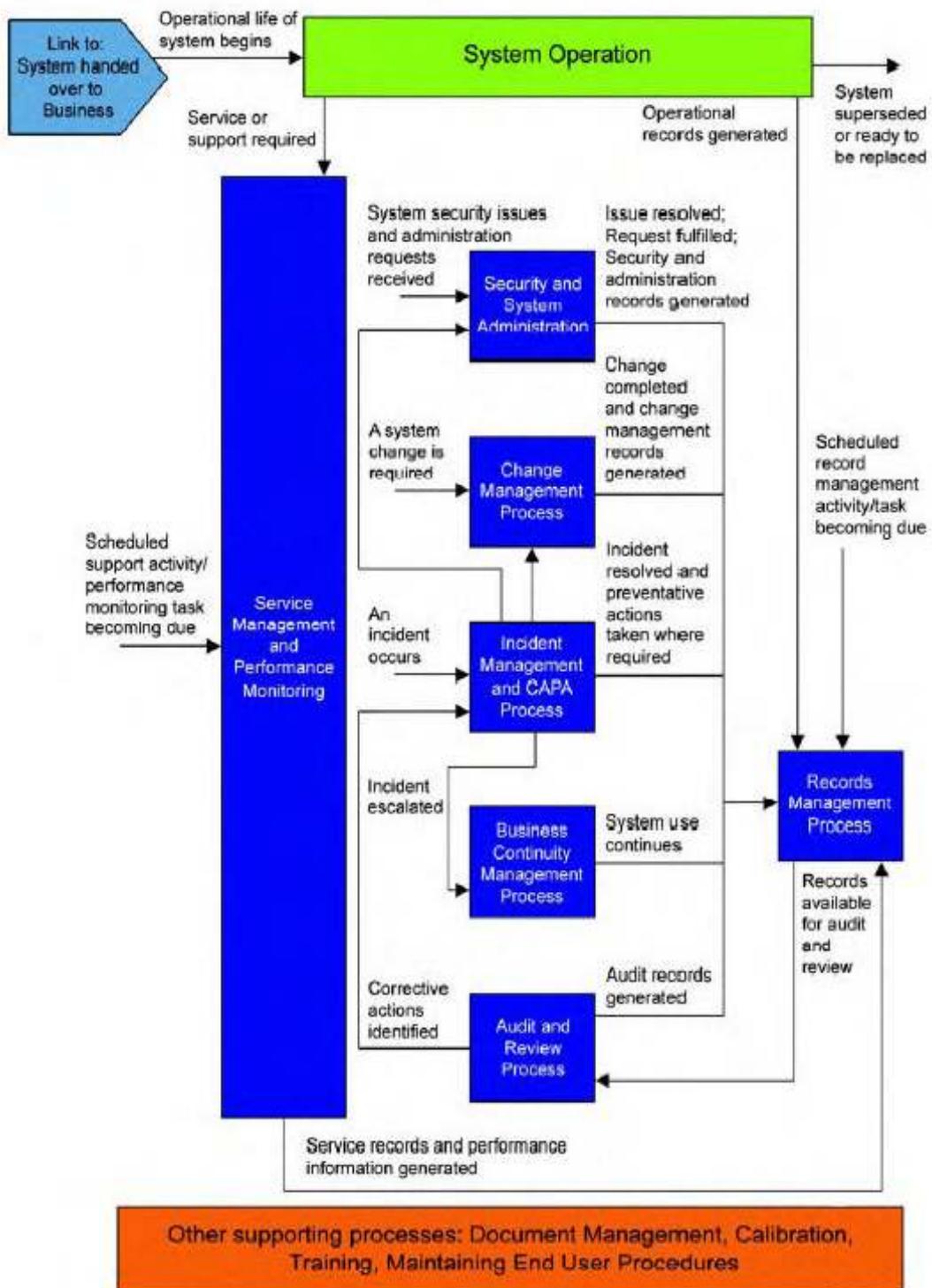
The operational phase of a system may last many years, and may include changes to software, hardware, the business process, and regulatory requirements. The integrity of the system and its data should be maintained at all times and verified as part of periodic review.

As experience is gained during operation, opportunities for process and system improvements should be sought based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures. Information from the Incident Management and CAPA processes can provide significant input to the evaluation.

Change management should provide a dependable mechanism for prompt implementation of technically sound improvements following the approach to specification, design, and verification described in this document. The rigor of the approach, including extent of documentation and verification, should be based on the risk and complexity of the change.

Maintaining system compliance involves many interrelated activities. Figure 4.5 shows the major relationships between related groups of these activities. Service management and performance monitoring occur throughout the operational life of the system. Other activities, such as change management, occur when triggered.

Figure 4.5: Major Information Flows between Operational Activities



Some of the groups of activities shown in Figure 4.5 contain several individual related processes, procedures, and plans, as described in Table 4.2.

Table 4.2: Grouping of Operational Processes

Group of Processes	Process	Appendix
Handover	Handover Process	O1
Service Management and Performance Monitoring	Establishing and Managing Support Services Performance Monitoring	O2 O3
Incident Management and CAPA	Incident Management CAPA	O4 O5
Change Management	Change Management Configuration Management Repair Activity	O6 O6 O7
Audits and Review	Periodic Review (Internal Quality Audits not covered by GAMP 5)	O8
Continuity Management	Backup and Restore Business Continuity Planning Disaster Recovery Planning	O9 O10 O10
Security and System Administration	Security Management Systems Administration	O11 O12
Records Management	Retention Archive and Retrieval	O13 O13

These processes are supported by QMS activities, such as document management, training management, and the maintenance of up to date end user procedures.

The individual support and maintenance processes required to maintain the compliance of computerized systems during operation are briefly described below and covered in more detail in the Operational Appendices as shown in Table 4.2.

See ITIL³ (Reference 36, Appendix G3) for further detail on IT service management. See Appendix G3 for other useful standards and guidance.

4.3.1 Handover Process

Handover is the process for transfer of responsibility of a computerized system from a project team or a service group to a new service group.

This is an important process; achieving compliance and fitness for intended use on its own may not be enough to guarantee a successful transfer into the operational phase.

The handover process will typically involve the project team (development group and/or supplier), process owner, system owner, and quality unit. The support group should be involved at the earliest opportunity.

See Appendix O1 for further details.

³ The IT Infrastructure Library® (ITIL) is the most widely accepted approach to IT service management. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally.

4.3.2 Service Management and Performance Monitoring

Figure 4.5 shows only the major relationships between operational processes. Service management and performance monitoring are shown related to records management due to records generated to demonstrate proper operation and performance of a system. In addition, there is potential interaction with incident management and CAPA and change management when the results of the service or monitoring indicate there are issues which need addressing. For clarity, these interactions are not shown in Figure 4.5.

4.3.2.1 Establishing and Managing Support Services

The support required for each system, and how it will be provided, should be established. Support may be provided by external or internal resources. This process should ensure that support agreements, maintenance plans, and SOPs are established.

See Appendix O2 for further details.

4.3.2.2 Performance Monitoring

The impact of system failure will vary depending on the criticality of the computerized system. Where appropriate, performance of the system should be monitored to capture problems in a timely manner. It also may be possible to anticipate failure through the use of monitoring tools and techniques.

The need for performance monitoring should be considered, and required activities scheduled and documented.

See Appendix O3 for further details.

4.3.3 Incident Management and CAPA

4.3.3.1 Incident Management

The incident management process aims to categorize incidents to direct them to the most appropriate resource or complementary process to achieve a timely resolution. There should be a procedure defining how problems related to software, hardware, and procedures should be captured, reviewed, prioritized, progressed, escalated, and closed. This includes the need for processes to monitor progress and provide feedback.

See Appendix O4 for further details.

4.3.3.2 Corrective and Preventive Action (CAPA)

CAPA is a process for investigating, understanding, and correcting discrepancies based on root-cause analysis, while attempting to prevent their recurrence.

In the operational environment the CAPA process for computerized systems should feed into, or be part of, the overall CAPA system used for the rest of operations. When incidents occur, or when opportunities to reduce process/system failures are identified by other means, corrective actions and preventive actions should be identified and processes established to ensure that these are implemented effectively. CAPA can provide a solution to problem control as described in ITIL Problem Management (Reference 36, Appendix G3).

See Appendix O5 for further details.

4.3.4 Change Management

4.3.4.1 Change Management

Change management is a critical activity that is fundamental to maintaining the compliant status of systems and processes. All changes that are proposed during the operational phase of a computerized system, whether related to software (including middleware), hardware, infrastructure, or use of the system, should be subject to a formal change control process (see Appendix O7 for guidance on replacements). This process should ensure that proposed changes are appropriately reviewed to assess impact and risk of implementing the change. The process should ensure that changes are suitably evaluated, authorized, documented, tested, and approved before implementation, and subsequently closed.

The process should allow the rigor of the approach, including the extent of documentation and verification, to be scaled based on the nature, risk, and complexity of the change. Some activities such as replacements and routine system administration tasks should be covered by appropriate repair or system administration processes.

Change management should provide a mechanism for prompt implementation of continuous process and system improvements based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures.

See Appendix O6 for further details.

4.3.4.2 Configuration Management

Configuration management includes those activities necessary to precisely define a computerized system at any point during its life cycle, from the initial steps of development through to retirement.

A configuration item is a component of the system which does not change as a result of the normal operation of the system. Configuration items should only be modified by application of a change management process. Formal procedures should be established to identify, define, and baseline configuration items, and to control and record modifications and releases of configuration items, including updates and patches.

See Appendix O6 for further details.

4.3.4.3 Repair Activity

The repair or replacement of defective computerized system components, typically hardware or infrastructure related, should be managed in accordance with a defined process. Such activities should be authorized and implemented only within the context of the change management process. Many repair activities are emergencies and require rapid resolution so the incident and change management processes should be designed to allow such activities to occur without delay or increased risk to the operational integrity of the computerized system.

See Appendix O7 for further details.

4.3.5 Periodic Review

Periodic reviews are used throughout the operational life of systems to verify that they remain compliant with regulatory requirements, fit for intended use, and meet company policies and procedures. The reviews should confirm that, for components of a system, the required support and maintenance processes and expected regulatory controls (plans, procedures, and records) are established.

Periodic reviews should be:

- scheduled at an interval appropriate to the impact and operation history of the system. Risk assessments should be used to determine which systems are in scope and the frequency of periodic review.
- performed in accordance with a pre-defined process
- documented with corrective actions tracked to satisfactory completion

Electronic data archives holding GxP data from retired systems also should be subject to periodic review. See the *GAMP Good Practice Guide: Electronic Data Archiving* (Reference 34, Appendix G3) for more details.

See Appendix O8 for further details.

4.3.6 Continuity Management

4.3.6.1 Backup and Restore

Processes and procedures should be established to ensure that backup copies of software, records, and data are made, maintained, and retained for a defined period within safe and secure areas.

Restore procedures should be established, tested, and the results of that testing documented.

See Appendix O9 for further details.

4.3.6.2 Business Continuity Planning

Business continuity planning is a series of related activities and processes concerned with ensuring that an organization is fully prepared to respond effectively in the event of failures and disruptions.

Critical business processes and systems supporting these processes should be identified and the risks to each assessed. Plans should be established and exercised to ensure the timely and effective resumption of these critical business processes and systems.

A Business Continuity Plan (BCP) defines how the business may continue to function and handle data following failure. It also defines the steps required to restore business processes following a disruption and, where appropriate, how data generated during the disruption should be managed.

The BCP also identifies the triggers for invoking the BCP, roles and responsibilities, and required communication.

See Appendix O10 for further details.

4.3.6.3 Disaster Recovery Planning

As a subset of business continuity planning, plans should be specified, approved, and rehearsed for the recovery of specific systems in the event of a disaster. These plans should detail the precautions taken to minimize the effects of a disaster, allowing the organization to either maintain or quickly resume critical functions. There should be a focus on disaster prevention, e.g., the provision of redundancy for critical systems.

See Appendix O10 for further details.

4.3.7 Security and System Administration

4.3.7.1 Security Management

Computerized systems and data should be adequately protected against wilful or accidental loss, damage, or unauthorized change.

Procedures for managing secure access, including adding and removing privileges for authorized users, virus management, password management, and physical security measures should be established before the system is approved for use.

Role-based security should be implemented, if possible, to ensure that sensitive data and functions are not compromised. Security management procedures should apply to all users, including administrators, super-users, users, and support staff (including supplier support staff).

See Appendix O11 for further details.

4.3.7.2 System Administration

Once a system is in operation the users of the system will require support. The System Administration process provides administrative support for systems, including performance of standard administration tasks. The extent of this process varies greatly depending on the nature of the system.

See Appendix O12 for further details.

4.3.8 Record Management

4.3.8.1 Retention

Policies for retention of regulated records should be established, based on a clear understanding of regulatory requirements, and existing corporate policies, standards, and guidelines.

See Appendix O13 for further details.

4.3.8.2 Archive and Retrieval

Archiving is the process of taking records and data off-line by moving them to a different location or system, often protecting them against further changes.

Procedures for archiving and retrieval of records should be established based on a clear understanding of regulatory requirements.

See Appendix O13 for further details.

The *GAMP Good Practice Guides: A Risk-Based Approach to Compliant Electronic Records and Signatures and Electronic Data Archiving* give further details.

4.4 Retirement

This section covers system withdrawal, system decommissioning, system disposal, and migration of required data.

4.4.1 Withdrawal

Removal of the system from active operations, i.e., users are deactivated, interfaces disabled. No data should be added to the system from this point forward. Special access should be retained for data reporting, results analysis and support.

4.4.2 Decommissioning

The controlled shutdown of a retired system.

4.4.3 Disposal

Data, documentation, software, or hardware may be permanently destroyed. Each may reach this stage at a different time. Data and documentation may not be disposed of until they have reached the end of the record retention period, as specified in the Record Retention policy.

Due to the volumes of data and records involved, retirement can be a major task, for IT systems in particular. Consideration should be given to:

- establishing procedures covering system retirement, including withdrawal, decommissioning, and disposal as appropriate
- documentary evidence to be retained of actions taken during retirement of the system
- GxP records to be maintained, their required retention periods, and which records can be destroyed
- the need to migrate records to a new system or archive, and method of verifying and documenting this process
- ability to retrieve these migrated records on the new system

Further guidance is also provided in the *GAMP Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures*.

See Appendix M10 for further details.

4.4.4 Data Migration

Data migration may be required when an existing system is replaced by a new system, when an operational system experiences a significant change, or when the scope of use of a system changes. The migration process should be accurate, complete, and verified.

See Appendix D7 for further details.

5 Quality Risk Management

Section 3 of this Guide introduced the concept of quality risk management as part of the life cycle approach. This section gives an overview of the quality risk management process and Appendix M3 provides more detail.

This section is primarily aimed at new computerized systems. It does not imply that formal risk assessments are required for all existing systems. The extent of risk management required for existing systems, including the need for formal risk assessments, should be considered as part of periodic review.

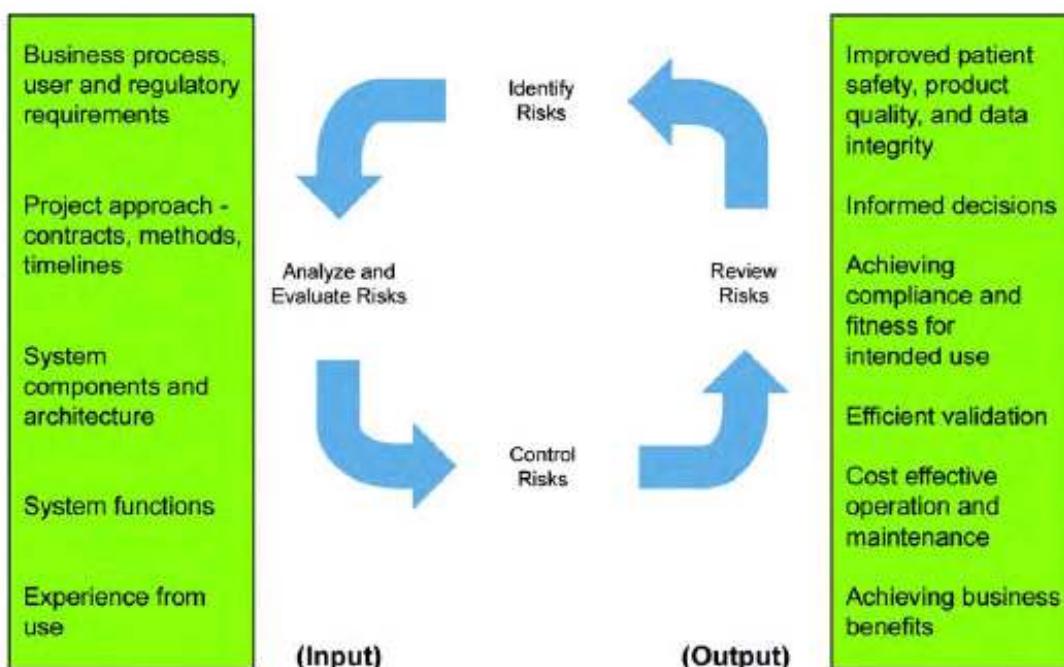
This section focuses on software products and custom applications rather than on infrastructure.

5.1 Overview

Quality risk management is a systematic process for the assessment, control, communication, and review of risks. It is an iterative process used throughout the entire computerized system life cycle from concept to retirement.

Figure 5.1 indicates key areas for risk management and the benefits of the approach.

Figure 5.1: Overview and Benefits of Risk Management



For a given organization, a framework for making risk management decisions should be defined to ensure consistency of application across systems and business functions. Terminology should be agreed upon, particularly regarding definitions and metrics for key risk factors.

Such a framework is most effectively implemented when it is incorporated into the overall QMS, and is fully integrated with the system life cycle.

5.2 Science Based Quality Risk Management

Determining the risks posed by a computerized system requires a common and shared understanding of:

- impact of the computerized system on patient safety, product quality, and data integrity
- supported business processes
- CQAs for systems that monitor or control CPPs
- user requirements
- regulatory requirements
- project approach (contracts, methods, timelines)
- system components and architecture
- system functions
- supplier capability

The organization also should consider other applicable risks, such as safety, health, and environment.

Managing the risks may be achieved by:

- elimination by design
- reduction to an acceptable level
- verification to demonstrate that risks are managed to an acceptable level

It is desirable to eliminate risk, if possible, by modifying processes or system design. Design reviews can play a key role in eliminating risk by design.

Risks that cannot be eliminated by design should be reduced to an acceptable level by controls or manual procedures. Risk reduction includes applying controls to lower the severity, decrease probability, or increase detectability.

A systematic approach should be defined to verify that the risk associated with a system has been managed to an acceptable level. The overall extent of verification and the level of detail of documentation should be based on the risk to patient safety, product quality, and data integrity, and take into account the complexity and novelty of the system.

The information needed to perform risk assessments may become available, and should be considered, at different stages in the life cycle. For example, the high-level risks associated with a business process need to be understood before the risks associated with specific functions of computerized systems can be assessed.⁴

The criticality of a business process is independent of whether it is manually processed, semi-automated, or fully automated. Systems that support critical processes include those that:

- generate, manipulate, or control data supporting regulatory safety and efficacy submissions

⁴ CQAs of drug development and manufacture will influence the understanding of the impact of the business process, while Critical Process Parameters will influence the impact of specific computerized functions.

- control critical parameters and data in pre-clinical, clinical, development, and manufacturing
- control or provide data or information for product release
- control data or information required in case of product recall
- control adverse event or complaint recording or reporting
- support pharmacovigilance

5.3 Quality Risk Management Process

The ICH Guideline ICH Q9 describes a systematic approach to quality risk management intended for general application within the pharmaceutical industry. It defines the following two primary principles of quality risk management:

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

In the context of computerized systems, scientific knowledge is based upon the system specifications and the business process being supported.

This Guide uses the following key terms taken from ICH Q9.

Harm: Damage to health, including the damage that can occur from loss of product quality or availability.

Hazard: The potential source of harm.

Risk: The combination of the probability of occurrence of harm and the severity of that harm.

Severity: A measure of the possible consequences of a hazard.

This Guide applies the general principles of ICH Q9 to describe a five step process for risk management as an integral part of achieving and maintaining system compliance. For simple or low risk systems, some of these steps may be combined. See Appendix M3 for further details on the quality risk management process.

This process is focused on managing risks during the project phase. Risk management also should be used appropriately both within specific activities and during the operation phase. Examples include:

1. determining the need for supplier audit as part of supplier assessment
2. determining corrective actions arising from test failures
3. determining impact of proposed changes as part of change management
4. determining frequency of periodic reviews

Application of risk management to the above activities is covered in the appropriate sections of this Guide.

Organizations may have established risk management processes, including the use of methods such as those listed in Appendix M3. While this Guide describes one suggested approach, 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 an overall quality risk management framework consistent with ICH Q9.

Figure 5.2: Quality Risk Management Process



Step 1 – Perform Initial Risk Assessment and Determine System Impact

An initial risk assessment should be performed based on an understanding of business processes and business risk assessments, user requirements, regulatory requirements, and known functional areas. Any relevant previous assessments may provide useful input, and these should not be repeated unnecessarily.

The results of this initial risk assessment should include a decision on whether the system is GxP regulated (i.e., GxP assessment). It also should include an overall assessment of system impact.

Based on this initial risk assessment and resulting system impact, it may not be necessary to perform the subsequent steps of the process, as the level of risk may already be at an acceptable level.

The specific level of effort, formality, and documentation of any subsequent steps should be determined based on level of risk and system impact. See Appendix M3 for further details.

If relevant, regulated electronic records and signatures should be identified. Again, existing assessments may provide useful input and should not be repeated. A detailed approach and specific guidance is provided in the *GAMP Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures*.

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

Functions which have an impact on patient safety, product quality, and data integrity should be identified by building on information gathered during Step 1, referring to relevant specifications, and taking into account project approach, system architecture, and categorization of system components.

Step 3 – Perform Functional Risk Assessments and Identify Controls

Functions identified during Step 2 should be assessed by considering possible hazards, and how the potential harm arising from these hazards may be controlled.

It may be necessary to perform a more detailed assessment that analyzes further the severity of harm, likelihood of occurrence, and probability of detection. See Appendix M3, Section 5 for an example detailed assessment process.

The judgment as to whether to perform detailed assessment for specific functions should be dealt with on a case-by-case basis and the criteria can vary widely. The criteria to be taken into account include:

- criticality of the supported process
- specific impact of the function within the process
- nature of the system (e.g., complexity and novelty)

Appropriate controls should be identified based on the assessment. A range of options is available to provide the required control depending on the identified risk. These include, but are not limited to:

- modification of process design
- modification of system design
- application of external procedures
- increasing the detail or formality of specifications
- increasing the number and level of detail of design reviews
- increasing the extent or rigor of verification activities

Where possible, elimination of risk by design is the preferred approach.

Step 4 – Implement and Verify Appropriate Controls

The control measures identified in Step 3 should be implemented and verified to ensure that they have been successfully implemented. Controls should be traceable to the relevant identified risks.

The verification activity should demonstrate that the controls are effective in performing the required risk reduction.

Step 5 – Review Risks and Monitor Controls

During periodic review of systems, or at other defined points, an organization should review the risks. The review should verify that controls are still effective, and corrective action should be taken under change management if deficiencies are found. The organization also should consider whether:

- previously unrecognized hazards are present

- previously identified hazards are no longer applicable
- the estimated risk associated with a hazard is no longer acceptable
- 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. 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.

The frequency and extent of any periodic review should be based on the level of risk.

6 Regulated Company Activities

Responsibility for the compliance of computerized systems lies with the regulated company. This involves activities at both the organizational level and at the level of individual systems.

Therefore, this section is divided into:

- Governance for Achieving Compliance
- System Specific Activities

6.1 Governance for Achieving Compliance

Achieving robust, cost effective, compliance requires strong governance. Key elements of successful governance include the following:

- establishing computerized systems compliance policies and procedures
- identifying clear roles and responsibilities
- training
- managing supplier relationships
- maintaining a system inventory
- planning for validation
- continuous improvement activities

Effective governance is achieved by integrating these activities into the management of the organization. Each activity is described further in the sub-sections below.

6.1.1 Computerized Systems Policies and Procedures

Each regulated company should have a defined policy for ensuring that computerized systems are compliant and fit for intended use. The policy should typically include a commitment to:

- identify and comply with all applicable GxP requirements
- integrate life cycle activities into the regulated company's QMS
- identify and assess each system
- ensure GxP regulated systems are compliant and fit for intended use according to established SOPs
- follow a validation framework, including the use of validation plans and validation reports as necessary
- maintain compliance throughout the life of a system

Further details should be documented, e.g., in more detailed policies or in SOPs, which may be supplemented by guidance and templates. These documents will typically address:

- maintaining the system inventory
- determining the impact of systems on patient safety, product quality, and data integrity
- defined roles and responsibilities
- the computerized system life cycle approach
- planning, supplier assessment, risk management, specification, verification, and reporting activities and documents
- system operation and management, including up to date operating procedures for end users and administrators, and all operational processes described in Section 4.3 of this Guide
- record and data management
- security management

Policies and procedures should be developed taking into account existing policies, procedures, and practices.

6.1.2 Identifying Clear Roles and Responsibilities

Roles and responsibilities for activities should be documented, allocated, and communicated. Key responsibilities include:

- defining, approving, and maintaining policies and SOPs
- compiling and prioritizing the system inventory
- producing plans and reports
- managing compliance and validation activities
- maintaining compliance during operation

The roles of process owner, system owner, quality unit, SME, end user, and supplier are particularly important and are covered separately and in more detail in Section 6.2.3 of this Guide. The appropriate and timely involvement of these key roles should be ensured.

6.1.3 Training

Training is the process that ensures that persons who develop, maintain, or use computerized systems have the education, training, and experience to perform their assigned tasks.

Procedures for training covering responsibilities, plans, and records should be established. The process owner is ultimately responsible for ensuring that all relevant persons are adequately trained. This responsibility may be delegated, e.g., maintenance staff may be the responsibility of the system owner, and development staff may be the responsibility of a project manager.

Persons in responsible positions should have the appropriate training for the management and use of computerized systems within their field of responsibility. This should include specification, verification, installation, and operation of computerized systems.

All users and support staff of a GxP regulated system, including contracted staff, should be given appropriate training including basic GxP training. They also should be given specific training covering regulatory aspects of using the computerized system, e.g., security aspects, or the use of electronic signatures.

For computerized systems, the regulated company should therefore:

- establish the necessary training needs, including users, suppliers, data centers, IT departments, engineering, maintenance
- provide training to satisfy these needs
- evaluate the effectiveness of the training
- ensure that staff are aware of the relevance and importance of their activities, e.g., GxP
- ensure that supplier staff are adequately trained, e.g., as part of supplier assessment
- maintain appropriate training records
- ensure training is maintained up to date, e.g., following system changes

A risk-based approach should be used to determine the rigor of training required, including measuring the effectiveness of training, and the retention of training records.

6.1.4 Managing Supplier Relationships

All phases of the computerized systems life cycle require cooperation between the regulated company and external and internal suppliers, including IT and engineering. Both regulated companies and suppliers have important roles to play in ensuring that suitable computerized systems are deployed as part of regulated activity.

Regulated companies should ensure that internal and external suppliers are made aware of the need for regulatory compliance. The regulated company should verify, prior to contract placement, that the supplier has adequate expertise and resources to support user requirements and expectations. The most common mechanism for this is the supplier assessment, which may include an audit depending on risk, complexity, and novelty.

It should be noted that some suppliers, e.g., suppliers of commercially available software products or systems, will have fulfilled a significant part of their responsibilities before any relationship is established with individual regulated companies, and that this will have a major influence on any ensuing co-operation.

Supplier activities are covered in Section 7 of this Guide.

6.1.5 Maintaining the System Inventory

Regulated companies should maintain an inventory of computerized systems, showing which are GxP regulated (see Section 5.3 of this Guide). The inventory should provide summary information such as the validation status, ownership, impact, current system version, and supplier. Automated equipment may be listed separately and duplication should be avoided.

Note: the inventory should be at the level of systems that support business processes, rather than individual items of hardware, such as keyboards and routers which would be covered by local IT procedures.

The system inventory may be used for planning periodic reviews.

6.1.6 Planning for Validation

Computerized system validation within a business unit is typically performed using a hierarchical framework of plans covering GxP regulated computerized systems.

Computerized system validation plans describe how to ensure compliance and fitness for intended use of specific systems. They specify scope, approach, resources, roles and responsibilities, and the types and extent of activities, tasks, and deliverables.

See Section 3.3 of this Guide for further details on the computerized system validation framework. See Appendix M1 for more detailed guidance.

6.1.7 Continuous Improvement Activities

Improving the processes used to achieve and maintain compliance and fitness for intended use is highly desirable. Performing these activities becomes more effective and efficient, and the risk of non-compliance is reduced.

Suppliers also benefit from improving their processes for product development and support, and for other services provided (see Section 7.3 of this Guide).

Achieving improvements depends on an understanding of the effectiveness of the current processes and obtaining relevant and objective measures of the quality of both the process and the product.

6.1.7.1 Understanding

Understanding the effectiveness of the current processes is best gained by considering current levels of conformance to the process (e.g., established by audit and trending performance) and by reviewing current processes against recognized good practices. This understanding should assist with identifying areas of the QMS that may require improvement. For example, persistent non-conformities in a particular process may be caused by problems within the process. Alternatively, a review of current processes may find scope for streamlining of these processes based on developments in recognized good practice.

6.1.7.2 Metrics

Metrics may be gathered throughout the system life cycle, including:

- design and development metrics (e.g., from design and code reviews)
- testing metrics (e.g., from analysis of test failures and resulting actions)
- operation and maintenance metrics (e.g., from incident management, change management, backup and restore)

Metrics should be collected only for a clear purpose. They typically provide information on one aspect of the operation of the QMS, and may assist with determining improvements to the QMS or to its use.

6.2 System Specific Activities

Table 6.1 shows the typical regulated company activities required for a configurable computerized system. Note: this table is indicative only. Activities required for a specific system should be determined based on risk, complexity, and novelty. This section provides further details on each task.

Table 6.1: Typical Activities for a Configurable Computerized System

Step	Task	Description
1.	Identify Compliance Standards	Compliance activities should be performed in accordance with applicable company policies and procedures.
2.	Identify System	The system should be added to an inventory of systems in accordance with documented procedures.
3.	Identify Key Individuals	These include Process Owner, System Owner, Quality Unit, SME, Supplier, End User
4.	Produce URS	The User Requirements Specification (URS) should define clearly and precisely what the regulated company wants the system to do, state any constraints, and define regulatory and documentation requirements.
5.	Determine Strategy for Achieving Compliance <ul style="list-style-type: none"> • Risk Assessment • Assessment of System Components • Supplier Assessment 	<p>An initial Risk Assessment should be performed during planning. Depending on the system, further assessments may be required as specifications are developed.</p> <p>System components should be assessed and categorized to determine the approach required.</p> <p>The quality capability of a supplier should be formally assessed as part of the process of selecting a supplier and planning for achieving compliance. The decision whether to perform a Supplier Audit should be documented and based on a Risk Assessment and categorization of the system components.</p>
6.	Plan	Activities including risk assessments, deliverables, procedures, and responsibilities for establishing the adequacy of the system should be defined in a plan.
7.	Review and Approve Specifications	The regulated company should review and approve specifications, as appropriate. This could involve one or several specifications depending on the system. Design reviews may be used where appropriate.
8.	Develop Test Strategy	The regulated company should determine what testing is required after considering the existing documentation available. Depth and rigor of testing should be based on level of risk and impact of system.
9.	Test	The regulated company should ensure that testing defined in test strategy is completed, and ensure review of test results.
10.	Report and Release	A report should provide evidence that all planned deliverables and activities have been completed and that the system is fit for intended use. Any deviations, or outstanding or corrective actions, should be explained and followed up as required by the regulated company. There should be a formal process covering release of system for operational use by end users.
11.	Maintain System Compliance during Operation	The regulated company should establish adequate system management and operational procedures. See Section 4.3 of this Guide for further details.
12.	System Retirement	The regulated company should manage the withdrawal of the computerized system from use, including migration of data to a new system, if applicable.

Table 6.1 shows typical regulated company activities for a configurable system. For a custom system, and based on risk, there may increased levels of specification, review, and testing required.

6.2.1 Identify Compliance Standards

Compliance and fitness for intended use should be achieved in accordance with applicable company policies and procedures. Industry guidance, such as GAMP, should be treated as supporting information and should not supersede company policies and procedures.

6.2.2 Identify System

The system should be assessed to determine whether it is GxP regulated and added to the system inventory in accordance with documented procedures (see Section 6.1.5 of this Guide).

6.2.3 Identify Key Individuals

This section describes key roles and responsibilities when achieving compliance. Designated individuals should have sufficient experience and training to perform their respective roles.

Specific activities may be delegated to appropriate nominated representatives.

6.2.3.1 Process Owner

The owner of the business process or processes being managed should be identified. The process owner is ultimately responsible for ensuring that the computerized system and its operation is in compliance and fit for intended use in accordance with applicable SOPs. The process owner also may be the system owner.

Specific activities may include:

- approval of key documentation as defined by plans and SOPs
- providing adequate resources (personnel including SMEs, and financial resources) to support development and operation of the system
- ensuring adequate training for end users
- ensuring that SOPs required for operation of the system exist, are followed, and are reviewed periodically
- ensuring changes are approved and managed
- reviewing assessment/audit reports, responding to findings, and taking appropriate actions to ensure GxP compliance
- coordinating input from other groups (e.g., finance, information security, safety/HSE, legal)

6.2.3.2 System Owner

The System Owner is responsible for the availability, and support and maintenance, of a system and for the security of the data residing on that system. The system owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable SOPs. The system owner also may be the process owner.

The System Owner acts on behalf of the users. Global IT systems may have a global system owner and local system owners to manage local implementation.

Specific activities may include:

- approval of key documentation as defined by plans and SOPs
- ensuring that SOPs required for maintenance of the system exist and are followed
- ensuring adequate training for maintenance and support staff
- ensuring changes are managed
- ensuring the availability of information for the system inventory and configuration management
- providing adequate resources (personnel including SMEs, and financial resources) to support the system
- reviewing audit reports, responding to findings, and taking appropriate actions to ensure GxP compliance
- coordinating input from other groups (e.g., finance, information security, safety/HSE, legal)

6.2.3.3 Quality Unit

The term Quality Unit is used here as an encompassing term that includes many quality-related roles that are important to developing and managing regulated computerized systems. The manner in which a Quality Unit addresses the responsibilities noted below may vary based on the applicable regulations. For example, the strict interpretation of the GLP requirement for separation of duties may lead some companies to interpret this as requiring that the GLP Quality Unit audit a validation document rather than approve it. Regardless of the mechanism, the intent of achieving acceptance from the Quality Unit is the same.

The Quality Unit has a key role to play in successfully planning and managing the compliance and fitness for intended use of computerized systems, and provides an independent role in the:

- approval or audit of key documentation such as policies, procedures, acceptance criteria, plans, reports
- focus on quality critical aspects
- involvement of SMEs
- approval of changes that potentially affect patient safety, product quality, or data integrity
- audit processes and supporting documentary evidence to verify that compliance activities are effective

The role may be split into Corporate and Operational Quality depending on the organization. The following example is indicative only and titles and details of responsibility may vary between organizations.

6.2.3.4 Corporate Quality

This group operates at the corporate level and is responsible for:

- setting policy
- maintaining an oversight of company standards
- auditing for compliance
- reviewing effectiveness of quality systems and processes

Regulatory authorities require the Corporate Quality Unit to be independent of the business activities.

6.2.3.5 *Operational Quality*

This, typically, is the Quality Unit of a division or business unit. This group is involved in the compliance of GxP regulated computerized systems within the division or business unit and typically covers:

- implementation of quality standards and procedures for the development and operation of computerized systems
- reviewing risk assessment and control activities
- support of project phase activities as defined in computerized system validation plans
- support of life cycle processes such as change control and document management
- training related to computerized systems quality and compliance
- agreeing approach to managing deviations with approval of any supporting rationales
- quality management of external service and application providers (e.g. contractors, outsourcing organizations, etc.)

Specific operational quality activities can be delegated to a variety of functions provided that independence can be demonstrated. For example:

- IT departments may have their own quality management function.
- Engineering departments may have their own standards groups.
- Suppliers and consultants may be authorized to assist.

Any such delegation should be clearly defined and their respective roles agreed and documented as part of planning. In all circumstances, the Quality Unit retains ultimate responsibility and accountability for compliance with regulations.

6.2.3.6 *Subject Matter Expert*

Qualified and experienced SMEs have a key role in performing reviews and assessments, and taking technical decisions, based on science based process and product understanding, and sound engineering principles. Different SMEs may be involved with different activities, e.g., during specification and verification.

SMEs should take the lead role in the verification of the computerized system. Responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results.

SMEs may come from a wide range of backgrounds as required, including business process, engineering, IT, supplier, quality, and validation.

6.2.3.7 *Supplier*

Suppliers (including internal suppliers, such as IT or engineering) should play an important support role in achieving and maintaining system compliance and fitness for intended use. Specific activities may include:

- provision of existing documentation (see Section 8.3 of this Guide)
- preparation and review of documentation
- acting as SME for technical aspects such as configuration and design options
- performing and supporting testing
- change and configuration management
- supporting processes geared toward maintaining system compliance, e.g., by providing software patches, providing second tier support for problem resolution processes, etc.

See Section 7 of this Guide for further details on supplier activities.

6.2.3.8 End User

In addition to using the system in accordance with approved procedures, end users also may be involved in the following activities through the life cycle:

- input to user requirements and specifications
- evaluation of prototypes
- testing
- acceptance of system and handover
- input to development of SOPs for use of system
- reporting defects
- identifying opportunities for improvement

6.2.4 User Requirements Specification

This describes what the system should do. The URS is the responsibility of the regulated company, but may be written by a third party or supplier. It should be adequately reviewed by SMEs and approved by the Process Owner. Other approvers may include the System Owner and Quality Unit representative.

See Appendix D1 for further details on User Requirements Specifications.

6.2.5 Determine Strategy for Achieving Compliance and Fitness for Intended Use

6.2.5.1 Risk Assessment

An initial risk assessment should be performed during planning to determine whether the system is GxP regulated, the impact of the system, and the need for further risk assessments. This process is described in Section 5 of this Guide.

See Appendix M3 for further details on Risk Assessment.

6.2.5.2 Assessment of System Components

This process uses the revised GAMP software categories and hardware categories as guidance in establishing the required activities, based on how the system is constructed or configured.

See Appendix M4 for further details on Categories of Software and Hardware.

6.2.5.3 Supplier Assessment and Education

The regulated company should formally assess each supplier to establish their quality capability. This is typically performed by an SME and may involve an audit of the supplier depending on risk, complexity, and novelty. The assessment may find that a supplier has either a well-established, formal, QMS, or has attained a recognized third party certification, such as ISO 9001. The strategy should take account of assessment conclusions.

If another regulated company has already assessed the supplier for the same reason, then subject to that company agreeing to share that information, an additional assessment may not be necessary. The justification for not assessing a specific supplier should be formally documented.

Regulated companies should be prepared to assist in the education and training of suppliers, either by direct involvement, or by providing advice on training requirements, sources of information, and sources of specialist training and education, such as ISPE. It may be beneficial to supply example documents, where possible, to establish the correct content and level of detail in the key documents.

See Appendix M2 for further details on Supplier Assessment.

6.2.6 Planning

Planning is an essential activity for any system development and should address all aspects, including activities that demonstrate compliance and fitness for intended use. Responsibilities, deliverables, and procedures to be followed should be defined. Since the supplier may provide deliverables or directly support these activities, planning provides the opportunity to decide how best to leverage supplier activities and documentation to avoid unnecessary duplication.

See Appendix M1 and Section 3.3 of this Guide for further details on Validation Planning.

6.2.7 System Specifications

There are a number of types of specification that may be required to adequately define a system. These may include Functional Specifications, Configuration Specifications, and Design Specifications.

The applicability of, and need for, these different specifications depends upon the specific system and should be defined during planning. See Section 4.2.6 of this Guide for typical examples of the level of specification required for non-configured products, configured products, and custom applications.

Functional Specifications are normally written by the supplier and describe the detailed functions of the system, i.e., what the system will do to meet the requirements. The regulated company should review and approve Functional Specifications where produced for a custom application or configured product. In this situation, they are often considered to be a contractual document.

See Appendix D2 for further details on Functional Specifications.

Configuration Specifications are used to define the required configuration of one or more software packages that comprise the system. The regulated company should review and approve Configuration Specifications.

Design Specifications for custom systems should contain sufficient detail to enable the system to be built and maintained. In some cases, the design requirements can be included in the Functional Specification. SMEs should be involved in reviewing and approving design specifications.

See Appendix D3 for further details on Configuration and Design.

A current system description should be available for regulatory inspection and training. This may be covered by the URS or Functional Specification, or a separate document may be produced.

See Appendix D6 for further details on System Descriptions.

6.2.7.1 Design Reviews

Design reviews evaluate deliverables against standards and requirements, identify issues, and propose required corrective actions. They are planned and systematic reviews of specifications, design, and development, and should be planned to occur at suitable stages during the life cycle. They are an important part of the verification process.

Design reviews should be performed by SMEs, and involve others as required.

For non-configured products (GAMP Category 3), design reviews by the regulated companies are not typically required.

For configured products (GAMP Category 4), regulated company design review activities should focus on the configuration and any customization activities to meet user requirements.

For custom applications (GAMP Category 5), design reviews are typically conducted at each level of detail of specification.

Supplier development activities, including reviews, should be verified during supplier assessment.

See Appendix M5 for further details on Design Review.

6.2.8 Development and Review of Software for Custom Applications

Software reviews are not required for configured and non-configured software products. Custom applications and custom software for configured products (e.g., interfaces, macros, and report generation) should be developed in accordance with defined standards.

The need for, and extent of, reviews of new software during development should be based on risk, complexity, and novelty. Such reviews should be performed by an SME. The regulated company should ensure that corrective actions resulting from such reviews are tracked to satisfactory completion.

See Appendix D4 for further details on Management, Development, and Review of Software.

6.2.9 Test Strategy and Testing

Section 4.2.3 of this Guide describes the use of testing as a fundamental part of verification activity, including the development of a test strategy.

The regulated company is responsible for ensuring that the test strategy will demonstrate compliance and fitness for intended use. The number and types of tests should be based on risk, complexity, and novelty as described in Section 4.2.3 of this Guide. The role of the supplier, including use of existing supplier documentation, should be considered when developing the strategy.

The results of testing should be documented against predefined acceptance criteria based on specifications. Test failures should be captured, reviewed, documented, and managed.

See Appendix D5 for further details on Testing of Computerized Systems. See Section 8.5 of this Guide for details on efficient testing practice.

The *GAMP Good Practice Guide: Testing of GxP Systems* provides comprehensive guidance on aspects of computerized systems testing.

6.2.10 Reporting and Release

At the conclusion of the project, a computerized system validation report should be produced summarizing the activities performed, any deviations from the plan, any outstanding and corrective actions, and providing a statement of fitness for intended use of the system. See Appendix M7 for further details.

In some cases, specific computerized system validation reports may not be required (see Section 3.3 of this Guide).

Release of the system into the operating environment in accordance with a controlled and documented process is discussed in Section 4.2.4 of this Guide.

6.2.11 Maintaining System Compliance During Operation

The regulated company is responsible for maintaining system compliance during operation (see Section 4.3 of this Guide).

6.2.12 System Retirement

System retirement is described in Section 4.4 of this Guide.

7 Supplier Activities

Although the responsibility for compliance with GxP regulations lies with the regulated company, the supplier may have considerable involvement in the process.

Regulated companies wish to leverage supplier knowledge and documentation, subject to suitability, following formal assessment. This may involve an audit depending on risk, complexity, and novelty.

This section is written specifically to help suppliers to meet the requirements and expectations of the regulated company. Some information from previous sections is included to give suppliers a more complete picture.

7.1 Supplier Products, Applications, and Services

Suppliers provide a range of products, applications, and services for hardware, software, and related technologies. The relationship between supplier and regulated company will vary significantly depending upon the product, application, or service being provided.

7.1.1 Non-Configured Product (GAMP Category 3)

If the product is purchased off-the-shelf and does not require configuration to support business processes, or where the default configuration is used by the regulated company, supplier involvement with the regulated company is, typically, limited to the provision of documentation, training, support, and maintenance. The product should be developed and maintained by the supplier in accordance with good practices (see Section 7.2 of this Guide).

7.1.2 Configured Product (GAMP Category 4)

If the product requires configuration to support specific business processes, supplier involvement with the regulated company will, typically, include support with specification, configuration, verification, and operation of the system (see Section 4 of this Guide).

Procedures to follow should be agreed between the regulated company and the supplier and be documented in the appropriate plan. Procedures adopted may be those of the regulated company or from the supplier QMS (see Section 7.2 of this Guide).

The product itself should be developed and maintained by the supplier in accordance with good practices (see Section 7.2 of this Guide).

7.1.3 Custom Application (GAMP Category 5)

For a custom application, the regulated company typically contracts a supplier to develop the application based on defined requirements. Therefore, the supplier will be involved during the full project life cycle of the system, and also to provide support during system operation as described in Section 4 of this Guide. Procedures to follow should be agreed between the regulated company and the supplier and be documented in the appropriate plan.

Procedures adopted may be those of the regulated company or from the supplier QMS (see Section 7.2 of this Guide).

7.1.4 Services

Suppliers that provide services should operate within a QMS (see Section 7.2 of this Guide). Quality planning should define the activities, procedures, deliverables, and responsibilities for establishing delivery and monitoring of the service. Such a plan is a contractual document, and as such, should be approved for use by both the supplier and the regulated company.

The required information may be satisfactorily covered by other contractual documents such as a Service Level Agreement, in which case a separate plan would not be required.

The extent to which the good practices described in Section 7.2 of this Guide apply to services will vary considerably depending on the scope and nature of the service and should be defined as part of the supplier QMS.

7.2 Supplier Good Practices

The table below lists good practice activities that apply to product and application development and support. These are further described in this section of this Guide.

The good practices also may apply to service provision (see Section 7.1 of this Guide).

Table 7.1: Supplier Good Practices

Step	Practice	Description
1.	Establish QMS	The supplier QMS should: 1. Provide a documented set of procedures and standards 2. Ensure activities are performed by suitably competent and trained staff 3. Provide evidence of compliance with the documented procedures and standards 4. Enable and promote continuous improvement
2.	Establish Requirements	The supplier should ensure that clear requirements are defined or provided by the regulated company.
3.	Quality Planning	The supplier should define how their QMS will be implemented for a particular product, application, or service.
4.	Assessments of Sub-Suppliers	Suppliers should formally assess their sub-suppliers as part of the process of selection and quality planning.
5.	Produce Specifications	The supplier should specify the system to meet the defined requirements.
6.	Perform Design Review	The design of the system should be formally reviewed against requirements, standards, and identified risks to ensure that the system will meet its intended purpose and that adequate controls are established to manage the risks.
7.	Software Production/ Configuration	Software should be developed in accordance with defined standards, including the use of code review processes. Configuration should follow any pre-defined rules or recommendations and should be documented.
8.	Perform Testing	The supplier should test the system in accordance with approved test plans and test specifications.
9.	Commercial Release of the System	System release to customers should be performed in accordance with a formal process. (Note: this is not release into GxP environment, which is a regulated company activity)
10.	Provide User Documentation and Training	The supplier should provide adequate system management documentation, operational documentation, and training in accordance with agreed contracts.
11.	Support and Maintain the System in Operation	The supplier should support and maintain the system in accordance with agreed contracts. The process for managing and documenting system changes should be fully described.
12.	System Replacement and Retirement	The supplier should manage the replacement or withdrawal of products in accordance with a documented process and plan. The supplier also may support the regulated company with the retirement of computerized systems in accordance with regulated company procedures.

7.3 Quality Management System

It is recommended that suppliers follow a QMS, preferably based on recognized standards. The QMS should define:

- the process being followed to deliver and support the product, application, or service
- responsibilities, including clear separation of authority between quality assurance and other groups, such as product development, product support, finance or marketing

- deliverables
- documentation
- planned reviews of the QMS and internal audits
- approach to continuous improvement of the QMS and its use

The QMS should be based on a life cycle concept for the development and subsequent support of the computerized system. There are many equally valid life cycle approaches that may be used by suppliers. This Guide does not recommend any particular approach, but rather highlights those activities expected of suppliers to support the regulated company in achieving and maintaining compliance.

The QMS should include formal procedures covering the activities that support system development, such as:

- software management, control, and release
- development change control
- configuration management
- traceability
- training of supplier staff
- document management
- backup and restore

Many systems developed today are based on software products and packages, which are configured to meet user requirements. Such products, normally, will come with supporting documentation, and where possible this documentation should be used in the system life cycle. Further modules of custom software may be required to provide specific functionality, such as interfaces and reports. The design and development of such software should be fully documented.

The QMS should cover the approach to continuous improvement. For example, CMMI (Reference 50, Appendix G3) provides an approach based on a framework for assessing and improving organizational capability and maturity. The use of metrics for measuring and improving the quality of software and hardware should be considered as part of the approach to improvement.

Industry guidance, such as GAMP, should be treated as supporting information and should not override the supplier's established QMS.

7.4 Requirements

Requirements may be developed internally by the supplier (in the case of product development).

Requirements also may be provided by the customer (for a configured product, custom application, or a service).

The requirements should define clearly and precisely what the system should do and state any constraints. Requirements should be reviewed and approved.

Changes to requirements should be controlled. Changes to subsequent specification documents that affect the requirements should lead to an update of the requirements.

Regulated companies wish to maximize the use of supplier testing to support their compliance activities. Therefore, requirements should be written such that they can be tested. Individual requirements should be traceable through the life cycle.

For configured products and custom applications, the regulated company should describe the business processes to be automated. In the case of configured products, these processes should be aligned with the functionality of the product to be used. This may require significant process re-engineering.

See Appendix D1 for further details on User Requirements Specifications.

7.5 Supplier Quality Planning

The supplier should define how the QMS will be implemented for a particular product, application, or service.

This should include defining the life cycle model being followed and the project organization, activities, procedures, deliverables, and responsibilities for establishing the fitness for intended use of the system. The approach may include prototyping or other software development techniques. The role of supplier Quality Assurance should be clearly defined.

These supplier quality requirements may be captured in a separate document entitled Quality Plan or other supplier documentation. In each case, the quality requirements should be clearly documented, reviewed, approved, accessible, and followed.

See Appendix M6 for further details on Quality and Project Planning.

7.5.1 Prototyping

Prototyping methods may be used to clarify user requirements or to evaluate areas of risk. Typically, a prototype is used to evaluate the acceptability of a user interface, the performance of critical algorithms, suitability of the overall solution, or aspects of system performance such as capacity and speed.

To be effective, the aims and objectives of the prototype should be clearly defined, and the prototype evaluated against these to ensure the objectives are met. Suppliers should define how information gained can be incorporated in a controlled manner into specifications for the final product. This requires rigorous version control and segregation of prototype and final software.

7.6 Sub-Supplier Assessments

Suppliers should formally assess their sub-suppliers as part of quality planning. They also should be periodically re-assessed in accordance with the QMS.

The decision whether to perform an audit of their sub-suppliers should be documented and based on a risk assessment. The supplier may find it advantageous to use the GAMP process for categorization of the system components in assessing risk.

See Appendix M2 for further details on Supplier Assessments.

7.7 Specifications

For product development, the supplier should document the functionality and design of the system to meet the defined requirements. This should cover software, hardware, and configuration.

Functional specifications should clearly and completely describe what the product will do. They should be produced such that objective testing can be subsequently performed.

Design specifications should be based on the functional specifications and should be sufficiently detailed so that the product can be developed.

Specifications may be covered by one or more documents depending on the complexity and risk of the product.

Specifications should be reviewed and approved with traceability established between related documents. They should be managed under change control with the awareness that change to one document may lead to a change being required in others.

It is recognized that not all suppliers use the specification terms described in this Guide, but may still meet the objective of providing adequate specifications through the provision of other documentation.

See Appendices D2 and D3 for further details on Specifications.

If the supplier is involved in configuring a product or developing a custom application, the number and level of specifications can vary considerably and should be agreed with the regulated company (see Section 6.2.7 of this Guide). Section 4.2.6 of this Guide provides examples of specification requirements for configured products and custom applications.

7.8 Design Reviews

Design reviews evaluate deliverables against standards and requirements, identify issues, and propose required corrective actions. They should be planned and systematic reviews of specifications, design, and development, and should be planned to occur at suitable stages during the life cycle, based on risk, complexity, and novelty. Design reviews aim to identify and eliminate issues that would otherwise lead to changes at a later stage.

See Appendix M5 for further details on Design Reviews.

7.9 Software Production/Configuration

The supplier should establish and maintain a formal system for controlling software production. Appropriate methods and tools should be used and the use of these should be documented. Rules and conventions, such as acceptable languages, coding standards, and naming conventions should be established. The use of code reviews should be considered.

Existing software should be used in accordance with documented build processes and taking into account any changes in the system hardware, interfaces, and peripherals.

If the supplier is involved in configuring a product, this should be performed in accordance with the controlling configuration specification and follow appropriate guidelines and recommendations.

See Appendix D4 for further details on Management, Development, and Review of Software.

7.10 Testing

For product development, the supplier should test the product in accordance with approved test plans and test specifications.

The test specifications, when executed, should demonstrate that all requirements, functionality, and design have been met.

This may involve one or many stages of testing, depending on the nature of the product. For example, a simple product may only need one test specification while a complex product may have:

- Module (Unit) Testing
- Integration Testing
- System Testing

Test records for each stage should be reviewed and approved, and retained for a period defined in the QMS (not to be shorter than the supported lifetime of the current software version).

Test failures should be managed in accordance with a formal documented process.

See Appendix D5 for further details on Testing of Computerized Systems.

If the supplier is involved in configuring a product or developing a custom application, the number and level of test specifications can vary considerably and should be agreed with the regulated company (see Section 6.2.9 of this Guide).

7.11 Commercial Release

System release to customers should be performed in accordance with a formal process that describes criteria for release, responsibilities, records to be retained, and items to be released, including software, hardware, and documentation. Release notes defining fixes, changes, and new features should accompany each release, including minor releases and patches.

This activity is particularly applicable to commercially available products. For custom applications, the regulated company would typically accept the system following regulated company procedures.

Note that commercial release by a supplier is not a release into the GxP environment, which is a regulated company activity (see Section 6.2.10 of this Guide).

7.12 User Documentation and Training

The supplier should provide adequate system management documentation, operational documentation, and provide training for both maintenance and operation in accordance with agreed contracts.

7.13 System Support and Maintenance During Operation

The supplier should support and maintain the system in accordance with agreed contracts. Formal procedures should be followed, typically covering areas such as:

- operational change control
- configuration management
- patch management
- incident management
- document management
- backup and restore
- business continuity
- managing software product releases
- training of supplier staff
- system maintenance

These topics are covered by separate sections and appendices in this Guide.

For specific systems, contracts may require that supplier documentation is subject to assessment during regulated company periodic review activities.

7.14 System Replacement and Retirement

The supplier should manage the replacement or withdrawal of products in accordance with a documented process and plans. Sufficient notice of retirement of a system or version should be given to regulated companies to allow them to plan for their own required activities.

The supplier also may support the regulated company with the retirement of computerized systems.

8 Efficiency Improvements

This Guide provides a flexible framework for achieving compliant computerized systems that are fit for intended use. The benefits will be obtained only if the framework is applied effectively in the context of a particular organization.

Aspects that can assist efficiency include:

- establishing verifiable and appropriate user requirements
- use of risk-based decisions
- leveraging supplier input
- leveraging existing documentation
- efficient testing practice
- well managed handover
- efficient change management
- anticipating data archiving and migration needs

8.1 Establishing Verifiable and Objective User Requirements

Requirements should be analyzed to ensure that they are fully defined and are verifiable and objective. For example:

Incomplete Requirement: Room shall be controlled at 20°C.

Complete Requirement: Room shall be controlled at 20°C ± 2°C. Excursions of no greater than 7°C are permitted for < 10 minutes.

The level of detail is dependent on the novelty and complexity of the processes and system being implemented.

Table 8.1 lists some aspects to consider when developing verifiable and objective requirements:

Table 8.1: Considerations When Developing Requirements

Aspect	Purpose
Process Knowledge	In order to identify key requirements of the system that are related to the business or manufacturing process
Business Knowledge	To ensure that requirements are challenged against business need and benefits can be realized
Ownership	To ensure clarity and understanding of the stated requirements
Analytical	To ensure that requirements are challenged to ensure they are complete and accurate
Technical/Product	To ensure that requirements are practical in terms of available technology
Process/Product Impact	To ensure requirements which impact the process or product are clearly identified
Technical Authorship	To ensure that requirements are written in concise, correct, and unambiguous language

8.2 Use of Risk-Based Decisions

Risk management provides an opportunity to scale life cycle activities. However, the benefit is achieved only if organizations are prepared to use risk assessments to justify the omission or inclusion of an activity. Examples of areas where risk assessments may help with scaling include:

- number and depth of design reviews required
- need for, and extent of, source code review
- rigor of supplier assessment
- depth and rigor of testing

Similar opportunities exist during system operation, for example:

- extent and level of specification and verification of changes
- rigor of backup and restore process
- level of business continuity required
- frequency and level of disaster recovery
- degree to which identity checks are completed prior to providing access rights
- scope and frequency of periodic reviews

The benefits of risk-based decision making can be maximized only if the conclusions and decisions can be leveraged. Therefore, there should be a practical, searchable means of access to conclusions and decisions available to those involved in decision making, e.g., during subsequent assessments or reviews, during change management, and on subsequent projects. Organizations may use a risk register to achieve this.

The risk-based approach should be focused and resourced for maximum effectiveness. Organizations should not invest more effort and time into the risk management process than is commensurate with the potential impact on the supported business processes.

8.3 Leveraging Supplier Input

Supplier documentation, including test documents, may be used as part of verification documentation, provided the regulated company has assessed the supplier and the documentation and determined both to be suitable, and the supplier is prepared to make the documentation available. This assessment may include a supplier audit, depending on the risk, complexity, and novelty of the system.

The regulated company should assess the supplier for evidence of:

- an acceptable supplier quality system
- supplier technical capability
- supplier application of good practice such that information obtained from the supplier will be accurate and suitable to meet the purpose of verification

Supplier documentation should be assessed for content and quality. Regulated company procedures and processes should be flexible regarding acceptable format and structures so that supplier documentation may be leveraged.

If inadequacies are found in the supplier quality system, technical capability, application of good practice, or documentation, then the regulated company may choose to manage potential risks by applying specific, targeted, additional verification checks or other controls, rather than repeating supplier activities and replicating supplier documentation.

The decision and justification to use supplier documentation to support the verification of the computerized system should be based on the intended use of the system, and should be documented and approved by SMEs which may include the Quality Unit for aspects critical to patient safety, product quality, and data integrity.

Suppliers also may have tools or techniques unique to the specification and testing of their product or used in their quality control, which may be leveraged by the regulated company during specification and testing.

8.4 Leveraging Existing Documentation

In addition to the use of supplier documentation, regulated companies also should leverage their own documentation from existing systems when introducing new, similar, systems. Examples include:

- laboratory equipment
- secondary manufacturing equipment
- packaging equipment

Relevant documents to reuse may include risk assessments, user requirements specifications, various plans, test specifications, and design reviews.

The new system should be assessed and any differences with the existing system identified and managed by the introduction of appropriate specification and verification as required. A review of existing documentation should determine which may be used. These conclusions should be documented.

The new system should be subject to installation and verification based on user requirements. The validation report should explain the rationale for reuse of documentation.

8.5 Efficient Testing Practice

Testing is a major, time consuming exercise. It perhaps offers the greatest opportunity for efficiency savings.

8.5.1 Reuse of Test Results

Many systems have large amounts of test results available as a result of suppliers following a QMS independently of a regulated company. On a project, there may be pre-delivery testing which may include Factory Acceptance Testing. Wherever possible, regulated companies should clearly communicate to suppliers the testing and document requirements in advance such that supplier test documentation is of the required standard to support compliance activities.

Testing also may take place to meet other business or legal requirements, such as safety, health, environment, and finance such as SOX. If so, unnecessary duplication of testing should be avoided. This is particularly true for large business systems.

8.5.2 Extent of Required Testing

The amount and type of testing should be risk-based. Types of testing include:

- normal case (positive)
- invalid case (negative)
- repeatability
- performance
- volume/load
- regression
- structural testing

See Appendix D5 for further details. The choice of controls to manage identified risks may result in some of these types of testing being required.

While user requirements should be verified by the regulated company by performing installation and acceptance tests, other required tests should be identified based on risk, complexity, and novelty. A review of the existing tests and results can then determine what, if any, further testing is required by the regulated company. The regulated company's procedures should allow for the use of such existing test evidence subject to a documented and justified review and approval by an SME, which may include the Quality Unit for aspects critical to patient safety, product quality, and data integrity.

8.5.3 Hardcopy Test Evidence

Regulated companies should take a justified and documented decision, based on impact, novelty, and complexity, on how much hardcopy test evidence is to be retained, as this can be a significant overhead.

For example, regulated companies may use screen prints as hardcopy test evidence. The use of such hardcopy test evidence should be focused on high impact functions. Test evidence may be retained electronically providing adequate security and retention mechanisms are established.

Systems may have audit trails that capture much of the information that is traditionally captured by screen prints. If such an audit trail exists, is secure, and is available for review by the SME, then capturing additional evidence may not be necessary.

Test evidence should be sufficient for objective review by the SME.

8.5.4 Use of Test Witnesses

The use of witnesses during testing may involve a significant overhead and should be considered carefully. Decisions to use witnesses should consider:

- knowledge and experience of testers:
 - Trained testers with sufficient knowledge of the system should be used. For example, nominated end users who have been given appropriate training in testing.

- practical issues:
 - systems, e.g., process control systems, may require two people; one in a control room and one operating/observing equipment on site
- level and degree of review by an SME:
 - use of independent witnesses may form part of the review process
- degree of automation of the tests and the resulting test evidence, e.g., audit trails

See Appendix D5 and the *GAMP Good Practice Guide: Testing of GxP Systems* (Reference 34, Appendix G3), for further details on testing of computerized systems.

8.6 Well Managed Handover

System handover (from the project team to the Process Owner, System Owner, and operational users) should be well-managed. It is a pre-requisite for the effective maintenance of system compliance during operation. Handover should be planned in accordance with pre-agreed criteria and should consider:

- support requirements for maintenance, as defined by IT or engineering
- outstanding problems or deficiencies
- how long business processes can be stopped to enable handover
- ability and steps required to rollback to a previous operational state
- documentation, including format (e.g., electronic or paper), required at handover (e.g., specification and verification documentation, user and maintenance manuals or guides)
- training needs (user and maintenance)
- clear communication between groups, e.g., with application support and client service groups who may need to provide help desk support
- the impact, e.g., on the change control process to apply during the handover period, where handover is to be phased
- responsibilities during handover, e.g., for acceptance of the system and for assessing the severity of outstanding problems or deficiencies

8.7 Efficient Change Management

Efficient change management should be executed in parallel with configuration management. Key elements include:

- documented description and business benefit of the change
- confirmation of availability of resource
- assessment of the impact of the change on the application, the underlying infrastructure, the people (users and engineering support staff), and the documentation

- leveraging the risk assessment information from the original project and assessing any new risks introduced by the change to define the strategy for maintaining compliance – this includes the need for any regression testing
- evaluation of the change from the financial, technical (IT or engineering), and compliance perspectives at the lowest technically competent level prior to management approval
- documentation and communication of the decision
- execution and verification of the change, using traceability to identify existing applicable tests
- closing the change record in a timely manner

Weaknesses in change management systems that may lead to inefficiencies include:

- lack of scalability, e.g., for minor changes or for standard infrastructure components that change regularly
- failure to execute change management steps in the appropriate sequence
- an inability to prevent unnecessary changes
- failure to keep specifications current
- failure to leverage existing documentation relating to risk assessment and control, traceability matrices, or protocols
- lack of follow-up processes to close a change record
- independent change processes leading to duplication of effort for processes, equipment, and computer systems
- the inappropriate application of like-for-like principles in change management (see Appendix O6 for further details)
- inadequate management of changes conducted by a supplier, leading to life cycle documents and configuration management records that are out of date
- lack of adequate follow-up after emergency changes (see Appendix O6 for further details)

See Appendix O6 for further details on change management. See also ITIL (Reference 36, Appendix G3) for further details on change management within an IT service environment.

8.8 Anticipating Data Archiving and Migration Needs

Data archiving and migration requirements should be considered to ensure that data structures and formats are efficient.

8.8.1 *Different Retention Periods*

It may be difficult to archive data with different retention periods, which share the same data structures.

It may be difficult to destroy retained data that is no longer required, e.g., to reduce risk exposure to lost data and retention costs, where data with different retention periods share the same data structures.

A data structure that separates data by retention period can address the requirements of archiving and data destruction, but may involve a complex database design.

8.8.2 Data Formats

The migration of custom data formats to a replacement system requires special attention and may cause difficulties. The use of standard data formats should assist subsequent data extraction and migration.

8.8.3 Static and Dynamic Data

Data migration may be complicated where static and dynamic data is combined in a form which is difficult to separate.

See the *GAMP Good Practice Guide: Electronic Data Archiving* (Reference 34, Appendix G3) for further details on data archiving and migration.

Validation Planning

1 Introduction

This appendix covers the production of validation policies, Validation Master Plans (VMPs) and individual computerized system validation plans for systems or projects.

Validation policies define management intent and commitment. VMPs describe the areas of the company where validation is required and provides an overview of validation planning. Computerized system validation plans describe in detail how the validation is to be performed for specific systems.

The terms validation policy, VMP, and computerized system validation plan are being used for consistency with other sections of this and other GAMP documents, and because they are the most commonly used terms in the industry. It is recognized that some companies use alternative terminology.

2 Scope

This guidance may be applied to all GxP regulated computerized systems. The guidelines apply to both new and existing computerized systems, and sites and organizations in which these systems are used.

Where a computer system is regarded as one component of a wider manufacturing process or system, particularly in an integrated Quality by Design (QbD) environment, specific and separate computerized system validation may not be necessary. This environment requires both complete product and process understanding and that the critical process parameters can be accurately and reliably predicted and controlled over the design space. In such a case, the fitness for intended use of the computer system within the process may be adequately demonstrated by documented engineering or project activities together with subsequent Process Validation or continuous quality verification of the overall process or system. The same principle applies to the adoption of Process Analytical Technology (PAT).

Where these pre-requisites are met, separate computerized system validation plans may not be required.

For automated manufacturing equipment, separate computer system validation should be avoided. Computer system specification and verification should be part of an integrated engineering approach to ensure compliance and fitness for intended use of the complete automated equipment.

3 Validation Policies

Regulated companies should have corporate or site level policy documents that define their overall approach to computerized system quality and compliance. Such documents should define, or make reference to, the following:

- roles and responsibilities for activities and support
- high level expectations for deliverables
- standards, templates, and procedures that are expected to be followed throughout the organization
- definition of high level processes, including the process to determine whether a system is GxP regulated

- requirements for management of documentation

These policies should be readily available to all those with responsibilities for verification and validation activities, and should be referred to by relevant planning documents.

4 Validation Master Plans

4.1 General Guidelines

A VMP may be used to define the overview plan for a given time period, large project, or program of work under which there may be several individual validation plans.

Computerized system validation is often a subset or chapter of a VMP covering all of an organization's validation activities. A VMP may be for the entire company, or there may be multiple VMPs for smaller business units.

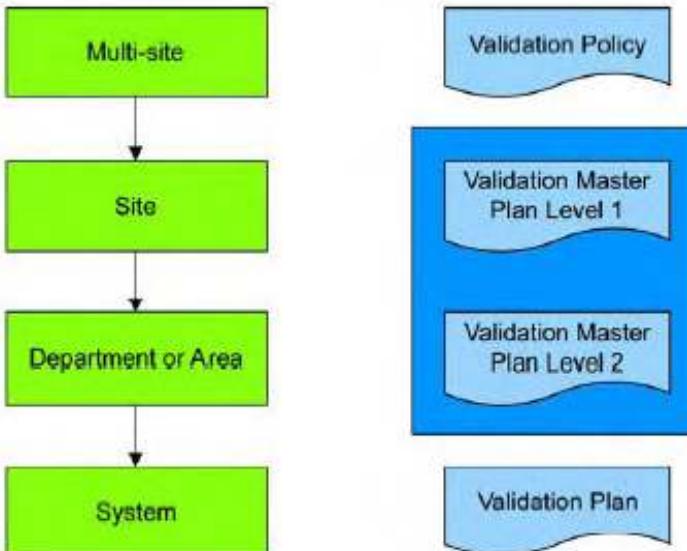
The VMP should be a clear and concise summary document, typically covering:

- summary of facilities, systems, equipment, or processes in scope
- current status of these facilities, systems, equipment, or processes
- change control process to be followed
- planning and scheduling (including activities for new systems, activities driven by change, and periodic review)

The VMP requires approval by management, and is often subject to regulatory inspection.

The structure of VMPs will depend on the way the regulated company is structured and on company preference and policy. Companies may have a management structure that is organized hierarchically, and some choose successive planning levels that reflect the way that the company itself is organized. Figure M1.1 gives an example planning hierarchy.

Figure M1.1: Planning Hierarchy



Within a site, there may be a single VMP for the site (VMP Level 1) and a number of separate plans for the individual areas on that site (VMP Level 2). For the individual systems within a given area, a detailed plan would define the validation activities for specific systems.

Companies may merge VMP Level 1 and Level 2 into a single plan, or operate with a collection of Level 2 VMPs, and not collate them into higher level plans.

4.2 Roles and Responsibilities

Responsibility for creating VMPs rests with senior management. Regardless of who prepares a VMP, senior management support is essential to ensure adequate resources for the required activities. Facility or area management should approve VMPs.

The Quality Unit should approve the policies and procedures for validation, including validation planning. The Quality Unit is responsible for verifying that the proposed approach complies with company quality standards and policies, and meets regulatory requirements.

The meaning of each approval signature should be defined.

4.3 Contents of the VMP

The VMP should be a summary document which is brief, concise, and clear. It should cover:

- scope
- reference to relevant policies
- organizational structure
- summary of facilities, systems, equipment and processes
- documentation format: the format to be used for protocols and reports
- planning and scheduling
- change control
- reference to existing documents

5 Computerized System Validation Plans

5.1 General Guidelines

A computerized system validation plan should be produced for each GxP regulated computerized system, focusing on aspects related to patient safety, product quality, and data integrity. It should summarize the entire project, identify measures for success, and clearly define criteria for final acceptance and release of the system.

The plan should define:

- what activities are required

- how they will be performed and who is responsible
- what their output will be
- what the requirements are for acceptance
- how compliance will be maintained for the lifetime of the system

The level of detail in the plan should reflect the risk, complexity, and novelty of the system. For simple or low risk systems a separate plan may not be needed; applicable aspects of planning may be covered within another document.

A generic or common plan may be used for similar systems (e.g., in a laboratory), but should adequately reflect the characteristics of specific systems. Where customization is performed or where supplier resources are to be leveraged, requirements should be communicated to the supplier at the start of the project so that the supplier may contribute to the content of the plan.

The plan defines how compliance and fitness for intended use is to be achieved and how the process is to be documented and reported. In some cases it may be convenient for a series of reports to be produced throughout the project. The plan should take this requirement into account and indicate the different types of report to be produced: covering progress made, issues raised, and acceptance of different phases of the project.

Planning should commence as early as possible; ideally no later than during the development of the user requirements specification (URS).

The plan may require modification during the project if there is a significant change in strategy or scope following initial approval, in which case project change control should be applied and the plan updated accordingly.

The plan, along with the associated report, may be one of the first documents offered during an audit to demonstrate regulatory compliance. It should, therefore, be written at a level suitable to be understood by a wide readership. Jargon and technical detail should be avoided.

See Appendix M7 for further details on computerized system validation reporting.

5.2 Roles and Responsibilities

Responsibility for computerized system validation planning ultimately rests with the Process Owner. This may be delegated to a Project Manager and also may involve the System Owner.

Typically, the computerized system validation plan is approved by the Process Owner and Quality Unit.

The meaning of each approval signature should be defined.

5.3 Contents of the Plan

Topics discussed in this section may be included in the plan. The guidance provided is intended to be neither prescriptive nor exhaustive.

The level of detail should reflect the risk, complexity, and novelty of the system. Separate sections may not be appropriate or necessary for all systems.

5.3.1 *Introduction and Scope*

Information provided should include:

- the scope of the system
- the objectives of the validation process
- review, maintenance, or update process for the plan itself

5.3.2 *System Overview*

A general description of the system in simple terms should be provided, including:

- business purpose and intended use for the system
- a description of the system at a high level
- an overview of the system architecture

Diagrams are encouraged.

5.3.3 *Organizational Structure*

Roles and responsibilities should be described, such as:

- project manager
 - project management and planning
 - control of project activities, resources, and costs
 - monitoring progress and initiating corrective action
 - ensuring issues and project objectives are correctly addressed and resolved
 - reporting to sponsor or senior management
 - liaising with the quality unit to ensure compliance
- quality unit
 - assuring compliance with appropriate regulatory and quality requirements and company policies
 - providing support for the review and approval of deliverables
 - approving the release of the system for use
- process owner and/or system owner
 - implementation and management of the system by the business user community
 - approving completion of stages/phases

Subject Matter Experts (SMEs) are those individuals with specific expertise and responsibility in a particular area or field (e.g., quality unit, engineering, automation, development, operations).

SMEs should take a lead role, as appropriate within their area of expertise and responsibility, in ensuring that systems are compliant and fit for intended use.

SME responsibilities may include planning and defining verification strategies, performing reviews, defining acceptance criteria, selecting appropriate test methods, executing verification tests, and reviewing results.

The number of personnel required to approve specific documents should be kept to a minimum.

5.3.4 Quality Risk Management

The quality risk management approach to be applied should be described.

An initial risk assessment should be performed based on an understanding of business processes and business risk assessments, user requirements, regulatory requirements and known functional areas. Any relevant previous assessments may provide useful input, and these should not be repeated unnecessarily.

The results of this initial risk assessment should include a decision on whether the system is GxP regulated (i.e., GxP assessment). It also should include an overall assessment of system impact.

The level of effort, formality, and documentation of subsequent risk management activities should be determined based on level of risk and system impact. Stages at which risk assessment will be performed should be identified. (See Section 5.3 of the Main Body and Appendix M3.)

Large enterprise systems, such as Enterprise Resource Planning (ERP) systems, may have some functionality declared as GxP relevant, while other functionality is declared outside the scope of GxP. In such cases the method by which this decision is made should be described and should consider:

- the requirement for deciding levels of GxP impact
- the procedures for performing the assessment
- the current status of the process (recognizing that the assessment may be repeated and the impact assessment updated)

Any specific quality risk management procedures or standards to be followed should be defined.

5.3.5 Validation Strategy

The strategy for achieving compliance and ensuring fitness for purpose should be described, based on consideration of:

- risk assessment
- assessment of system components and architecture
- supplier assessment

The key conclusions of any assessments performed should be included.

Any specific procedures or standards to be followed should be defined.

The validation strategy should describe:

- the life cycle model
- the application of hardware and software categories
- the inputs and outputs required for each stage of the project
- the acceptance criteria for each stage
- approach to traceability
- approach to design review

See Appendix M4 for further details on categories of software and hardware, and Appendix M5 for further details on design reviews and traceability.

5.3.6 Deliverables

The deliverable items to be produced should be listed, including responsibility for production, review, and approval.

5.3.7 Acceptance Criteria

The overall acceptance criteria for the system (e.g., successful completion of defined project phases or stages) should be described. The approach to handling significant deviations should be defined.

5.3.8 Change Control

The requirements for project change control should be defined, including reference to relevant procedures.

The stage at which operational change control will be applied should be defined.

5.3.9 Standard Operating Procedures

The Standard Operating Procedures (SOPs) to be created or updated as a result of the implementation of the system should be defined, and the plan should identify responsibility for their production, review, and approval.

5.3.10 Supporting Processes

Details of relevant supporting processes should be defined or referenced, including, but not limited to:

- training (including project team and user training)
- documentation management
- configuration management
- maintaining compliance and fitness for intended use

5.3.11 Glossary

Definitions of any terms and abbreviations that may be unfamiliar to the readership of the document should be included.

Supplier Assessment

1 Introduction

This appendix provides a risk-based approach to performing supplier assessments. Regulated companies should consider formally assessing each supplier of GxP regulated computerized systems and services. The assessment approach should be based on the criticality of the system/service being provided. Documented justification should be provided for not assessing suppliers of GxP regulated systems/services.

Topics covered in this appendix include:

- the reasons for carrying out supplier assessments
- the different types of assessment
- the assessment process
- on-site and postal audits
- joint and shared audits
- corporate audits
- supplier preparation for an audit
- supplier certification
- international standards and certification

Note that in this appendix the term audit is used to cover both a formal visit to the supplier and a formal assessment using a questionnaire (known as a postal audit).

This appendix covers both assessments of prospective suppliers of computerized systems, and existing suppliers who have not yet been assessed.

The material contained within this appendix also may be used by regulated companies to assess the competence of:

- external service providers (e.g., validation, project management, engineering support, maintenance) who support one or more of the various life cycle phases of computerized systems
- internal functions, such as IT and engineering

Open Source Software (OSS) is a developing area and requires special consideration (Reference 52, Appendix G3).

Example checklists and questionnaires for this appendix are supplied separately. They are intended for guidance only and may be tailored to suit a particular type of supplier, as there may be other factors which require consideration when assessing individual suppliers.

2 Reasons for Supplier Assessment

Regulated companies require a high level of confidence that computerized systems will meet their technical, commercial, and regulatory requirements. They also wish to leverage the knowledge, experience, and documentation of the supplier.

Financial and commercial audits of key suppliers have been a regular practice for some time, as have quality audits for raw material suppliers and contract companies.

Regulated companies should assess the quality and reliability of their computerized system suppliers and service providers. Regulated companies require documented evidence that computerized systems will consistently perform as intended, and assurance of the structural and functional integrity of the software.

The computerized system supplier should build quality and integrity into a software product during development, as it cannot be added effectively (e.g., through testing and re-work) later by the regulated company. The supplier is also better positioned to produce much of the required documented evidence during the development process. Suppliers should, therefore, be assessed to determine the adequacy of their development and support processes, and the supplier assessment approach described in this appendix provides a scaleable approach to carrying out such an assessment.

For many systems there is likely to be more than one supplier and each of the suppliers within the supply chain should be considered for assessment. In some cases a single supplier may provide a number of components or perform a number of activities, in other cases multiple suppliers may be involved.

Consideration should be given to the scope of products and services to be assessed. It is considered inefficient to focus the process solely on one product required by a project when the regulated company is likely to use a wider range of products or services from the supplier. By adopting a broader approach, multiple assessments can be avoided – this is often a particular issue for larger, global regulated companies where supplier assessment co-ordination across the company can be difficult.

Supplier assessments also are an opportunity to develop relationships with suppliers, to clarify expectations and intentions, and to identify misunderstandings and risks. The assessment process enables the regulated company to establish a picture of the supplier's operation, which is vital input when planning specification and verification activities. The assessment report should, therefore, provide a balanced view of what was found, including positive observations, along with a list of concerns.

3 Types of Assessment

On-site auditing may be expensive and time-consuming in terms of preparation, travel, the availability of personnel and facilities during the audit, and the time needed to write-up and review reports. The use of a risk-based supplier assessment approach that focuses on key suppliers can help to reduce these costs and is the basis of this appendix.

There are three main options for performing a supplier assessment:

1. basic assessment based on available information. (For components which are considered as commodities, e.g., common desktop applications, a documented decision not to perform any assessment may be appropriate)
2. postal audit, using a questionnaire
3. on-site audit, by relevant specialist, auditor, or audit team

Typically, a basic assessment is sufficient for lower impact systems, while higher impact systems may require formal audits. Postal audits may be appropriate for suppliers of standard and configurable products and services.

4 Assessment Process

The overall assessment process is shown in Figure M2.1. The main steps are, with further details given in the subsequent sections:

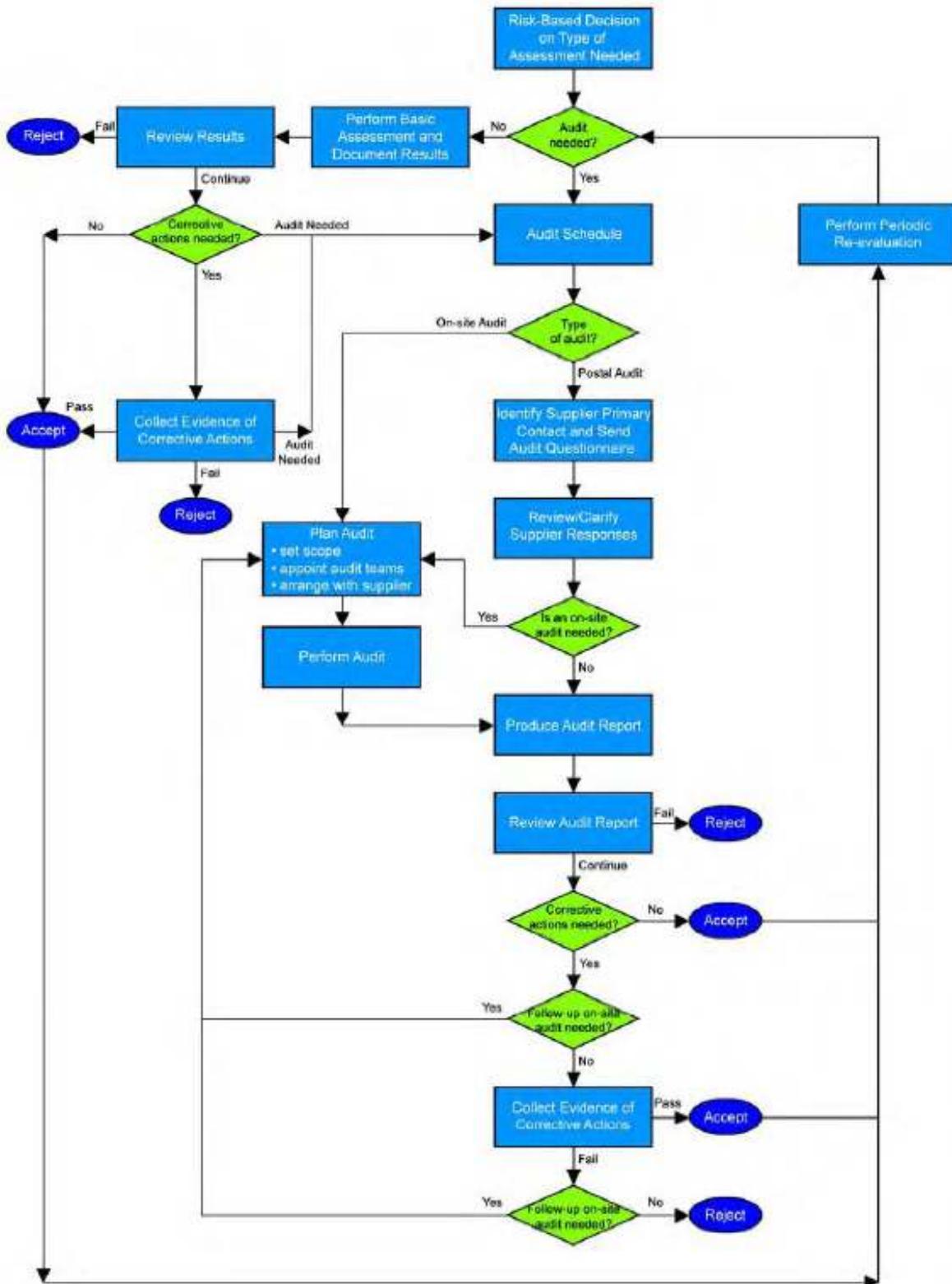
- take risk-based decision on most appropriate assessment route
- perform basic assessment if this is deemed sufficient – Otherwise, perform either a postal audit or an on-site audit, as determined following the initial risk assessment. An on-site audit also may be required based on the findings of the postal audit.
- document assessment or produce audit report
- determine corrective actions and follow them up, which could involve a follow-up on-site audit
- accept or reject the supplier

Once suppliers have been accepted, they may be subject to periodic re-evaluation by the regulated company at a frequency specified in their Standard Operating Procedures (SOPs). Periodic re-evaluation can be performed by a basic assessment, postal audit, or an on-site audit. Suppliers should be made aware of this possibility in advance of the initial audit.

Regulated companies normally maintain a supplier audit schedule, which indicates which suppliers have been audited, when the audit took place, the reason for the audit (e.g., new supplier, follow-up audit, surveillance audit, see Section 4.4.2 of this Appendix). Audit schedules also help regulated companies to plan joint audits of suppliers.

Useful guidance on planning, performing, and documenting audits of quality systems may be found in ISO 19011 - Guidelines for quality and/or environmental management systems auditing (Reference 26, Appendix G3).

Figure M2.1: The Assessment Process



4.1 Need for Audit

A decision should be taken on the need for an audit based on the results of the initial risk assessment and system impact (see Section 5.3.1 of Appendix M3), taking into account novelty and complexity, and the categorization of components (see Appendix M4).

4.2 Basic Assessment

A basic assessment may be based on:

- a review of public domain information
- market reputation
- knowledge and experience of prior performance
- discussions with other regulated companies

The results of the assessment should be documented, either in a separate assessment report or as part of another document. Identified issues should be addressed satisfactorily and documented. The assessment may determine that an audit is necessary.

For components which are considered as commodities, e.g., common desktop applications, a documented decision not to perform any assessment may be appropriate.

4.3 Postal Audits

There is a significant cost to both regulated companies and suppliers associated with conducting audits at the supplier's premises. This cost is associated both with the regulated company representatives travelling to the supplier and with the number of days of effort from both parties required to support an audit. A postal audit provides a mechanism for reducing these costs. Any problems found during the review of the postal audit may be resolved via more information from the supplier or escalated into an on-site audit which either replaces the postal audit or which focuses on specific areas of concern and provides supplementary information that can be appended to the postal audit.

A postal audit can provide a good understanding of the supplier's systems. It also may provide an indication of how a supplier approaches the management of quality, which may be confirmed by a site visit.

The value of a postal audit is enhanced when all documentation requested is provided by the supplier. The postal audit then comes closer to being a desktop version of an on-site audit. Only limited value may be obtained from the postal audit when no supporting documentation is provided in response to the audit challenges.

4.3.1 Applicability of Postal Audits

A postal audit may be used as:

- a part of the tendering process in order to determine if a supplier merits further consideration. It can assist in the production of a shortlist of potential suppliers who may, or may not, be subject to a detailed postal audit or an on-site audit prior to award of contract
- a preliminary audit to provide information to the audit team in order to focus efforts in critical areas during an on-site audit, thus potentially reducing the length of the audit at the supplier's premises

- a broad audit of the supplier's business processes to determine whether or not the system or service can be considered to be a mature, trustworthy product, which does not require an on-site audit. The assessment would typically review company information, number of customer installations, product history, product release information, the supplier quality manual and key procedures, and system life cycle and support activities supported by documented evidence.
- a follow-up audit for suppliers that have successfully passed an on-site audit with outstanding corrective actions
- a means of periodically re-assessing a supplier who provides an on-going service or who is an on-going supplier of products
- a means of auditing other premises of the supplier where the same Quality Management System (QMS) is implemented
- a means to address a broad range of topics and to determine any areas of weakness in the supplier's business processes which may indicate that an on-site audit of the supplier is required.

4.3.2 *Postal Audit Primary Contact*

To ensure continuity in communication between the supplier and the regulated company a primary contact should be established for both parties as part of the postal audit process. It is also recommended that the person providing the information required in the postal audit on behalf of the supplier is independent of the product or service being audited, e.g., from the supplier quality assurance function.

4.3.3 *Postal Audit Questionnaire*

The content of the postal audit questionnaire will depend on its purpose. The postal audit questionnaire for producing a shortlist of suppliers will tend to be high level. If there is a need to assess a specific product or service, however, the questions should be more detailed and specific. An example postal audit questionnaire is supplied separately. This questionnaire can be used as a framework for the production of other questionnaires such as: supplier selection short list postal audits (e.g., focus on organization and QMS plus product literature), and product and area specific postal audits (e.g., focus on QMS and software life cycle activities).

Postal audit questionnaires are sent to the supplier for completion and may include the following:

- company overview including any product-specific locations
- organization, roles and responsibilities, staff training and experience
- key products and/or service history and development plans
- QMS implementation at company level and for product-related processes
- product/project management
- software development life cycle processes and deliverables
- software development life cycle support processes
- service delivery processes
- user training
- product support/maintenance

- security
- use of sub-contractors, including both external organizations and individuals

The assessment of software products will normally be version specific and so the questionnaire should be drawn up accordingly.

The returned questionnaire is examined by the regulated company and clarification sought for areas of discrepancy. A summary of the audit findings and conclusions and the status awarded to the supplier are written up in a short report which is sent to the supplier for verification. Once agreement is reached, the report is issued to the regulated company for review and approval.

If, during the review of the supplier's response to the questionnaire, problems or concerns are found, the Postal Audit process may be terminated and an on-site audit scheduled, conducted, and documented. The final audit report should mention the reason(s) for changing to an on-site audit.

4.3.4 *Postal Audit Evidence*

The value of any postal audit will be limited or even irrelevant if there is no evidence supplied to support the completed postal questionnaire. The postal audit questionnaire should, therefore, request supporting evidence wherever possible, including real examples of the work performed.

4.4 On-site Audit – Preparation and Organization

4.4.1 *Planning/Scheduling*

Planning for the on-site audit involves defining the scope, deciding on the audit team, and arranging the audit with the supplier.

4.4.2 *Define Scope of the Audit*

The audit scope is determined by the purpose of the audit (e.g., detailed, follow-up, or surveillance), and the supplier's main activities (e.g., software product development, equipment manufacture, software integration and support services).

- detailed audits usually cover all aspects relating to the product or service under consideration. They can, however, also be used to assess the supplier's capability to produce a quality product when custom services are being sought.
- follow-up audits usually concentrate on specific areas of concern, as identified during previous audits, or the progress made on agreed corrective actions
- surveillance audits, when used by the regulated company, normally focus on areas of weakness found during previous audits, on new products and services, and can provide a vehicle for monitoring on-going compliance.

The nature of the supplier's services will determine which areas the on-site audit needs to cover, e.g., product development, custom software development, or support services.

The scope should be defined to meet the overall audit objective.

Example

A regulated company has decided that a follow-up audit of a software product supplier is needed. This was due to concerns raised during the on-site audit regarding the lack of documented testing carried out by the supplier. The follow-up audit would, therefore, concentrate on the following:

- the test strategies adopted at each stage of development
- evidence of both structural and functional testing
- evidence that each key function of the product has been tested thus providing traceability
- evidence of stress testing, and testing of abnormal conditions
- the use of testing tools
- the documentation standards employed, including the generation of pre-agreed life cycle specifications which have traceability to controlling or preceding specifications; test results and raw test data and their traceability back to the test specifications/definitions; review of test results; actions taken in event of test failure
- involvement of the supplier quality assurance function in the testing process
- the independence and qualifications of testers and reviewers
- verification that traceability from requirements through to testing is available and adequately documented

In order to cover the above topics effectively, the auditor would need to be refreshed about the supplier's organization, the software life cycle used, the quality processes followed for testing, and the appropriate controlling specifications, recognizing that these areas will have been covered already during the on-site audit.

The audit scope, therefore, drives the development of a suitable audit agenda.

4.4.3 Select Audit Team

The scope of the on-site audit to be performed determines the size and makeup of the audit team. On-site audits of complex systems may require a team of at least two people, e.g., a lead auditor plus a system user or technical specialist. Less complex systems may require only a single auditor.

A lead auditor should be appointed who has overall responsibility for the execution of the audit. The lead auditor should be an experienced auditor, with formal auditing qualifications and experience in the development of computerized systems, as applicable, and their use in a regulated environment. At least one member of the audit team should have an understanding of the technology being supplied and of the proposed application.

The audit team may also include less experienced auditors, a technical specialist, a user representative, a quality unit representative, or a purchasing representative.

The supplier should be informed in advance whenever a third party auditor is proposed to conduct, or take part in, the on-site audit so that any objections or concerns regarding conflict of interest or confidentiality may be raised and discussed.

4.4.4 *Supplier Notification*

Audit details should be confirmed in writing with the supplier. The reason, objective, scope, location, timing, and audit team details, including the use of third party auditors, should be included. A provisional agenda should also be provided, so that the supplier can prepare accordingly or suggest improvements. The required availability of supplier staff (including technical staff) should be made clear. The need for a confidentiality agreement should be addressed in advance of the audit.

4.5 On-site Audit – Performing the Audit

An on-site audit has three parts:

1. opening meeting
2. review and inspection
3. closing meeting

These are described in this section of this appendix.

4.5.1 *Opening Meeting*

This meeting allows for formal introductions and permits the lead auditor to summarize the purpose and scope of the audit. The agenda can be confirmed, or rearranged depending on the availability of supplier staff. Other issues, such as the provision of a quiet room, lunch arrangements, and access to documentary records are usually clarified.

The auditors should attempt to accommodate the supplier's suggestions or preferences, providing the audit objectives are not compromised. The supplier may wish to provide a presentation to the auditors to familiarize them with the company, and with relevant products and services as identified in the scope. This is acceptable if a time limit is agreed and observed.

4.5.2 *Review and Inspection*

This is the main part of the audit, where the audit team examines the supplier's practices and records in accordance with the agreed scope and agenda. While each auditor will have an individual style, the purpose of the audit is to establish, through questioning and inspection, the adequacy of the supplier's operations, and to identify any areas of concern and to bring them to the attention of the regulated company's management. The auditor should adopt a 'show me' approach when explanations are provided, making sure to interview designers and operatives as well as the management.

The auditor should consider the use of a checklist based on the agreed scope and agenda to ensure that key areas are covered and to provide a roadmap for the audit process. Example checklists and questionnaires for this Guide are supplied separately.

Any checklist used does not constrain the auditor from following up a topic in greater detail, based on professional judgment and experience. In practice, auditors will cover all checklist topic areas to a certain minimum level but will choose some areas for a more detailed inspection.

Issues of potential concern found during the audit should be raised with the supplier when they are found and examined further until the auditor is satisfied that enough relevant information has been gathered. Audit findings should have a reference to verifiable objective evidence (e.g., traceable to specific documents/records, visual observations).

4.5.3 *Closing Meeting*

The closing meeting allows the lead auditor to list observations noted during the audit, covering both positive issues and areas of concern. It also gives the supplier representatives an opportunity to respond to these findings. This response should be documented in the audit report.

The lead auditor should explain the next steps following the audit. A typical process outline would be:

- a. A draft audit report is produced by the lead auditor and may, as a courtesy, be submitted to the supplier for comment before formal submission to the regulated company's management. This can help to ensure that the report correctly describes the areas visited and the findings highlighted, and that the supplier has not been misrepresented.
- b. The lead auditor should consider any comments received from the supplier, and should obtain clarification where needed. The lead auditor may consider, but is not bound by, this input and may incorporate agreed comments into the final report. The audit report should not contain any significant issues not discussed during the audit or at the closing meeting.
- c. A formal audit report is produced and issued to the supplier and the regulated company management by the lead auditor. The supplier should be told when it could be expected.
- d. The report is reviewed by the regulated company management and required supplier corrective actions determined.
- e. The regulated company's representative contacts the supplier to agree a plan for implementing any corrective actions. This plan may include further audits.

4.6 Audit Report for Postal and On-site Audits

The audit report for both postal and on-site audits is a quality record which:

- provides a formal record of the audit and its findings
- acts as a major input when determining corrective action
- provides objective evidence to support the selection or continued use of a supplier

The report should present an accurate, objective record of the findings, and auditors should gather copies of key documentation as support material. References made in the audit report to documentation examined during the audit should be unambiguous (e.g., by title, reference, date, version, copy number, and author). The supplier and regulated company should treat the report as confidential. Audit reports should be retained by the regulated company as part of the documentation set for the system.

The audit report will normally contain:

- introduction
- scope of the audit
- organization of the audit, including agenda, criteria, representatives
- detailed findings: the checklist format may be used as the basis for presenting the information gathered in each area inspected and any findings

- record of the closing meeting
- conclusions

A suitable date for receipt of the corrective action plan from the supplier in response to the audit findings should be documented and agreed with the supplier.

Some regulated companies also require that the audit report include specific recommendations by the audit team.

4.7 Supplier Acceptance and Rejection

Based on the outcome of the audit, the regulated company may decide:

- to use the supplier unconditionally
- to use the supplier for certain products or certain versions only
- to use the supplier subject to specific corrective actions being addressed
- to provide additional regulated company supervision of the supplier and/or conduct additional testing to overcome shortfalls in the supplier's processes and/or deliverables
- to agree with the supplier on the application of a documented QMS for the purposes of the contract
- to prohibit the use of the supplier

4.8 Corrective Actions and Follow-up Audits

If the supplier is requested to carry out corrective actions as a result of a quality audit, then the regulated company should follow these up and obtain documentary evidence of successful completion. Evidence could include copies of new procedures, testing records, design review, and code review documents. A letter of confirmation from the supplier is not normally sufficient.

If a follow-up on-site audit is required then it should be planned, carried out, and documented. It should, however, be noted that the lead auditor should not be constrained to just the area of the corrective actions; follow-up audits often raise further corrective actions.

The outcome of the review of the audit report should be formally recorded and documented by the regulated company.

4.9 Re-evaluation

Once suppliers have been accepted, they should be subject to periodic re-evaluation by the regulated company at a frequency, and following the process, specified in their SOPs. The periodic re-evaluation process should determine whether a re-audit is required based on risk and, if so, whether this will be a postal audit or an on-site audit.

The decision on whether to re-audit the supplier can be influenced by:

- the criticality of the product/service provided
- change of supplier ownership (acquisitions/mergers)

- changes in the supplier management structure at technical/operational (business focus) level
- changes to the QMS (e.g., new business processes; changes to the certification standard; changes in the scope of certification)
- change of license model (e.g., transition from closed source to open source or freeware)

The frequency of re-evaluation will depend on factors including the results of previous assessments and experience based on use. Typically, re-evaluation will focus on specific areas rather than the whole of the supplier's QMS, thus taking several re-evaluations to assess the whole QMS in detail.

If a formal supplier surveillance program is required (e.g., for on-going service providers), this should form part of re-evaluation.

5 Joint Audits

Maintaining individual regulated company audit programs has several drawbacks:

- it is resource intensive, leading to duplicated activities by regulated companies and suppliers
- it places a heavy burden on supplier time and effort
- multiple auditing standards may develop, which could confuse suppliers

Joint audits involve representatives from more than one regulated company performing an audit together, and a number of such audits have already been carried out. Several benefits have been identified:

- reduced time and effort for both regulated companies and suppliers
- increased co-operation between regulated companies
- progress towards common auditing standards

There are a number of potential problems to overcome, however, when organizing joint audits. These include:

- confidentiality and liability
- the makeup and size of the audit team
- common and consistent auditor training
- follow-up on corrective actions

Building on the experience of previous joint audits, further co-operation is likely between regulated companies.

6 Shared Audit Reports

Some regulated companies have established a practice of sharing their audit reports after conducting a supplier audit. If an audit report is to be shared the following topics should be documented:

- that the scope of the audit is valid for the recipient of the audit report
- that the auditor(s) qualifications meet the requirements of the recipient of the audit report
- that the audit process, including the use of any checklists, is acceptable to the recipient of the audit report

There may be liability and confidentiality issues where audit reports are shared. If reports are shared, then the agreement of all parties involved should be obtained and documented, including that of the supplier. Individual agreements may be made between companies, or a third party may provide this service.

If a shared audit is used, the regulated company should ensure that it covers the relevant aspects of the particular application scope.

Further information on shared audits may be found in PDA Technical Report 32 (Reference 37, Appendix G3).

7 Corporate Audits

Regulated companies often have a number of departments both at local and global level which conduct supplier audits including:

- Business Quality Units
- Regulatory Compliance
- IT Quality Assurance
- Engineering/Project Management/Validation groups
- Purchasing

There can be a number of the above departments each serving different business lines and in different parts of the business (e.g., Research and Development (R&D), Manufacturing).

The regulated company should try to maintain a centralized audit repository so that audit effort can be leveraged within the company and to avoid a supplier being audited by different parts of the same regulated company. The harmonization of audit requirements and reporting would help in the sharing of these audit reports.

8 Supplier Preparation for an Audit

This appendix is intended to provide suppliers with an indication of which products or services would require a supplier audit and the type of audit which would be appropriate. It benefits both the regulated company and the supplier if the supplier is prepared for the audit.

The supplier can prepare for a postal audit by:

- providing answers to all questions in a clear and concise manner
- providing the quality and technical documentation requested

The supplier can prepare for an on-site audit by:

- making the requested personnel available (or a suitable designee)
- providing answers to questions in a clear and concise manner
- making quality and technical documentation easily available to reduce time and to prevent disruption to the audit flow

9 Supplier Certification

There is an increasing dependence on suppliers to provide quality assured solutions and services. Suppliers who operate to very high standards of quality may be certified against the regulated company's quality standards. In such cases, direct involvement in the design, implementation and testing of the system by the regulated company may be limited, as greater assurance and trust in the supplier's quality approach is obtained during the audit process.

In such situations, the audit process should be very rigorous and detailed and periodic re-evaluation of the supplier is essential.

10 International Standards and Certification

The certification of a supplier against a nationally or internationally recognized accredited quality standard, such as ISO 9001 (Reference 22, Appendix G3), and any associated accredited sector schemes, such as TickIT, for software development (Reference 38, Appendix G3), may be taken into consideration when planning the scope of the audit program. It is, however, very important to understand the scope and current applicability of certification.

Using ISO 9001 as an example, this mandates specific quality processes and the generation of records in a number of areas including:

- quality procedures

Some mandatory procedures are identified in the standard. The standard also requires that an organization has the documentation needed to ensure effective planning, operation, and control of its processes.

- internal audits

These should take place periodically in accordance with a defined schedule and should cover all business processes under the certified scope of the QMS. They also can be project based. Business critical and/or problem areas can be audited with greater frequency. Auditors should not audit their own work. Mandatory records of internal audits should be maintained.

- purchasing

This includes the identification and protection of purchased goods and the use and control of suppliers and sub-contractors (the term sub-contractors applies to both individual persons and companies who are providing specific services, e.g., the use of a systems integrator for software development). Suppliers should be evaluated, selected, and periodically re-evaluated, and mandatory records of this process should be maintained.

- design and software reviews

records of design and software reviews should be maintained

- document control

This covers control, review, and retention of specified quality records. The standard also identifies which records should be maintained.

- change management and product identification (configuration management)

Evaluation of changes is required and mandatory records of change reviews should be maintained. Product should be suitably identified throughout product realization and, where traceability is a requirement, mandatory product identification records should be maintained.

- use of design and coding standards

Part of the ISO 9001 product realization process. Design and coding standards are required for verifying that the design outputs adequately meet the design input requirements.

- control of non-conforming product

Mandatory records of the nature of non-conformities and any subsequent activities (e.g., re-work processes) should be maintained.

- resource management

Staff should be qualified to perform their roles via appropriate education, training, skills, and experience. Competency assessments should be performed and mandatory records of education, training, skills, and experience should be maintained.

Science Based Quality Risk Management

1 Introduction

This appendix provides further detail on the quality risk management process introduced in Section 5 of the Main Body.

Quality risk management is a systematic process for the assessment, control, communication, and review of risks to patient safety, product quality, and data integrity, based on a framework consistent with ICH Q9 (Reference 10, Appendix G3). It is used:

- to identify risks and to remove or reduce them to an acceptable level
- as part of a scaleable approach that enables regulated companies to select the appropriate life cycle activities for a specific system

Organizations may already have established risk assessment methods and tools (see Section 6 of this appendix). While this Guide describes one suggested approach to risk management, it does not intend or imply that these existing processes and techniques should be discarded. They should continue to be used as appropriate as part of an overall quality risk management process.

2 Scope

This appendix is applicable to all types of computerized systems used in regulated activities, including those supporting clinical trials, toxicological studies, Active Pharmaceutical Ingredients (API) production, formulated product production, warehousing, distribution, and pharmacovigilance.

Separate and existing risk assessment processes may be relevant to some systems, e.g., in relation to analytical methods, chemical processes, Health, Safety, and Environment (HSE), and Process Analytical technology (PAT). These should be taken into consideration and leveraged.

3 Benefits

Application of quality risk management enables effort to be focused on critical aspects of a computerized system, in a controlled and justified manner, leading to specific benefits, such as:

- identification and management of risks to patient safety, product quality, and data integrity
- scaling of life cycle activities and associated documentation according to system impact and risks
- justification for use of supplier documentation
- better understanding of potential risks and proposed controls
- highlighting of areas where more detailed information is needed
- improving business process understanding
- supporting regulatory expectations

4 Roles and Responsibilities

Quality risk management is part of the overall responsibility of the business process owner, which may be delegated to project team members. Key roles are shown in Table M3.1.

Table M3.1: Risk Management Roles and Responsibilities

Role	Responsibilities
Process Owner/System Owner	<ul style="list-style-type: none">• establish team and provide resources (may be delegated to nominated project manager)• involvement in risk assessments as required• approve documentation
Team consisting of Subject Matter Experts (SMEs) and key users ¹	<ul style="list-style-type: none">• identify, analyze and evaluate risks to patient safety, product quality, and data integrity• develop controls
Quality Unit	<ul style="list-style-type: none">• identify, analyze and evaluate those risks associated with regulatory compliance and maintaining company quality standards and policies• involvement in risk assessments as required• approve documentation
Supplier	<ul style="list-style-type: none">• provide information on their product, how it works and how it might fail• provide advice on controls• involvement in risk assessments as required

¹ SMEs may include as necessary Process Owner, System Owner, Quality Unit, Business or IT Application Support, IT or Engineering Operations Support, Infrastructure specialists, supplier, or any other appropriate specialist.

5 Guidance

Section 5.3 in the Main Body describes a five step process, as shown in Figure M3.1.

Figure M3.1: Quality Risk Management Process



The Main Body describes each of the steps. This appendix provides further guidance on the following topics:

- scalability of the process
- applying risk management based on the business process
- risk management throughout the system life cycle
- risk assessment method
- the selection and use of controls
- residual risk
- using risk assessments to scale system life cycle activities
- risk communication and documentation
- examples of applying the process to different types of systems

5.1 Scalability of the Process

The five step risk management process has been designed such that it may be scaled according to risk, complexity, and novelty of individual systems, with each step of the process building upon the previous output.

As an example, Figure M3.2 shows how the process is applied to a typical Category 3 product.

Figure M3.2: Process Applied to a Typical Category 3 Product



Other examples showing the scalable approach of applying the process are given in Section 7 of this appendix.

The process may also be used during operation, e.g., during change control. In this case steps 2 to 5 typically should be used and information from the original step 1 should still be available and should be used as appropriate.

5.2 Applying Risk Management Based on the Business Process

In order to effectively apply a quality risk management program to computerized systems, it is important to have a thorough understanding of the business process supported by the computerized systems, including the potential impact on patient safety, product quality, and data integrity. Aspects to consider include:

- **What are the hazards?**

To recognize the hazards to a computerized system requires judgment and understanding of what could go wrong with the system, based on relevant knowledge and experience of the process and its automation. Consideration should include both system failures and user failures.

- **What is the harm?**

Potential harm should be identified based on hazards. Examples of potential harm include:

- production of adulterated product caused by the failure of a computerized system
- failure of an instrument at a clinical site that leads to inaccurate clinical study conclusions
- failure of a computerized system used to assess a toxicology study that leads to incomplete understanding of a drug's toxicological profile

- **What is the impact?**

In order to understand the impact on patient safety, product quality, and data integrity, it is necessary to estimate the possible consequence of a hazard.

- **What is the probability of a failure?**

Understanding the probability of a failure occurring to a computerized system assists with the selection of appropriate controls to manage the identified risks. For some types of failure such as software failure, however, it may be very difficult to assign such a value, thus precluding the use of probability in quantitative risk assessments.

- **What is the detectability of a failure?**

Understanding the detectability of a failure also assists with the selection of appropriate controls to manage the identified risks. Failures may be detected automatically by the system or by manual methods. Detection is useful only if it occurs before the consequences of the failure cause harm to patient safety, product quality, or data integrity.

- **How will the risk be managed?**

Risk can be eliminated or reduced by design, or reduced to an acceptable level by applying controls which reduce the probability of occurrence, or increase detectability. Controls may be automated, manual, or a combination of both.

The above considerations are context sensitive. For example, risks associated with solid oral dosage manufacturing area are very different to those in a sterile facility, even when the same computerized systems are used.

Similarly, the risks associated with an adverse event reporting system are very different to those in a training records database. The former can have a direct effect of patient safety, whereas the latter system is very unlikely to affect patient safety.

The acceptable level of risk, sometimes known as risk tolerance, should be considered.

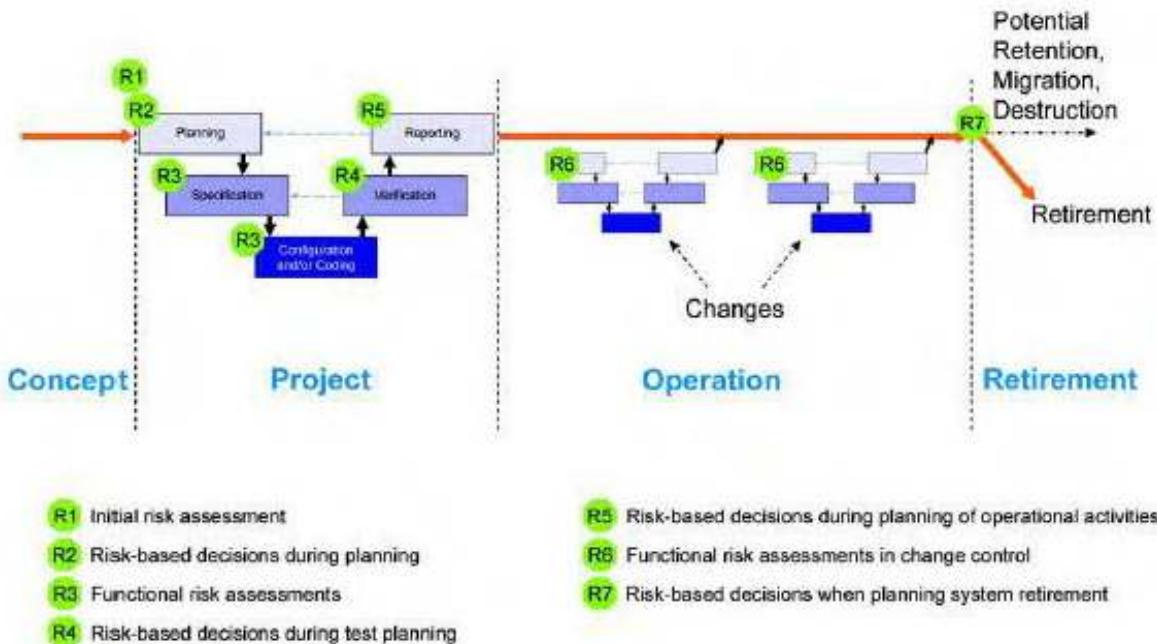
5.3 Risk Management Throughout the System Life Cycle

Appropriate risk management processes should be followed throughout the life cycle in order to manage identified risks and to determine the rigor and extent of the activities required at each phase of the life cycle.

While risk-based decision making should be used throughout the life cycle, different approaches may be appropriate to different situations, ranging from formal risk assessments to decisions taking into account pertinent risk factors. For example, formal risk assessments are usually performed at several stages when developing new software. A formal risk assessment would normally not be required, however, when determining the need for a formal supplier audit. This risk-based decision, typically, is made and documented by the project team also taking into account novelty and complexity, the categorization of components, and any intention to leverage supplier documentation.

Figure M3.3 shows the typical use of risk-based decision making throughout the life cycle.

Figure M3.3: Typical Use of Risk-Based Decision Making



5.3.1 Initial Risk Assessment

An initial risk assessment should be performed at (or before) the beginning of the project phase. This is Step 1 of the process described in this section of this appendix.

The assessment follows, or is in parallel with, development of the User Requirements Specification (URS).

The assessment should be based on an understanding of business processes and business risk assessments, user requirements, regulatory requirements, and known functional areas. Any relevant previous assessments may provide useful input, and these should not be repeated unnecessarily.

Risks introduced by computerization of the business process (e.g., electronic record integrity) should be included in the assessment.

This risk assessment is likely to focus on important risks to GxP and to the business process, rather than detailed functions and technical aspects. The process owner and the quality unit, typically, are involved at this stage in addition to the input of appropriate SMEs.

Important pre-requisites for this assessment are:

- a clear understanding of the business process
- a defined boundary around the business process
- the role of the computerized system in supporting the business process
- sufficiently defined requirements (development of requirements may be iterative and influenced by the risk assessment)

Benefits of the initial risk assessment include:

- early identification of key areas that require focus in subsequent stages, including Critical Quality Attributes (CQAs) and Critical Process Parameters (CPPs) where appropriate
- information for requirements development, system specification and system descriptions
- information to assist with developing the strategy for achieving compliance and fitness for intended use

5.3.1.1 *GxP Determination*

The initial risk assessment should include a decision on whether the system is GxP regulated (i.e., a GxP assessment). If so, the specific regulations should be listed, and to which parts of the system they are applicable. For similar systems, and to avoid unnecessary work, it may be appropriate to base the GxP assessment on the results of a previous assessment, provided the regulated company has an appropriate established procedure.

5.3.1.2 *System Impact*

The initial risk assessment should determine the overall impact that the computerized system may have on patient safety, product quality, and data integrity due to its role within the business processes. This should take into account both the complexity of the process, and the complexity, novelty, and use of the system. Categorization assists in assessing system complexity and novelty (see Appendix M4).

In general, high impact systems typically include those that:

- generate, manipulate, or control data supporting regulatory safety and efficacy submissions
- control critical parameters or data used at any stage, including pre-clinical, clinical, development, and manufacture
- control or provide data for product release
- control data required in case of product recall
- control adverse event or complaint recording or reporting
- support pharmacovigilance

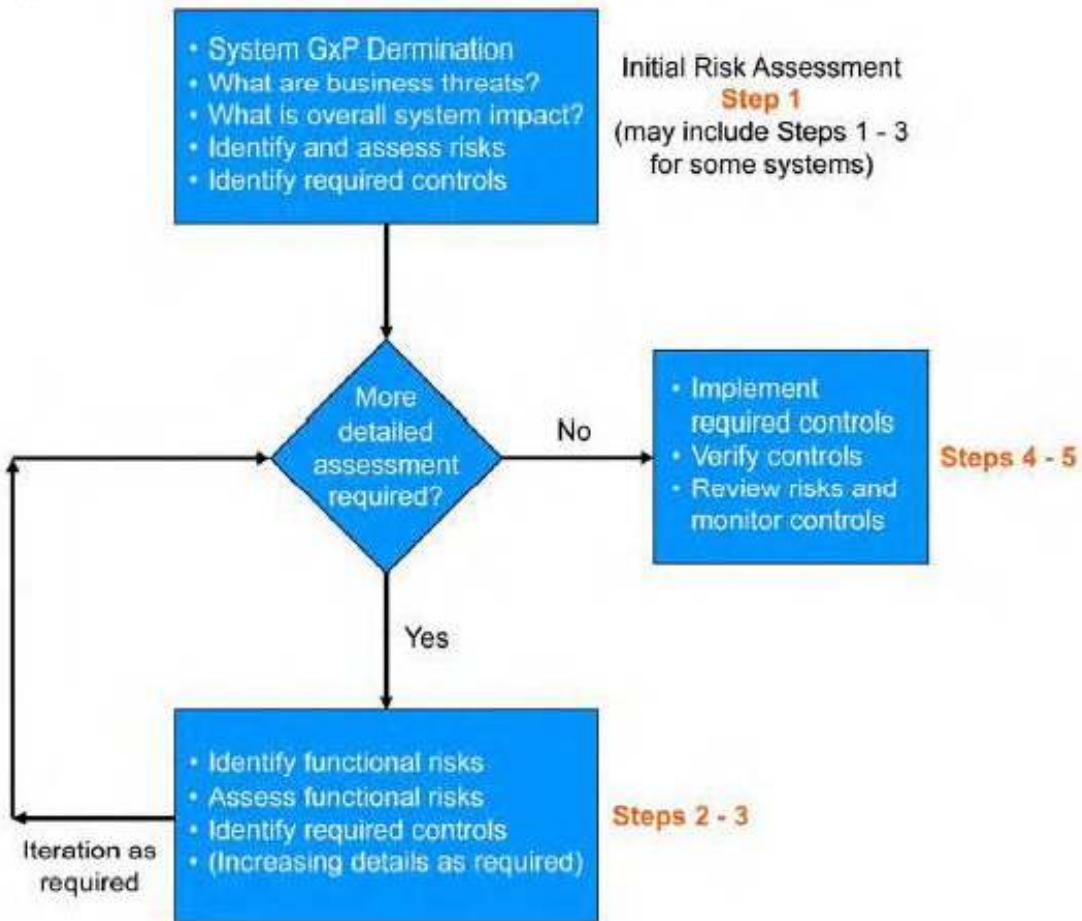
Process knowledge assists with determining system impact (see Section 7.2 of this appendix for an example).

Systems that are of lower overall impact can be documented and tested less rigorously (see Section 5.7 of this appendix).

5.3.1.3 Need for Further Assessments

The amount of information available when performing the initial risk assessment depends on both the business process and on the GAMP category. For Category 3 products the amount of information available at the time of the initial risk assessment may be sufficient for all relevant risks to be identified, assessed, and controlled without the need for further risk assessments. This would not be the case for a custom application (Category 5), where further more detailed assessments would be required as the system is developed, as shown on Figure M3.4.

Figure M3.4: Deciding on the Need for Further Assessment



The need for further risk assessments, therefore, varies widely. See Section 7.1 of this appendix for examples of typical approaches for different categories of systems.

5.3.2 Risk-Based Decisions During Planning

Risk management is an integral element of good project management practice and the approach for achieving compliance should be integrated within the overall approach.

The outcome of the initial risk assessment described in Section 5.3.1 of this appendix should contribute to the planning process. Key risk-based decisions taken during planning include:

- need for, and rigor of, supplier assessment

- using the results of supplier assessments to assist planning to achieve compliance and fitness for intended use, including determining the involvement of the supplier
- determining activities, deliverables, and responsibilities for achieving compliance and fitness for intended use, including extent of specification and verification
- need for further risk assessments, when they are required in the life cycle, and the method to be used. A risk assessment method is provided in Section 5.4 of this appendix. When deciding on the level of further assessment required information already gathered should be taken into account (e.g., results of supplier assessment, degree of standardization)

These decisions should be documented.

Employing risk-based decisions for achieving and maintaining compliance allows improved efficiencies at two levels:

1. Scalability: At the system level, systems that are of lower overall impact can be documented and tested less rigorously; see section 5.7 of this appendix for further details
2. Focusing: At the functional level, greater rigor can be applied to the testing and control of functions that are of the highest risk, with less rigor applied to low risk functionality

5.3.3 Functional Risk Assessment

Where these are required, functional risk assessments should be used to identify and manage risks to patient safety, product quality, and data integrity that arise from failure of the function under consideration. This is covered by steps 2 and 3 of the process.

Functions with impact on patient safety, product quality, and data integrity are identified by referring to the URS, functional specification (FS), and the output of the initial risk assessment.

A method for performing functional risk assessment is provided in Section 5.4 of this appendix. The assessments should be performed by SMEs.

Computerization may introduce particular risks (e.g., electronic record integrity, system availability, security, infrastructure) not otherwise associated with the manual business processes. The design of computerized systems may provide controls for identified risks, but may introduce other risks that require controlling. This should be included in the assessment.

More information on the use of risk assessments for particular system types and for infrastructure is given in the relevant GAMP Good Practice Guides (Reference 34, Appendix G3).

5.3.4 Risk-Based Decisions During Test Planning

Testing is often performed at several levels depending on the risk, complexity, and novelty of the system.

Significant savings may be realized if the need for additional controls for the business process or the computerized system is recognized early in the development process. Measures identified to manage risk should be implemented and verified. Verification of controls, typically, is covered during testing of the system and should cover any additional controls required to address deficiencies found during testing.

The results of functional risk assessments should influence the extent and rigor of verification. Testing should be focused on the high risk functionality, minimizing effort on low risk areas. See example in Section 7.5 of this appendix.

If additional controls have been added subsequent to the functional risk assessment, it may be appropriate to reassess the conclusion of that assessment, since the new controls may allow the adoption of simpler test cases.

Other information also may affect test planning, such as the results of supplier assessments.

These decisions should be documented.

5.3.5 Risk-Based Decisions During Planning of Operational Activities

Operational activities should be selected and scaled according to the nature, risk, and complexity of the system in question. Opportunities for risk-based decisions when planning operation include:

- system availability
- frequency and level of backup and recovery
- disaster planning
- system security
- change control (see Section 5.3.6 of this appendix)
- periodic reviews

Any critical business processes should be identified and the risks to each assessed. Plans should be established and exercised in order to ensure the timely and effective resumption of these critical business processes in case of failure.

5.3.6 Functional Risk Assessments in Change Control

Change management should provide a dependable mechanism for prompt implementation of technically sound improvements following the approach to specification, design, and verification described in this document. The rigor of the approach, including extent of documentation and verification, should be based on the risk and complexity of the change.

5.3.7 Risk-Based Decisions When Planning System Retirement

Risk-based decisions are required when planning system retirement, e.g.:

- approach to data and record retention and migration
- approach to verification

5.4 Risk Assessment Method

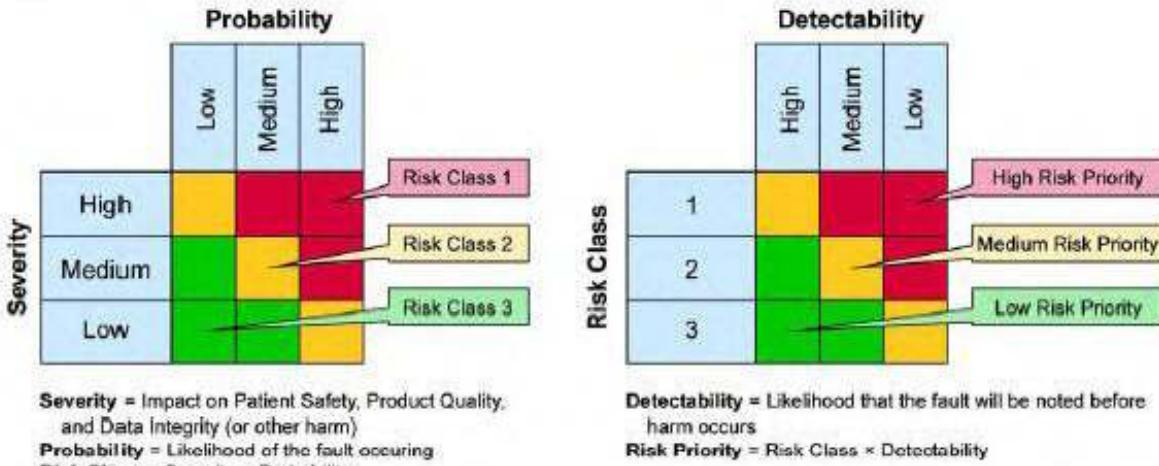
Risk management aims to establish controls such that the combination of severity, probability of occurrence, and detectability of failures is reduced to an acceptable level. Severity refers to the possible consequence of a hazard.

The method presented in this section provides a simplified functional risk assessment tool. It is not mandatory – other detailed risk assessment methods may be used. It is used, if necessary and appropriate, during step 3 of the 5 step process.

Each of the hazards identified for a function is assessed in two stages, as shown in Figure M3.5:

1. Severity of impact on patient safety, product quality and data integrity is plotted against the likelihood that a fault will occur, giving a Risk Class.
2. Risk Class is then plotted against the likelihood that the fault will be detected before harm occurs giving a Risk Priority.

Figure M3.5: Risk Assessment Method



The Risk Priority obtained helps to focus attention on areas where the regulated company is most exposed to hazards. These should be considered in relation to the risk tolerance, which varies from company to company based on a variety of business and regulatory drivers.

Successful application of this method depends on the ability to agree on the meaning of High, Medium, and Low for each segment of the assessment. These should be considered specifically in the context of the system in each project. An example form for documenting the functional risk assessment is provided separately.

5.4.1 Scaling the Method

In order to use resources most effectively, functional risk assessment should be focused on functions with highest impact. Other aspects, such as probability of occurrence and detectability should be investigated in more detail later when performing the functional risk assessment. An example approach to scaling functional risk assessments based on impact is provided in Section 7.3 of this appendix.

Function impact is context sensitive. For example, failure of an instrument in an in-process Quality Control (QC) laboratory for chemical intermediates is far less likely to affect patient safety than the same instrument in a QC laboratory that releases drug product to market, because there are many additional controls between the intermediate and the patient in the former case, where there may be none in the latter.

5.5 The Selection and Use of Controls

Controls are measures that are put in place to reduce risk to an acceptable level. They may be part of a computerized system function, in parallel manual procedures, or they may be downstream, intended to trap fault conditions after they have occurred, e.g., QC release testing.

Controls typically are aimed at:

- eliminating risk through process or system redesign
- reducing risk by reducing the probability of a failure occurring
- reducing risk by increasing the in-process detectability of a failure
- reducing risk by establishing downstream checks or error traps (e.g., fail-safe, or controlled fail state)

In some cases, it may not be possible to reduce risk through downstream controls (e.g., for an adverse event reporting system, for which there is no downstream), so controls in such cases generally are integral to the system or process and are aimed at preventing the failure from occurring or making it more detectable if it does. In other cases, the identified risk may be sufficiently low or easily detectable such that specific controls are not required.

Controls for a given process may be automated within the system, such as alarms, restrictions to data fields, required data fields, or dialog box prompts for verification. Alternatively, they may be entirely independent external processes, such as subsequent chemical or physical analyses, or operator checks.

Examples of controls that could be used to reduce risk are shown in Table M3.2.

Table M3.2: Examples of Controls to Reduce Risk

Control Strategy
Introduction of automated checks of data quality in downstream computerized systems.
Introduction of procedures to the business process to counter possible failures, such as QC testing of products.
Introduction of automated controls within the computerized system being assessed, e.g.: <ul style="list-style-type: none">• data verification checks within the system design to reduce the likelihood of data entry errors (such as acceptable input ranges)• User prompts to verify inputs to increase the detectability of a user error
Use is made of proven methods, tools and components; fault-tolerance may be built into the computerized system (e.g., using replicated parts, system mirroring); the operating environment may be controlled.
Increased rigor of verification testing to demonstrate that the computerized system performs as expected and can handle error conditions.
Enhanced training of users

If the selected controls are still not adequate to bring risk to an acceptable level, wider risk control strategies should be considered, such as those shown in Table M3.3.

Table M3.3: Wider Risk Control Approaches

Modify Project Strategies
<ul style="list-style-type: none">Project structure and makeup: The experience and qualifications of staff; the type of project organization; the level of education and training provided.Level of documentation and review: Alter the amount of documentation that is approved and controlled; introduce or remove formal review points to reflect identified risk.
Modify the Business Process
<ul style="list-style-type: none">How the computerized system is used in the business process: If the computerized system introduces or increases risk, consider alternative approaches to how the system is used.Redesign of the business process: Change the business process to lessen or eliminate key points of risk.
Risk Avoidance
The risks are so high that the new way of working should not be implemented.

5.6 Residual Risk

Residual risks after implementing control measures should be considered, e.g., after testing, to determine whether selected control strategies for the system should be adjusted.

If the residual risk is above the threshold of acceptable risk, then appropriate controls should be implemented and verified, and the impact on previously implemented risk control measures should also be considered.

5.7 Scaling Life Cycle Activities

Activities aimed at ensuring GxP compliance and fitness for intended use, throughout the life of the system, should be scaled according to:

- system impact on patient safety, product quality and data integrity (risk assessment)
- system complexity and novelty (architecture and categorization of system components)
- outcome of supplier assessment (supplier capability)

Specific activities that may be scaled include:

- levels of specification
- need for and extent of design reviews
- need for and extent of code reviews
- extent and rigor of verification activities

Examples showing the levels of specification and verification for different categories of system, and how the five step process is applied, are given in Section 7 of this appendix.

The strategy for supplier assessment also can be scaled, based on system impact, GAMP category, and the maturity of the product. Suppliers also may contribute substantially to the risk assessment process as subject matter experts.

5.8 Risk Communication and Documentation

As defined in ICH Q9 (Reference 10, Appendix G3), Risk Communication is the sharing of information about risk and risk management between the decision makers and others. The output of the risk management process, including the assessments of impact and risk and the evaluated effectiveness of monitored controls, should be shared by the decision makers with other involved parties, such as the quality unit, the business process owner, and as appropriate the supplier.

This communication should take place throughout the risk management process. Although it is not necessary to communicate the acceptance of every risk, special emphasis should be given to communication to the appropriate individuals when a risk or impact has changed, so that any necessary adjustments can be made. Where necessary, the process should enable escalation of risks to senior managers in a timely fashion.

This information can also be used to improve the efficiency of the change management process. Every change to be applied can use the risk assessment information to identify the areas of the system or process impacted by the change and the risks involved in doing so. To facilitate this, risk assessments should be documented such that the results can be easily accessed during the life cycle. This may be achieved using a risk register.

The risk-based approach will be effective only if the risk control strategies that are put in place are monitored during the life of the computerized system to ensure they remain in place and are effective. Hence, as part of the periodic review, the risk register should be reviewed to ensure that all the control strategies remain appropriate.

6 Risk Assessment Methods and Tools

The following are commonly used methods and tools for risk assessment:

- Hazard and Operability Analysis (HAZOP)
- Computer Hazards and Operability Analysis (CHAZOP)
- Failure Mode and Effects Analysis (FMEA)
- Failure Mode, Effects, and Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- Hazard Analysis and Critical Control Points (HACCP)
- Basic Risk Management Facilitation Methods
- Preliminary Hazard Analysis (PHA)
- Risk Ranking and Filtering

For further details see ICH Q9 Annex I: Risk Management Methods and Tools (Reference 10, Appendix G3).

7 Examples

This section includes examples of the application of risk management. They are indicative and not intended to be definitive. Other approaches are equally applicable.

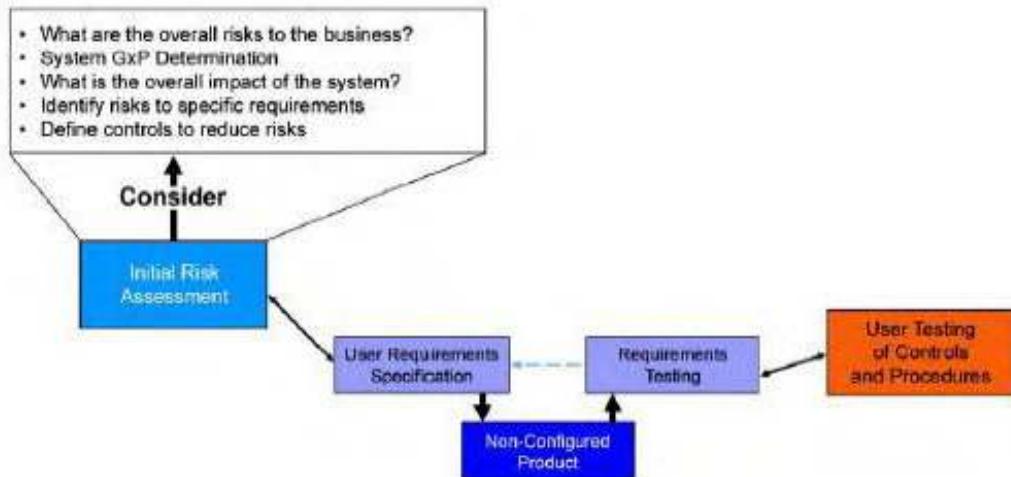
7.1 Example 1 – Approaches for Different Categories of Systems

The examples provided in this appendix show the risk management process applied to three categories of system.

7.1.1 Example Category 3 Non-Configured Product

For a typical Category 3 product it may be possible to cover all relevant risks in a single assessment as shown in Figure M3.6. For a specific system it may be decided that further assessments are required and these should be planned as appropriate.

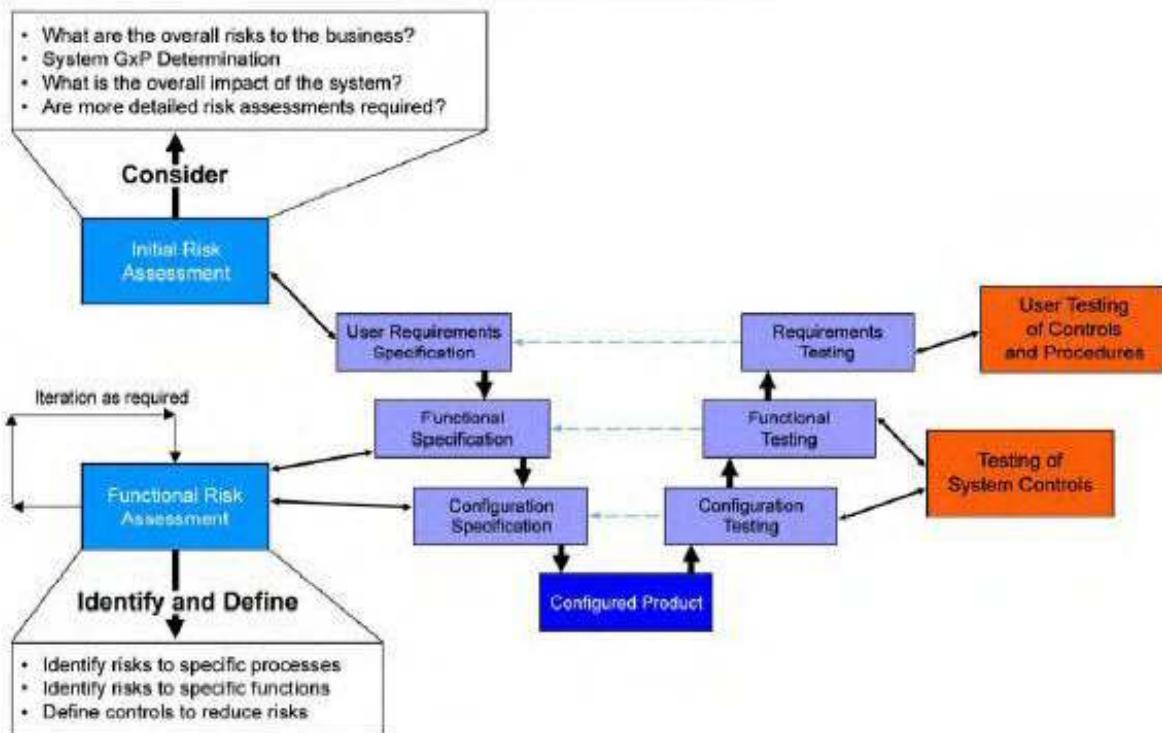
Figure M3.6: Risk-Based Approach for Non-Configured Product (Category 3)



7.1.2 Example Category 4 Configured Product

For a typical Category 4 product it may be necessary to carry out an initial risk assessment to determine whether the system is GxP regulated and to understand the overall system impact, followed by one or more detailed risk assessments as the system specification is developed. However, for some systems it may be possible to cover all risks in the initial assessment; see Figure M3.7.

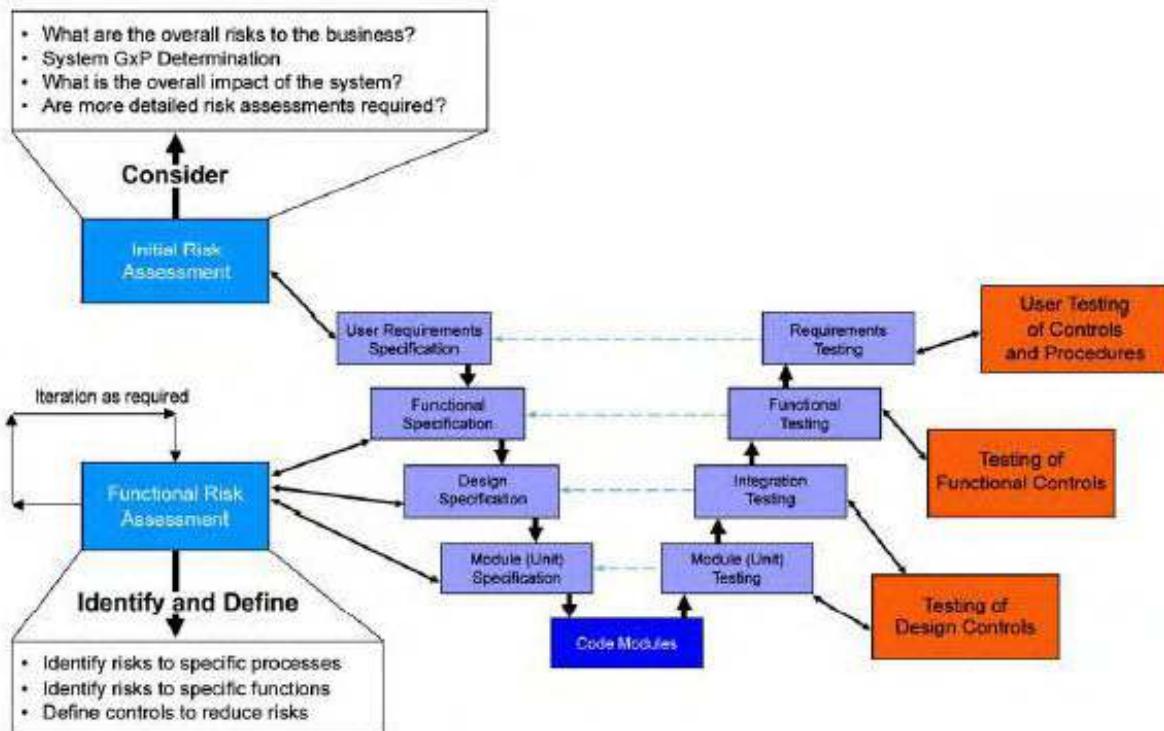
Figure M3.7: Risk-Based Approach for Configured Product (Category 4)



7.1.3 Example Category 5 Custom Application

For a typical Category 5 custom application it is necessary to carry out an initial risk assessment to determine whether the system is GxP regulated and to understand the overall system impact, followed by one or more detailed risk assessments as the system specification and design is developed; see Figure M3.8.

Figure M3.8: Risk-Based Approach for Custom Application (Category 5)

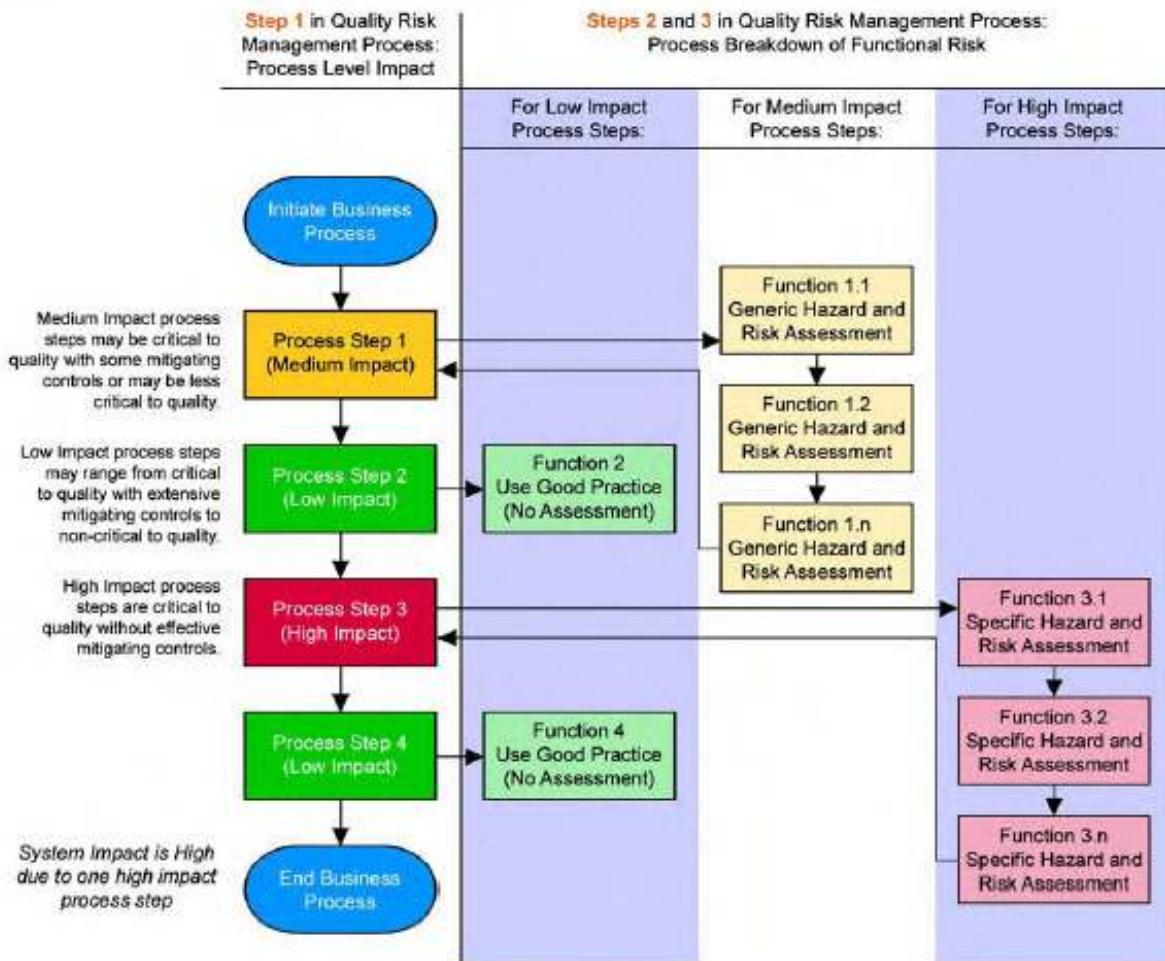


7.2 Example 2 – Determining System and Functional Impact

This example presents a method of determining system impact and provides information that can be used later as part of functional risk assessments.

Figure M3.9 shows how process knowledge helps determine system impact, and how the understanding of the importance of the process steps assists with the determination of functional risk in step 2 of the 5 step process. System impact is chosen to be the impact for the highest assessed process step. System impact can be used to scale compliance activities.

Figure M3.9: Analyzing the Business Process for Steps 1, 2, and 3 in the Five Step Process



7.3 Example 3 – Functional Risk Assessment Based On Impact

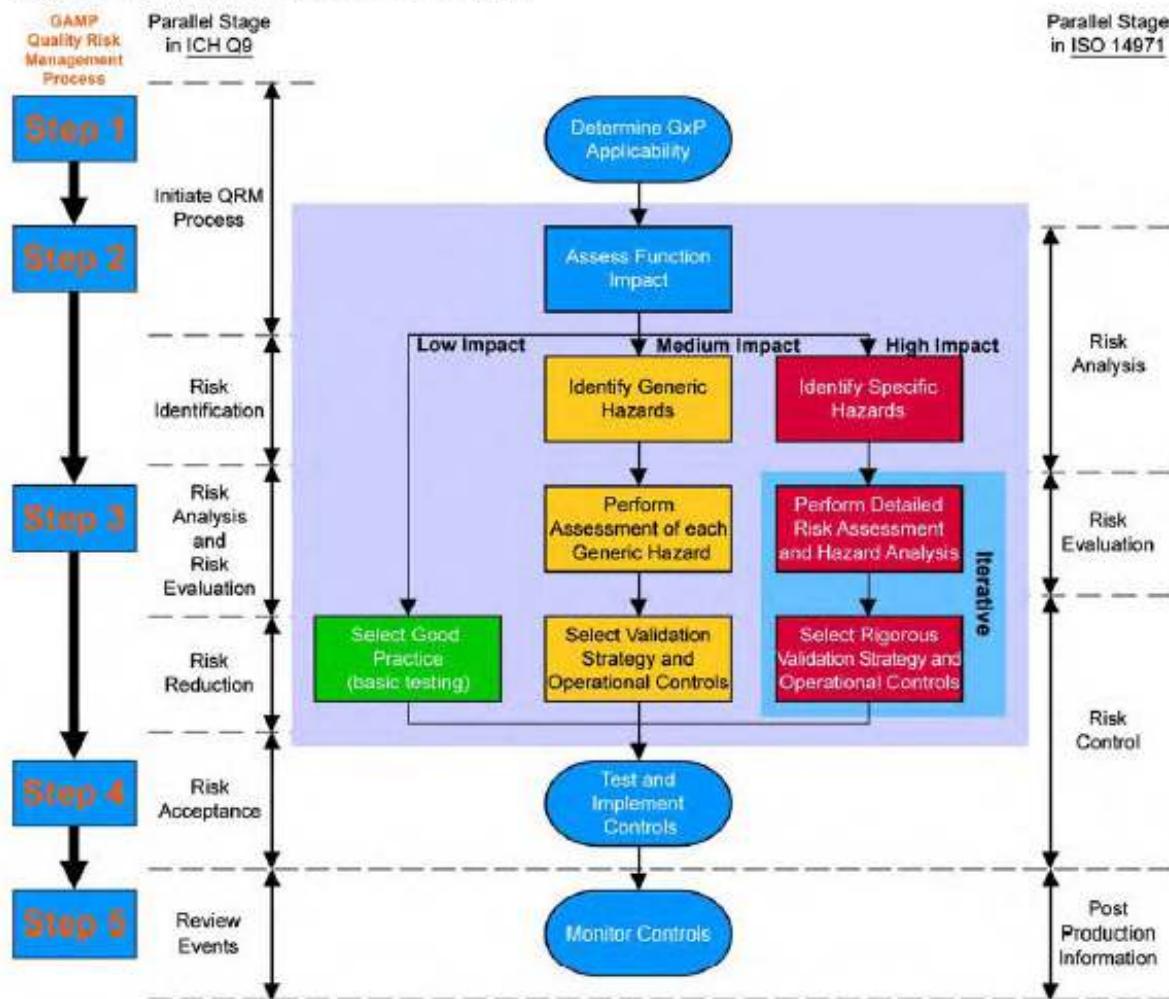
Figure M3.10 shows the 5 step process with step 3 expanded to provide an approach to functional risk assessment based on impact. This example classes functions as one of high, medium, or low impact. Depending on impact more or less rigorous assessment is performed.

For high impact functions it may be necessary to carry out a detailed assessment of hazards based upon the probability of occurrence and detectability.

For low impact, it is reasonable to forego formal risk assessment, applying good practice to provide adequate control. For medium impact, hazard scenarios should be considered, but hazards can be grouped generally, whereas for high impact functions more detailed and specific hazards should be considered.

Section 7.2 provides an example of how the impact of individual functions can be established. Section 7.4 provides examples of Medium and High impact functions. The risk assessment method described in Section 5.4 may be used to carry out the assessment, such as for the high impact functions shown on the figure.

Figure M3.10: Risk Assessment Based on Impact



7.4 Example 4 – Example of Medium and High Impact Functions

Table M3.4 shows five examples of system functions, and compares the generic assessments appropriate for medium impact functions, to the greater level of detail appropriate for high impact functions. In both cases, consequences related to corresponding risk scenarios should be assessed for Risk Priority.

Table M3.4: Examples of Risk Assessments for Medium and High Impact Functions

System	Function	Risk Scenarios for Medium Impact* Functions		Risk Scenarios for High Impact* Functions	
		Generic Hazard	Consequence	Specific Hazard	Consequence
Packaging Line	Thermal Seal	Control failure	Package or product damage	Control failure – high temperature	Package damage Product damage
				Control failure – Low temperature	Package not sealed
Liquid Filling Line	Filling	Power problem	Inaccurate vial fill	Voltage spike	Damage to electronics
				Brief voltage drop due to initiation of co-located equipment	No impact
				Prolonged voltage drop (e.g., brownouts)	No impact as long as uninterruptable power supply (UPS) maintains backup; inaccurate vial fill if UPS battery runs out
				Power loss <30 min	No impact (UPS assumes load)
				Power loss >30 min	If controlled shutdown not initiated, line crashes
IT Change Control Database	Change status of request	Move change status to "approved" fails	Change status stays "submitted"	Move change status to "approved" fails	Change not executed
					No documented approval for executed change
Toxicology Database	Audit Trail	Audit trail fails	Inadequate change documentation	Audit trail fails	Data changes inadequately attributed
					Old versions of data lost
Antivirus Software	Automated Virus Definition Update	Updates not downloaded	Exposure to potential virus attack	Updates not downloaded	Virus causes temporary loss of system
					Viruses cause loss of data

Table M3.4: Examples of Risk Assessments for Medium and High Impact Functions (continued)

System	Function	Risk Scenarios for Medium Impact* Functions		Risk Scenarios for High Impact* Functions	
		Generic Hazard	Consequence	Specific Hazard	Consequence
HPLC Control System	Solvent Pump Control	Control failure	Incorrect assay	Control failure – high flow	Incorrect assay result due to loss of peak resolution or misidentification of peaks
				Control failure – low flow	Incorrect assay result due to incorrect component peaks being assigned to reference standard or expected component peak windows

*Note that there is no implication that these functions should always be defined as high or medium impact; such an assignment must be made within the context of the business process. They are simply used as examples to illustrate the concept of generic versus specific hazard analysis and risk assessment.

7.5 Example 5 – Risk-Based Decisions During Test Planning

This example shows how the results of risk assessments may be used to decide on the appropriate level of testing.

The data input field should only accept values from 10.0 to 20.0. Appropriate challenges might be as shown in Table M3.5.

Table M3.5: Example on use of Risk Assessment Results

Function	Low Risk	Medium Risk	High Risk
Input Function with Acceptable Data Range of 10.0 – 20.0	Verify normal data is accepted	Boundary testing: 1 value below 10, 1 value in range, 1 value above 20	Boundary testing: 9.9, 10.0, 10.1, 19.9, 20.0, 20.1
		Null value challenge	Null value challenge
			Incorrect decimal precision
			Alpha character
Temperature Control for an Instrument or Vessel	Verify calibration procedures	Verify accurate calibration throughout operating range	Verify accurate calibration throughout operating range
		3-Point boundary testing for alarms	6-point boundary testing for alarms
			Challenge control precision against defined process parameters
Interactive Voice Response System	Verify that the system is connected via a toll-free number	Run test case to verify that an error message is returned if the subject is under 18 years old	Run test case to determine that system can track and trace availability of rescue drug kit for specific subjects
		Test date value entry and age calculation against local system date	

Categories of Software and Hardware

1 Introduction

This appendix describes how software and hardware components of a system may be analyzed and categorized. These software and hardware categories may then be used along with Risk Assessment and Supplier Assessment to determine a suitable life cycle strategy. Confirmation of the categories often forms part of the supplier assessment process.

The examples given in Section 4.2.6 of the Main Body show how the selection of appropriate life cycle activities can be based on the assessment of the system components.

Any examples of types of software and hardware given are purely for guidance, and are not intended to imply that all software or hardware of a particular type always fit into a particular category.

It should be noted that Categories 3 to 5 are effectively a continuum with no absolute boundaries, and that activities recommended for another category might be appropriate for a system or component that falls between categories.

Changes from the GAMP 4 approach to categories are described in Section 5 of this appendix.

2 Using the GAMP Categories

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

Most systems have components of varying complexity, such as an operating system, un-configured components, and configured or custom components. Effort should be concentrated as follows:

Custom > Configured > Non-Configured > Infrastructure

Categorization can help focus effort where risk is greatest.

There are two main ways to use the categories:

- Whole-system assessment
- Detailed component assessment

On a whole-system level, the category of the main component may be used to help define the approach to supplier assessment or the selection of life cycle deliverables. Combining categorization with an assessment of system impact can help to decide whether a site audit is required.

At a component level, the categories are useful when applied in conjunction with other risk management tools, and with consideration of complexity and size of system. Most computerized systems comprise multiple components, and categorization of such components may be used to scale specific life cycle activities.

For example, a chromatography management system may have PC-based data and control software that runs on an operating system and a database manager, plus firmware-based subsystems such as pump-controllers, autoinjectors, and column heaters. The latter components are much less complex than the data and control software, and it is reasonable to expend more effort on the PC-based application than on the other subsystems.

A programmable logic controller (PLC) or other controller may be an integrated part of process equipment, and verification of correct operation forms part of the overall verification of the integrated equipment. In such cases, detailed analysis of categories of individual components may not be required.

3 Categories of Software

3.1 Category 1 – Infrastructure Software

Infrastructure elements link together to form an integrated environment for running and supporting applications and services.

There are two types of software in this category:

- **Established or commercially available² layered software:** Applications are developed to run under the control of this kind of software. This includes operating systems, database managers, programming languages, middleware, ladder logic interpreters, statistical programming tools, and spreadsheet packages (but not applications developed using these packages. See Appendix S3).
- **Infrastructure software tools:** This includes such tools as network monitoring software, batch job scheduling tools, security software, anti-virus, and configuration management tools. Risk assessment should, however, be carried out on tools with potential high impact, such as for password management or security management, to determine whether additional controls are appropriate.

Layered software is not subject to specific functional verification although their features are functionally tested and challenged indirectly during testing of the application. The identity and version numbers of layered software and operating system should be documented, and verified during installation.

Infrastructure software tools are generally highly reliable, and significantly removed from any aspect of patient risk. All infrastructure software should be controlled and managed. See the *GAMP Good Practice Guide: IT Infrastructure Control and Compliance* for further guidance (Reference 34, Appendix G3).

3.2 Category 2 – This Category is no longer used in GAMP 5 (See Section 5 of this Appendix)

3.3 Category 3 – Non-Configured Products

This category includes off-the-shelf products used for business purposes. It includes both systems that cannot be configured to conform to business processes and systems that are configurable but for which only the default configuration is used. In both cases, configuration to run in the user's environment is possible and likely (e.g., for printer setup). Judgment based on risk and complexity should determine whether systems used with default configuration only are treated as a Category 3 or Category 4.

² Any use of the term commercial is not intended to discriminate against Free or Open Source software.

A simplified life cycle approach may be applied to Category 3 products, as shown Section 4.2.6 of the Main Body. Supplier assessment may not be necessary. The need for, and extent of, supplier assessment should be based on risk. User requirements are necessary and should focus on key aspects of use. Functional and design specifications are not expected from the user, although there should be sufficient specification to enable testing (typically covered by the User Requirements Specifications (URS) and other relevant documentation). Verification typically consists of a single test phase.

All changes to software should be controlled, including supplier-provided patches. Standard Operating Procedures (SOPs) should be established for system use and management, and training plans implemented.

Configuration management should be applied. For systems where the default configuration is used, configuration management demonstrates that the defaults are accurately selected.

3.4 Category 4 – Configured Products

Configurable software products provide standard interfaces and functions that enable configuration of user specific business processes. This typically involves configuring predefined software modules.

Much of the risk associated with the software is dependent upon how well the system is configured to meet the needs of user business processes. There may be some increased risk associated with new software and recent major upgrades.

A life cycle approach as shown in Section 4.2.6 of the Main Body is appropriate for configured products. Detailed URSs are necessary. The approach to assessment of the supplier and of the configurable product should be risk-based and documented (see Appendix M2).

While Functional Specifications (FSs) may not be owned by the user, there should be adequate specification available to ensure traceability and adequate test coverage. Verification should ensure that the software product meets the user requirements with particular focus on the configured business process. Custom modules should be handled as Category 5 components.

The approach should address the layers of software involved and their respective categories. The approach should reflect the outcome of the supplier assessment, GxP risk, size, and complexity. It should define strategies for the mitigation of any weaknesses identified in the supplier's development process.

Since each application of the software product is specific to the user process, support of such systems needs to be carefully managed. For example, when new versions of software products are introduced, serious problems can arise from the dependency of custom code on features of the software product which may have changed.

Custom software components such as macros developed with internal scripting language, written or modified to satisfy specific user business requirements, should be treated as Category 5.

In the absence of an adequate supplier Quality Management System (QMS), suppliers should be encouraged to develop such a QMS based on the principles in this Guide. Under such circumstances the software should be considered as Category 5. Regulated companies are, however, responsible for ensuring the quality of the software and hardware, and the fitness for purpose of the computerized system when used in the GxP environment.

3.5 Category 5 – Custom Applications

These systems or subsystems are developed to meet the specific needs of the regulated company. The risk inherent with custom software is high. The life cycle approach and scaling decisions should take into account this increased risk, because there is no user experience or system reliability information available.

The life cycle approach is similar to configured products, with the addition of design as shown in Section 4.2.6 of the Main Body. The approach to supplier assessment should be risk-based and documented. A Supplier Audit is usually required to confirm that an appropriate QMS is established to control development and ongoing support of the application. In the absence of an adequate QMS, suppliers may use this Guide to provide the foundation for managing application development and support.

The approach should address the layers of software involved and their respective categories. It should reflect the assessment of the supplier and any audit observations, GxP risk, size, and complexity. It should define strategies for the mitigation of any weaknesses identified in the supplier's development process.

3.6 Typical Examples and Approaches

Table M4.1 provides examples of each category and typical approaches to follow for each software category.

Table M4.1: Software Categories, Examples, and Typical Life Cycle Approach

Category	Description	Typical Examples	Typical Approach
1. Infrastructure Software	<ul style="list-style-type: none">Layered software (i.e., upon which applications are built)Software used to manage the operating environment	<ul style="list-style-type: none">Operating SystemsDatabase EnginesMiddlewareProgramming languagesStatistical packagesSpreadsheetsNetwork monitoring toolsScheduling toolsVersion control tools	<ul style="list-style-type: none">Record version number, verify correct installation by following approved installation proceduresSee the <i>GAMP Good Practice Guide: IT Infrastructure Control and Compliance</i>
3. Non-Configured	Run-time parameters may be entered and stored, but the software cannot be configured to suit the business process	<ul style="list-style-type: none">Firmware-based applicationsCOTS softwareInstruments (See the <i>GAMP Good Practice Guide: Validation of Laboratory Computerized Systems</i> for further guidance)	<ul style="list-style-type: none">Abbreviated life cycle approachURSRisk-based approach to supplier assessmentRecord version number, verify correct installationRisk-based tests against requirements as dictated by use (for simple systems regular calibration may substitute for testing)Procedures in place for maintaining compliance and fitness for intended use

Table M4-3.1: Software Categories, Examples, and Typical Life Cycle Approach (continued)

Category	Description	Typical Examples	Typical Approach
4. Configured	Software, often very complex, that can be configured by the user to meet the specific needs of the user's business process. Software code is not altered.	<ul style="list-style-type: none"> • LIMS • Data acquisition systems • SCADA • ERP • MRPII • Clinical Trial monitoring • DCS • ADR Reporting • CDS • EDMS • Building Management Systems • CRM • Spreadsheets • Simple Human Machine Interfaces (HMI) <p>Note: specific examples of the above system types may contain substantial custom elements</p>	<ul style="list-style-type: none"> • Life cycle approach • Risk-based approach to supplier assessment • Demonstrate supplier has adequate QMS • Some life cycle documentation retained only by supplier (e.g., Design Specifications) • Record version number, verify correct installation • Risk-based testing to demonstrate application works as designed in a test environment • Risk-based testing to demonstrate application works as designed within the business process • Procedures in place for maintaining compliance and fitness for intended use • Procedures in place for managing data
5. Custom	Software custom designed and coded to suit the business process.	<p>Varies, but includes:</p> <ul style="list-style-type: none"> • Internally and externally developed IT applications • Internally and externally developed process control applications • Custom ladder logic • Custom firmware • Spreadsheets (macro) 	<p>Same as for configurable, plus:</p> <ul style="list-style-type: none"> • More rigorous supplier assessment, with possible supplier audit • Possession of full life cycle documentation (FS, DS, structural testing, etc.) • Design and source code review

Note: An acronyms list is provided in Appendix G2.

4 Categories of Hardware

4.1 Hardware Category 1 – Standard Hardware Components

The majority of the hardware used by regulated companies will fall into this category.

Standard hardware components should be documented including manufacturer or supplier details, and version numbers. Correct installation and connection of components should be verified. The model, version number and, where available, serial number, of pre-assembled hardware should be recorded. Pre-assembled hardware does not have to be disassembled. In such cases the hardware details can be taken from the hardware's data sheet or other specification material. Configuration Management and Change Control apply.

4.2 Hardware Category 2 – Custom Built Hardware Components

These requirements are in addition to those of standard hardware components. Custom items of hardware should have a Design Specification (DS) and be subjected to acceptance testing. The approach to supplier assessment should be risk-based and documented. In most cases a Supplier Audit should be performed for custom hardware development. Assembled systems using custom hardware from different sources require verification confirming compatibility of interconnected hardware components. Any hardware configuration should be defined in the design documentation and verified. Configuration Management and Change Control apply.

5 Changes from GAMP 4

Readers familiar with previous versions of the GAMP Guide will note that the category definitions have changed. There are now only four software categories, 1, 3, 4, and 5.

The previous Category 1 Operating Systems is expanded to include Infrastructure Software, and now also includes such layered software components as database managers, middleware, and ladder logic interpreters. Also included are tools used to manage the infrastructure, such as network performance monitors, batch scheduling tools, etc.

Category 2 Firmware is no longer a separate category, since modern firmware can be so sophisticated that there is no longer any justification for differentiation. Firmware can fit into any of the categories depending on the nature of the embedded software. For example there could be non-configured firmware in a simple laboratory instrument or custom firmware in a novel Process Analytical Technology (PAT) system.

The previous Category 3 Standard Software has been renamed Non-Configured Product and includes many examples of firmware. Non-Configured in this sense refers to configuration to meet the needs of a business process; run-time parameters can still be configured. Off-the-shelf software has grown in sophistication to the point where some examples are configurable to meet the business process, and hence could be considered Category 4. A simplified approach (Category 3) is allowed, however, if a user chooses not to configure a simple configurable product, and applies the default configuration.

The remaining categories are essentially unchanged from previous usage.

Note that a refinement of the GAMP categories for laboratory instruments appears in the *GAMP Good Practice Guide: Validation of Laboratory Computerized Systems* (Reference 34, Appendix G3). That approach describes further sub-division of categories for such systems and equipment, and is specifically tailored for the laboratory environment.

Design Review and Traceability

1 Introduction

This appendix covers the design review process and requirements traceability for computerized systems.

Defects should be identified and corrected at the earliest opportunity in the life cycle. Design reviews and traceability assist with assuring that computerized systems are fit for intended use and also with keeping the overall cost of projects down, through the early identification of defects and resolution of problems.

Design review and traceability can help assure that:

- all requirements have been addressed
- the functionality is appropriate, consistent, and meets pre-defined standards
- the system is appropriately tested

2 Scope

This appendix is intended to cover GxP regulated systems, but the methods are appropriate to all system types. Design review and traceability also may cover operational, commercial, safety, and environmental considerations.

3 Design Review

Design Reviews evaluate deliverables against standards and requirements, identify issues, and propose required corrective actions. They are planned and systematic reviews of specifications, design, and development performed at appropriate points throughout the life cycle of the system. They are an important part of the verification process.

Design Review should be performed by appropriate Subject Matter Experts (SMEs). The individuals performing the review should be identified.

The rigor of the design review process and the extent of documentation should be based on risk, complexity, and novelty.

Aspects that should be considered when planning Design Reviews include:

- the scope and objectives of the review
- what method or process will be followed
- who will be involved
- what the outputs will be

For non-configured products (GAMP Category 3) a design review by the regulated company typically is not required.

For systems based on configured product, a significant part of the Design Review activities should have been performed by the supplier during development of the product. This should be verified during supplier assessment. User Design Review activities should focus on the configuration activities.

For custom applications, Design Reviews typically are conducted at each level of detail of specification, i.e., at Functional Specification (FS) and at each level of Design Specifications.

4 Traceability

4.1 Introduction

Traceability establishes the relationship between two or more products of the development process.

Traceability ensures that:

- requirements are met and can be traced to the appropriate configuration or design elements
- requirements are verified, and can be traced to test or verification activity that shows that requirement has been met

Accurate traceability can also provide benefit by:

- enabling more effective risk management and design review processes
- judging potential impact of a proposed change
- facilitating risk assessment for a proposed change
- identifying scope of regression testing for changes
- enabling fast and accurate responses during an inspection or audit

This section describes methods of achieving traceability. The approach applied should be selected based on the level of GxP risk, complexity, and novelty.

4.2 Principles

A means of linking relevant specifications to testing should be established and maintained. It should also be possible to trace from testing back to the relevant specifications. Traceability provides a method to ensure that all applicable elements of specification, including requirements, have been verified. It also enables easier documentation identification during regulatory inspection. Accurate traceability depends upon the completeness and accuracy of the specifications.

The rigor of traceability activities and the extent of documentation should be based on risk, complexity, and novelty, for example a non-configured product may require traceability only between requirements and testing.

For more complex systems, the relationship between user requirement specifications (URSs), FSs, configuration specifications, design specifications, and verification may not be simple, e.g.:

- multiple requirements can be covered by a single design specification and verified by a single test

- multiple design specifications may be linked to a single requirement
- multiple tests can be required to address one requirement or one design specification

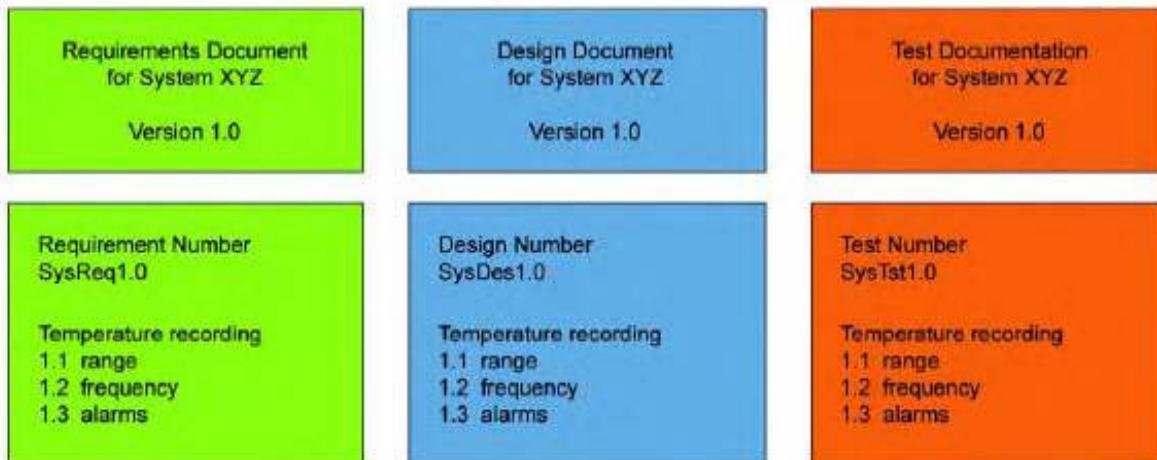
The documentation or process used to achieve traceability should be documented and approved during the planning stage, and should be an integrated part of the complete life cycle.

4.3 Methods of Achieving Traceability

Traceability may be achieved in a number of ways, including a Requirements Traceability Matrix (RTM), automated software tools, spreadsheets, or embedding references directly within documents. An RTM may be generated as a separate deliverable or as part of an existing deliverable, such as the requirement document.

Traceability for simpler systems can be achieved through common or consistent numbering of requirements, designs, and testing documentation, rather than a separate matrix; see Figure M5.1.

Figure M5.1: Example of Embedded Traceability



The numbering for temperature recording is the same in the requirements, design, and test documentation; thereby enabling traceability without creating a separate traceability matrix. This method is considered appropriate for smaller system in low risk situations.

For non-configured products, traceability between user requirements and verification may be sufficient.

For configured products, the Design column may be replaced with a link to configuration items, providing traceability between user requirements, configuration, and verification.

For custom applications, traceability should be provided from requirements through each level of specification to the appropriate verification. Figure M5.2 provides a simple example RTM for a custom application.

Figure M5.2: Custom Application Example RTM

Requirements	Design		Testing
	Functional Specification	Design Specification	
U1.1.1	F2.4.1	D2.5	T1.1
U1.1.2	F2.4.5	D2.4	T1.2
U1.2.1	F3.1	D1.1	T2.3.1
U1.2.2	F3.2	D1.2	T8.1
U1.2.3	F3.3	D3.3	T8.2

Each reference within the matrix, e.g., U1.1.2, F3.1, D1.2, T8.2, could be a reference to a section or subsection within the relevant document, or to a totally separate document.

In practice there often is not a simple one-to-one relationship from the requirements through the different design documents. One function may fulfill different requirements or one requirement may require different design elements.

4.4 Additional Options for the Requirements Traceability Matrix

A requirements traceability matrix may be enhanced by adding more information, such as:

1. A column to include a brief written description of each requirement, which may assist verification that matrix contents are referenced correctly.
2. A column to include change control numbers to enable tracking the system history and change impact. A reference to other documentation and processes which impact the system, such as deviations or Standard Operating Procedure (SOP) changes may be beneficial.
3. A column to indicate the criticality of the requirements to assist levels of testing applied to any given requirement. High criticality requirements may have more detailed testing applied and may, therefore, reference multiple tests, whereas low criticality requirements may have a reference to a single test.
4. A column to indicate where a requirement has been met by a procedure along with the reference to the procedure and version number. In this case design column will be blank, but the testing may not, as the use of the procedure may be tested at the requirements testing level.
5. The test column may be expanded to indicate:
 - at what level the testing occurs, (e.g., unit, integration, or acceptance)
 - when (e.g., development, test, or operational)
 - where the testing occurs (e.g., global or local)

In this case the level of effort in testing should relate to the criticality of the requirement and the level of acceptable risk. For example, a high-risk requirement may be tested many times and at many levels, but reduced testing may be applied to lower risk elements.

6. A column linking a test to a maintenance or calibration record for the instrument required for a test and requirement. For process automation it may be advantageous to link documents such as installation records, loop checks and tuning, and cable integrity checks, thus enabling traceability from the calibration certification on an instrument all the way through to the use of that measurement in the business process and system testing.

Any such additions to the traceability matrix may, however, make it more difficult to navigate and maintain.

For large projects other tools, such as a document management system, having the capability to maintain the links between documents (both in the document management system and reference to documents generated and stored outside) may be used.

4.5 Practical Issues to Consider

The level of detail required for traceability can be a difficult balance to strike. The following considerations seek to help in balancing usefulness, complexity, and maintainability.

1. The strategy for traceability should be established during planning. Traceability should be considered during development of user requirements.
2. Level of traceability could stop with a reference to supplier documentation, if documentation needs are met and supported by supplier assessment.
3. The supplier should have their own traceability for the documentation and testing under their control. This should be verified during Supplier Assessments where this is appropriate.
4. Requirements need not trace to technical controls in all circumstances. Requirements can trace to procedural controls in which case a cross-reference to identified SOPs is appropriate.
5. For simple systems a RTM is not recommended as sufficient traceability can be incorporated within document cross-references.
6. For global systems early and careful planning for traceability is required since the control and tracking of local and global requirements should be resolved.

Supplier Quality and Project Planning

1 Introduction

This appendix gives high level guidance for suppliers on Quality and Project Planning for individual projects. The Quality and Project Plan defines how the supplier will fulfill the quality requirements of the project, and how the supplier Quality Management System (QMS) will be applied. The Quality and Project Plan defines the activities to be performed, their timing, who will perform them, the control mechanisms to be used, and the deliverable items.

It provides example contents of Quality and Project Plans, and additional guidance on issues to consider when planning projects that involve interfaces between systems.

This appendix is not intended to give detailed guidance on project management, which is outside the scope of this document. Note that the ISPE Project Management Community of Practice is a forum for professionals creating a body of knowledge on project management (see www.ispe.org).

2 Scope

This appendix may be used as the basis for Quality and Project Plans for supplier development projects. It also is a suitable starting point for the production of a product Quality Plan, for developers of base software products.

The Project and Quality Plan may relate to development of a custom or configured system for a specific customer, or the same principles can be applied to the supplier developing or enhancing their base products which are subsequently configured (by the Supplier or others) for use in the end-user environment.

The guidance also covers the aspects of reporting against Quality and Projects Plans in order to verify activities have been completed to plan, and to highlight and assess any deviations.

Quality and Project Plans are not required for all systems. The information contained in them may be covered in other existing plans such as Validation Plans or Verification Plans. Terminology used may also differ from case to case.

3 Contents of the Quality and Project Plan

This section lists topics that may be included in the Quality and Project Plan; not all sections or sub-sections may be relevant. The guidance provided is intended to be neither prescriptive nor exhaustive.

The Quality and Project Plan may be a contractual document and, in such cases, typically is approved by appropriately authorized representatives of the supplier and customer.

3.1 Introduction

Information provided should include:

- who produced the document, under which authority, and for what purpose

- the contractual status of the document
- relationship with, and reference to, relevant policies, procedures, standards and guidelines (such as GAMP)
- relationship with, and reference to, other plans such as Validation Plan or Verification Plan

3.2 Overview

The project and technologies used should be briefly described.

3.3 Quality Plan

Quality related verification activities, responsibilities, and procedures to be followed, should be described.

3.3.1 *User Quality Requirements*

Relevant regulated company quality requirements should be listed. User quality requirements take precedence over the supplier's QMS.

3.3.2 *Supplier Quality System*

A description of how the regulated company quality requirements are to be met by the supplier should be provided.

This includes defining which quality activities are to be handled under the supplier QMS and which under the customer QMS.

The activities to be undertaken, the procedures to be followed, and responsibilities should be defined. Activities that should be considered are described in Table M6.1.

Table M6.1: Activities to be Considered

Activity	Typical Considerations
Specification	Describe input documents, e.g., user requirements, marketing, regulatory, enhancements etc. Single or multiple documents.
Development Methods or Models to be used	E.g., traditional top-down functional decomposition, waterfall, spiral, Rapid Application Development (RAD), rapid prototyping, other iterative approach
Risk Management	Risk management approach to be adopted – consider aspects such as technical risks, resources. How to ensure requirements identified by the customer as presenting high risks (to patient safety, product quality and data integrity) will be specifically addressed.
Traceability and Design Reviews	What tools will be used to provide traceability of requirements through the life cycle and across documentation, how will these be maintained? What areas will be subject to design reviews and how will this process be controlled?
Programming standards and Code Reviews	What technologies are used – where will code/configuration need to be subject to review – will this be on a sample basis or will all code be reviewed?
Testing	How will the test stages be defined and planned, how will testing be related to risk management? At which stage will testing transition from informal to formal, what test tools will be used, and how will the test methodology be determined (e.g., regression, boundary and stress testing). How will test (specification) approval and review be conducted and recorded?
Installation	How will installation be controlled, what environments will be used (and controlled) through the project (e.g., sandpit, development, pre-production etc.)?
Data Migration	What strategy will be used, how will this be verified (sample or full testing)?
Acceptance (both supplier factory and user site acceptance testing)	How will the testing be planned, specified, and executed. What level of customer involvement/witnessing will be necessary? How will the testing be related to risk assessment?
Project Audits	Are periodic projects reviews to be conducted, if so at what stages and by whom?
Reporting	How will progress against the overall Project and Quality Plan be reported? How will any non-conformances with the Plans be assessed and addressed?
Document Management	How will documentation be controlled – at what stage do documents enter formal control? Will documents be stored electronically or on paper – are electronic approvals/signatures to be used, and if so how will this be managed where customer approvals are required?
Change Control	When will formal change control apply? Consider the transition from the supplier change control system to the end user change control system. Consider that once the system enters formal testing it is expected that formal change control is in place.
Configuration Management	How will Configuration Management be applied? Tools and techniques used?
Issue Management	How will issues be reported, assessed and addressed – the method may change (and become more formal) as the system progresses into formal testing stages.
Project Training	What training requirements are there for development staff (both for the supplier and user) – are any new technologies being used?
Product Release and Handover to support organization	How will product release be managed and documented? How will handover be managed? What format will the material be in – paper, electronic etc. How will competency of those to whom the system is being handed-over be assessed?

3.4 Project Plan

If a Project Plan Section is included, the following typical contents should be considered. Other project management plans, tools, techniques, and methods may be used and referenced.

3.4.1 *Project Organization*

Typically this is an organization chart that shows:

- The supplier project team showing personnel and job titles. The supplier contact for the purposes of customer complaints should also be indicated.
- the interface between the supplier project team and the supplier's Quality Assurance function within the organization
- nominated customer contacts

3.4.2 *Deliverable Items*

Definition of deliverable items, how they are to be identified, and in what form they are to be supplied, e.g., which format and media.

3.4.3 *Activities*

Typically covering:

- Project milestones. These are pre-determined, clearly identifiable project events
- Project activities (e.g., Design Reviews or other reviews)
- personnel allocated to activities
- planned start date and end date of each activity

Activities are subject to regular review and update and may be included as an appendix to the main plan or be a separately controlled document.

4 Additional Guidance on Interfaces

When several suppliers are involved in delivering interfacing systems, or a single supplier delivers a system with complex interfaces the definition of, and responsibilities associated with, these interfaces should be clear.

This section gives guidance on the co-ordination and management of interfaces on larger projects.

Steps to be followed should include:

- define interfaces and allocate responsibilities
- produce interface specifications
- produce interface test specifications

- perform testing and produce the review reports

These steps may be performed by either the regulated company or suppliers, but responsibilities for activities should be defined in the Quality and Project Plan, or in a separate document referred to from that plan.

Due to the diversity of systems and suppliers that may be involved, no specific formats for specifications, test specifications, and reports are defined in this appendix. Other appendices covering functional and design specifications and testing documentation should be used as guidance. The following should be addressed:

- Who produces, reviews, and approves the specifications of the interfaces?
- Is a simulator needed to test one part of the interface? If so, who is responsible for developing this?
- Who produces, reviews, and approves the test specifications for the interface?
- Who is responsible for testing the interface? Is supplier factory testing and user site testing required?
- Who is responsible for defining and providing test data?
- Who produces, reviews, and approves any test reports associated with the interface?

It may be useful to produce a matrix of interfaces, showing how data is exchanged, provided, or used.

Validation Reporting

1 Introduction

This appendix describes the computerized system validation reporting process. It covers the activities involved, the roles and responsibilities, and identifies where the process fits within a typical computerized system life cycle.

Accurate and informative planning and reporting are key elements of effective and successful governance, and the Validation Report is often the first document related to a system that is examined during a regulatory inspection.

This appendix should be read in conjunction with Appendix M1, which discusses computerized system validation planning.

2 Scope

This appendix gives guidance on the reporting of the outcome of validation activities relating to the implementation of either a specific computerized system, or a group of related systems in an area or site.

3 Roles and Responsibilities

Specific roles and responsibilities will vary depending upon the scope and scale of the project. These roles should be defined in the appropriate section of the corresponding plan and will cover who is responsible for the creation, the review, and the approval of the computerized system validation report(s). Any changes in roles and responsibilities that were made during project should be noted in the report.

The Quality Unit is responsible for ensuring that the generated document(s) comply with requirements specified in the corresponding plan, are produced in line with company policies and procedures, and meet the appropriate regulatory requirements.

4 Reporting Process

Where required by a computerized system validation plan, a validation report should be produced, focusing on aspects related to patient safety, product quality, and data integrity. It should summarize the activities performed, any deviations from the validation plan, any outstanding and corrective actions, and a statement of fitness for intended use of the system.

The level of detail in the report should reflect the risk, complexity, and novelty of the system. For simple or low risk systems a separate document may not be needed; applicable aspects may be covered by another document.

The structure of the report should mirror the structure of the corresponding plan, although there are some components of the plan (e.g., organizational structure) that typically will not have a corresponding section in the report unless a significant change has been made.

The report should be approved, as a minimum, by the process owner and the Quality Unit. It also may be appropriate for other approvers of the corresponding plan to approve the report, such as the system owner.

It is common to produce one final report. There may, however, be other reports that either feed into this document or are created after it and which supplement it.

For example, for larger systems it may be advantageous to issue sub-reports to cover phase completion (such as specific testing or verification phases) and there may be an interim report to release the system. In general, each plan should be addressed in a corresponding report and the scope of the report should correspond to the scope defined in the related plan.

4.1 Contents of the Computerized System Validation Report

This section lists topics that may be included in the computerized system validation report; not all sections or sub-sections may be relevant. The guidance provided is intended to be neither prescriptive nor exhaustive.

4.1.1 *Introduction and Scope*

The introduction should reflect the corresponding plan, and highlight any differences that have arisen since the plan was issued. It should contain the following information:

- purpose and scope of the report
- who created the report, and under what authority
- summary of approach adopted
- cross reference to controlling plans, policies, or procedures

4.1.2 *Scope Changes*

It may be necessary to modify the original approach; the report should highlight and justify such scope changes.

In large complex projects the recording of such events may be centralized as part of a formal tracking system, e.g., a Risks, Actions, Issues, Decisions (RAID) log. In such cases this section of the report may reference such sources of information.

4.1.3 *Supplier Assessment*

Supplier assessment activities should be summarized, or a reference made to other sources of information, such as a Supplier Assessment or Audit Report.

If supplier documentation was leveraged, there should be discussion of the measures taken to ensure its adequacy.

Information already available in other documents should not be repeated.

Contents of supplier audit reports should not be included.

4.1.4 *Summary of Activities*

The summary should refer to existing documentation, e.g., verification or test reports, and information should not be duplicated.

This section may include sub-sections relevant to each phase.

4.1.5 *Summary of Deliverables*

The report should verify that all of the deliverables noted in the corresponding plan are completed and approved. This includes system development documentation and Standard Operating Procedures (SOPs) required for operational support.

4.1.6 *Summary of Deviations and Corrective Actions*

The report should describe any activities and results that did not conform to the expectations specified in the plan, and explain the impact including corrective actions. Outstanding corrective actions should be highlighted and appropriate next steps identified or referenced.

4.1.7 *Statement of Fitness for Intended Use*

There should be a clear statement on the status of the system and whether it is fit for intended use, bearing in mind any outstanding deviations or corrective actions.

4.1.8 *Training*

The report should verify that personnel involved with new processes, equipment, or systems have been trained and that this training is documented.

4.1.9 *Maintaining Compliance and Fitness for Intended Use*

The report should outline how the compliant status of the system will be maintained. This may be efficiently achieved by referring to relevant policies and procedures or other Quality Management System (QMS) elements. See the Operational Appendices for further details.

4.1.10 *Glossary*

Definitions of any terms that may be unfamiliar to the readership of the document should be included.

4.1.11 *Appendices*

There may be a requirement for appendices, depending on the purpose, size, and complexity of the report, and the corporate styles and policies adopted for reporting. These may include references to project specific documentation and references to other relevant documentation such as policies and procedures, guidelines, and standards.

Project Change and Configuration Management

1 Introduction

This appendix covers change and configuration management of computerized systems during the development phases prior to acceptance and handover to operational use.

Any controlled item that undergoes review, approval, or test should be governed by appropriate configuration management and every controlled item should be subject to appropriate change management.

Change management should be applied to each controlled item upon its first formal approval to avoid unintentional or unauthorized change. Different controlled items may require different levels of formality and rigor. The project change management approach should be documented. The project manager and the user should agree the level of user involvement.

Project change management processes typically are simpler than those for operational GxP systems, due to fewer people involved, faster communication, and lower risk.

The point of transfer from project to operational change management should be clearly defined before handover to operational use.

See Appendix O6 for further details on operational change and configuration management.

2 Scope

This appendix applies to changes to controlled items such as documentation, application software, operating software, firmware, hardware, and system, master, and configuration data within the scope of the specified computerized system, during its project phase.

This appendix is not aimed at changes to project scope, which typically are initiated and managed by change procedures forming part of project management processes, and which may have significant financial implications. This appendix is aimed at changes to controlled items which may be triggered by such project scope changes amongst other reasons.

3 Guidelines

3.1 Configuration Management

All components of a computerized system, and changes to them, should be controlled. The exact hardware and software configuration of the system should be documented throughout the life of the system. The level of formality is greater for an operational system than for a system early in its development, but the principles that apply are the same.

Configuration Management should begin as early as possible during development. The more formality is introduced during development, the easier it is to document the baseline configuration for operational Configuration Management.

Configuration Management consists of:

- Configuration Identification (*WHAT* to keep under control)
- Configuration Control (*HOW* to perform the control)
- Configuration Status Accounting (*HOW* to document the control)
- Configuration Evaluation (*HOW* to verify that control)

Configuration Management activities, responsibilities, procedures, and schedules should be clearly defined. For a large or complex project or product, a separate Configuration Management Plan should be produced.

The use of automated Configuration Management tools can bring significant advantages, and should be considered. The selection, verification, and use of such tools should be documented and based on risk, complexity, and novelty.

See Appendix O6 for further details on Configuration Management.

3.2 Change Management

Project changes should be controlled and documented. As the project advances the formality of the change management process generally increases. This progresses from informal project team meetings and discussions, through formally recorded project meetings, to formal Change management requests. The increase of rigor and formality depends on the impact on both the preceding and subsequent deliverables in the documentation set, as these are developed and linked to each other. Some controlled items may require different levels of formality and rigor. Projects should define their approach to project change management during project planning.

All deliverables should be identified so that the controlled items subject to change management may be defined. These may include:

- Planning Documents
- User Requirements Specifications (URSs)
- Functional Specifications(FSs)
- Design Specifications
- Quality Review Documents
- Test specifications including acceptance criteria
- Testing results
- Reports
- Hardware (e.g., Programmable Logic Controllers (PLCs), Personal Computers (PCs), minicomputers, servers, communication interfaces, printers)
- Developed software code (e.g., PLC code, source code, executables, data files)
- Third party software (e.g., operating systems, firmware, library files, configurable products, drivers, compilers). This includes software delivered with the system and customer supplied software items.

- Configuration files (for configurable products, alarm and process setpoints, etc.)
- Manuals (e.g., user manuals, system manuals)

3.2.1 Changes during Development and Prototyping

Formal control should not be introduced too early during development in order to minimize non-productive work during what are naturally iterative or evolutionary processes. Documents should be held in a draft status during development without formal change control. Version control should track the current working draft and ensure that documents are not unintentionally modified simultaneously by different project team members.

At the end of the development phase document review and approval should act as the formal verification that the document content is complete, accurate, and fit for intended use.

Changes made during approved prototyping work are exempt and should be subject to these controls only when they become documented design proposals.

3.2.2 Changes to Code

Changes to code should be managed effectively to avoid unintended or unauthorized changes. The best solution is the use of an automated code management tool. These tools use a check-in and check-out process to protect code so that two developers cannot be simultaneously working on the same file, which could lead to errors and wasted effort. They also make it less likely that a developer will edit an old file, leading to loss of intervening developments or the possible re-introduction of corrected defects (see Appendix D4 for further details).

3.2.3 Key Change Management Steps

3.2.3.1 Raising a Change

Any member of the project should be able to raise a change in accordance with the project change management procedure. Each change should be uniquely identified and indexed.

3.2.3.2 Change Review and Authorization

Each project should have a designated project manager responsible for ensuring that all changes to the system are implemented in a controlled manner. The project manager may delegate this responsibility.

Each change raised should be reviewed. Based on a risk assessment there should be a decision to accept or reject the change. If accepted, the activities required to specify, carry out, and verify the change should be defined, including:

- the scope of the change, and which controlled items are affected, including documentation
- the impact of the proposed change and the need for further risk assessments
- what verification is required
- the risks associated with making the change, and any back out plans if the change fails at implementation

The review, risk assessment, the decision to proceed or the decision to reject with reasons, and activities required should be recorded and retained as part of the project documentation.

The authority and responsibility for accepting and rejecting changes should be clearly defined. Controlled items that have been approved by the regulated company (e.g., User Requirements Specifications (URS), contractual documents, tested and accepted software) should be changed only after prior approval of the change.

If more than one controlled item is to be changed then each change should be tracked to completion. A Change Plan may be required for complex activities and resources.

3.2.3.3 Change Completion and Approval

When the change has been implemented, documentation revised, and appropriate verification performed, the change should be approved by the project manager or nominated representative and closed.

Example forms to assist with the process of managing a change are supplied separately.

Document Management

1 Introduction

This appendix covers the areas to manage during the preparation, review, approval, issue, change, withdrawal, and storage of documents.

2 Scope

This appendix is applicable to all system life cycle documentation. The guideline principles apply to documentation both in paper and electronic formats.

It describes an approach applicable to large projects in a GxP environment. It is not intended to be prescriptive. Simpler projects may adopt less formal methods. Suppliers may choose to adopt other approaches.

3 Guidelines

A procedure should be established for management of documentation, covering:

- production
- review
- approval
- issue
- change
- withdrawal
- storage

Where documentation is produced by a supplier, consideration should be given at the planning stage of projects to agree document standards and ensure that regulated company and supplier expectations are aligned. The regulated company may assess the supplier approach to document management as part of the supplier assessment processes.

Documentation should be assessed for suitability, accuracy, and completeness. There should be flexibility regarding acceptable format, structure, and documentation practices.

Example forms to assist with Document Management are supplied separately.

3.1 Document Production

Documentation standards should be agreed, covering document layout, style, and reference numbering. Documents should be produced in accordance with these standards.

Documents should be under version control and in draft form prior to formal issue. Draft and approved versions should be clearly distinguished, e.g., by their version identifier.

The document normally is the author's responsibility prior to review.

A Document Index should be maintained, showing the status of each document. If formal configuration management is applied, then the Configuration Item List will provide this information. A Document History also should be maintained for each document or maintained within the document itself. The use of the document history should be defined, e.g., whether the history of an approved document should list only the approved versions.

3.2 Document Review

Document reviews should be carried out prior to formal issue of a document. Independent review by a Subject Matter Expert (SME) (i.e., not solely by the author) is recommended.

The review can take a number of forms, ranging from circulation of the document and collection of comments through to formal review meetings. Copies of the document under review should be circulated in good time.

Where formal review meetings are arranged, each section of the document should be covered and minutes taken.

Actions arising from the document review should be resolved prior to approval and issue. Responsibility for this should be defined, and will normally rest with the author. Queries or disputes over required changes should be resolved with the review team. Once the agreed changes have been incorporated the document is ready for approval. Reviewers do not necessarily approve the document.

Review Reports, if used, should be logged and indexed. Individual actions noted on the Review Reports should be logged and progressed through to closure.

3.3 Document Approval

The reason for each approval signature should be defined and documented, e.g., technical approval. Approval signatories should be identified by title in each document. Approvals should be dated. Unnecessary approvals should be avoided since this can cause significant delays.

The Document Index and Document History should be updated to indicate the new document status.

Subsequent changes to the document should be carried out under the applicable Change Control procedure.

3.4 Document Issue

The Document Index should be updated to indicate the document is being issued. Superseded versions of the document should be removed from use and clearly marked as such.

The procedure for managing controlled copies, if required, should be documented. Where a system of controlled copies is in operation, uncontrolled copies should be clearly identifiable.

3.5 Document Changes

Modifications to approved documents should be progressed in a controlled manner. For example, the document may be reset to the next draft version, updates made and the document reviewed, approved, and issued in accordance with defined procedures.

During periods where documents may undergo significant revisions, techniques such as "redlining" (i.e., clearly annotating the master paper document with handwritten updates) are acceptable as long as this is clearly controlled, and there is a mechanism for ensuring at agreed milestone points that such updates will be fully incorporated (and review/approved) into the document.

The Document Index and Document History should be updated as part of this process; the document history may be incorporated within the document itself or held as a separate document.

Modifications to approved documents should be reviewed and approved by the same functions or organizations that performed the original review and approval, unless specifically designated otherwise.

3.6 Document Withdrawal

There should be a defined procedure for withdrawal of approved documentation, which would normally be handled through Change Control.

The Document Index and Document History should be updated to indicate the document is being withdrawn. Any controlled copy holders should be notified of the withdrawal and those copies removed from circulation. If required to be retained, the withdrawn document should be stored in a manner secure from use and its status should be clearly identified.

3.7 Document Records and Storage

Documentation and associated information should be stored safely and securely (whether by paper based or electronic means), and according to defined procedures. They should be protected against accidental and malicious damage, and should be retrievable throughout the defined retention period. Safeguards should prevent the unintended use of unapproved, superseded, and withdrawn documents.

System Retirement

1 Introduction

This appendix provides guidance on planning the orderly retirement of computerized systems.

This appendix assumes that the regulated company has already made a decision to retire a system. This appendix also assumes that the systems to be retired are compliant with applicable regulations, e.g., due to effective change control and periodic review processes.

2 Scope

This appendix covers retirement planning for all GxP regulated computerized systems. The guidance focuses on the controlling computer system and associated data rather than associated controlled equipment.

This appendix gives comprehensive guidance on all aspects of system retirement planning. Not all aspects will be relevant to all systems. The extent of planning and other activities will depend on the GxP risk, size and complexity of the system.

3 System Retirement Planning

3.1 General Guidelines

The system retirement process should be documented in a system retirement plan, which typically should receive input from functions, such as process owner, Quality Unit, system owner, and IT.

Inputs to the planning process may include:

- record retention and destruction requirements for historic data or records
- identification of the current software and hardware configuration as well as interfaced systems, equipment or instruments
- identification of any external systems that rely on data or records from the system

The extent and rigor of planning should be based on the system impact and risks associated with loss of data.

The System Retirement Plan typically should be approved by the process owner and Quality Unit, and others as required such as the system owner.

3.2 Contents of the System Retirement Plan

The System Retirement Plan should describe the approach to be undertaken, including:

- introduction

- roles and responsibilities
- overview and implications
- business process description
- retirement approach
- data and record migration, archiving and destruction
- verification approach
- ending system maintenance and support
- change management
- schedule
- retirement execution
- system documentation

This appendix provides further detail on each of these topics; not all sections may be relevant. The guidance provided is intended to be neither prescriptive nor exhaustive.

3.2.1 *Introduction*

The introduction should include:

- Who produced the document, under which authority, and for what purpose
- Relationship with, and reference to, relevant policies, procedures, standards and guidelines (such as GAMP)
- Relationship with, and reference to, other documents.

3.2.2 *Roles and Responsibilities*

The roles and responsibilities associated with the retirement process should be documented in the plan, and should cover the process owner, Quality Unit, system owner, the retirement team and its members, and any other contributing parties as appropriate.

3.2.3 *Overview and Implications*

Consideration should be given to the effect of system retirement on aspects such as:

- Strategy – document the impact on the overall technology strategy and initiate any updates to documentation or other necessary actions
- Process – describe the impact on the support of the business process going forward
- Technology – The scope and boundaries of the system to be retired should be determined and documented, as well as the rationale and justification for the retirement. Identify other systems, instruments, or equipment that interface with the retiring system. Data or sources of information may be in place between various systems. Identify infrastructure components (networking, etc.) that will need to be decoupled from the system.

- Personnel – describe the impact on the user base

3.2.4 Business Process Description

The pre-retirement business process should be documented and understood from the perspectives of the process, user base, and data/records. This helps to ensure that all business process impacts are identified and all angles of support or automation of the process are translated into the post-retirement scenario. The to-be scenario also should be documented and understood, especially regarding changes to business processes and/or user base, and the location of, and effect on, data/records.

3.2.5 Retirement Approach

A decision on whether the system will be replaced should be documented. If it is to be replaced, retirement planning should be referenced and synchronized with implementation planning for the replacement system. The approach to interface decoupling, infrastructure disconnection, ending or transition of technical support, and any assumptions, exclusions, limitations or dependencies, should be documented.

System retirement is a formal system life cycle phase, and should be treated as such by identifying the required inputs, outputs, standards, activities and deliverables.

3.2.6 Data and Record Migration, Archiving and Destruction

The plan should identify which data should be migrated, archived, or destroyed, and the associated approval process.

The approach to data migration and archiving should be determined based on the anticipated frequency of access, the need for re-processability, and the record risk level and media robustness. Controls should be established to ensure that records and data remain secure, complete, and accurate, and that signature/record linking is preserved where applicable.

The approach should take into consideration:

- If data is to be retained, it should be backed up and stored, per data retention schedules and company procedures.
- Before the data is moved or archived from the system, the appropriate data retrieval procedures should be available and tested.
- Archived data media should be stored and maintained, per the manufacturer recommendations and under the required environmental conditions.
- If data and records are to be migrated to a replacement system, the migration should be planned, conducted, and verified in such a manner as to ensure data integrity. The migration procedures should be tested or confirmed before the data is completely transferred out of the system.
- For any data migration or data conversion requirements, the methods to be used for migration/conversion and verification of the data records should be defined. This may include piloting work to be done before the actual migration takes place or a requirement for temporary parallel operation of both new and existing systems.
- If data is to be moved to a replacement system, the test strategy for verifying the migration should be defined. If an automated migration or conversion tool is to be used, the approach to ensure its fitness for intended use should be documented.

See Appendix D7 for further details on data migration.

For further information on the compliant handling of electronic records during data migration, archival, and retrieval, refer to:

- *GAMP Good Practice Guide: A Risk-Based Approach to Electronic Records and Electronic Signatures*, Appendix 3 (Reference 34, Appendix G3)
- *GAMP Good Practice Guide: Electronic Data Archiving* (Reference 34, Appendix G3)

3.2.7 Verification Approach

Verification documentation needed as part of the system retirement process should be identified.

3.2.8 System Maintenance and Support Discontinuance

The required actions associated with the modification or ending of internal and external support agreements, operations, backup and restore, disaster recovery and business continuity plans, technical support, security and user administration, and configuration management programs, should be planned and documented.

The retired system should also be removed from any inventory lists.

3.2.9 Change Management

Formal change management procedures should be followed for the retirement of a computerized system to ensure the retirement process is controlled and managed using established procedures for assessing change impacts.

Changes resulting from the system retirement should also be addressed, such as changes in support roles (technical support, super-users, etc.) and the associated training.

The approach to communicating the impact of the system retirement on affected stakeholders should be documented.

3.2.10 Schedule

The individual retirement tasks should be documented, along with who is responsible, the associated due dates, and any task dependencies. Critical milestones and checkpoints also should be included in the schedule.

Separate project schedules may be more efficient and effective than including this information directly in the plan.

3.2.11 Retirement Execution

The timing of the retirement execution should be carefully considered. For example, this may include cutover to a replacement system (which could be phased, in parallel, or a clean cutover.)

Business continuity plans should be in place in case any problems arise during the retirement or migration work. Additionally, a back-out plan is suggested, and should include detailed steps or references to configuration and reinstallation procedures in order to make the retired system operational again, if deemed necessary.

Any relevant documentation should also be defined.

3.2.12 System Documentation and Software

System documentation and software including source code (life cycle documentation, validation documentation, change history, system related standard operating procedures and other system documents) should be defined. Documentation to be retained should have a responsible owner and designated, secure location. Affected

inventories, procedures, or other documentation should be updated in a timely manner.

Decisions regarding whether to retain specific documents and software should be based on their potential future usefulness and an assessment of the risk associated with destroying them.

4 System Retirement Reporting

After the system retirement plan is executed, a summary report should be created to describe the execution and the results. If testing or verification activities were executed, the results of these tests should be summarized and any deviations should be discussed along with their resolution. This report also may include an index or registry of all documentation related to the retired system and where it is stored.

User Requirements Specifications

1 Introduction

This appendix provides guidance for the production of a User Requirements Specification (URS), a document that specifies the requirements for a computerized system or system component.

The extent and detail of requirements should be commensurate with risk, complexity, and novelty, and should be sufficient to support subsequent risk analysis, specification, configuration/design, and verification as required. The results of any existing studies, such as business needs analysis, may assist with determining the extent and detail of requirements.

For example, for a commercially available and low risk system it may be appropriate to include the requirements in purchasing documentation, while a complex and custom application may require several levels of requirements specification. The requirements should define the intended use in the operating environment including limits of operation.

The approach should be top-down, and based on product and process understanding including where appropriate Critical Quality Attributes (CQAs), and understanding of relevant regulatory requirements. This understanding facilitates the adoption of a Quality by Design (QbD) philosophy.

The URS is the responsibility of the regulated company, but may be written by a third party or supplier.

2 Scope

This appendix provides general guidance on the development of requirements for a wide range of computerized systems. It also provides specific guidance on the typical contents of a URS. For systems such as commercially available and low risk systems, the requirements may be incorporated into purchasing documentation rather than provided in a separate URS.

3 Guidance

3.1 General Guidelines

A URS defines, clearly and precisely, what the regulated company requires the system to do. It should be driven by the business process needs. Requirements may be developed independently of a specific solution prior to selection, e.g., for Category 4 and Category 5 systems. There may be a limited number of suppliers or a preferred supplier for some systems, in which case requirements may be based on the available solution. This is particularly relevant to many Category 3 systems. Such a decision should be based on risk, complexity, and novelty. In such cases requirements related to patient safety, product quality, and data integrity still should be specified.

Requirements may not initially be fully defined, e.g., for some Category 5 systems, and requirements will be developed during subsequent phases of the project. The initial URS should recognize this and should be updated as information becomes available.

The content of a URS typically includes, but is not limited to, as appropriate:

- operational requirements
- functional requirements
- data requirements
- technical requirements
- interface requirements
- environment requirements
- performance requirements
- availability requirements
- security requirements
- maintenance requirements
- regulatory requirements
- migration of any electronic data
- constraints to be observed
- life cycle requirements

These are discussed further in Section 3.3 of this appendix.

Development of requirements may be assisted through iterative prototyping (see Section 7.5.1 of the Main Body).

Template user requirements for a broad range of equipment are available through the JETT Web site (Reference 51, Appendix G3).

3.1.1 Quality Critical Requirements

Requirements should address applicable GxP regulations and should highlight those aspects that are critical to patient safety, product quality, and data integrity. For example, the URS should not include requirements such as "Part 11 compliant" or "GMP-compliant"; it should define what functionality the users need in the system to manage risk to patient safety, product quality, and data integrity.

Identification of quality critical requirements enables companies to focus on those aspects of systems that are critical to patient safety, product quality, and data integrity during subsequent risk analysis, specification, configuration/design, and verification activities.

3.1.2 Requirements Good Practice

Requirements should be:

- sufficient and appropriate:
 - Specific

- Measurable
- Achievable
- Realistic
- Testable
- specific enough for testing and checking:
 - unambiguous
 - clear
 - precise
 - self-contained
- Able to support full traceability through configuration/design and testing. See Appendix M5 Design Review and Traceability.
- providing a basis for formal testing, and be used during supplier selection
- Prioritized with emphasis on identifying the mandatory requirements. For example, a three level prioritization scheme could be used:
 - mandatory (high)
 - beneficial (medium)
 - nice to have (low)
- uniquely identified and version controlled, and a change history maintained
- linked to the associated business process step(s) where appropriate
- enabling clear communication and management of the critical requirements throughout the life cycle rather than being seen just as a paper exercise
- providing the supplier with the definitive statement of mandatory and other desired requirements where appropriate

It may be useful to consider categorizing requirements in some other way, e.g., by quality, safety, or business. For commercially available and low risk systems prioritization may not be necessary.

3.2 Ownership

Ownership of requirements lies with the regulated company. Without user ownership the business operational needs and any associated issues can never be fully understood and captured. Documented requirements form the basis for acceptance of the system by users.

Subject Matter Experts (SMEs), including those from third parties, may help both the user and technical communities analyze and understand the operational needs and develop and document appropriate requirements.

3.3 Contents of the Document

Listed below are topics that may be included in the URS.

Where there is a limited number of suppliers or a preferred supplier for a system, requirements may be based on the available solution. This is particularly relevant to many Category 3 systems where the requirements may be included in purchasing documentation. Such a decision should be based on risk, complexity, and novelty. This section still may provide useful guidance for such systems.

The guidance provided in this section is not intended to be exhaustive. If required information is already available elsewhere it should be referenced and not duplicated.

3.3.1 *Introduction*

The introduction should provide information on:

- who produced the document, under what authority, and for what purpose
- the contractual status of the document (if applicable), e.g.,
 - custom development
 - outsourcing
- relationship to other documents (e.g., Business Process Definition, Request for Proposal (RFP))

3.3.2 *Overview*

An overview of the system should be provided, explaining why it is required, and what is required of the system. The following should be considered:

- background: describes the overall goal of the system in context of the present and desired state
- scope:
 - what portion of the long-term vision the current system will address
 - system limits and boundaries: what business process or portion of a business process is being automated
 - key objectives and benefits
 - applicable GxP requirements
 - other applicable regulations

3.3.3 *Operational Requirements*

Operational requirements include:

- functions
- data
- technical requirements

- interfaces
- environment

Process descriptions or flowcharts may be included as appropriate.

Special consideration should be given to critical GxP requirements. These should be clearly defined, with references to the relevant regulation, where possible.

All requirements should be verifiable. It should be noted that some requirements may be difficult to define and verify because they are subjective and therefore may be subject to different interpretation. The measurement or acceptance criteria for these requirements should be specifically defined as part of the approved requirement.

3.3.3.1 Functions

Those functional requirements that would enable a system to perform the business process being automated should be documented. The following should be addressed as appropriate:

- Calculations, including all critical algorithms (e.g., those required for compliance with regulations or internal process requirements). Critical algorithms should be documented with references to their scientific sources. Algorithms that have been custom developed should be scientifically derived.
- safety
- security including access control
- audit trails
- use of electronic signatures
- output (e.g., reports, files)
- unambiguous error messages

3.3.3.2 Data

Data handling requirements should be documented. Consideration should be given to understanding the impact upon patient safety, product quality, and data integrity. The following should be addressed as appropriate:

- definition of electronic records
- definition of data, including identification of characteristics, formatting, critical parameters, valid data ranges, limits and accuracy, character sets, etc.
- required fields
- data migration
- data input and subsequent editing
- backup and recovery
- archive requirements

- data security and integrity

3.3.3.3 Technical Requirements

System technical requirements should be defined. The following should be addressed as appropriate:

- changes in system operation (e.g., start-up, shutdown, test, failover)
- disaster recovery
- Performance and timing requirements. These should be quantitative and unambiguous.
- action required in case of failure
- capacity requirements
- access speed requirements
- hardware requirements
- portability
- efficiency (speed with which it loads, updates screens, generates reports)
- configurability

3.3.3.4 Interfaces

System interfaces should be defined. The following should be addressed as appropriate:

- Interface(s) with users. These should be defined in terms of roles, (e.g., plant operator, warehouse administrator, system manager) or functions as appropriate.
- Interface(s) with other systems
- Interface(s) with equipment, such as sensors and actuators. This may include I/O listings for process control systems.

3.3.3.5 Environment

The environment in which the system is to work should be defined. The following should be addressed as appropriate:

- layout: the physical layout of the plant or other work place may have an impact on the system, such as long distance links or space limitations
- physical conditions (e.g., temperature, humidity, external interference, shielding against radio-frequency, electromagnetic and/or UV-interference, dirty, dusty, sterile, or high vibration environment)
- physical security
- power requirements (e.g., voltage, amperage, filtering, loading, earthing protection, uninterruptible power supply (UPS))

- any special physical or logical requirements

3.3.4 *Constraints*

The constraints on the specification and operation of the system should be identified. The following should be addressed as appropriate:

- compatibility, taking into account
 - any existing systems or hardware
 - any regulated company strategy or policy
- availability
- reliability requirements
- maximum allowable periods for maintenance or other downtime
- statutory obligations
- working methods
- user skill levels
- expansion capability
- likely enhancements
- expected lifetime
- long term support

3.3.5 *Life Cycle Requirements*

Any specific requirements that may impact the supplier's development life cycle and any subsequent verification activities should be identified. If this information is already provided elsewhere this should not be repeated.

The following should be addressed as appropriate:

- development requirements, (e.g., minimum standards to be met by supplier's methodology)
- procedures for project management and quality assurance
- mandatory design methods
- special testing requirements
- test data
- load testing
- required simulations

- factory acceptance testing
- how deliverable items are to be identified
- in what form deliverables are to be supplied (e.g., format and media)
- documentation the supplier is expected to deliver (e.g., functional specification, testing specifications, design specifications, user and maintenance guides or manuals)
- data to be prepared or converted
- tools
- training courses
- archiving facilities
- support and maintenance required after acceptance

3.3.6 *Glossary*

Definitions of any terms that may be unfamiliar to the readership of the document should be provided.

3.3.7 *Approvals*

The approvers should be defined. At a minimum this needs to include the appropriate process owners. Other signatories should include the system owner and quality unit.

Once approved, additions, changes or deletions to the URS should be handled via Change Management and should be re-approved.

3.4 Out of Scope Topics

This section is aimed at systems with multiple levels of specification and verification, and may not be applicable to commercially available, low risk, Category 3 systems.

The information listed below should not be included in the URS:

- system configuration/design details
- implementation details
- project deadlines
- cost
- project organizational details

System configuration/design details are a part of the solution to how the requirements will be met, which will be defined in subsequent specifications. Implementation details also are totally dependent on the solution and may not be known at this point.

While a regulated company may have deadlines and budget for a project, the final timeline will be driven by the solution selected, as will cost. When submitting the URS to a supplier in the context of an RFP the desired timeline and available funds can be included as a requirement, but they are not a part of the definition of what a system is required to do.

4 Requirements Capture

For Category 4 and 5 systems, this is often the most difficult and time consuming aspect of producing a URS. Developing the URS is one of the most important tasks the regulated company will undertake in the project.

A suitably experienced individual should be identified and made responsible for managing the requirements capture process.

4.1 Requirements Capture Process

There are a variety of ways that business needs can be captured and refined.

4.1.1 *Discussions and Interviews*

Discussions and interviews should be planned and should include participants such as:

- process and system owners
- business process participants and users
- SMEs

Asking the participants general questions is not effective. The following specific aspects should be considered:

- participants should be asked open-ended questions so that their requirements can be investigated
- The participant's actual involvement in the process that is to be automated should be determined. It should be noted that a different level of involvement will have a different focus.
- Participants should be asked to identify the weaknesses of the existing process. It should be determined whether a new system needs to fulfill further requirements in order to resolve those weaknesses.
- the individual who provided specific items of information should be documented, to identify who should be asked for clarification, as required
- how a system should respond to errors should be determined
- terms familiar to the participants should be used; they should not be expected or required to learn technical terms
- a project glossary should be developed, to ensure a common understanding among all members of the project team
- Requirement gathering teams should avoid proposing solutions.

- Proposing solutions stifles consideration of what is actually needed
- Documentation such as Issue Logs from an existing system being replaced may provide valuable information, and such documentation should therefore be examined.

4.1.2 *Observation*

The business function should be observed during this activity:

- The current business process should be understood, noting that 'what is done today may not be the best solution for tomorrow'
 - Caution should be exercised regarding "designing" a new system to duplicate the current business process; the current process may not be the best way to meet all requirements
- All aspects of the current business process and its interaction with other aspects of the company's overall business process should be examined
- The parts of the current business process to be automated (project scope) should be considered

4.1.3 *Workflow Analysis*

This activity involves the examination of workflows and the development of use cases:

- a use case describes the interactions between a system and hardware/software/equipment and people outside the system
- use cases are tools that aid in:
 - gathering requirements
 - developing Standard Operating Procedures (SOPs)
 - developing training materials
 - writing test scripts
 - designing a system

4.1.4 *Workshops*

Workshops usually involve multi-functional meetings:

- participants should be focused on the task under discussion
- while ensuring that all affected user groups are represented, the size of the workshop or team groups should be manageable
- all participants should understand their role in the workshop
- participants should focus on their area of expertise

- speculation about what someone else wants should be avoided; however, awareness that a fresh viewpoint may offer a new perspective on a problem is important
- tangential discussions that may disrupt the workshop should be minimized
- those persons representing an area should be empowered to make decisions for that area
- secondary workshops or teams that focus on a specific area's needs or a specific category of requirement(s) may be appropriate for large projects

4.2 Requirements Planning Pitfalls

Aspects of the requirements capture process require particular attention, including:

- a common understanding of the requirements among team members should be established
- all required levels of the business should be involved during requirements capture
- ambiguous requirements should be avoided and, where possible, requirements should be measurable
- requirements should be classified to ensure that appropriate focus is given to critical requirements
- functionality that will not be used should be avoided
- scenarios that unduly hold up requirements capture and which may lead to other key requirements being missed or misunderstood should be avoided
- the original scope should be maintained, extending the scope should be possible only through a formal change control process
- an effective and efficient change management process should be implemented, incorporating impact assessment of changes based on risk, and formal version control
- multiple requirements within a single requirement statement should be avoided

Further sources of information are given in Appendix G3.

Functional Specifications

1 Introduction

This appendix provides guidance for the production of a Functional Specification (FS). The FS defines a system to meet the user's needs as described in a User Requirements Specification (URS) (see Appendix D1).

2 Scope

This appendix may be used for the production of FSs covering the range of computerized systems, from standalone systems to multi-site business systems.

The applicability of, and need for, an FS depends upon the specific system and should be defined during planning.

For some systems, such as commercially available and low risk Category 3 systems, a simple approach consisting of one level of specification and verification typically is appropriate and a separate FS is not required. See Section 4.2.6 of the Main Body for typical examples of the level of specification required for non-configured products, configured products, and custom applications.

3 Guidance

3.1 General Guidelines

An FS defines what the system should do, and what functions and facilities are to be provided. It provides a list of design objectives for the system. Formal testing will often be based on the FS (see examples in Section 4.2.6 of the Main Body).

The FS typically is produced by the supplier and should be reviewed and approved by the regulated company. It is often considered to be a contractual document.

The following guidelines should be followed during the production of the specification:

- All design constraints (i.e., the externally-defined limitations that a system must meet, e.g., hardware and/or software platform, speed, power, test, environmental and operating conditions) should be explicitly documented
- Ambiguity, duplication, and contradiction should be avoided
- Consistent naming conventions should be used
- Each function and facility described should be testable
- Internal and external interfaces should be clearly defined
- The FS should be clear enough to enable design to proceed without frequent consultation with the author:
 - Both users and programmers should understand the FS
 - The use of diagrams and graphics where appropriate is recommended

The specification should be prepared and organized in a way that permits traceability through the life cycle from individual requirements to associated tests.

See Appendix M5 for further details on design review and traceability.

3.2 Contents of the Document

Listed below are topics that may be included in the FS. The guidance provided is intended to be neither prescriptive nor exhaustive.

3.2.1 *Introduction*

The following information should be provided:

- Ownership of the document
- Who produced the document, under what authority, and for what purpose
- The contractual status of the document (if applicable)
- Relationship to other documents (e.g., URS)

3.2.2 *Overview*

An overview should be provided, stating the essential system functions and interfaces to the outside world. It should cover the following as appropriate:

- Background: Scope and key objectives
- Reference to relevant GxP regulations
- Impact upon patient safety, product quality, and data integrity
- High level description: this should give a breakdown of the primary components (e.g., sub-systems, segments)
- The main interfaces between the system and other systems and/or the environment (both to and from)
- Assumptions/Restrictions: these should state any design or implementation assumptions or constraints (e.g., use of standard products, operating system, hardware)
- Non-conformance with URS: any divergence between the FS and the URS should be fully documented and justified

3.2.3 *Functions*

The high level description should be broken down to the level of the individual functions. This should describe the functions and facilities to be provided, together with specific modes of operation.

The following aspects should be addressed as appropriate:

- The objective of the function or facility, and the details of its use, including interface with other parts of the system. Inputs, outputs, critical calculations, algorithms, and impact on other functions and/or other systems and/or the environment should be highlighted.

- performance: response, sizing, centralized or distributed processing, and throughput – these should be quantitative and unambiguous
- safety and security: the topics may include: action in case of selected software or hardware failures, self checking, input value checking, redundancy, access restrictions, time-outs, and data recovery
- functions which are configurable and any limits to the configuration
- traceability to specific requirements in the URS
- error conditions, failure actions, logfiles, and diagnostics

3.2.4 Data

The data on which the system is to work should be described. The following aspects should be addressed as appropriate:

- definition: the data should be defined in a hierarchical manner with complex objects being built up from simpler objects (e.g., files of records; complex types defined in terms of simple types). Critical parameters should be highlighted.
- access (e.g., which sub-systems need read or write access to each data item, call sequencing, access method, speed and update time, read/write interlocks)
- allowed range of values for all inputs and outputs
- required fields
- data validation checks
- data relationships
- data capacity, retention time, and details of data archiving
- data integrity and security
- data migration

3.2.5 Interfaces

System interfaces should be described, defining how the systems or sub-systems interact, what they each provide, and what they require. For GxP regulated systems, the security of the interfaces is important. The following should be addressed as appropriate:

- Interface with users: this should be defined in terms of roles, e.g., operator, administrator, clerk, or system manager. Topics to consider include types of peripherals, general format of displays and reports, error handling and reporting, and security. Mode(s) for user input should be defined, e.g., keyboard and mouse, touchscreen, handwriting via stylus, hardened keyboard
- Interface with equipment, such as sensors and plant equipment
- Interface with other systems: this should cover the nature and timing of the interaction, and the methods and rules governing the interaction. If there are middleware constraints, this should be noted.

Topics to consider for any interfaces are listed below:

- data transmitted and received
- data type, format, ranges, and meaning of values
- timing
- rates of data transfer
- communications protocol: initiation and order of execution
- any data sharing, creation, duplication, use, storage, or destruction
- mechanisms for initiation and interruption
- communication through parameters, common data areas, or messages
- direct access to internal data
- error handling, recovery, and reporting
- access and security

3.2.6 Non-functional Attributes

The way in which the system will meet non-functional requirements should be described. The following should be addressed as appropriate:

- availability (e.g., reliability, redundancy, error checking, stand-by operation)
- maintainability (e.g., expansion and enhancement possibilities, spare capacity, likely changes in environment, lifetime)

3.2.7 Environment

Any special logical or physical requirements, e.g., encryption or physical hardening, should be addressed.

3.2.8 Glossary

Definitions of any terms that may be unfamiliar to the readers of the document should be provided.

3.2.9 Appendices

Where appropriate, e.g., small systems, appendices may be provided to define hardware and software specifications.

Configuration and Design

1 Introduction

This appendix provides guidance for defining the required configuration of system components and for system design.

Based upon the type of system (e.g., configurable or custom), configuration and design specifications provide a detailed, technical expansion of the Functional Specification (FS) (see Appendix D2). They explain how the system will do what is defined in the FS. This information provides the basis for subsequent configuration management (see Appendix O6).

Note: In previous versions of the GAMP Guide there were separate appendices for hardware and software design specifications. These are now combined in this single appendix.

2 Scope

This appendix applies to the production of all configuration and design specifications.

Separate documents may not always be needed to adequately define configuration and design aspects. A hierarchy of specifications may be required for larger systems, while specifications may be combined for smaller, simpler, systems or system classed as low risk.

3 Guidance

3.1 Overview of Configuration and Design

3.1.1 Configuration

Configuration specifications should be provided for configured products and cover the appropriate configuration of the software products that comprise the system to meet specified requirements. This includes the definition of all settings and parameters.

These specifications typically are produced by the supplier and reviewed and approved by regulated company Subject Matter Experts (SMEs).

It may be possible to maintain configuration information electronically in systems with robust configuration management, e.g., audit trails. Such an approach should be clearly documented.

3.1.2 Design

Custom applications require design of hardware and software, and also may require Configuration Specifications.

Hardware design defines the hardware components of a system, e.g., system or component architecture, or interfaces.

Software design occurs at two levels. At the higher level it defines the software modules (sub-systems) that will form the complete software system, the interfaces between these modules and also the interfaces to other external systems. At the lower level the design describes the operation of the individual software modules. These specifications should be unambiguous, clear, and precise.

Design specifications typically are produced by the supplier and reviewed and approved by regulated company SMEs.

The regulated company should have a unified approach to the specification and verification of infrastructure that supports the system design, and such activity should not be repeated for each system, see the *GAMP Good Practice Guide: IT Infrastructure Control and Compliance* (Reference 34, Appendix G3).

3.2 General Guidelines

The use of tables and diagrams to illustrate Configuration and Design Specifications is highly recommended. If such tables or diagrams are produced elsewhere then these should be cross-referenced in the appropriate specification. Standardized tables can help ensure that all relevant parameters and settings have been defined. Diagrams can be helpful in software design to clarify and explain data flow, control logic, data structures, and interfaces. Diagrams in hardware design can aid understanding of architecture and connectivity.

Configuration and design should cover both hardware and software aspects. Depending on the risk, size and complexity of the system this may be covered by a single specification or may require a hierarchy of specifications covering software and hardware separately. Each specification should be uniquely referenced and traceable back to its appropriate higher level specification.

All specifications should be structured in a way that supports traceability through the life cycle from individual requirements to associated testing.

See Appendix M5 for further information on design review and traceability.

3.3 Information Required

The topics described in this section should be covered by each appropriate specification; not all information is required for all types of system. The level of detail should be based on risk, complexity, and novelty. This may be covered by a single document or by a hierarchy of documents.

The guidance provided is intended to be neither prescriptive nor exhaustive.

3.3.1 Introduction

This is common to all types of specification and should contain the following information:

- ownership of the document
- who produced the document, under what authority, and for what purpose
- the contractual status of the document (if applicable)
- relationship to other documents (User Requirements Specifications (URSs), Functional Specifications (FSs), other configuration or design specifications, etc.)

3.3.2 Overview

The overview should briefly describe the configuration and/or design as defined in the document. Depending on the complexity of the system, this may cover the complete system, hardware, and/or software. The overview should not contain detailed design information.

The overview may be illustrated using diagrams.

3.3.3 Configuration

The required configuration of components to be provided as all or part of the solution should be defined. This includes but is not limited to:

- required configuration settings or parameters
- reason for setting, with reference to controlling specification
- tools or methods that will be used to set the required options
- dependencies and impacts on other modules or systems
- infrastructure items such as operating systems and layered software
- security of settings

For small systems it may be possible to incorporate this information into the FS.

3.3.4 Hardware Design

3.3.4.1 The Computer System

The overall architecture of the hardware required should be defined. At a high level this may be illustrated by means of an annotated block diagram showing both the functions of the parts and their functional relationships. The following should be covered as appropriate:

- main computer system

This should describe the primary hardware components of the main computer system(s), e.g., central processing unit (CPU), memory, bus type, clock accuracy

- storage

This should describe all proposed storage devices with their maximum storage capacities, e.g., hard disk, CD writer, tape

- peripherals

This should describe peripheral devices required. Any special housings and mountings should be described as appropriate.

- interconnections/networks

This should describe all interconnections of the hardware components and any connections to other equipment, devices, and computer systems. The following elements may be included in this description:

- Cable specifications
- Connector specifications
- Screening/shielding requirements
- Drawing schedules
- Network and other external connections
- configuration (unless covered in separate configuration specifications)

This should cover configuration details such as Dual In-line Package (DIP) switch settings, device addresses, pin assignments, as appropriate.

As noted above, it may be possible to maintain configuration information electronically in systems with robust configuration management, e.g., audit trails. Such an approach should be clearly documented.

- embedded systems (within process equipment)
 - layout diagrams to detail control panel and interior and exterior arrangements
 - location diagrams to indicate where sensors and other devices are installed on the equipment
 - electrical wiring diagrams
 - Piping/Process and Instrumentation Diagram (P&ID) drawings
- reference to relevant standards

3.3.4.2 Inputs and Outputs

Input and output formats should, where necessary, be specified. These may include digital and/or analog signals.

For external equipment the following elements should be considered:

- accuracy
- isolation
- range of current and voltage
- type and numbers of interface cards
- timing

3.3.4.3 Environment

The operating environment for the hardware should be defined. The following topics should be considered:

- temperature
- humidity

- external interference
- physical security
- shielding against radio-frequency, electro-magnetic and/or UV-interference
- hardening against physical hazards such as dust or vibration

3.3.4.4 *Electrical Supplies*

The electrical supply requirements for the configured hardware system should be described. The following elements should be considered:

- filtering
- loading
- grounding protection
- uninterruptible power supplies (UPS)
- power consumption and/or heat emission to calculate the necessary capacity of the air conditioning or Heating, Ventilation, and Air Conditioning (HVAC) system

3.3.5 *Software Design*

Software should be designed in accordance with recognized design standards where appropriate.

Design Specifications covering software design are required for custom applications. This is not normally required for configurable products, where software design is normally reviewed or evaluated as part of supplier assessment.

3.3.5.1 *Software Description*

The modules that will form the system should be described, briefly stating the purpose of each. A list of all interfaces between modules, and any interfaces to external systems should be given. A system diagram is recommended.

3.3.5.2 *System Data*

System data and the major data objects should be defined. The data should be characterized in a hierarchical manner with complex objects being built up of simpler objects. The objects may include the following:

- databases and collections of files
- files
- records

A description of the data objects will include such things as:

- data types (integers, floating point numbers, characters, Boolean, string, object, etc.)
- data format (alpha-numeric or numeric, field length, date, etc.)
- data precision

- data accuracy

Each file and data structure should be uniquely identified. The use of formal data description methods such as Entity Relationship Models or similar should be considered.

It is acceptable to have all system data defined separately, such as in a data dictionary. If data is defined separately then this fact should be clearly explained and documented.

3.3.5.3 Module Description

For each module the following should be covered:

- module operation: the description may take the form of pseudo code or a flow chart
- interfaces to other modules: these may refer to the system diagram, if one is produced
- error handling and data checking
- data mapping to each module
- software module data (see Section 3.3.5.2 of this appendix)

For each sub-program in the software module, the following should be covered:

- sub-program operation: the description may take the form of pseudo code
- the steps involved in each process to be performed and the inputs to and outputs from each step
- parameters: each parameter should be identified as one of the following:
 - input parameter
 - output parameter
 - input and output parameter
- algorithms
- each parameter should be identified as:
 - pass by value
 - pass by reference
- any side-effects of the sub-program
- language, including version
- reference to any programming standards
- description or examples of all display screens (may be in user documentation, e.g., operator manual, and may be referenced)
- sub-program data (see Section 3.3.5.2 of this appendix)

- description or examples of all implemented reports, their meaning and handling, and when they are generated

This level of detail may be provided in separate specifications.

3.4 Glossary

Definitions of any terms that may be unfamiliar to the readership of the document should be provided.

Management, Development, and Review of Software

1 Introduction

This appendix provides guidance for the management, development, and review of software. It also includes general guidance on coding practices. Software tools to assist with these activities are available, and in general, automation of these processes will lead to better compliance and reproducibility when compared to manual approaches.

Software development should be performed within a phased life cycle. The criteria for releasing developed software for formal testing should be understood and defined and should be based upon approved requirements and specifications.

This appendix is not intended to constrain the choice of development methods and models in any way. Suppliers should select and use the most appropriate methods and models for their use. The Guide is not intended to place any constraints on innovation and development of new concepts and technologies. Any examples used, or technologies assumed, are intended to illustrate general principles and are not intended to be restrictive.

2 Scope

This appendix may be used to define procedures and standards for software development and review for GxP regulated computerized systems.

While the main focus is on software development using high level and low level languages, the principles of this appendix also may be applied to various techniques used for process control system software development. For further information on this topic see the *GAMP Good Practice Guide: Validation of Process Control Systems* (Reference 34, Appendix G3).

3 Guidance

3.1 Software Development

Each project should define the program coding standards, directory structure standards, and file naming conventions to be followed. These should be documented in accordance with the project approach being used. The principles described in the following sub-sections may be used when preparing such standards.

Where command files are necessary for build management, including compilation of source modules or linking of object modules, these also should be controlled in accordance with documented procedures.

Source code should be subject to a documented review. The need for, and extent of, such reviews should be based upon risk to patient safety, product quality, and data integrity. The review should take place before acceptance testing of the software commences. See Section 3.2 of this appendix for further details.

Software should be subject to Configuration Management and documented version control. Such control is an aspect of Configuration Management that is closely related to change control and is especially important during software development, as mistakes in this regard can lead to problems such as re-introduction of previously removed defects.

Any software development tools used should be assessed for suitability and fitness for purpose.

See Appendix M8 for further details on configuration management.

3.1.1 General Design and Documentation Principles

Software should be based on a documented, reviewed, well-structured design, and developed following established programming practices, such that it is:

- meeting design requirements
- reliable
- robust
- maintainable
- capable of handling error conditions
- efficient
- modular in structure
- well laid out and commented

3.1.2 Software Module Identification

Each software module should have at least the following information in the module header:

- module name
- means of reference to controlling design specification(s)
- constituent source file names
- module version number
- project name and number (if applicable)
- brief description of the module (if module name is descriptive, that may be adequate)
- any specific command files required to compile and build the module

3.1.3 Software Module Change Traceability

All software module changes should be clearly identified in the source code files or by using version control tools.

Additions should be identified by the use of commentary that references the relevant change request number.

Deletions should be identified either by:

- commenting out the code and indicating the deletion by referencing the relevant change request (for minor changes, e.g., a few lines of code deleted)

or

- deleting the code and indicating the deletion by referencing the relevant change request (for major changes, e.g., when a significant amount of code is removed)

It should be possible to obtain a history of changes made, which should include the following information for each change:

- change request number(s) (if applicable)
- applicable version number(s)
- dates change(s) made
- identity of person(s) changing the code
- summary of the changes

Where version control tools are used, the features of these tools should be used to manage these processes in the most efficient and effective way.

3.1.4 Maintainability

Software should be written in a way that a competent programmer (other than the software author) would be able to maintain and enhance the software if required. The code should be clearly laid out and commented.

The following should be considered:

- Breaking down procedures into logically distinct blocks, each performing just one step in the processing sequence or logic. Each block normally should be preceded by a comment.
- only one action per line of code (except for cases such as multiple initializations)
- indentation of code should be used to indicate different levels in the logic, e.g., for 'DO', 'WHILE', 'UNTIL' loops, and 'IF...THEN...ELSE' conditional blocks
- code should be vertically aligned where appropriate, e.g., declarations, sequences of assignments ('=' signs), trailing comments
- brackets should be used in logical or arithmetic expressions, even if not strictly necessary, if they make the expression clearer
- consideration should be given to readability, both on-screen, and in printed form, including page numbering
- limiting the size and complexity of procedures (using appropriate measures such as function points, or lines of code)

3.1.5 Modular Structure

Individual modules normally should perform a single, easily identifiable function. Modules should be distinct and as logically separate as possible. The use of subroutine or function side effects should be avoided. If required such usage should be justified and clearly documented.

3.1.6 Removal of Dead Code

This is code that cannot be executed due to the logic of the program, and should be removed. It is usually a symptom of poor maintenance, and may have been left over by accident from development or code changes.

Code that has been included for purposes of testing or for later diagnosis during support work, and which can be configured on or off, is not regarded as dead code. Any such code should be clearly documented.

If the code is configurable or general purpose code that may be used in many different projects, each with different configurations of options, the unused options should not be removed. The software review and the testing processes, however, should demonstrate that the correct options have been selected and that they work, and that the deselected options have been correctly deselected and do not function.

Code that has been properly commented-out during the operational change process is not regarded as dead code and may be an appropriate technique for minor changes during the operational phase. The cleanup of commented-out code prior to formal testing of the initial and subsequent major releases of software should be considered, as an aid to code maintenance.

3.1.7 Variable Naming and Initialization

The names of variables should be meaningful to programmers reading the code. Documented, language specific, naming conventions should be established.

Where applicable, all variables should be declared, including both those internal to the module and those that also are used externally in other modules. It is good practice to do this even in languages that do not require it. If the compiler can be configured to check for undeclared variables, this should be enabled.

Each variable should be used only for one purpose.

Loop counters may be reused, provided each use is independent, and provided that they are used for no other purpose. Loop counters with the same name should not be nested.

All variables should be initialized before they are used. Variables of the correct type and precision (or size) should be declared for their intended use, especially where the language permits similar data types of different precision to be used. The declaration and initialization of variables that are not subsequently used should be avoided.

3.1.8 Labels and Branching

The code should be written using structured programming techniques to the extent that the programming language allows it, and this should ensure that the use of labels is minimized. For any labels that remain, their names should be meaningful. In programming languages that allow only numerical labels, the labels should have increasing numerical value within the code for a module.

In languages that allow (but do not require) declaration of labels, all labels should be declared. Unused labels should be removed. Branches to labels should, as far as possible, be forward.

Branches into 'DO', 'DO WHILE', or 'DO...UNTIL' loops, or 'IF...THEN...ELSE' blocks, or 'CASE' blocks, should always be avoided. Branching out of such loops should only be used in necessary and defined circumstances, e.g., for error and exception handling. The impact on the integrity of data, such as that contained in counters and pointers, should be considered whenever branching.

3.1.9 Cross Reference Tables

Before code is released for formal testing, a cross-reference table of symbols (i.e., variables, procedures, labels)

should be generated for each module (if the language compiler or other utility provides this option), and static analysis checks should be made for all variables to ensure that they are declared, initialized, and used correctly. The following checks should be made for each symbol listed (as appropriate):

- Are all symbols used?
- Are all variables initialized or set before they are used?
- Is there any potential confusion between global and local variables with the same name?
- Are all variables declared?
- Are all procedures called somewhere within the code?

3.1.10 Switches, CASE Statements, and Multi-way Branches

Multiple options should include a default option for all values outside of the expected range. The processing for each option normally should exit properly to the next step in the process, and not 'run on' into the next coded option. If the code is intended to 'run on' into the next option, a comment should be included to explain the reason why. All exits from a procedure should be through a single exit point, normally at the end.

3.1.11 Comparing Values

Integer and string or character expressions can be directly compared for equality. The use of equality comparisons between real expressions should be carefully considered, bearing in mind the constraints of the programming language, operating system environment, and the hardware architecture. Where comparison within a tolerance is required, the absolute value of the error should be compared with the required tolerance, even for comparisons with zero.

3.1.12 Error-prone Language Features

The following features of some languages have been found in various studies of software reliability to be potentially error prone, and should be used with great care, following language specific conventions and best practices.

- GOTO, Assigned GOTO, and GOSUB
- floating-point numbers
- pointers
- parallelism
- recursion
- interrupts
- dynamic allocation of memory

3.1.13 Compiler Switches

Most compilers allow options to be switched on and off during various compile time and run time checks, e.g., underflow, overflow, array bound checking, range checking. Compile time checks should be switched on for all compilations, and all run-time checks enabled, at least during software development and initial testing, and preferably through to final testing and operation.

If it is not possible to leave them switched on for the final version, because of program size or speed limitations, tests should be performed both with and without run time checks. For GxP critical software, the benefits, and potential risks of switching on code optimization should be considered, and the decision documented.

3.1.14 Reliability and Error Recovery

The software should either recover from incorrect data or incorrect operation of any equipment, or fail in a safe and predictable manner. 'Defensive' coding techniques should be employed. For example, input values should be checked, and subroutines should check that the values of the received parameters are within range. In the event of a failure, a safe, documented error recovery or a controlled shutdown should be performed, with an informative error message.

3.2 Source Code Review

Source code reviews have two objectives:

- to ensure that programming standards, such as those described in Section 3.1 of this appendix, are consistently and correctly applied
- to ensure that the code is written in accordance with the design specifications

The review aims to ensure that the code is fit to enter testing (module, integration or system tests), and that the code can be effectively and efficiently maintained during the period of use of the application.

The review should be carried out in accordance with a documented procedure, and performed by at least one independent person with sufficient knowledge and expertise, in conjunction with the author of the code. Further guidance on code inspections and walkthroughs may be found in G.J. Myers: *The Art of Software Testing* (Reference 42, Appendix G3).

Automated source code review comparison tools are particularly useful when making small changes to existing code.

3.2.1 Software Review Planning

The requirement for, and extent of, software review to be performed, should be documented in accordance with the project approach being used. This may include the following details:

- the modules to be reviewed and their versions
- standards to be applied and their versions
- the design documents that the modules will be checked against and their versions
- checklists to be used and their versions
- how the reviews will be documented
- who will perform the reviews: roles and responsibilities
- any exclusions: what will not be reviewed, with rationale and justification

A decision based upon known risks should determine the extent of software review required for a given project. The criteria for making this assessment, and the outcome, should be documented. Factors that may influence the extent of the software review include the criticality of the application or specific module, the complexity of the design, and the experience of the developers.

3.2.2 Software Review Documentation

Problems found during the review should be recorded, and corrective actions defined. A summary document should be produced which provides evidence of the review process, findings, and corrective actions. Agreed actions should be resolved prior to formal testing.

Reviews should be documented as appropriate.

An example Review Report form is provided separately.

3.3 Third Party Software

While the requirements noted in Sections 3.1 and 3.2 of this appendix represent good practice, documentation of these activities may not be readily available for software obtained from outside suppliers or as free and open source software (OSS). The need for documented evidence of these processes, or alternative controls such as testing, and the degree of effort to be expended, should be risk-based.

3.3.1 Purchased Software

In most cases evidence of software control can be obtained through standard mechanisms for supplier assessment, such as supplier audit; see Appendix M2. Conclusions of the assessment should be documented. If inadequacies are noted, the regulated company may require remedial actions by the supplier, possibly enforced via a Service Level Agreement (SLA) or other contractual means, or may decide that further testing is required.

3.3.2 Free and Open Source Software

OSS often plays an important role in the infrastructure of regulated companies. Examples include the Linux operating system, and many web design, programming, and support tools.

Evaluation of software control for free and open source software is similar in scope and approach to that of purchased software (following established GAMP software categories). However, the nature of OSS is different. Although there is potential for less control, the output (open source code) is public and can be reviewed. This may not be possible with commercial software. Furthermore, required changes may be implemented more rapidly than they could be by a commercial supplier, due to the availability of several possible coding authors. If enhancements are not developed by the original supplier or community project on request, there is a possibility for driving improvement through contractual agreements with third parties on demand or even internally because source code is available.

Some organizations that manage OSS take great care to manage code structure, commenting, version control, and release notes. Others do not. Companies considering using OSS should thoroughly investigate these factors. Any one-off modifications will result in custom code that will have to be managed by the regulated company.

To determine whether there is an adequate level of software maturity and control, a risk assessment should be performed to determine the business and GxP risks of using OSS software products, and to identify appropriate controls.

Factors that should be considered in assessing the GxP risk of free and open source software in a regulated environment should include the evaluation of:

- Identifiable developers, including knowledge of their qualifications
- Stability of the OSS application
 - Widespread use of the application is one indicator of stability and maturity.
 - Experience of existing users may provide valuable insight.
- Availability of commercial support by project team, distributor or third parties
- Organizational structures within the developer community, such as:
 - project management
 - definition of a core team
 - maintainers of subprojects
- Configuration management, including formal release processes, availability of patches and release information
- Availability of source code for long-term operation (migration, Application Programming Interface (API)¹ – specification) versus effort and cost of code escrow and accessibility with closed source software.
- Intended use of the software (part of infrastructure, operating system, development tool, application framework, database, direct business process support)
- The GAMP software category (see Appendix M4)

The conclusions of the evaluation should be documented and the decision to use such software justified and approved.

If a decision is taken to use OSS, then such software should be implemented in accordance with the appropriate life cycle activities as for commercial software.

¹ API is a technology that facilitates exchanging messages or data between two or more different software applications.

Testing of Computerized Systems

1 Introduction

This appendix covers the testing of GxP computerized systems.

Testing fulfills objectives such as:

- identifying defects so they can be corrected or removed before operational use
- preventing failures that might affect patient safety, product quality or data integrity
- providing documented evidence that the system performs as specified
- demonstrating the system meets its requirements
- providing confidence that the system is fit for its intended use
- providing a basis for user acceptance
- meeting a key regulatory requirement

Testing often is performed at several levels depending on the risk, complexity, and novelty. One level of testing may be appropriate for simple and low risk systems, while multiple levels may be required for complex configured or custom systems.

Testing should be carried out in accordance with an appropriate test strategy based on the risk, complexity, and novelty of the system.

This appendix is aligned with Sections 4.2.3 and 6.2.9 in the Main Body. See also the *GAMP Good Practice Guide: Testing of GxP Systems* (Reference 34, Appendix G3) which provides further details on aspects of testing.

2 Scope

This appendix applies to testing of all GxP regulated computerized systems. It covers the following key aspects:

- Roles and responsibilities
- Test strategy
- Test execution
- Test reporting
- Supplier test activities
- Automated testing
- Good testing practice

- Typical testing activities for different categories of system

3 Roles and Responsibilities

The regulated company should define roles and responsibilities covering testing. This typically is included in an appropriate planning document, test strategy, or company procedure.

Roles and responsibilities may include:

- user – responsible for the system in question and for the approval of key test documents.
- Subject Matter Experts (SMEs) – may act as test managers, testers, reviewers or authorizers
- Test manager – planning testing and writing test plans
- Test analyst – responsible for developing test cases and test scripts
- Tester – testers should be as independent as possible. They should not be authors of the software, or of the test scripts if possible. Key users make good testers.
- Test reviewer – responsible for reviewing test cases, test scripts, and test results - should not be the same person as the tester
- Quality Unit – as specified in Section 6.2.3 of the Main Body
- Supplier – may act as test planners, testers, reviewers or authorizers of some of the tests

Writing good test strategies, specifications, and scripts is a discipline that requires expertise and experience. Persons responsible for writing test documents should be selected carefully and appropriately trained.

For further details on testing roles and responsibilities, see *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T2, Section 3 (Reference 34, Appendix G3).

4 Test Strategy

The test strategy (also sometimes known as the test plan) should define an appropriate approach to the testing of a specific system. The test strategy is based upon the following:

- results of risk assessments
- an understanding of system components (GAMP categories) and system complexity and system novelty
- results of supplier assessments, if relevant

The test strategy will vary widely, e.g., between a simple Category 3 system and a complex Category 5 system. It should be defined as early in the project life cycle as feasible, and preferably in parallel with the development of system specifications. The test strategy should be reviewed and approved by appropriate SMEs.

The test strategy should define:

- which types of testing are required
- the number and purpose of test specifications
- the use of existing supplier documentation in accordance with the results of the supplier assessment
- test phases
 - location and timing of each test phase
 - resources required for each test phase
 - responsibilities for each test phase
 - planned coverage for each test phase (and traceability against established requirements)
- the approach to supporting test evidence (e.g., printouts)
- procedures for managing test failures
- format of test documentation
- the use of test metrics

Further guidance to assist with the development of the test strategy is provided in the following sub-sections:

- testing documentation
- inputs to the test strategy
- types of testing
- test environments
- acceptance testing

Important considerations for developing an efficient test strategy are provided in Section 8.5 of the Main Body, covering:

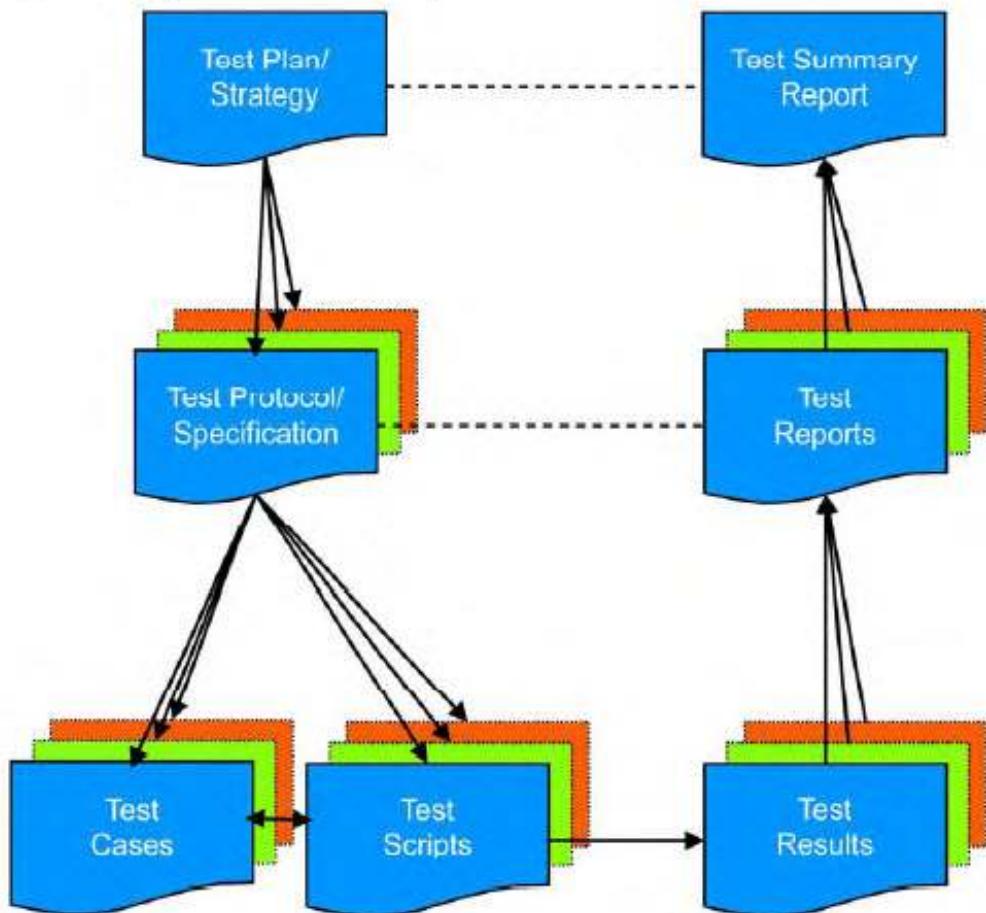
- reuse of test results
- extent of required testing
- hardcopy test evidence
- use of test witnesses

For further details on Test Planning and Test Strategies see also the *GAMP Good Practice Guide: Testing of GxP Systems*, Section 2.3 and Appendices T1 and T2 (Reference 34, Appendix G3).

4.1 Testing Documentation

Figure D5.1 shows a typical structure for testing documentation.

Figure D5.1: Typical Structure for Testing Documentation



The use of templates for testing documentation such as test specifications, recording test results and test reporting, aids consistency, facilitates review, and avoids documentation errors.

For further details on Test Documentation see the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T3 (Reference 34, Appendix G3).

Each document type shown in Figure D5.1 is described in this section.

4.1.1 Test Strategy

The Test Strategy (sometimes called a Test Plan) is described in Section 4 of this appendix.

4.1.2 Test Specification

Test specifications are sets of test scripts that are suited for a specific purpose at a specific phase in a project.

Test specifications should cover as appropriate:

- introduction
- who produced the document, under what authority, and for what purpose
- the contractual status of the document defined
- relationship to other documents
- scope - this should state where the test specification fits within the overall test strategy
- those test scripts/cases to be carried out
- version of software or configuration under test
- purpose
- resources
- personnel required at each test or group of tests
- methods
- any logical grouping or ordering of tests
- prerequisites
- environment
- tools including automated test tools
- references to specifications
- required documentation
- reviews and approvals needed

Test specifications should be created as early in the project life cycle as feasible, and preferably in parallel with the development of corresponding specifications.

4.1.3 Test Scripts/Cases

Test scripts should contain the details of the tests. The test script should be described in sufficient detail to enable consistent repetition of the test.

Each test script should, where possible, include the following:

- unique test reference
- cross reference to controlling specification
- title of test

- description of test, including the test objective
- test steps – a step-by-step description of the actions to be performed by the testers along with the expected results
- acceptance criteria – the defined set of expected results that should be met for the test to be deemed to have passed.
- pre-test steps – including any test pre-requisites or set-up
- data to be recorded - A description of the test specific data to be collected and recorded. This can be input, output, or descriptive data and should include serial numbers of any test equipment used and supporting calibration certificates where necessary. Also the requirement for use of screen shots and other electronic documentation should be specified.
- post-test actions – This optional section details those actions required to return the system to a known state. Examples include resetting process parameters, putting the system in a safe state, or rebooting the system.

Separate test cases may be prepared for some tests, which may describe complex test data sets, test methods, test input data, test environment set-up, and expected results.

When testing small or simple systems, test specifications, test inputs, test environment set-up, and expected results may all be covered within a single document.

4.1.4 Test Results

Test results should be available for subsequent review and inspection. The information to be retained should include passed tests, failed tests, test failure records, test reports and any supporting documentary evidence required by the tests, such as printouts, screen shots, notes, and pictures.

4.1.5 Test Report and Test Summary Report

Test reports normally contain:

- introduction
- scope of testing
- organization of testing
- who performed and who reviewed the testing
- summary of test results in tabular form
- summary of test failures
- conclusions

For large or complex projects which have multiple test reports overall conclusions may be documented in a test summary report.

For further information about content and structure of test report documents, see *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T7 (Reference 34, Appendix G3).

4.2 Inputs to the Test Strategy

4.2.1 Company Policies and Procedures

Company procedures should define the general framework for testing including documentation and terminology. Section 4.2.6.4 of the Main Body discusses verification terminology, including the use of Installation Qualification (IQ), Operation Qualification (OQ), and Performance Qualification (PQ).

The test strategy should define and document how the general framework described by company procedures is to be applied to a specific system.

4.2.2 Using Results of Risk Assessments

Risk assessments carried out during the life cycle (see Appendix M3) may have identified various controls to manage risks to an acceptable level. These controls may require testing. Alternatively the risk assessments may have identified the need for particular types of testing such as invalid case testing (negative case or resistance testing).

The test strategy should incorporate the results of such risk assessments.

4.2.3 Using Results of Supplier Assessments

The results of the supplier assessment (see Appendix M2) should indicate the supplier tests that have been performed and which ones can be leveraged to avoid unnecessary repetition or duplication of effort.

The test strategy should incorporate or reference the results of such supplier assessments.

4.2.4 Using GAMP Categories

The number of levels of testing and the number of test specifications required will vary based in part on GAMP categories (see Appendix M4). Practical examples of this are provided in Section 4.2.6 of the Main Body.

4.2.5 Other Documents

The following documents should be considered when developing a test strategy, and depending on the category of system being considered, some documentation may be combined:

- requirement specification
- initial risk assessment
- Functional Specification (FS) (may be a supplier document)
- functional risk assessment
- configuration specification (may be a supplier document)
- design documents (may be supplier documents)
- results from other test activities from different stages in the software development life cycle (these may be supplier documents)
- traceability matrix

4.3 Types of Testing

This section discusses the types of testing that should be considered when developing the test strategy.

Two general types of testing activities may be identified:

- *White Box Testing* is also known as code-based testing, or structural testing. Test cases are identified based on source code knowledge, knowledge of Detailed Design Specifications and other development documents.
- *Black Box Testing* is based on the functional specification, thus often known as functional testing.

Black box testing may be sufficient providing the supplier assessment has found adequate evidence of white box testing.

Specific types of testing should be considered, depending on the complexity and novelty of the system and the risk and supplier assessments of the system to be tested, including:

- *Normal Case testing (Positive Case or Capability testing)* challenges the system's ability to do what it should do, including triggering significant alerts and error messages, according to specifications.
- *Invalid Case testing (Negative Case or Resistance testing)* challenges the system's ability not to do what it should not according to specifications.
- *Repeatability testing* challenges the system's ability to repeatedly do what it should, or continuously if associated with real time control algorithms.
- *Performance testing* challenges the system's ability to do what it should as fast and effectively as it should, according to specifications.
- *Volume/Load testing* challenges the system's ability to manage high loads as it should. Volume/Load testing is required when system resources are critical.
- *Regression testing* challenges the system's ability to still do what it should after being modified according to specified requirements, and that portions of the software not involved in the change were not adversely affected.
- *Structural/Path testing* challenges a program's internal structure by exercising detailed program code.

See the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T1 (Reference 34, Appendix G3) for details on types of testing.

4.4 Test Environments

The test strategy should consider and define the environments required for testing. For a typical Category 3 system there will only be one environment. For more complex systems, testing may take place in different environments during a project, which may include:

- development environment where prototyping or programming takes place
- testing environment where formal testing is performed
- operational environment where the system is in its target environment

The development environment is normally used for the prototyping or development of software code, software

configuration, or initial testing by the developers, prior to testing in a controlled environment.

Formal tests should be performed either in the operational environment (where test records should be clearly distinguishable from production records or where test records can be archived prior to operational use) or in a separate test environment. Test documents should specify which environment to use. When using test environments the test strategy chosen should justify the equivalency of test results, i.e., justify that similar results would have been achieved in the operational environment.

Formal tests executed at the supplier premises should take place in a dedicated supplier controlled test environment.

Formal tests should be executed only in environments under configuration management.

See the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T4 (Reference 34, Appendix G3) for further details on test environments.

4.5 Acceptance Testing

There may be a need for specific tests to satisfy contractual requirements, which are typically called acceptance tests. Typically these are a pre-defined set of functional tests that demonstrate fitness for intended use and compliance with user requirements.

In such circumstances the test strategy should leverage these tests to satisfy GxP verification requirements and avoid duplication.

Acceptance may be carried out in two stages, Factory Acceptance and Site Acceptance.

- Factory Acceptance Tests (sometimes abbreviated to FAT) are performed at the supplier site before delivery to show that the system is working well enough to be installed and tested on-site.
- Site Acceptance Tests (sometimes abbreviated to SAT and sometimes called System Acceptance Testing) show that the system is working in its operational environment and that it interfaces correctly with other systems and peripherals

This approach is often used for automated equipment and process control systems. For further details see the *GAMP Good Practice Guide: Validation of Process Control Systems* (Reference 34, Appendix G3).

The environment for acceptance testing (e.g., test or operational) should be defined.

5 Test Execution

All tests should be executed according to predefined and approved specifications and scripts maintained under version control. This should not prevent a tester from noting any unexpected events during a test, even if not covered by these documents.

5.1 Prerequisites

The following general requirements should be fulfilled before initiating formal test execution:

- Formal configuration management should be in place prior to conducting formal testing. All testable entities (firmware/software/hardware) within scope of the specific test phase should be baselined and placed under change control prior to the execution of the tests.

- All necessary documentation should be available as described in the test specification.
- All required prerequisites should be in place, e.g., the system is released for test, test data is in place.
- If calibration of necessary test equipment is required, it should be performed and documented. Calibration equipment should be certified, traceable to national standards and referenced in accordance with the customers procedures; see *GAMP Good Practice Guide: Calibration Management* (Reference 34, Appendix G3).
- All staff responsible for test execution, including end-users, should be trained in test procedures and should be able to demonstrate sufficient confidence in operating the system under test. Training should be documented.

5.2 Execution

Tests should be executed as follows:

- Tests should be executed according to a pre-defined and pre-approved specification.
- Each test should be run according to the test script and all test results should be recorded. Necessary data should be collected and attached to the corresponding test script. Any data sheets or screen shots should include reference to the appropriate test step, be paginated, dated, and should be traceable to the tester.
- Each test should be performed by an adequately trained tester.
- Test results should be documented directly as testing occurs, and should be retained.
- All test results should be immediately and accurately recorded.
- The identity of the tester should be recorded (e.g., by signing or initialing, and dating by the tester).
- Manual test recording should be legible. Shorthand notations such a tick mark should generally be avoided and actual values should be recorded wherever possible. If tick marks are applied at certain tests, there should be a description of exactly what is meant. Records should be complete and marks, such as ditto marks or arrows are not sufficient. If fields on a test record are not filled out, they should be clearly marked as not applicable with a short explanation to demonstrate that the test execution has been completed.
- Corrections should be crossed out with a single line (leaving the original content readable), initialed, and dated with a brief explanation. Correction fluid and other correction techniques that obscure the original entry should not be used.
- The tester should decide if the acceptance criteria are met and the test can be passed. The test script should clearly state if the test has PASSED or FAILED.
- In case of a FAILED test, the tester should decide whether to continue testing, to abort, or to refer to Test Review (see Section 5.4 of this appendix) in accordance with approved test procedures. All failed tests should be recorded.
- Test procedures should be sufficiently flexible to allow the tester to make decisions on whether to continue, e.g., where the system has performed correctly but where the test script was incorrect.
- All failed tests should be traceable during correction and retest through to final closure. Failed test corrections may require regression testing to verify that the corrections did not introduce new problems in other areas.

Test execution should be audited periodically on a sample basis, as a minimum, by either the regulated company Quality Unit or the supplier quality assurance function.

See the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T5 (Reference 34, Appendix G3) for further details on test execution.

5.3 Test Supporting Documentation

Supporting documentation such as printouts, screen shots, notes, pictures, etc., may be helpful to support test results depending on the nature of the test, and the GxP impact, complexity, and novelty of the area tested. Unnecessary supporting documentation that does not add value to the normal test results should be avoided.

Higher impact systems require more extensive and thorough supporting documentation than lower impact systems. For a higher impact system it may be helpful for computer generated supporting documentation to document testing of critical steps, test failures and re-testing of corrections via change control. For a low impact system supporting documentation may not be required, but it is good practice for test results to be reviewed by an SME.

Those test results that require to be supported by screen shots or other computer generated supporting documentation should be agreed upon in advance.

See Section 8.5 of the Main Body and the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T6 (Reference 34, Appendix G3) for further details on supporting documentation.

5.4 Test Review

Upon completion of test execution the results should be reviewed to check:

- that all testing has been covered
- for legibility, accuracy, and completeness of tests
- that all relevant documents are included and documentation is complete
- that the acceptance criteria are fulfilled
- all test failure records are included
- compliance with procedures

Alternatively, a review may be requested by a tester during testing following test failure to determine next steps.

Reviews should be performed and documented by an SME other than the tester (i.e., test reviewer or group).

In the case of test failures the test reviewer should decide which course of action to take and what re-testing, if any, is required. These decisions should be documented. Test failures may result from:

- Error in the way a test script is written
Corrective action: Update test script, approve test script and consider the need for a retest
- Error in the way a requirement is defined
Corrective action: Update requirement, possibly retest and explain in test report
- Error in how the test is executed by the tester
Corrective action: Repeat the test

- Error in the system
Corrective action: Apply a change via change control and repeat the test

Solutions to problems that involve changes to the system should follow the defined change control procedures.

See the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T6 (Reference 34, Appendix G3) for further details on test reviews.

6 Test Reporting

Test reports should be produced that summarize activities and findings, and state the final conclusions.

Approval of the report constitutes the formal release of entities for subsequent life cycle steps (e.g., proceed to the next phase of testing, process validation, validation of analytical procedures, or release to operation/production).

Test reports should comply with requirements of the corresponding test specifications, or in the case of the test summary report with the requirements of the test strategy.

See the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T7 (Reference 34, Appendix G3) for further details on test reporting.

7 Supplier Test Activities

There are many different models for software development, including:

- Waterfall models
- Spiral models
- Prototyping
- V models

These are all equally acceptable. Whatever model is used, the supplier should define the implementation of the model, including necessary quality controls, and describe the way it is used to demonstrate that the computerized system is fit for intended use.

Testing strategies should be established, implemented, and reported accordingly. More information on software testing is given in ISO 90003, TickIT Guide, various IEEE standards, and other publications (see Appendix G3).

Configuration of hardware and software used for testing should be documented. This includes underlying software (such as operating system, database, and network) and hardware for networks, servers, and clients as appropriate.

7.1 Testing During Software Development

Internal supplier tests should be executed in accordance with defined and approved test specifications. Common types of test types to be executed are:

- Acceptance testing for purchased hardware and software: Purchased hardware and software should be subject to acceptance testing before being used for the system's development.
- Unit/Module tests: Stand alone tests for software components, ensuring readiness for further integration into the complete system. Such tests are best written at the same time that the software is developed.
- Integration and System tests: Test of integrated software components, sub-systems, and the complete system.

7.2 Contractual Testing

Testing and verification activities may be defined for business purposes between the supplier and regulated company. Such activities are contractual and are often related to meeting project milestones, the supply of key deliverables such as training materials or user manuals, and other commercial issues. These also are known as hand-over activities. See Section 4.5 of this appendix for further details on FAT and SAT.

See the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix C2 (Reference 34, Appendix G3) for further details on supplier test activities.

8 Automated Testing

Automated test execution tools can be used to improve test execution efficiency and effectiveness. Automated test tools can be used both for black box testing and white box testing. They can significantly improve the efficiency and coverage of regression testing. Regression tests performed by an automated test execution tool may be based on an existing manually executed specification.

Any use of automated test execution tools should be defined in the test strategy. Tools should be used in accordance with defined instructions and manuals as appropriate, and the tool should be held under Configuration Management. Commercial or established tools are normally considered to be GAMP Category 1; see Appendix M4. If an automated test execution tool is used on a GxP regulated system, the tool itself should be subject to appropriate specification and verification based on an assessment of risk prior to use.

It is important that responsibility is assigned for:

- test tool ownership, administration and maintenance
- test data maintenance
- test document maintenance (including test specifications, test scripts, test results)
- instructions and manuals for use

Maximum benefit is gained from automated testing when the tool is capable of handling electronic signatures and electronic records in compliance with regulatory requirements.

See the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendix T5, Section 2 (Reference 34, Appendix G3) for further details on automated testing.

8.1 Examples of Automated Test Execution Tools

The following are examples of automated test execution tools (source code debugging and testing tools) for source code testing:

- automated test drivers (automatic test execution)
- test data generators
- environment simulators
- static analyzers
- dynamic testers
- symbolic executors
- load/volume drivers

Not all computer based testing tools automate the testing of software – some provide only a paperless test environment for manual test execution.

8.2 Automated Test Documentation

Automated test scripts should be controlled in accordance with a documented procedure.

The computer generated logs resulting from the execution of the automated test scripts are normally automatically generated from the execution of the scripts.

The header for the log should provide the following information:

- log identification
- execution date and time
- name and version of the test script
- identity of the tester and the name of the test environment

Logs should neither be edited nor deleted. They should by default be 'read-only' files to be retained and be available for future reviews or audits.

The automated test documentation should be maintained to at least the standard which applies to paper based testing.

The use and management of automated test documentation should be agreed in advance with the Quality Unit as part of developing the test strategy.

9 Testing Applied to Different Categories of Systems

This section provides practical considerations when planning testing for GAMP Category 3, 4, and 5 systems. Specifically, guidance is given on each of the examples found in Section 4.2.6 of the Main Body. Additional examples are provided in the *GAMP Good Practice Guide: Testing of GxP Systems*, Appendices E1 – E5 (Reference 34, Appendix G3).

9.1 Aspects which Apply to all Categories of Systems

9.1.1 Installation Testing of Hardware/Software

Many companies call this Installation Qualification or IQ. The purpose is to verify and document that system components are combined and installed in accordance with specifications, supplier documentation, and local and global requirements. Installation testing provides a verified configuration baseline for subsequent verification and validation activities and also verifies any installation methods, tools or scripts used. This forms the basis for configuration management of the installed system.

Installation testing should verify that the following documents are available where appropriate:

- user and technical guides
- standard operating procedures
- training schedules
- service level agreements
- security procedures
- log book
- hardware inventory
- instrument list
- specification sheets
- certificates and calibration procedures
- loop sheets
- Piping/Process & Instrumentation Diagram (P&ID) drawings
- equipment list and specification sheets
- software inventory (including installation procedure, system software list, application software list, data list, initial data settings for start up)
- program source code
- preventive maintenance program
- list of critical spare parts

9.1.2 Points to Consider for all Systems

The following is a general checklist for all systems. It should be used to help ensure appropriate test coverage of the installed system:

- power failure testing especially
 - prevention against loss of critical data or loss of control action
 - ease of controlled restart
- system access and security features
- audit trails and logging of critical actions including manual interactions
- manual data entry features, input validation
- electronic signature features
- alarms and error messages
- critical calculations
- critical transactions
- transfer of critical data into other packages or systems for further processing
- interfaces and data transfers
- backup and restore
- data archival and retrieval
- ability to deal with high volume loads especially if the system is accessed by many users as part of a network application

9.2 Typical Testing Activities for a Non-Configured Product

These are software products which are used off-the-shelf (i.e., which are either not configurable for a specific business process or where the default configuration is used) and are typically classified as GAMP Category 3.

The regulated company may decide to assess the supplier to verify the quality of the product being used depending on risk. Based on satisfactory supplier and risk assessments, a simple approach consisting of one level of specification and verification is typically applicable.

Testing should focus on:

- installation testing as described above
- requirements testing that demonstrate fitness for intended use, this may include testing the system functionality against requirements depending on risk.

- requirements testing should also include delivery and acceptance of the final documentation set from the supplier, including specifications, manuals, and drawings, if not already covered.
- any further or more rigorous tests as a result of risk and supplier assessments
- any other relevant aspects listed in Section 9.1.2 of this appendix not already covered.

Further details on the testing of Category 3 software is provided in the *GAMP Good Practice Guide: Testing of GxP Systems*, Section 2.5.3 (Reference 34, Appendix G3).

9.3 Typical Testing Activities for a Configured Product

A common type of computerized system involves the configuration of commercially available software products running on standard hardware components. Software products which are configured for a specific business process typically are classified as GAMP Category 4.

In such cases, and based on satisfactory supplier and risk assessments, a testing approach based on the three levels of configuration, functionality, and requirements is typically applicable. The number of test documents required to cover these three levels will depend on the complexity and impact of the system. For example, for a small or low risk system the functional and configuration specifications may have been combined into one document, and so one test specification also may cover both these aspects.

Testing should focus on:

- installation testing as described above
- Configuration testing – for each Configuration Specification, an associated Configuration Test Specification should be produced. The tests should verify that the package has been configured in accordance with the specification. The tests could take the form of inspections or check of supplier documentation.
- Functional testing – functionality that supports the specific business process based on risk and supplier assessments (this is an area where supplier documentation may be leveraged; see Section 4.2.3 of this appendix)
- Requirements testing that demonstrate fitness for intended use. This may include testing the system functionality against requirements depending on risk.
- requirements testing should also include delivery and acceptance of the final documentation set from the supplier, including specifications, manuals, and drawings, if not already covered
- any further or more rigorous tests as a result of risk and supplier assessments
- any other relevant aspects listed in Section 9.1.2 of this appendix not already covered

Further details on the testing of Category 4 software is provided in the *GAMP Good Practice Guide: Testing of GxP Systems*, Section 2.5.4 (Reference 34, Appendix G3).

9.4 Typical Testing Activities for a Custom Application

Some computerized systems are developed to meet individual user requirements, where no commercially available solution is suitable. The software developed for such systems is classified as GAMP Category 5.

In such cases, and based on satisfactory supplier and risk assessments, a testing approach based on the four levels of module (unit) design, integration, functionality, and requirements typically is applicable. The number of documents required to cover these levels will depend on the complexity and impact of the system. For example, for a small system the design specifications may be combined into one document, and so one test specification also may cover these aspects.

Testing should focus on:

- installation testing as described in this appendix
- code review for new code required as a result of risk assessments; see Appendix D4
- software module testing to test software modules defined in the design specification – for each Software Module Design Specification, an associated Software Module Test Specification should be produced. The Software Module tests to be carried out should ensure that the software module meets its specification.
- software integration testing to test that the modules work when operating together – the Software Integration Test Specification defines those tests that demonstrate that all software modules communicate with each other correctly and that the software system meets its design specification. A Software Integration Test Specification should be produced where more than one software module has been produced.
- configuration testing (if applicable) – for each Configuration Specification, an associated Configuration Test Specification should be produced. The tests should verify that the system has been configured in accordance with the specification. The tests could take the form of inspections or check of supplier documentation
- functional testing – functionality that supports the specific business process based on risk and supplier assessments (this is an area where supplier documentation may be leveraged; see Section 4.2.3 of this appendix)
- requirements testing that demonstrate fitness for intended use; this may include testing the system functionality against requirements depending on risk.
- requirements testing should also include delivery and acceptance of the final documentation set from the supplier, including specifications, manuals, and drawings, if not already covered.
- any further or more rigorous tests as a result of risk and supplier assessments
- any other relevant aspects listed in Section 9.1.2 of this appendix not already covered.

Additional guidance on the testing of Category 5 software is also provided in the *GAMP Good Practice Guide: Testing of GxP Systems*, section 2.5.5 (Reference 34, Appendix G3).

System Descriptions

1 Introduction

This appendix provides guidance on the contents of System Descriptions.

EU GMP Annex 11, Clause 4, requires that there is an up to date description of every GxP regulated computerized system:

A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures.

The need for a system description may be covered by one or more existing specifications or other documents, or a separate document may be produced.

The principal use of such a document is to help new users and regulators understand what the system does, and as such is written in non technical language as far as possible.

2 Scope

This appendix covers information that may be required for a wide range of GxP computerized systems. Not all the information will be required or relevant for all systems. The level and detail of information should be based on system risk, complexity, and novelty.

3 Guidance

3.1 General Guidelines

The System Description should be maintained up to date throughout the life cycle of the system.

For complex systems spanning multiple departments or sites (e.g., Enterprise Resource Planning (ERP)) a separate document may be appropriate. For simpler systems it is common practice to include the System Description in another specification or other document.

The development of the system description may begin early in the life cycle and evolve iteratively as the development process progresses. A complete system description meeting regulatory expectations should be established before the system is released for operational use.

The System Description should be subject to change control and periodic review.

3.2 Contents of the Document

Listed below are topics that may be required in the System Description depending on the nature and type of system. The guidance provided is intended to be neither prescriptive nor exhaustive.

The System Description should cover only the main features of the system. Detailed information on specific topics should be included in other specifications and not repeated.

3.2.1 *Introduction*

This should explain the context of the system within the business process and regulated company in general. This should be considered from the following perspectives as appropriate:

- departmental
- site-wide
- division-wide
- global

3.2.2 *Main System Functionality*

This is a description of the key functions of the system, both GxP and non-GxP (many of which could be business-critical). The functions may be grouped to maintain the description at a high level. The use of diagrams is encouraged to explain relationships between key functions.

3.2.3 *Regulatory Impact*

This should include a description of the key GxP functions of the system. The impact that the system has upon patient safety, product quality, and data integrity should be considered.

Other regulatory requirements should also be covered as appropriate.

3.2.4 *The Computing Environment*

This may be covered by a high level diagram of the architecture supporting the system covering, as appropriate:

- the infrastructure that supports the system (e.g., server configurations, storage arrangements)
- interfaces to users
- interfaces to equipment
- interfaces to other systems
- interfaces outside the company
- the flow of data through the interface
- Security features such as firewalls

3.2.5 *System Components*

An indication of the main hardware and software components should be provided. This may include information regarding servers and storage devices, as well as the operating systems, databases, and application layers. It should make reference to any configuration documentation relevant to the system. A detailed inventory of all components is not required here.

3.2.6 *System Interfaces*

This is an overview of the key interfaces to other systems and equipment, and the data flowing to or from the system.

3.2.7 *Access Control*

This is an overview of the access control features of the system, both physical (if relevant) and logical.

3.2.8 *Security Controls*

This is an overview of the established system security controls both physical and logical. These should include software for the protection of data and records, e.g., virus protection software.

3.2.9 *Electronic Records and Signatures*

An indication of the types of electronic records created and managed by the system, and the type of electronic signatures used should be provided, if relevant.

3.2.10 *Glossary*

Definitions of any terms that may be unfamiliar to the readership of the document should be provided.

Data Migration

1 Introduction

This appendix provides guidance for the migration of electronic data in the regulated environment. This covers planning, execution and reporting of the activity.

Migration activities should be focused on aspects critical to patient safety, product quality, and data integrity and their extent should be commensurate with risk, complexity, and novelty.

See the *GAMP Good Practice Guide: Electronic Data Archiving* (Reference 34, Appendix G3) for further details.

2 Scope

This appendix can be used by, or on behalf of, regulated companies to define quality and compliance-related procedures and standards for planning, executing, and verifying data migration activities.

This appendix does not cover routine transfer of data from one system to another as part of an on-going business process. Such situations should be covered by normal specification and verification activities.

3 Guidance

3.1 General Guidelines

Data migration is an activity that can occur often during the life cycles of the various computerized systems used by regulated companies. Data migration is the activity of transporting electronic data from one system to another, or simply the transition of data from one state to another. In practice, data migration efforts can vary greatly in scope, complexity, and risk, e.g.:

- An *in-place* version upgrade of a database or application
- Data conversion (e.g., from one supplier's database to another)
- *Same system* migration (e.g., transporting an application's data from one server platform to another)
- Migration from one source system to one target system
- Migration from multiple source systems to a target system

The complexity and risk of the data migration effort also may increase significantly if rules are used to select a subset of data from the source system, or if data is transformed (e.g., data type conversion, filtering, cleansing, aggregation, renormalization) prior to being inserted into the target system. The ultimate goal of any data migration is to have data that remains usable and retains its contextual meaning. Quality management controls should be in place to assure that data migration efforts are successful, compliant, and repeatable.

Each data migration should be managed within the framework of a Data Migration Plan and Report.

3.2 Quality Management

3.2.1 System Life Cycle

Data migration may take place multiple times during the life cycle of a single computerized system, e.g.:

- during initial system development and deployment
- during application upgrades
- during system retirement

Despite this, organizations that have defined a system life cycle may not have a defined or documented data migration process. As with other life cycle phases and activities, data migration efforts will be more consistent and successful if the life cycle contains procedures, tools, templates, and examples for data migration. A comprehensive life cycle should provide guidance for all aspects of data migration including roles and responsibilities, documentation requirements, quality and compliance controls, technical and verification activities, and project management. A standard operating procedure (SOP) may be the best method for describing and documenting the process, including quality and compliance requirements.

3.2.2 Risk Management

The life cycle should include an established risk management process with guidance for assessing risks that are specific to activities related to computerized systems. In addition to risks typically found with technology projects, the following should be evaluated when migrating regulated data:

- The inherent quality and compliance risk associated with the data being migrated i.e.
 - Impact upon patient safety, product quality, and data integrity
 - Risk associated with the business processes that the computerized systems involved are supporting
- Risk to the business due to systems being unavailable or data being unreliable
- The level of complexity (e.g., multiple source or target systems; multiple phases; a high degree of data transformation)
- Technology risk due to the use of complex or leading edge systems or tools

3.2.3 Configuration Management and Change Control

Migration of electronic data in the regulated environment should be performed under change control. Similarly, all appropriate data migration project documents and tools should be controlled using configuration management.

During a data migration project, system changes unrelated to the migration should be prohibited. This is because the success of a data migration effort depends on various characteristics of the systems (e.g., software versions, database schemas) remaining unchanged during the project. Unrelated system changes can increase the complexity of the data migration effort, which will in turn increase the overall project risk.

Typical good practice is to use one or more intermediate staging areas for data that has been extracted from source systems, prior to being loaded into the target system. A typical migration effort will include at least three system platforms or areas that should remain under configuration management during the entire project: the source system(s), the staging area, and the target system.

3.3 Areas of Concern

3.3.1 *Fitness of Software Tools for Intended Use*

Data migration efforts typically involve the use of software tools to automate some or all of the extraction, transformation, loading, and verification activities. These tools tend to be GAMP software Category 1 infrastructure tools (e.g., database migrators, and verifiers purchased from a software supplier) or Category 5 custom application (e.g., SQL scripts, C programs developed in-house).

The infrastructure tools should be fit for intended use. The rigor of related specification and verification activities should be commensurate with associated risks. Depending upon the scope, complexity, and customization of the software tools being used, required deliverables may range from evidence of basic testing to full software specifications and formal verification. A Subject Matter Expert (SME) should ensure that appropriate life cycle activities and deliverables are identified and executed. The Quality Unit should review and approve key documentation in accordance with company procedures.

For software tools that move or transform data, there are three principal areas of risk:

1. data will be moved or transformed incorrectly or incompletely
2. data already residing in the target system will be harmed
3. in the case where not all data is being migrated, residual data in the source system is adversely affected by the removal of the migrated data

In theory, these risks would require that a high level of effort be applied to demonstrate the fitness for intended use of software migration tools. In practice, however, through the use of data verification the risks can be significantly mitigated and therefore the rigor of software migration tool verification can be reduced. It should be noted that the development and approval of a data mapping table (i.e., fields from the source system data model mapped to the target system data model) is still necessary when using software migration tools.

3.3.2 *Data Verification*

Data should be verified each time it is moved (either within a system platform or from one system to another) or its state is transformed. There are two general types of post-migration data verification: test environment verification and operational environment verification.

In test environment verification a target test system is initially populated with data, then a migration test run is performed, and finally data in the target test system is verified to show that all required data migrated successfully and without adversely impacting existing data. This verification provides objective evidence that the data migration software tools are fit for intended use, and also provides a level of confidence in the overall migration process. A typical approach during this step is to work with a relatively small amount of data, which can then be completely verified to assure that no data errors occurred.

The intent of operational environment verification is the same: to verify the outcome of the migration process on both migrated and existing data. The amount of data involved, however, typically is very large and, therefore, more difficult to verify. There are two general approaches to solving this problem: data sampling and automated data verification tools. In data sampling, a statistical sample of the population of migrated data and/or existing data is verified in the target system. Standards such as ANSI/ASQ Z1.4 and ISO 2859 (References 29 and 21, Appendix G3) may be used to determine the appropriate sample size to verify the conformance of the entire population of data at the desired level of confidence.

As an alternative to sampling, automated software tools can be used to verify 100% of data in the target environment. However, such software tools present the highest level of risk and accordingly their suitability should be rigorously determined.

Data mapping and transformation are not the only issues to be addressed. An important part of data migration is confirming that all of the required data has been migrated. Verification techniques, such as checksum, can be used to corroborate complete data transmission.

Objective evidence of data verification should be generated. Verification scripts and data sheets, screen shots, error logs, and hardcopy reports should be created when appropriate and feasible.

3.3.3 Reliability of Source Data

If the source system is maintained in compliance with regulatory requirements, then the combination of the source system's controls and the controls exercised during the migration process should provide sufficient assurance of the accuracy and integrity of the migrated data. To document this, the data migration plan should reference the appropriate source system documentation.

If the status of the source system is unknown then two problems exist: first, the veracity of data migrated from the source system may not be verifiable; second, the migrated data will mix with reliable data already in the controlled target system. After the migration effort is complete, the trustworthy existing data and the questionable migrated data will be indistinguishable unless steps are taken to identify the migrated data as such (e.g., differences in record dates and notations in user-defined fields). If this is not possible, then the possible data inconsistencies should be documented explaining the controls in place on the source system and justification of why the migrated data should be trusted.

3.3.4 Usability of Migrated Data in Target System

There are three main issues to consider relating to usability of migrated data on a target system:

- target system functionality does not allow performance of tasks previously carried out in the source system
- lack of completeness of migrated data affects the usability of the data
- It may not be sufficient to migrate the data. Separate migration of metadata or configuration of the target system also may be required. For example, the source data has some access rights defined for it, such as user groups and user rights. Migrating the data may not normally migrate this metadata, which is normally separate from the data. However, these user groups and rights also may be required on the target system.

3.3.5 Audit Trails

Audit trails can be problematic for data migration efforts. If the target system has an audit trail but the source system does not, documentation should be created reflecting that auditing for migrated records began when they were loaded onto the target system. If possible, these records should be distinguishable from records that were created on the target system (e.g., using a notation in a user-defined field).

If both the source and target systems have audit trails and it is technically feasible, the audit trail should be migrated along with the audited data. If it is technically unfeasible to migrate the audit trail (e.g., due to data transformation) or if it would constitute too great a risk to do so, then the original audit trail should be archived in a format that can be retrieved over time.

When possible, a computer-generated audit trail should be created during the movement and transformation activities associated with the data migration effort; because this audit trail serves not only as a verification tool for the migration team but also as a historical record of changes to the data, it should be archived in a format that can be retrieved over time.

3.4 Data Migration Plan

Different data migration efforts can require very different activities and deliverables. This appendix is not intended to provide specific project or technical methodology guidance. However, every data migration project should have a data migration plan as a required deliverable. Similar to plans for computerized system development projects, the data migration plan serves as a high-level roadmap that guides project team members in performing a compliant and successful technical effort.

The data migration plan should describe the entire migration process, including as a minimum:

- migration project purpose and scope
- system description(s)
- roles and responsibilities
- required deliverables
- risk management strategy
- configuration management strategy, including the source, staging, and target environments
- software tool overview and strategy for ensuring compliance and fitness for intended use
- migration steps and technical activities
- data mapping and modeling activities
- transformation rules
- data verification strategy and acceptance standards
- cutover plan
- rollback strategy

The data migration plan should be approved by the process owner, system owner, Quality Unit, and SMEs as appropriate.

It may be appropriate to reuse the same data migration plan more than once. An example of such reuse is the deployment of an electronic document management system (EDMS): the approved data migration plan can be used multiple times as different functional groups or geographic sites migrate their electronic documents into the system. Each time the plan is executed, a data migration report should be created.

3.5 Data Migration Report

The data migration report summarizes the activities that were conducted during the data migration effort. It describes any anomalies or deviations that were encountered and lists the results of verification activities (including objective evidence as appropriate). Because the report will be used to establish the reliability of the migrated data, it should clearly state the overall outcome of the migration activity (e.g., full success, partial success, failure).

The data migration report should be approved by the process owner, system owner, Quality Unit, and SMEs as appropriate.

In the case where data migration is being performed as part of a computerized system project, such as a system replacement or upgrade, the data migration report can be documented as appropriate within the project documentation, and may not need to be a separate document.

Introduction to Operation Appendices

1 Introduction

The Operational Appendices have been constructed to present information in a consistent and accessible manner. Each Appendix starts with a brief description of the process and remaining sections are organized as follows:

- **Key Requirements:** a brief statement of the critical controls (processes and records) that should be in place for that process.
- **Process Outline:** a high-level schematic of the operational support or review process.
- **Guidance:** further guidance regarding each process and its application.

2 Objectives

The objective is to present practical and relevant guidance to ensure that:

- Areas relating to maintaining compliance and fitness for intended use of GxP regulated computerized systems throughout their life cycle are covered
- Interrelationships between these operational support processes are understood
- Scalability is appropriately considered, i.e., the controls can be implemented at a level of formality and complexity appropriate to individual organizations and across a wide range of systems: straightforward controls for simple systems; more sophisticated tools and procedures for systems with increased impact, size, and complexity.

Note: While the operational management and control procedures may be combined in different ways by different organizations, and the level of detail contained in these procedures may vary, organizations should ensure that all the elements of the key requirements are met and are verifiable. Suitable evidence should be generated and retained, but procedures should not commit organizations to producing evidence that will normally not be generated.

3 What Organizations should do

3.1 Introduction

In view of the diversity of computerized systems and organizations, it is not considered appropriate to be prescriptive regarding how operational controls are implemented.

To ensure compliance with regulatory expectations regulated companies should be able to demonstrate that they have considered and reviewed the maintenance and support needs for each system and decided what procedures, processes, and records should be established and maintained.

Table O.1 shows how operational processes are related and how they may trigger other operational processes.

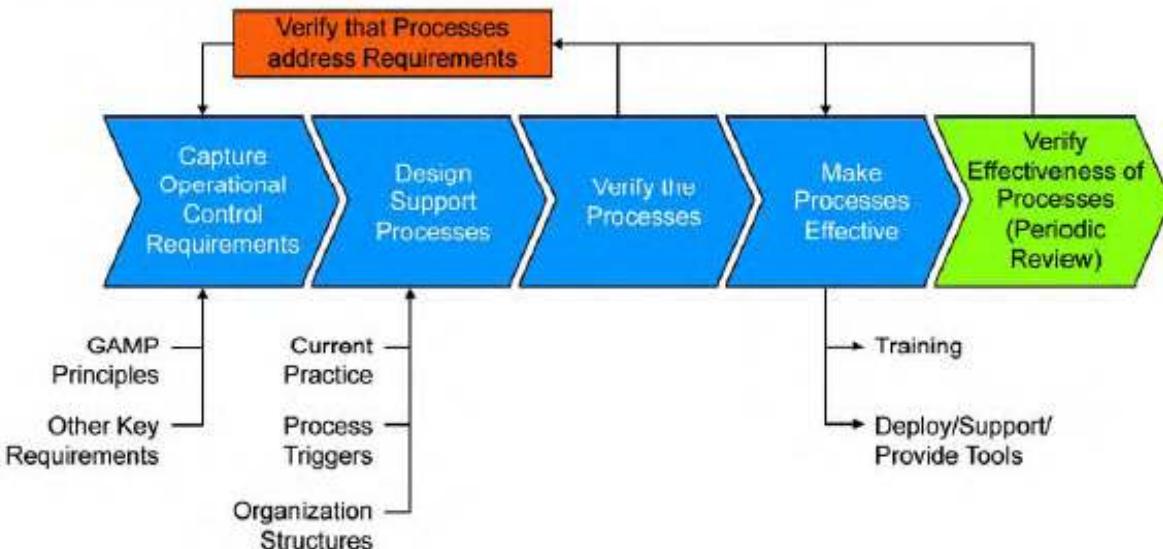
A possible approach to establishing operational control is discussed in the following sections of this appendix.

The key steps of this approach include:

- capture operational control requirements
- design support processes
- verify the processes
- make the processes effective
- verify effectiveness of processes

The relationship between these steps is shown below and described in this appendix.

Figure O.1: Establishing Operational Control



3.2 Capture Operational Control Requirements

Key operational control requirements for each of the processes are identified within the Operational Appendices.

An organization should be able to demonstrate that processes to achieve these requirements are established and that records are maintained for the required retention period to demonstrate that controls are effective.

The interrelationships between these processes should also be considered in order that operational incidents and changes to systems during their operational life cycle are effectively managed, and that the security and integrity of critical records and processes are maintained.

An organization should try to achieve a consistent approach regarding how these issues are addressed across systems. Business and regulatory requirements that may be within the scope of activity of the organization's operations, e.g., Environmental, Health and Safety (EHS) regulations, Sarbanes-Oxley (SOX) controls, Privacy and Data Protection regulations, and any local regulations should be considered.

3.3 Design Support Processes

Current practices for the operational management of existing systems within the organization need to be understood before developing a detailed plan for the implementation of operational controls. There may be a significant number of support and review processes established, which already may have been subject to audit and review.

Where there are existing processes a gap analysis can be developed against the operational control requirements statements in order to identify improvement activities.

Controlling procedures which describe the processes should be practical. A definition of the current processes should be produced by consulting those involved. It is generally better to improve and simplify existing processes rather than to create new procedures.

Where a gap is identified and there is no current process supporting a set of key requirements a new process will need to be designed and implemented. The need to understand how the various processes interrelate is critical to maintain operational control; process design should consider how other processes may be triggered and responsibilities for each process step should be clearly assigned.

A critical consideration in the design of processes and the creation of procedures is the organizational structure of the enterprise; this will determine who has overall responsibility for each process and who is responsible for task steps within the process. For small organizations some of these controls may be achieved through the consistent application of written procedures. For larger organizations electronic systems may be used to assign roles and permissions, keep track of critical records, and ensure that activities are notified to the correct individuals or teams and escalated appropriately e.g., in the case of service or control failures.

3.4 Verify the Processes

Once the processes have been established and procedures documented they should be verified to ensure that the required control is in place.

3.5 Make Processes Effective

Once the processes have been verified they should be deployed consistently throughout the organization. This may be achieved by an implementation plan which should include a communication plan and the roll-out of training where appropriate.

3.6 Verify Effectiveness of Processes

For GxP regulated systems the Quality Unit should be involved in the review and approval of operational processes. The scope and depth of involvement of the Quality Unit depends on the impact of a system on patient safety, product quality, and data integrity, and should be documented.

The Quality Unit should verify effectiveness by audit and review of operational control processes using internal assessment tools and Periodic Review.

Appropriate metrics help to ensure key performance indicators are being met and to support investigation or improvement initiatives.

4 Process Relationships

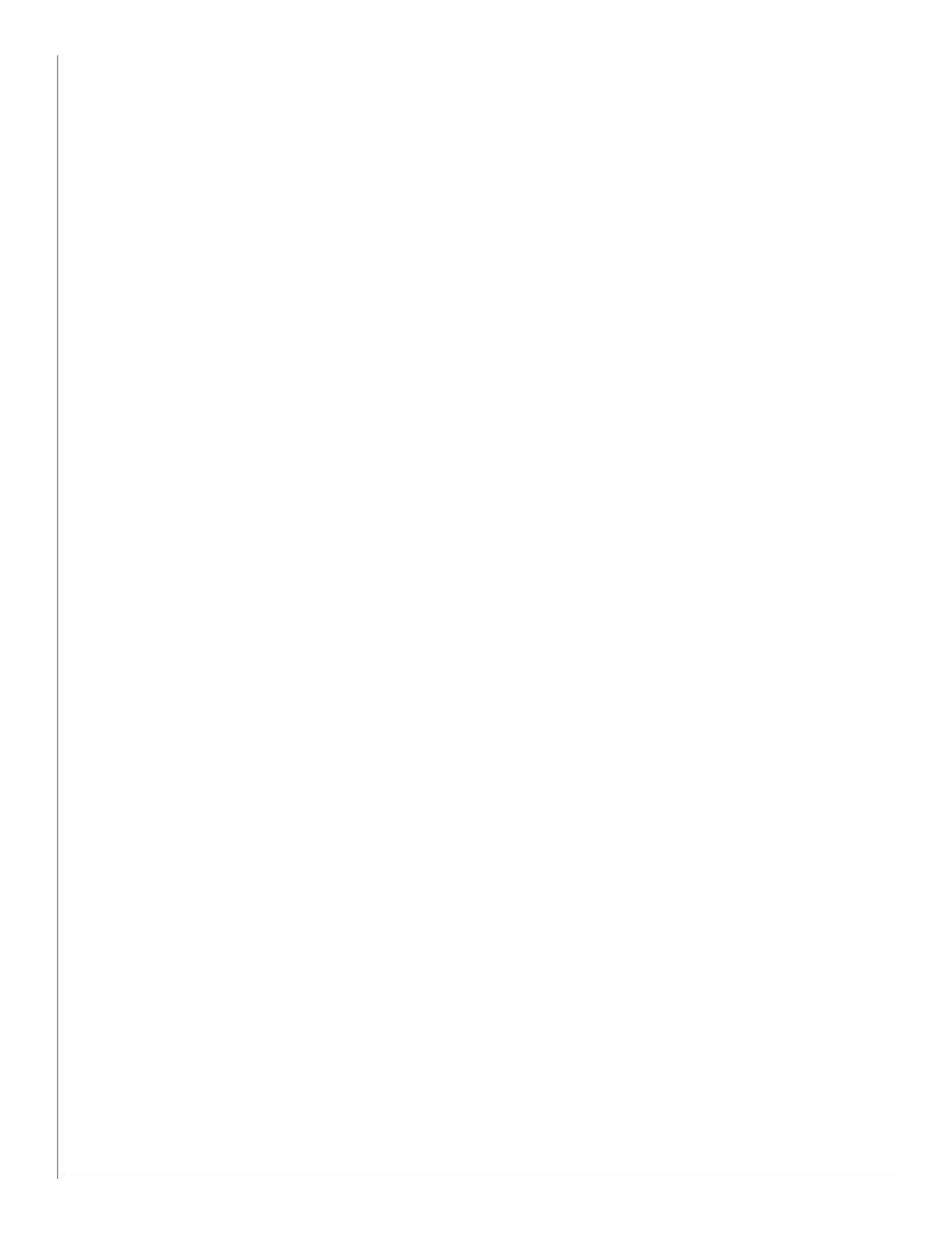
Table O.1 shows the interrelationships and dependencies between operational management processes and other GAMP processes.

This table is intended to help organizations implement a comprehensive set of operational processes and records in a structured way by:

- Ensuring completeness: showing which processes should be supported by controlling procedures.
- Providing an aid to navigation: supporting users when undertaking an impact analysis to establish what other processes may be triggered.

Table O.1: Interrelationships and Dependencies between Operational Management Processes and other GAMP Processes

	O1 Handover	O2 Establishing and Managing Support Services	O3 Performance Monitoring	O4 Incident Management	O5 Corrective and Preventive Action	O6 Operational Change and Configuration Management	O7 Repair Activity	O8 Periodic Review	O9 Backup and Restore	O10 Business Continuity Management	O11 Security Management	O12 System Administration	O13 Archiving and Retrieval	D7 Data Migration	M10 System Retirement
O1 Handover															
O2 Establishing and Managing Support Services	c		t	t	t		c								
O3 Performance Monitoring	c	c			t	t	c/t		t						
O4 Incident Management	c	t	t/c				c	t		t	t	t			
O5 Corrective and Preventive Action	c	t	t	t			t		t						
O6 Operational Change and Configuration Management	c		t	t	t	t	c		t						
O7 Repair Activity	c		t/c	t	t		c		t						
O8 Periodic Review	c			t	t										
O9 Backup and Restore	c			t	t		c		t					t	t
O10 Business Continuity Management	c			t	t		c								
O11 Security Management	c			t	t		c								
O12 System Administration	c			t	t		c								
O13 Archiving and Retrieval	c					t	c							t	
D7 Data Migration	c					t	c						t		t
M9 Document Management	c			t	t	t	c								t
M10 System Retirement	c					t	t								
The following topics do not have a dedicated Appendix but are covered in appropriate sections of GAMP 5:															
• Training		c			t	t	t	c		t	c				
• Calibration		c			t	t	t	t	c						
• Application Specific Operational SOPs		c			t	t	t	c							
• Life Cycle Processes and Procedures Including Specification and Verification		c				t	t	c							t



Handover

1 Introduction

Handover is the process for transfer of responsibility of a computerized system from a project to operation.

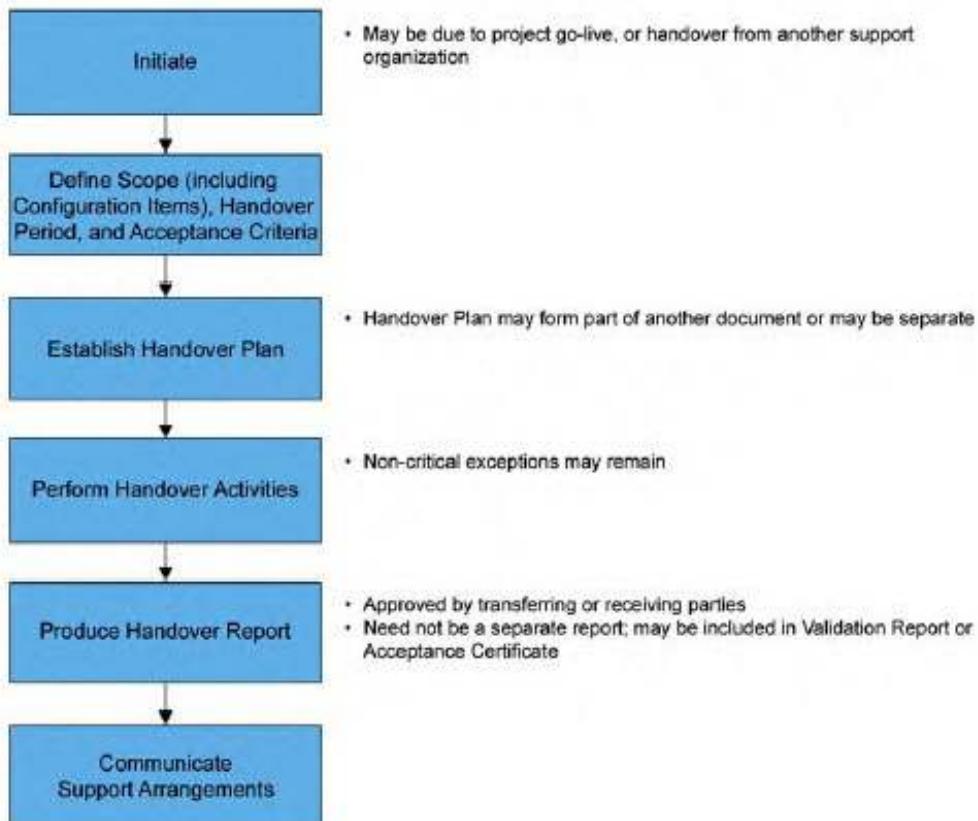
2 Key Requirements

Regulated companies should be able to demonstrate formal acceptance of systems after testing and controlled transfer into the live operational environment.

These activities should be documented.

3 Process

Figure O1.1



4 Guidance

4.1 General Approach

The project management approach should include a process for Handover of a system from the project phase into the operational phase. A checklist may be used to ensure acceptance and transfer of responsibilities during handover.

Handover may involve the transfer of the system and associated support processes from one Quality Management System (QMS) to another, and this transfer should be carefully controlled, documented, and communicated.

An important aspect of handover is establishing the agreement for the (justified) closure or transfer of any open issues and incomplete activities or documentation from the project implementation environment into the operational environment.

Particular attention should be given to incomplete issues which could have an impact on GxP and where non-completion could compromise the compliance status of the system.

4.2 Responsibilities

The Project Manager is responsible for preparing the system for handover and the process owner and system owner are responsible for accepting the system into operational use. The responsibility for completion of any outstanding actions at the point of handover should be agreed between the parties.

Consideration should be given to defining a period for monitoring the system after handover and to defining a rollback strategy in the event of a significant problem during the monitoring period.

Establishing and Managing Support Services

1 Introduction

The process for Establishing and Managing Support Services ensures that support services (whether internal or external) are appropriately specified and managed. This is often managed through the use of Service Level Agreements (SLA).

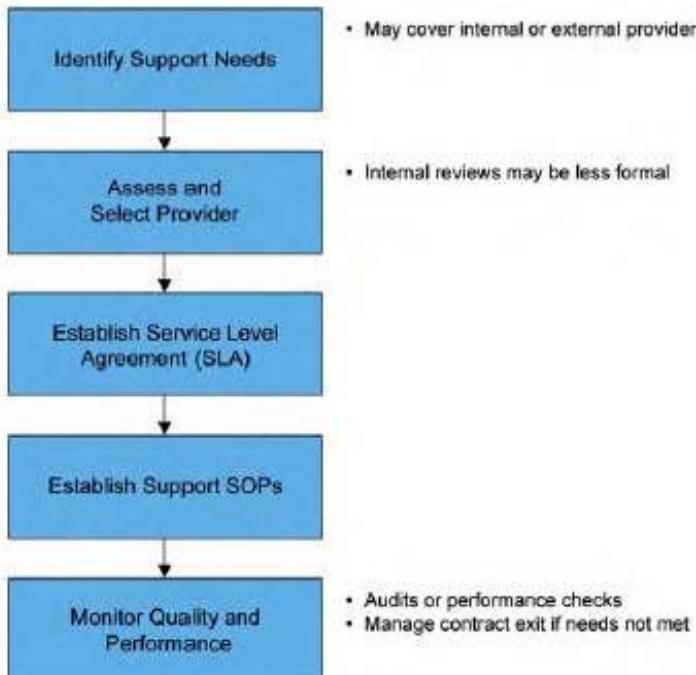
2 Key Requirements

When suppliers are used to provide a service, there should be a formal agreement including a clear statement of the responsibilities of that supplier.

In this context *supplier* is interpreted as meaning both external third parties and internal departments managed under different authority.

3 Process

Figure O2.1



4 Guidance

4.1 General Approach

Maintaining a system in a state of compliance is often dependent upon services provided by organizations outside the direct control of the system owner. Some of the organizations providing service may be sub-suppliers, providing the service to the system owner indirectly through another supplier.

One service level model is defined by ITIL, which defines the Service Level Agreement (SLA) as an Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer.

SLAs may be established separately for individual systems or to cover groups of similar systems (e.g., instruments in a single laboratory).

It may be useful to have a common format for SLAs, and regulated companies should consider having a Standard Operating Procedure (SOP) to describe how to prepare an SLA. A risk-based approach to the content and detail should be considered.

The SLA should be agreed, understood, and approved by both the system owner and the service supplier.

The capability of the service supplier should be assured and monitored using appropriate supplier assessment processes.

While this appendix focuses on the use of SLAs there may be a hierarchy of agreements established which may include the following in addition to SLAs.

- Operating Level Agreement (OLA): An Agreement between an IT Service Provider and another part of the same Organization. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties.

An example is an agreement between a primary support organization and a storage management group regarding the time required to restore a file or application.

- Underpinning Contract (UC): A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.

An example is a contract between a regulated company and a telecommunications provider for maintenance and troubleshooting of the company's Wide Area Network (WAN).

Contractual and legal implications associated with SLAs, OLAs, and UCs are outside the scope of this Appendix.

4.2 Responsibilities

It is the responsibility of the system owner to ensure that support needs are identified and that an SLA is established, followed, monitored, and reported upon. It is the responsibility of the system owner to ensure that the service supplier is subject to the appropriate supplier assessment processes.

It is the responsibility of the service supplier to ensure the competency of the support staff, and that they are appropriately trained and work in compliance with the agreed procedures and SLA.

It is the responsibility of the support organization identified in the SLA to execute the terms of the SLA.

4.3 General Guidelines

The SLA should unambiguously define the system to be supported. It should define how the service is to be provided, and define responsibilities of the support staff and the system owner's organization. It also should be possible to measure the performance of the support service being delivered against the requirements defined.

The service supplier should maintain adequate procedures to underpin the support service agreed with the regulated company in the SLA. These should be documented in the service suppliers internal SOPs and other procedures and may be supported through OLAs with internal partners and UCs with external partners. The regulated company should reserve the right to verify that this is the case, through review or audit.

The service supplier should be assessed for suitability against defined criteria, and this assessment should be documented. An audit of the supplier should be considered. This assessment can contribute key information to the development of the SLA as it helps to set the baseline for service capabilities. See Appendix M2 for further details.

4.4 Contents of the Document

Listed below are topics that may be included in the SLA. The guidance provided is intended to be neither prescriptive nor exhaustive.

4.4.1 *Introduction*

The introduction should provide the following information:

- purpose of the document
- the contractual status of the document
- relationship to other documents

4.4.2 *Scope*

The scope should describe:

- definition of the covered system(s)
- any exclusions
- duration of the SLA

4.4.3 *Roles and Responsibilities*

The roles and key responsibilities relating to the SLA should be defined, in terms of organizational groupings.

4.4.4 *Service Description*

The service to be provided should be described. Each computerized system component and process to be supported should be identified (at an appropriate level of granularity) and the level of service required for each should be identified. A typical SLA should address the following, as applicable:

- fault reporting and response, including feedback processes
- prioritization of faults
- escalation processes
- resolution and closure
- installation of software patches and upgrades
- software backup
- data backup
- data archiving
- system management, administration and housekeeping
- support of underlying hardware and infrastructure
- routine testing and calibration
- use of escrow accounts
- business continuity and disaster recovery
- handling usage queries and questions
- providing workarounds
- maintenance of spares and consumables
- software tools to be used
- retention and retrieval of records – including archived records

The information should be provided in terms of processes and measurable performance targets. Specific details, such as names, costs, and phone numbers should not be included, but listed in separate appendices (see Section 4.4.8 of this Appendix).

4.4.5 Measurement and Reporting

The method of monitoring and reporting service performance should be defined, in terms of:

- what is to be measured, referencing the performance targets set in Section 4.4.4
- how it is to be measured, including any calculations required
- who is responsible for collecting the data
- the format and frequency of summary reports, and the target audience
- the process of responding to queries on, and challenges to, the reports produced

4.4.6 Service Review

The need for and extent of reviews of the service being provided should be defined. Topics to consider include:

- performance against targets, using the summary reports as input
- specific user or service supplier concerns
- emerging trends
- required attendees
- frequency
- implication of need to refine or upgrade agreements

Service reviews should be conducted annually, as a minimum, or more frequently if required.

4.4.7 Glossary

Definitions of any terms that may be unfamiliar to the readership of the document should be provided.

4.4.8 Appendices

Contract specific information, and details that may vary from time to time, should be provided. Typical appendices include:

- contact points (customer and service supplier)
- escalation contact details
- report distribution lists
- fixed costs
- charge out rates
- contractual terms and conditions

Performance Monitoring

1 Introduction

Performance monitoring is that part of overall preventive maintenance that obtains performance data that is useful in diagnosing system problems. It provides trends that may indicate performance problems, which can be used as part of Corrective and Preventive Actions (CAPA) to reduce application or system down time.

There also is potential to use the performance monitoring data to influence other operational processes, such as:

- change management, where it can be used to support risk and impact assessment, and evaluation of any proposed change and the subsequent effect of implementing the change.
- periodic review, where it can assist in the evaluation of whether the system is performing according to specification.

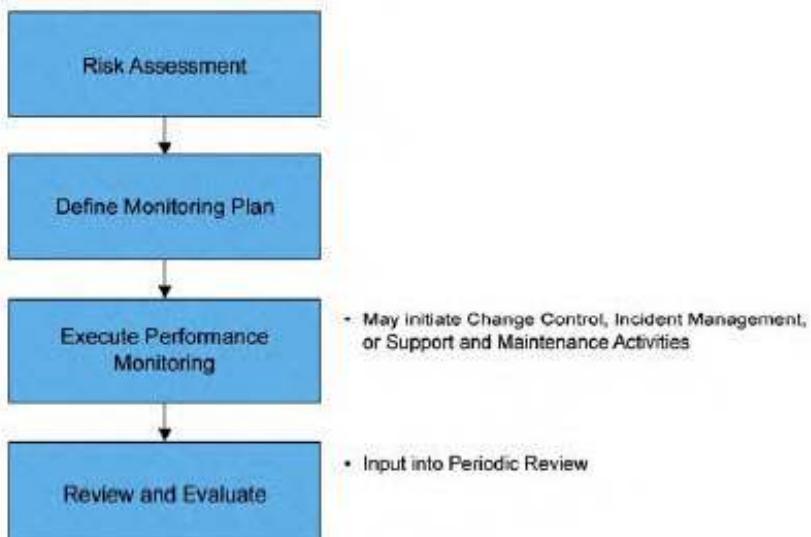
2 Key Requirements

The need for, and extent of, monitoring activities should be based on risk to patient safety, product quality, and data integrity.

Appropriate performance parameters to monitor should be defined based on the identified risks.

3 Process

Figure O3.1



4 Guidance

4.1 General Approach

Performance Monitoring Plans are usually system specific. However, it may be helpful to put in place a Standard Operating Procedure (SOP) on how to author these plans and it may be possible to develop some generic monitoring parameters (see list in Section 4.3 of this appendix).

The level of detail in the plan should reflect the risk, complexity, and novelty of the system. For simple or low risk systems a performance monitoring plan may not be needed; any applicable aspects may be covered by another document.

Performance Monitoring Plans may be integrated into the Establishment and Management of Support Services via a Service Level Agreement (SLA).

Performance monitoring may be an automatic or manual process, or more often a combination of both.

Performance monitoring records should be subject to periodic internal audits.

4.2 Responsibilities

It is the responsibility of the system owner to ensure that a system's performance is monitored and appropriate action taken.

It is the responsibility of the system owner to inform the process owner and Quality Unit of any performance issues that could have an impact on patient safety, product quality, and data integrity, and to invoke the Incident Management process.

4.3 Parameters to be Monitored

Depending on the GxP risks of the applications running in the environment and the type of computer equipment, the following system conditions may be checked with suitable tools at appropriate intervals:

- servers/workstations/PCs/control systems:
 - CPU-utilization
 - cache-utilization
 - interactive response time
 - number of transactions per time unit
 - average job waiting time
 - disk capacity utilization
 - I/O-load
 - system error messages, including operating system fault and warning messages

- hardware status (e.g., condition or readiness of Uninterruptible Power Supplies(UPSs))
- existence of critical batch jobs
- existence of critical processes
- availability of printer queues
- alarms
- network:
 - availability of components (e.g., server, router)
 - network load (e.g., number of collisions)
 - broadcasts
- applications:
 - monitoring of application error messages
 - response times
 - number of concurrent users
 - overall system availability to users

Note that these conditions are examples only, and not a complete list.

4.4 Notification Mechanisms

Depending on the risk of the monitored parameter, mechanisms such as one or more of the following should be chosen to notify appropriate personnel of exception conditions:

- message on the system console
- email to system operator
- email to external services
- pager message to system operators
- printed lists or logs
- audible or visual alarms

4.5 Structure of a Monitoring Plan

The monitoring plan should cover the following areas. A tabular format is recommended.

- the monitored parameter (see Section 4.3 of this appendix)

- warning limit
- frequency of observation
- monitoring tool
- notification mechanism and person/system to be informed
- documentation of the monitoring results
- period of storage of the results

The Monitoring Plan should be documented. An example template is provided separately.

4.6 Review of the Monitoring Plan

The following items should be checked during the review of the monitoring plan:

- appropriate parameters and components are monitored
- the risks determined in the risk analysis have been addressed appropriately
- the time intervals and the warning limits for the observed parameters are adequate
- the methods of notification are used and allow timely alert
- the monitoring results are retained safely and securely

Incident Management

1 Introduction

The primary objective of Incident Management is to ensure that any unplanned issues that could impact patient safety, product quality, and data integrity are addressed before any harm occurs.

The Incident Management process should also be designed to return the system or service to users as quickly as possible.

The Incident Management process is related to many other support processes as shown in the Table O.1 in Section 4¹ of the Introduction to the Operational Appendices.

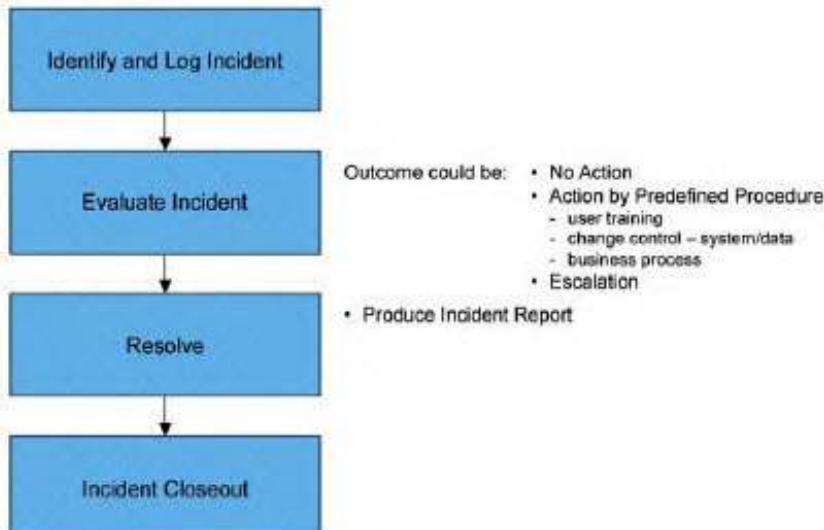
2 Key Requirements

The incident management process should ensure that operational events which are not part of the standard operation (i.e., issues, problems, and errors) are identified, evaluated, resolved, and closed in a timely manner.

These activities should be documented.

3 Process

Figure O4.1



¹ Note that ITIL closely links Incident Management with Problem Management, where multiple related Incidents are analyzed and addressed with corrective actions. In this guidance, the parallel process with which Incident management interfaces is CAPA.

4 Guidance

4.1 General Approach

This process and procedure is typically generic and can be applied to all systems.

Incidents should be assessed for any impact on patient safety, product quality and data integrity; the Quality Unit should be consulted when setting up criteria for this assessment, and during assessment of the incident as required. Decisions and resolutions should be based on this assessment.

Incidents should be trended over time to identify and understand possible systemic issues and root causes.

Incident Management records should be subject to periodic internal audits.

4.2 Responsibilities

It is the responsibility of the process owner to ensure that an Incident Management process and procedure are in place that can be used to support the system.

It is the responsibility of the appropriate SME to assess incidents, to consult with the Quality Unit for those with potential impact on patient safety, product quality and data integrity, and to apply appropriate corrective action.

It is the responsibility of the system owner to ensure that incidents are progressed and closed as appropriate.

It is the responsibility of the Quality Unit to assure that incident procedures are followed and appropriate actions have been taken and documented.

4.3 Help Desks

Help desks are often the first point of contact for incident management. Help desk personnel should be trained to recognize circumstances where incidents should be fed directly into the CAPA process, and help desk procedures should facilitate analysis of incidents to recognize patterns which may require CAPA.

Corrective and Preventive Action

1 Introduction

Corrective and Preventive Action (CAPA) is a process for investigating, understanding, and correcting discrepancies while attempting to prevent their recurrence, and for recognizing potential discrepancies to prevent their occurrence. The equivalent process as defined in ITIL is Problem Management.

The CAPA process is closely associated with the Incident Management process and the Repair process.

2 Key Requirements

The CAPA process should cover:

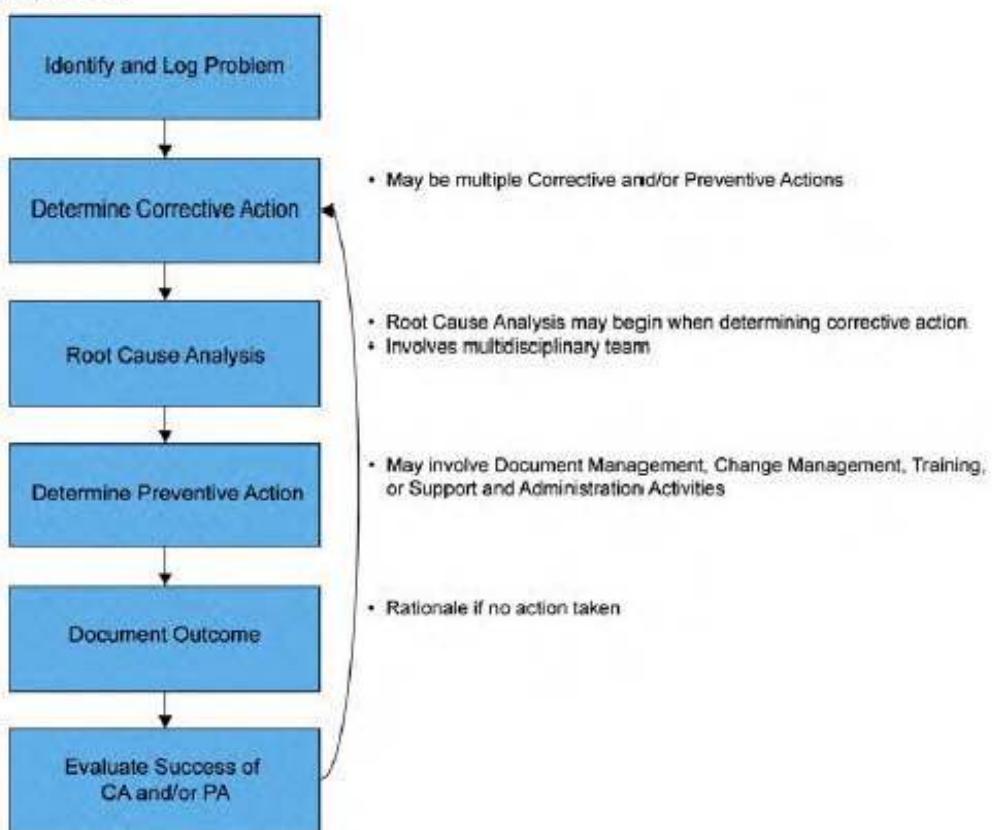
- remedial corrections of an identified problem or potential problem
- root cause analysis with corrective action to help understand the cause of the deviation and potentially prevent recurrence of a similar problem
- preventive action to avert recurrence of a similar potential problem

A procedure should be established to record and analyze incidents and to enable corrective action to be taken.

These activities should be documented.

3 Process

Figure O5.1



4 Guidance

4.1 General Approach

The CAPA process is usually generic in nature, i.e., one process can be applied to all systems. Consideration should be given to whether one CAPA log is maintained for all systems, or whether it is more appropriate to maintain one CAPA log for groups of similar systems, or for each system individually.

Any corrective or preventive action taken to eliminate the causes of actual or potential nonconformities should be to a degree appropriate to the magnitude of problems and commensurate with the risks encountered.

CAPA records should be subject to periodic internal audits.

4.2 Responsibilities

It is the responsibility of the process owner to ensure that a CAPA process is in place and implemented for the system, and responsibilities are often delegated to the system owner.

It is the responsibility of the Quality Unit to assure that CAPA procedures are followed and appropriate actions have been taken and documented.

It is the responsibility of the appropriate subject matter experts (SMEs) to ensure that the agreed corrective and preventive actions are taken and completed.

Operational Change and Configuration Management

1 Introduction

Change management is the process of controlling the life cycle of changes. The primary objective of change management is to enable beneficial changes to be made, without compromising regulated processes or records and with minimum disruption to services.

Configuration management comprises those activities necessary to be able to precisely define a computerized system at any point during its life cycle, from the initial steps of development through to retirement.

Configuration management and change management are closely related. When changes are proposed, both activities need to be considered in parallel, particularly when evaluating impact of changes.

Both change and configuration management processes should be applied to the full system scope including hardware and software components and to associated documentation and records, particularly those with GxP impact.

This appendix covers operational change and configuration management.

Change and configuration management during project development phases is covered by Appendix M8.

The point of transfer from project to operational change management should be clearly defined before handover to operational use.

2 Key Requirements

Operational change management, once established, should continue until system retirement. If data is retained after system retirement, management of that data should continue to be subject to change control.

All changes should be reviewed, impact and risk assessed, authorized, documented, tested, and approved before implementation. These activities should be documented.

The hardware and software configuration of the system should be documented throughout the life of the system. The level of formality is greater for an operational system than for a system early in its development, but the principles are the same. The level of detail should be sufficient to allow the system to be effectively and efficiently rebuilt in the event of complete system loss.

Relevant documentation should be updated as part of a change.

Testing of changes should be commensurate to the risks to patient safety, product quality, and data integrity introduced by the change. Testing should prove that:

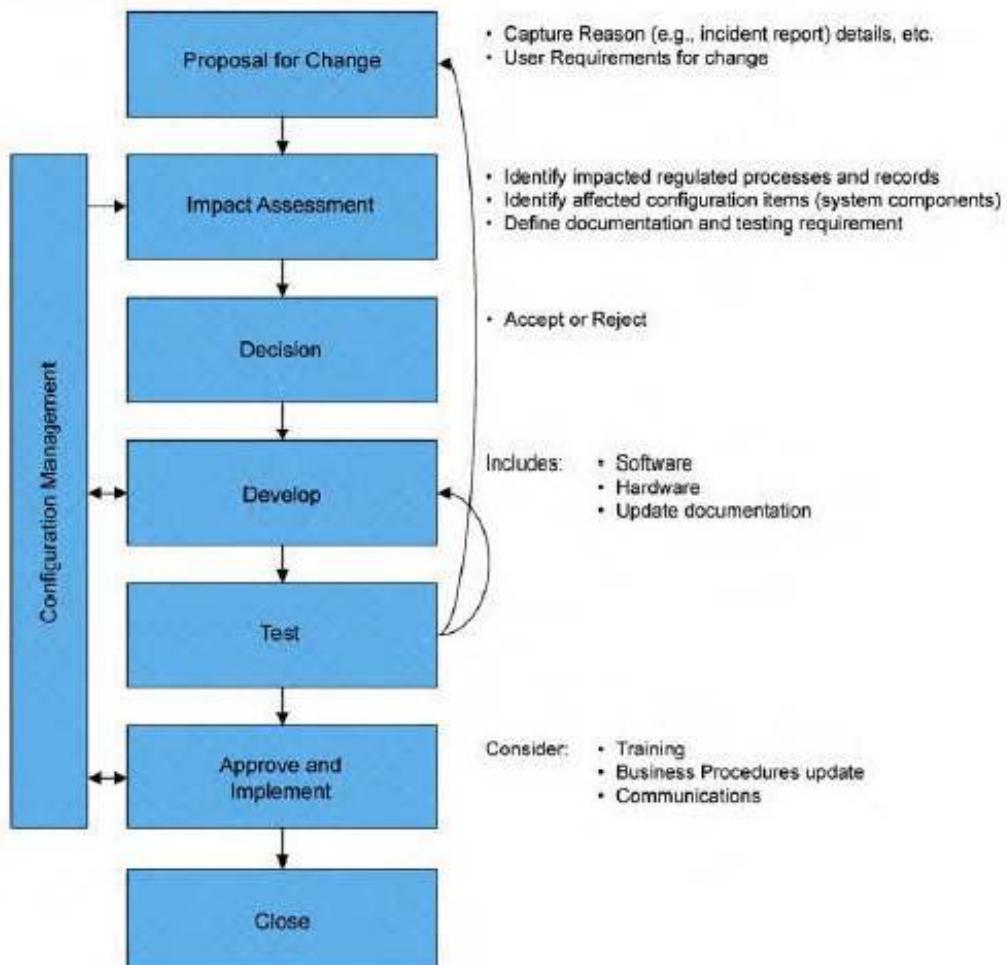
- The new or changed system function behaves as specified
- The change has not introduced unforeseen consequences to other parts of the system's function or to related or interconnected systems' functions.

The original system risk assessments used to define initial system functional testing can provide a good basis for the scope of testing functional changes. It should be noted that the changes implemented may trigger the need for revised risk assessments.

Where required, user training should be updated and delivered, and business process standard operating procedures should be updated before implementation of changes.

3 Process

Figure O6.1



4 Guidance

4.1 General Approach

The change control and configuration management process and procedure are usually generic in nature, i.e., the same process can be applied to many or all systems.

Example forms to assist with the processes of managing a change are provided separately.

4.2 Responsibilities

It is the responsibility of the process owner to ensure that a change control and configuration management process and procedures are in place that can be used to support changes to the system.

It is the responsibility of the Quality Unit to assure that the process and procedures are followed.

It is the responsibility of each member of the team associated with each change to execute that part of the process assigned to them accurately and completely.

4.3 Change Management

The point of transfer from project change management (see Appendix M8) to operational change management should be clearly defined and documented, e.g., in the computerized system Validation Plan, validation report, system release documentation, or other means.

Operational change management should start no later than handover for operational use, where handover is defined as the point that the process owner accepts the system from the project team into operational use, once the system, its documentation, and support arrangements are agreed and in place.

The change process should address the following key steps:

- describe the proposed change
- document and justify the change
- evaluate risks and impact of the change
- accept or reject the request for change
- develop and verify the change
- approve and implement the change
- close the change

When changes are undertaken, system specifications should be reviewed and where appropriate they should be updated and reapproved.

Specific processes or variations to the standard process may be required for the following types of changes:

- *Like-for-like replacements.* These changes can be controlled by maintenance procedures designed to control materials usage and record system history. Like-for-like is not always easy to assess and consideration should be given to their impact. See Appendix O7.
 - *System Administration Changes.* Some system administration activities may involve changes to system components. Any such changes and associated responsibilities should be defined as part of system administration procedures, see Appendix O12.
 - *Emergency Changes.* Implementation of emergency changes should be based on risk and should be subsequently reviewed, documented, verified, and approved in a timely fashion according to the appropriate procedure. What constitutes an emergency change should be clearly defined. Changes should not be allowed to escalate to emergency status through the accumulation of internal failures or delays.
 - *Temporary Changes.* These are changes which are planned to be in place for a limited period (as defined by the regulated company). Any such changes may introduce new or increased risk which should be assessed and managed. Particular attention should be paid to the reversal of temporary changes to ensure that they are 'rolled back' and properly reviewed through the formal change management process before being made permanent.
 - *Global Changes.* For additional information related to managing change in a globally implemented computerized system, see the *GAMP Good Practice Guide: Global Information System Control and Compliance* (Reference 34, Appendix G3).

There is also potential to use performance monitoring data to influence change management, where it can be used to support risk and impact assessment, and evaluation of any proposed change and the subsequent effect of implementing the change.

Change Management records form a key part of the overall documentation for a system and should be subject to periodic internal audits.

4.4 Configuration Management

Operational configuration management should start with the baseline configuration and associated configuration management records that should form part of system handover. The more formality that has been introduced during development, the easier it is to bring about this handover.

Configuration management consists of the following activities:

- Configuration Identification (WHAT to keep under control)
 - Configuration Control (HOW to perform the control)
 - Configuration Status Accounting (HOW to document the control)
 - Configuration Evaluation (HOW to verify that control)

Configuration management activities, responsibilities, procedures, and schedules should be planned and documented. Responsibilities and activities for operational configuration management should be defined in a Standard Operating Procedure (SOP).

Configuration management and the associated records play a key role in the event of disaster recovery, where the system and its components should be correctly re-assembled and integrated to re-establish a fully operational system. All required components should, therefore, be included in the back up process.

The use of automated configuration management tools can bring significant advantages, and should be considered. The selection, verification, and use of such tools should be documented and based on risk, complexity, and novelty.

4.4.1 Configuration Identification

The components of the system subject to configuration management should be clearly established. For this purpose the system should be broken down into configuration items, which should be identified during system specification and development.

A configuration item is a component of the system which does not change as a result of the normal operation of the system. Configuration items should be modified only by application of a change management process (see Section 4.3 of this appendix). Examples of configuration items are application software, layered software, hardware components, and system documentation.

The formally established list of configuration items and their versions is called the configuration baseline, and it serves as reference for further activities.

The level of detail in defining items should be determined by the needs of the system, and the organization developing that system.

4.4.2 Configuration Control

Changes to configuration items should be coordinated and controlled. This includes the following activities:

- version control
- change control
- configuration item storage
- delivery control

A unique name and a version number should identify each configuration item. These should be updated in case of change.

Change control should be applied to all configuration items. Changes to hardware, software, and configuration should be made by authorized personnel and appropriate records kept.

Configuration items should be stored and controlled in such a way that they are protected from unwanted or unauthorized changes. Methods, responsibilities, and location of storage should be documented.

The release and delivery of software and documentation should be controlled. Master copies of code and documentation should be maintained securely, according to defined procedures.

4.4.3 Configuration Status Accounting

Documentation showing the status and history of configuration items should be maintained. Such documentation may include details of changes made, latest version numbers, and release identifiers. This provides a means to demonstrate that system specifications are reviewed, updated and reapproved. This may be accomplished in a number of ways, e.g., through version controlled configuration baseline documents, or using automated tools.

4.4.4 Configuration Evaluation

The documentation described above should be subject to document control, review, and approval according to defined procedures. These activities should ensure that status accounting is accurate and up to date, and provide an audit of the configuration management function.

Periodic review of operational systems should include verification that the current configuration information for the system is accurate (see Appendix O8).

Repair Activity

1 Introduction

Repair is the process of managing repair or replacement of a failed or defective component, which may be a configuration item. It is a form of change control in which the relevant specifications do not change.

2 Key Requirements

The procedures to be followed if the system fails or breaks down should be defined, approved, and verified.

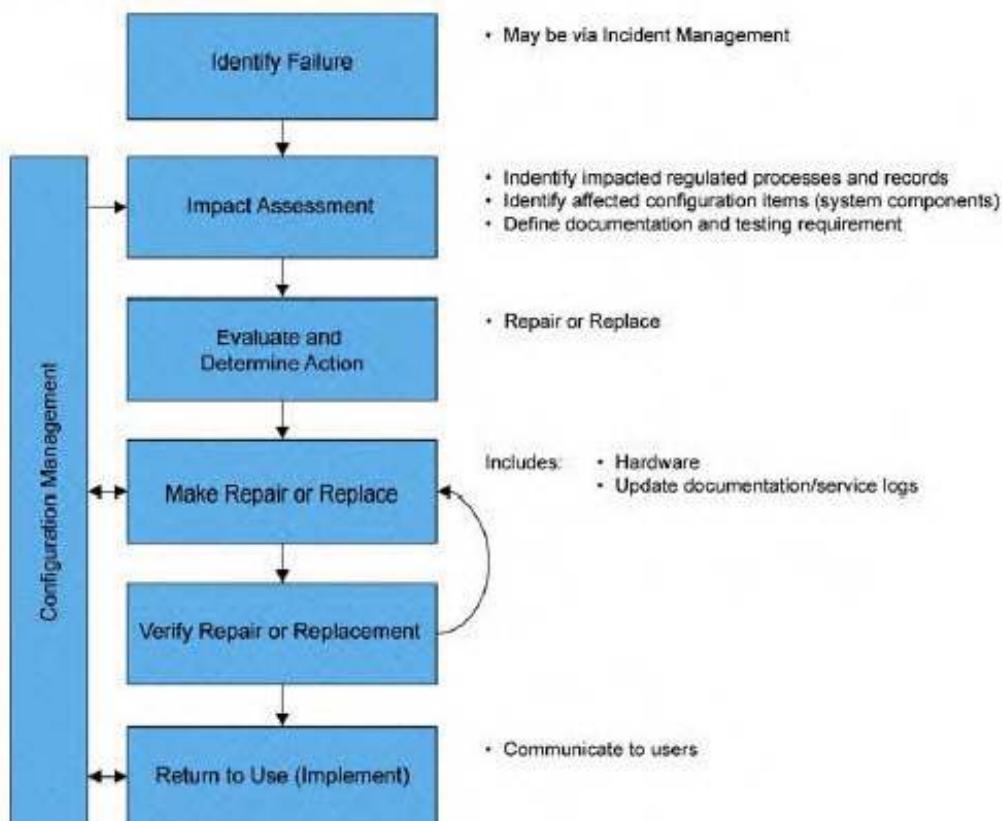
Any failures and remedial action taken should be recorded.

A procedure should be established to record and analyze errors and to enable corrective action to be taken.

These activities should be documented.

3 Process

Figure O7.1



4 Guidance

4.1 General Approach

The repair process may be integrated into the change and configuration management process but is likely to take a simplified route.

The repair process at a high level is likely to be generic but each system subject to the repair process may require a system specific list of components eligible for repair or replacement under the authority of the procedure. This may also form the basis for an agreed spares list.

Where the failure (or the repair) could impact patient safety, product quality, or data integrity then the incident management process should be initiated.

Repair or replacement records should be subject to periodic internal audits and their review should be part of the performance monitoring process.

4.2 Responsibilities

It is the responsibility of the system owner to identify those components eligible for repair or replacement. Relevant information from the project phase may be available before and during handover, such as the basis for an agreed spares list when the system becomes operational.

It is the responsibility of the system owner to ensure that the process and procedure are followed.

It is the responsibility of the team effecting the repair (or replacement) to execute the procedure completely and accurately, including updating records as necessary (e.g., the system log).

It is the responsibility of the Quality Unit to assure that repair procedures are followed and appropriate actions have been taken and documented.

Periodic Review

1 Introduction

Periodic reviews are used throughout the operational life of a computerized system to verify that it remains compliant with regulatory requirements, fit for intended use, and satisfies company policies and procedures. The review should confirm that, for all components of a system, the required support and maintenance processes are established and that the expected regulatory controls (plans, procedures and records) are established and in use.

2 Key Requirements

A process for timing and scheduling of reviews should be defined. The review periods for specific systems should be based on system impact, complexity, and novelty. These risk-based decisions should be documented.

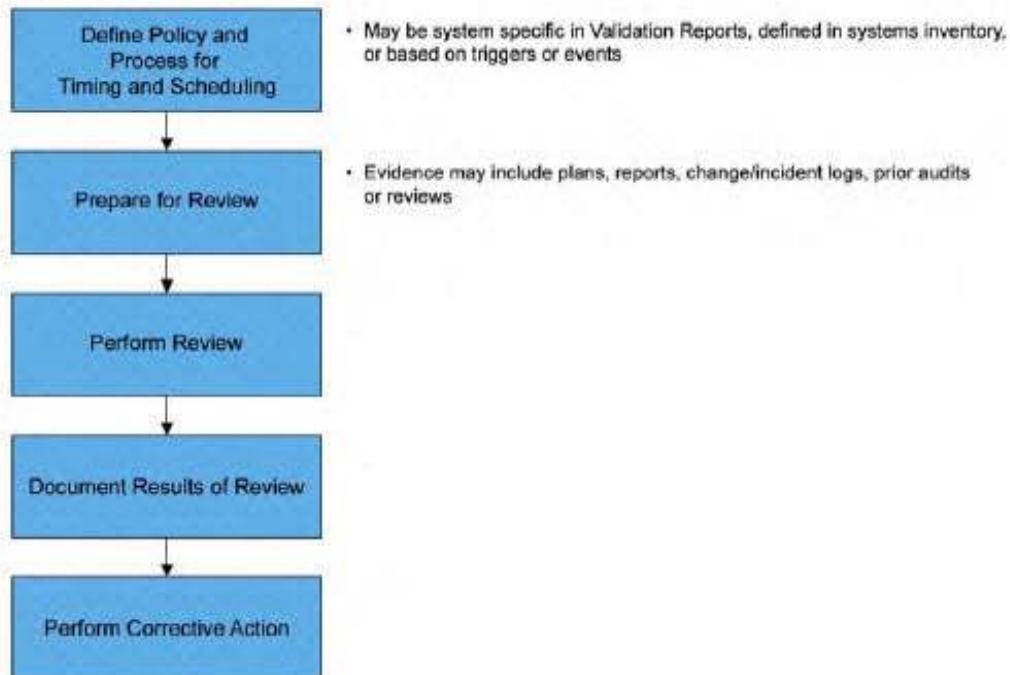
Problems found during the review should be documented, along with recommended corrective actions. Consideration should also be given to possible wider implications.

Agreed corrective actions should be resolved and approved.

These activities should be documented.

3 Process

Figure O8.1



4 Guidance

4.1 General Approach

The periodic review process should be generic and applicable to all systems. It should apply to operational environments and not to any supporting development or test environments. The depth and rigor of review should be based on system impact, complexity, and novelty or on the nature of an incident or event that triggers a review. Where appropriate, computerized system periodic review may be completed as part of a broader activity, such as periodic review of a manufacturing process.

Periodic reviews should take account of and reference other appropriate reviews, such as review of security logs, and not duplicate activities.

It may be helpful to develop specific periodic review checklists for particular systems.

4.2 Responsibilities

It is the responsibility of the process owner to ensure that periodic reviews are conducted for the system and to take account of and respond appropriately to the findings of the review.

It is the responsibility of the Quality Unit to assure that periodic reviews are scheduled, performed and documented.

The review should be conducted by one or more persons depending on the scope of the review. Participants might include Quality Unit, Subject Matter Expert (SME), users, IT, engineering, compliance. Findings should be documented.

4.3 Timing and Scheduling

A process for timing and scheduling of reviews should be defined. Review periods for specific systems should be based on system impact, complexity, and novelty. Acceptable methods include:

- Defining the review period for specific systems in computerized system validation reports. This has the advantage that a schedule of reviews can be planned. The frequency of review should be based on system impact, complexity, and novelty.
- A defined decision process based on regular review and analysis of the system inventory
- A defined decision process based on specific events, either planned or unplanned
- A defined decision process based on the number and complexity of system change requests

Whatever method (or combination of methods) is chosen, the process should be documented and approved by regulated company management, and the responsibility and criteria for decisions clearly defined.

The responsibility for managing the timing and scheduling process, and allocating resources to reviews, should also be clearly defined.

4.4 Review of a System

4.4.1 Preparation

Relevant information should be made available for the review including, but not limited to, the following as appropriate:

- documentation for the system including, e.g., plans, specifications, verification including testing, reports, traceability, risk management documentation, design reviews, user manuals, training materials, and records
- Operational and maintenance Standard Operating Procedures (SOPs)
- configuration management information
- change management information
- incident logs
- security and access control information
- any prior audits of individual systems
- Validation Report

The objectives, staffing, and agenda for the review should be defined. The review team should ensure that necessary reference material and people are available, and that the process owner is committed to taking due account of the outcome of the review.

4.4.2 Conducting the Review

Problems found during the review should be documented, along with recommended corrective actions. They should also be considered for possible wider implications. Depending on the overall management process, a follow-up audit may be scheduled.

When defining the agenda for the review, the following should be considered:

- That the documentation is complete, up-to-date, and correct, including:
 - Specification and verification documentation
 - Operation and maintenance documentation
 - Configuration item list
- Any change of use of the system
- The level of change that a system has been subject to and the nature of those changes
- Outstanding actions required by a Validation Report
- Previous audit reports, and the actions which resulted
- That any controls implemented to manage risk are still in place and functioning effectively

- Evidence of unstable or unreliable operation
- Changes in environment, process or business requirements, legislation or accepted best practice
- Operational procedures (including access control)
- Business continuity planning
- Personnel (including qualifications, training, experience, and continuity)
- System security and access control
- System maintenance and incident logs
- Software and data backups

4.4.3 *Output from the Review*

The minimum output should be a documented justification of the continued acceptability for use of the systems under review. It may be necessary to produce an agreed, prioritized, and resourced plan to perform follow-up or corrective action. For complex or critical systems a summary report should be produced covering:

- The outcome of the review
- Deviations or problems found
- Required remedial work

Actions identified in the summary report should be completed and approved, prior to closure.

Backup and Restore

1 Introduction

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

Backup and restore should not be confused with archiving and retrieval processes which are covered by Appendix O13.

See Appendix O7 and Appendix O10 for further details on hardware restoration.

2 Key Requirements

Procedures should be established to cover routine back-up of records, data, and software to a safe storage location, adequately separated from the primary storage location, and at a frequency based on risk.

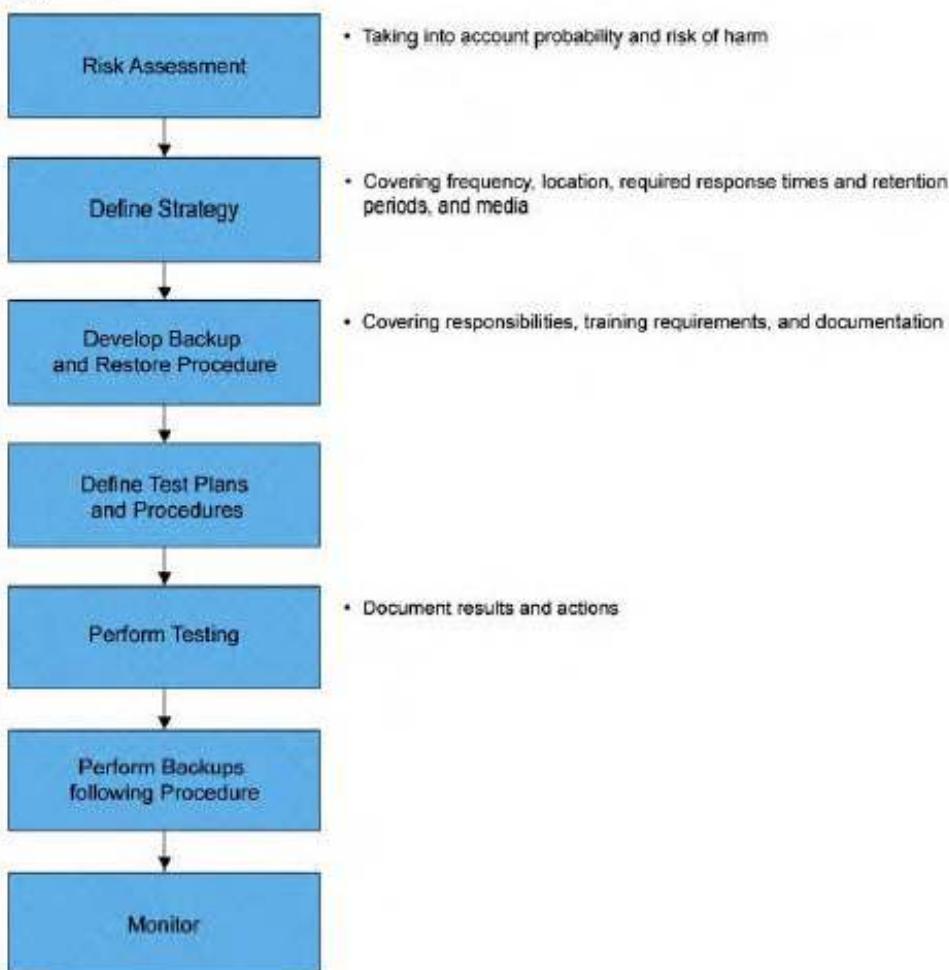
There should be written procedures for recovery following a breakdown to ensure documented restoration and maintenance of GxP records and data.

The back-up procedure, storage facilities, and media used should ensure integrity. There should be a backup log with references to the media used for storage. The media used should be documented and justified for reliability.

Backup processes should be verified when they are established. In addition, there should be procedures and plans for regular testing of backup and restore capability. Such activities and subsequent action taken should be documented. It is an acceptable common practice to combine testing of the backup process with testing of Disaster Recovery procedures (see Appendix O10).

3 Process

Figure O9.1



4 Guidance

4.1 General Approach

The Backup and Restore SOP may be generic, i.e., the process is applicable to many systems. However, there will be system specific elements in the actual conduct of the process, e.g., identification of the directories requiring backup. Further consideration should be given to how any other system specific elements are covered, for example, within system specific work instructions.

Effective system configuration management and change control processes should be established to support backup and restore.

4.2 Responsibilities

The process owner (with the agreement of the Quality Unit as necessary) is responsible for:

- definition of the data requiring backup, which should include GxP relevant data
- defining the availability and access control requirements for such data

The system owner is responsible for:

- ensuring that the organization of software backup and restore for operational systems is defined and is compliant with applicable regulations (with the agreement of the Quality Unit as necessary)
- ensuring the adequate performance of software and data backup and restore for operational systems
- ensuring appropriate access controls

During the implementation project, some of the above responsibilities may have previously rested with the project manager.

4.3 Backup Media

Backup should be performed onto suitable media, and media should be used in accordance with the recommendations of the manufacturers. When choosing and using storage media, the following should be considered:

- recommended service life
- acceptable environmental conditions for storage
- verification, refresh, and rewrite requirements

Guidance on the storage, transportation, and maintenance of various types of magnetic and optical media is available from national and international standards organizations.

4.4 Backup and Restore Process

The backup and restore process should be defined in company procedures.

4.4.1 Software Backup

Software backups are created in order to ensure that in the case of a failure, or after modifications during development or during operation, that the latest and correct software versions are available and can be restored at short notice, without error.

All software components required for the operational system should be included in scope (i.e., operating system, layered software and tools, base products(s), custom code, configuration and data) to ensure the full system can be restored.

During project execution, the software (source code as well as compiled executables and system configuration) should be periodically backed-up. The frequency of backups, the period of retention before recycling of the backup media, the use of full and incremental backup techniques, backup logging and actions on backup failure, should be defined and documented. Further guidance on these topics is given in Section 4.4.2 of this Appendix, Data Backup.

At predetermined points, such as prior to formal testing and prior to handover, a baseline version of each software component should be established, and a backup taken and retained.

The backup process for software once the system is in operation should be defined and documented. This can occur:

- After every software modification, in which case backup of the modified software components may be sufficient. This should be documented as part of Change Control
- At regular intervals (e.g., annually) as a complete backup

Backup copies should be stored in a secure location. The need for remote storage of backups should be based on risk. The backup media should be physically secured and protected from fire, water, and other hazards. The storage process, standards, and access should be defined and documented.

If restoration is time critical, then a copy of the backup should be held locally, in addition to the remote copy for use in case of disaster.

At least two generations of backup copies should be stored, the current one and the one dating from before the last modification. Based on risk, more generations may be advisable to guard against the possibility of propagated errors in all available back-up copies. The frequency of software backup should be based on risk and the nature of the business process.

The following information should be clearly and securely associated with the backup media, either on the label itself, or in a separate log with a unique identification code linking the log entry and the media:

- creation date
- system designation
- software designation
- version and/or software/firmware build number, if applicable
- current number (generations and possibly multiple backups)
- reason for the software backup
- date of backup
- identity of person performing backup

Software backups should be performed while the system is in operation. A log of software backups should be maintained. Software backup and restore instructions should be stored securely with the backup media.

Based on risk and the backup process, backups should be subject to periodic checks and in addition the backup restoration should be periodically executed to verify that it will work successfully when needed.

4.4.2 Data Backup

GxP regulated electronic data should be maintained securely for the defined retention period. Other data may be held on systems on a short-term basis for evaluation and processing. While data is often held on hard disk devices using redundancy concepts or mirrored disks, additional backup of GxP regulated data forms a key part of avoiding data loss in the case of a failure. The data should be retrievable at short notice and without error, and copies held remotely to avoid loss due to common mode failure in one location (e.g., fire). Type and frequency of backup required should be based on risk.

Organization of Data Backup

The data should be periodically saved on backup media. The system owner should establish and document the organization of data backup, covering the following aspects:

Type of Data Backup

- full backup
- incremental backup

Interval

- daily backup
- weekly backup
- monthly backup
- quarterly backup
- annual backup
- non-cyclic backup (i.e., retain permanently)

Number of Generations

The number of generations defines the number of retained identically performed data backups. Since backup media are often reused, after the defined number of generations is reached, subsequent backups are typically written over the oldest one currently retained. For example, if the defined number of generations is four, the fifth backup overwrites the first; the sixth overwrites the second; and so on.

Backup Failure

Actions to be carried out in the case of a failure should be considered, such as repetition of the backup during the day in restricted operation. The actions undertaken on failure should be documented (e.g., in the system log) by the person responsible for the computerized system.

Observations

Where applicable, further comments should be recorded, for instance about the data backup type or exceptions.

Labeling of Backup Media

The following information should be clearly and securely associated with the backup media, either on the label itself, or in a separate log with a unique identification code linking the log entry and the media:

- system designation
- software/data designation
- version and/or software/firmware build number, if applicable
- date of creation
- date of first usage
- current number (generations, possibly multiple backups)
- date of backup
- reason for the backup
- identity of operator

Duration of Use

Media should only be used for as long as it is guaranteed.

Type of Media

The type of media should be documented.

Storage Location

The storage locations should be safe and secure, and identified in a centrally accessible index.

Data Backup Tools and Corresponding Procedures

GxP regulated data should be stored in a state suitable for restoration. The location and name of controlling procedures should be documented. The procedures should cover the initiation of restoration, verification activities, and re-start after system failure.

Data Backup Review

The system owner, or designated representative, is responsible for ensuring that the successful completion of the data backup is checked. Failures should be investigated, and potentially faulty media discarded and replaced. Actions should be documented, e.g., in the system log.

4.4.3 Restore

This section applies to the restoration of data (e.g., to recover data loss after hard disk defect during batch run) in accordance with the appropriate disaster plan.

The process owner, or their designated representative, should authorize restoration of data, based on a documented incident. They are responsible for ensuring that the procedure complies with GxP regulations.

If restoration is to be carried out for technical reasons, the system owner and process owner should consider the process and possible risks. The method of restoring and the control of the restore operation should be documented, in the system log for example. Re-synchronization may be required in the case of inter-dependent systems.

Documented and tested procedures should be used for restoration. When the restoration process is manual, it should be recorded and signed (e.g., in the system log).

The full backup of any available data should be performed before attempting a restoration, in order to avoid any additional data loss.

There may be a requirement based on risk to use the transaction log file in addition to the latest backup to ensure that the system is returned to its current state immediately prior to failure.

An example form for the restoration of data is provided separately.

4.5 Long-term Integrity

Electronic media degrades over time, and the re-use of backup media should be in accordance with manufacturer recommendations for the practical lifetime of the media. In the unlikely event that a backup copy is held for a period approaching the recommended lifetime of the media, the integrity of retained backups should be reviewed in accordance with manufacturer's specifications. In some cases it may be more straightforward to copy the data onto new media rather than to review the old one.

The backup and restore procedure should be verified periodically. The frequency should be based on risk. This can be done by restoring the backup to a test system and verifying its correct operation. A common and pragmatic process is to combine verification of the backup process with disaster recovery testing. Restoring the backup for test purposes to the production system is not recommended, as any error in the procedure may result in data loss.

If a necessary change of hardware or software means that stored data can no longer be read or printed in the new system configuration, one of the following processes should be applied based on risk:

- Migrate the data to a new system
- Migrate the data to a non-processible format such as paper or PDF. This option is far less desirable as it assumes a significant risk: restoration of the data to the system will most likely require manual transcription.

Backup and restore procedures and documentation should be checked during Periodic Review. The conclusions should be documented.

Business Continuity Management

1 Introduction

Business continuity management encompasses the steps required to restore business processes following a disruption while continuing to provide product or services to the customer. It includes steps often described as Disaster Recovery (DR).

DR planning is subordinate to business continuity management and covers the technical recovery of a specific system while business continuity encompasses business process sustainability. DR is typically the responsibility of a support organization such as IT, and includes restoration of the system. A DR Plan should be in place for each required system, and should encompass not only a process for restoring the system, but also any infrastructure required for the system to operate.

Business continuity planning may cover several levels varying from departmental to corporate. It typically covers multiple systems and is owned by the business as opposed to a support organization. A Business Continuity Plan (BCP) includes process owner responsibilities such as defined procedures for re-starting business operations. The BCP will identify the triggers for invocation of the plan, people to be involved and required communication, as well as the interim processes to manage the disruption.

2 Key Requirements

Patient safety, product quality, and data integrity should not be compromised by system failure or breakdown.

The regulated company should perform business continuity planning to actively protect its ability to continue to supply the public, and to comply with the regulatory requirements.

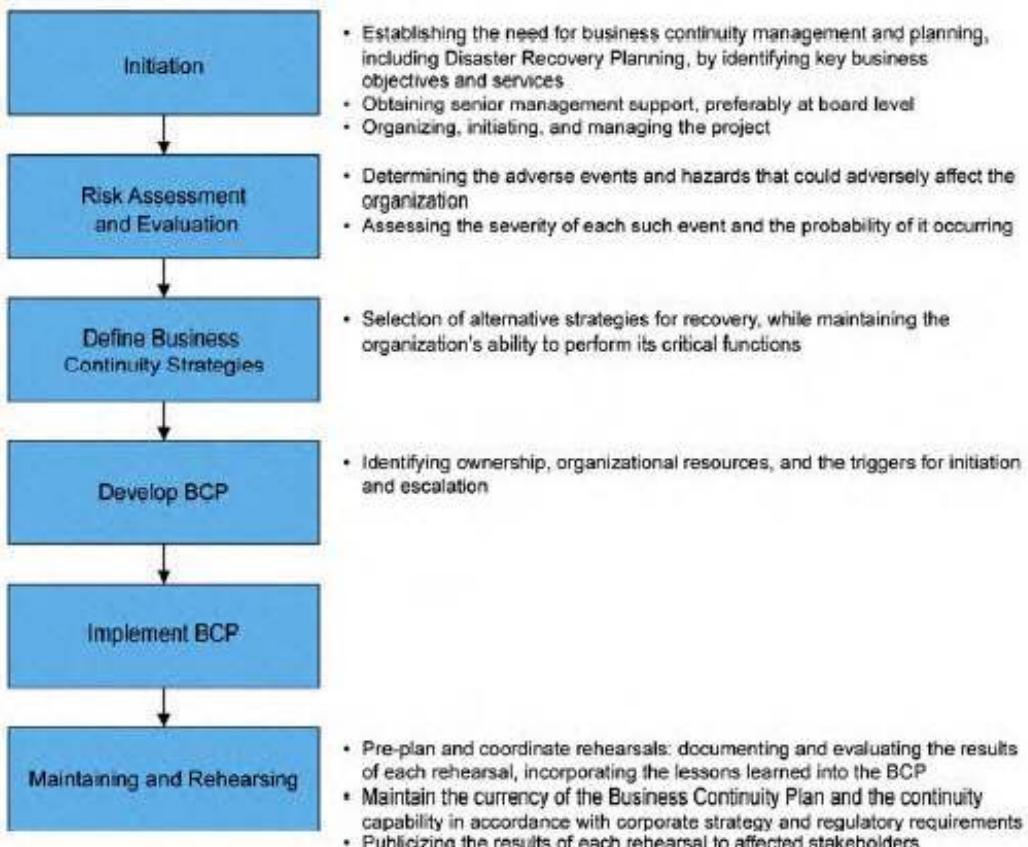
BCPs should provide for alternative procedures or processes to be implemented and followed to replace absent system functionality and allow the safe continuance of business during the failure.

BCPs should be defined and include provisions for rehearsal. Alternative processes required by the BCP should be suitably documented, and personnel should be adequately trained.

Companies should be able to demonstrate that they can ensure that critical services and processes can continue, and that there is a timely resumption of essential business functions.

3 Process

Figure O10.1



4 Guidance

4.1 General Approach

Regulated companies should define a process for the production of BCPs including the use of common formats. It is likely that a BCP will cover many systems. A risk-based approach to the content and detail should be taken so that each system is adequately covered.

BCPs and their rehearsals should be subject to periodic internal audits.

Consideration should be given to maintaining BCP procedures off-site and maintaining the information on paper-based systems.

The communication process is an important aspect of BCP; key contacts (e.g., process owner, system owner, supplier(s), and Quality Unit) should be listed with their contact details.

The BCP should include a clear process for prioritizing system restore as the disruption may involve failure or unavailability of multiple systems which may be within or outside the regulated company.

Where manual processes are invoked to allow the business to continue to operate, it is important to consider how any associated electronic records or data will be synchronized once the electronic systems have been restored.

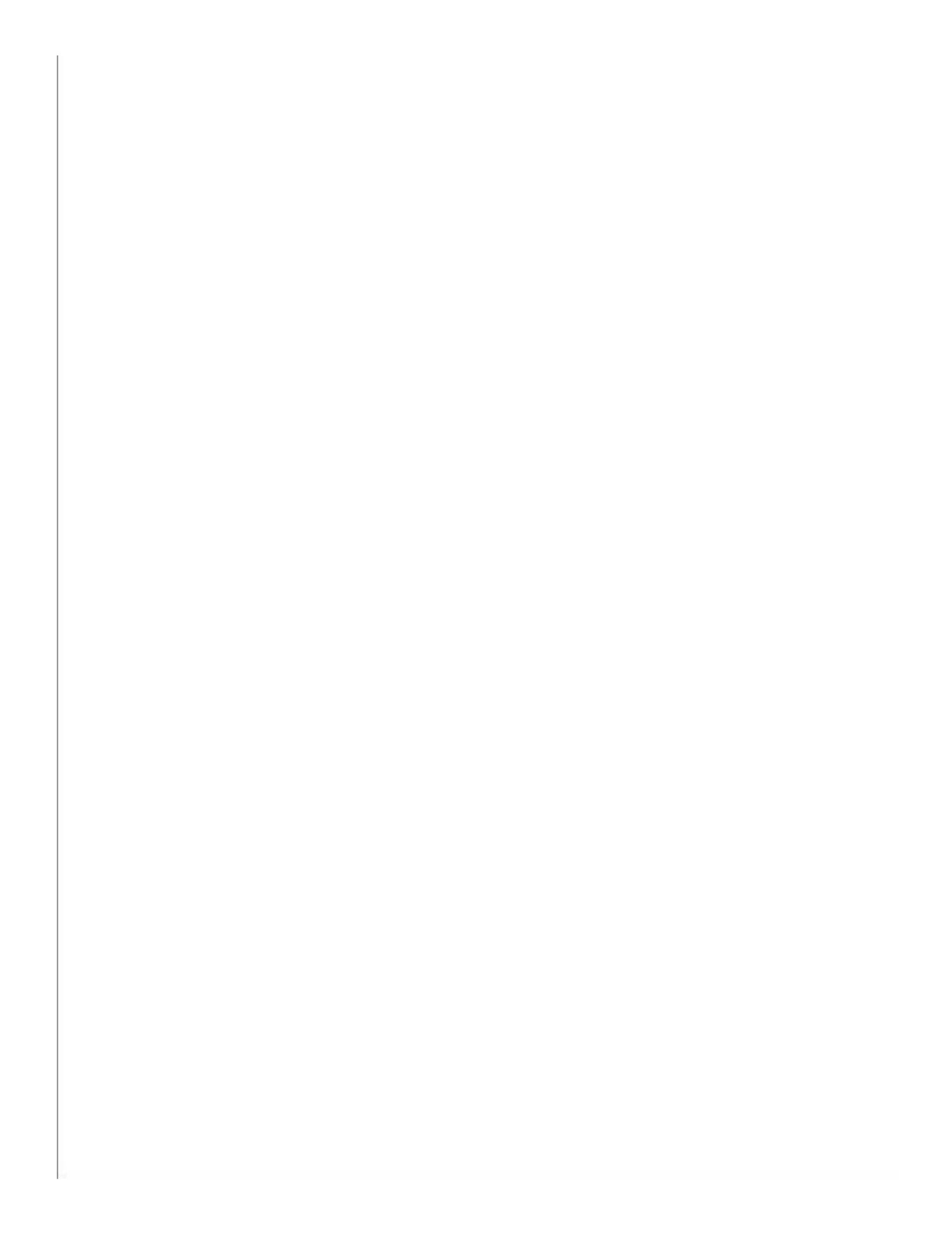
The BCP should consider the need for defining both short-term and long-term business continuity options and when they might be used.

Business Continuity Plans can be rehearsed or tested in several ways, such as through reviews, brainstorming, walkthroughs, testing of sections of the plan, re-installation of servers, switching to hot sites, and full testing.

4.2 Responsibilities

It is the responsibility of company management (including process owners, system owners and Quality Unit) to ensure that appropriate BCPs are established, are tested periodically, and once initiated, are followed and reported upon.

It is the responsibility of process and system owners to ensure that appropriate disaster recovery plans are in place for their systems to support the BCPs, and are tested.



Security Management

1 Introduction

Security Management is the process that ensures the confidentiality, integrity and availability of an organization's regulated systems, records and processes.

Effective security management protects assets to minimize the business impact of security vulnerabilities and incidents.

See also ISO 17799 for further details on information security management (Reference 25, Appendix G3).

2 Key Requirements

Measures should be implemented to ensure that GxP regulated computerized systems and data are adequately and securely protected against willful or accidental loss, damage, or unauthorized change.

Such measures should ensure the continuous control, integrity, availability, and (where appropriate) the confidentiality of regulated data.

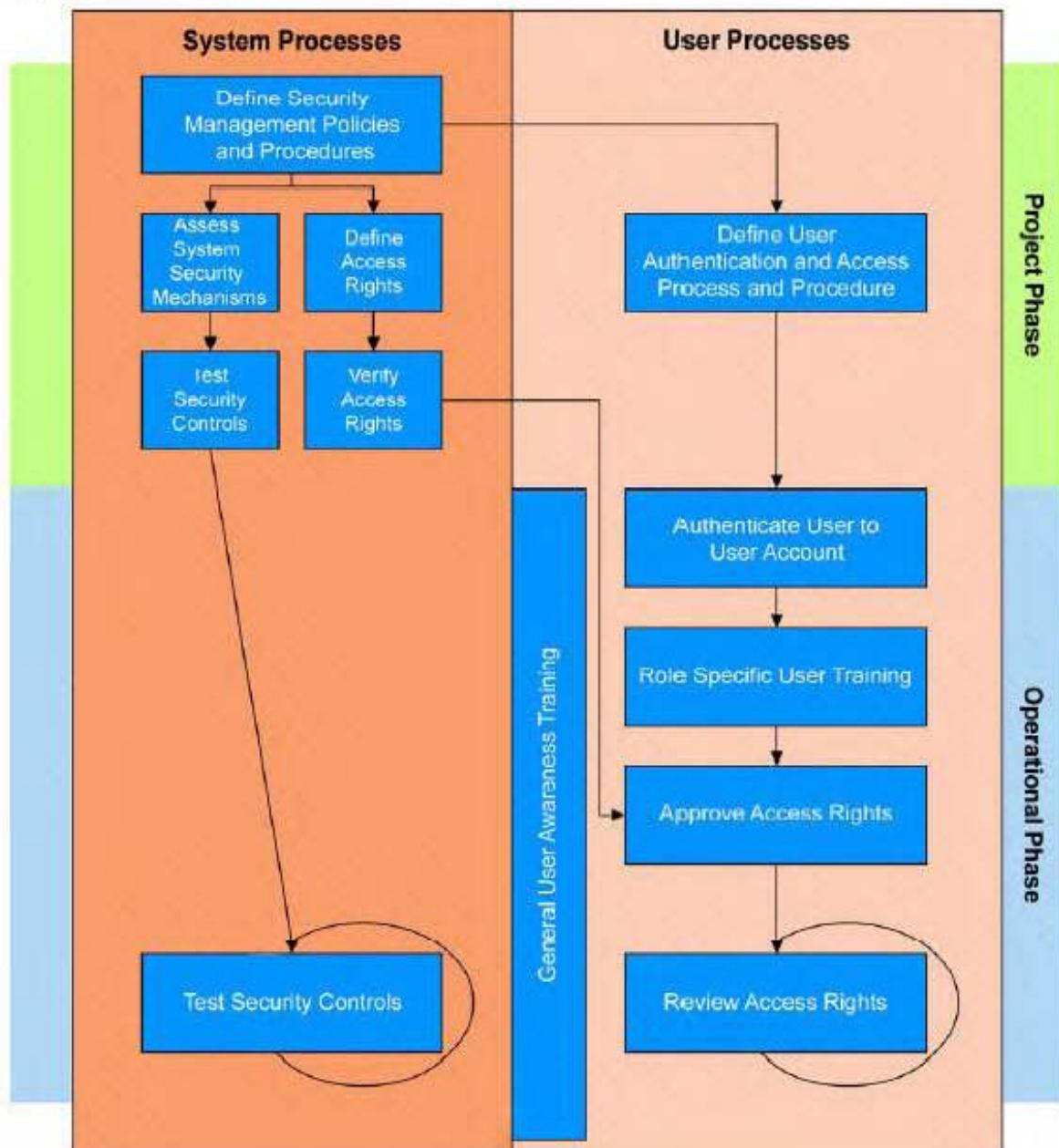
This process should include:

- Establishing and maintaining security roles and responsibilities, policies, standards, and procedures
- Performing security monitoring and periodic testing, e.g., manual check of system access log, automated notification of lockouts, testing of tokens
- Implementing corrective actions for identified security weaknesses or incidents.
- Ensuring a list of those authorized to access the system is established and maintained

The design of the system's physical and technical security mechanisms should be assessed and (if necessary) tested.

3 Process

Figure O11.1



4 Guidance

4.1 General Approach

Security processes and procedures typically are generic in nature, i.e., one process or procedure will be applicable to all systems. However, each system may have specific aspects to its security which should be documented, e.g., the configuration and/or approval of user access rights.

Records associated with system security should be subject to periodic internal audits.

4.2 Responsibilities

Responsibility for security of the system including control of system access should be agreed between the process and system owner.

Some responsibilities may be delegated, e.g., to those responsible for infrastructure elements of security management (sometimes referred to as platform owners).

It is the responsibility of the Quality Unit to assure that security procedures are followed.

The user of the computerized system is responsible for complying with the defined security requirements during the daily use of the computerized system.

4.3 Principles

Security Management measures should be planned and implemented based on consideration of the following:

- system impact
- employee awareness
- incident management
- information security policy

4.3.1 System Impact

The initial risk assessment performed during the project phase should determine the overall impact that the computerized system may have on patient safety, product quality and data integrity due to its role within the business processes. This should take into account both the complexity of the process, and the complexity, novelty and use of the system. See Appendix M3 for further details.

Based on the impact of the system, the process owner should ensure that suitable controls are defined to provide an appropriate level of protection for supported processes and records during operation.

4.3.2 Employee Awareness

The regulated company should ensure that employee awareness of computerized systems security is maintained via the implementation of effective communication and education programs. Such programs should include all employees (permanent, part-time, and short term contract) and any others with access to systems.

Line management should ensure that end users are made aware that their activities may be monitored and that action could be initiated against any employee not following policies and procedures.

4.3.3 Security Incident Management

Security incidents should be reported to the system owner. Significant security incidents (i.e., those involving fraudulent activity, falsification or adulteration of data, loss of data or external breaches of network security) should be reported to senior management. The incidents should be formally documented; the causes investigated and corrective action proposed, implemented, and closed out. A regular review of incidents should be undertaken to determine if any trends or threats can be identified.

4.3.4 Information Security Policy

The company or organization should develop an Information Security policy outlining the rules and guidance regarding use and access to systems. The policy should state conditions for the use of computerized systems, e.g., rules for private use. The policy should also account for the use of controlled or verified PCs to ensure compliance is not compromised. Topics that should be covered include:

- physical security
- system access security including granting and revoking access, e.g., issuing user-ids and control of passwords
- third party access
- electronic messaging systems
- shared network resources
- internet access and use
- use of mobile computing resources, including, for example, laptop computers, PDAs and smart mobile phones.
- connectivity to external computer systems
- anti-virus policies
- intrusion detection

System Administration

1 Introduction

System administration involves routine management and support of systems to ensure that they are running efficiently and effectively.

2 Key Requirements

Support processes should be established, and appropriate resource made available before a computerized system becomes operational.

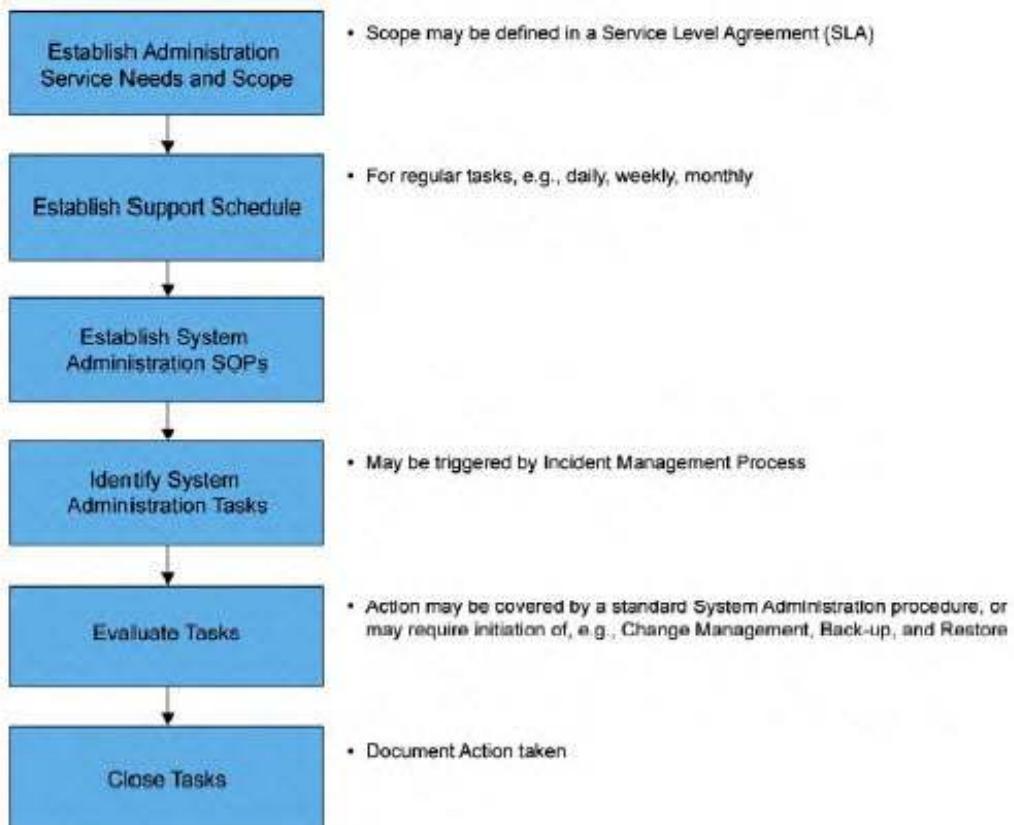
System administration tasks should be identified, documented and be supported by controlling procedures. System Administrators should be trained to perform these tasks and evidence of their competency retained. System administration duties generally should be segregated from operational processing duties.

Any activities relating to the system which are not covered by standard administration procedures should be subject to Operational Change and Configuration Management.

These activities should be documented.

3 Process

Figure O12.1



4 Guidance

4.1 General Approach

At a high level system administration tasks may be generic but it is likely that each system will also have specific tasks associated with it, such as access control.

System Administration task records should be subject to periodic internal audits.

4.2 Responsibilities

The system owner has overall responsibility for ensuring that processes and procedures are in place to ensure the system is used and maintained in a compliant manner.

It is the responsibility of the system owner to ensure that tasks delegated to the System Administrator are clearly identified and documented.

It is the responsibility of the System Administrator to develop sufficiently detailed procedures/work instructions relating to System Administration tasks and to ensure that such tasks are executed in compliance with the procedure(s).

Archiving and Retrieval

1 Introduction

Archiving is the process of taking records and data off-line by moving them to a different location or system, often protecting them against further changes. It may also be necessary to retain in archive the applications that support the records and data. Archived records should be readily retrievable for business or regulatory purposes.

Archiving and retrieval should not be confused with backup and restore processes, which are covered by Appendix O9.

2 Key Requirements

GxP records and data should be secured by physical or electronic means against wilful or accidental damage, throughout the required retention period.

Roles, responsibilities and procedures for archiving and retrieval should be defined.

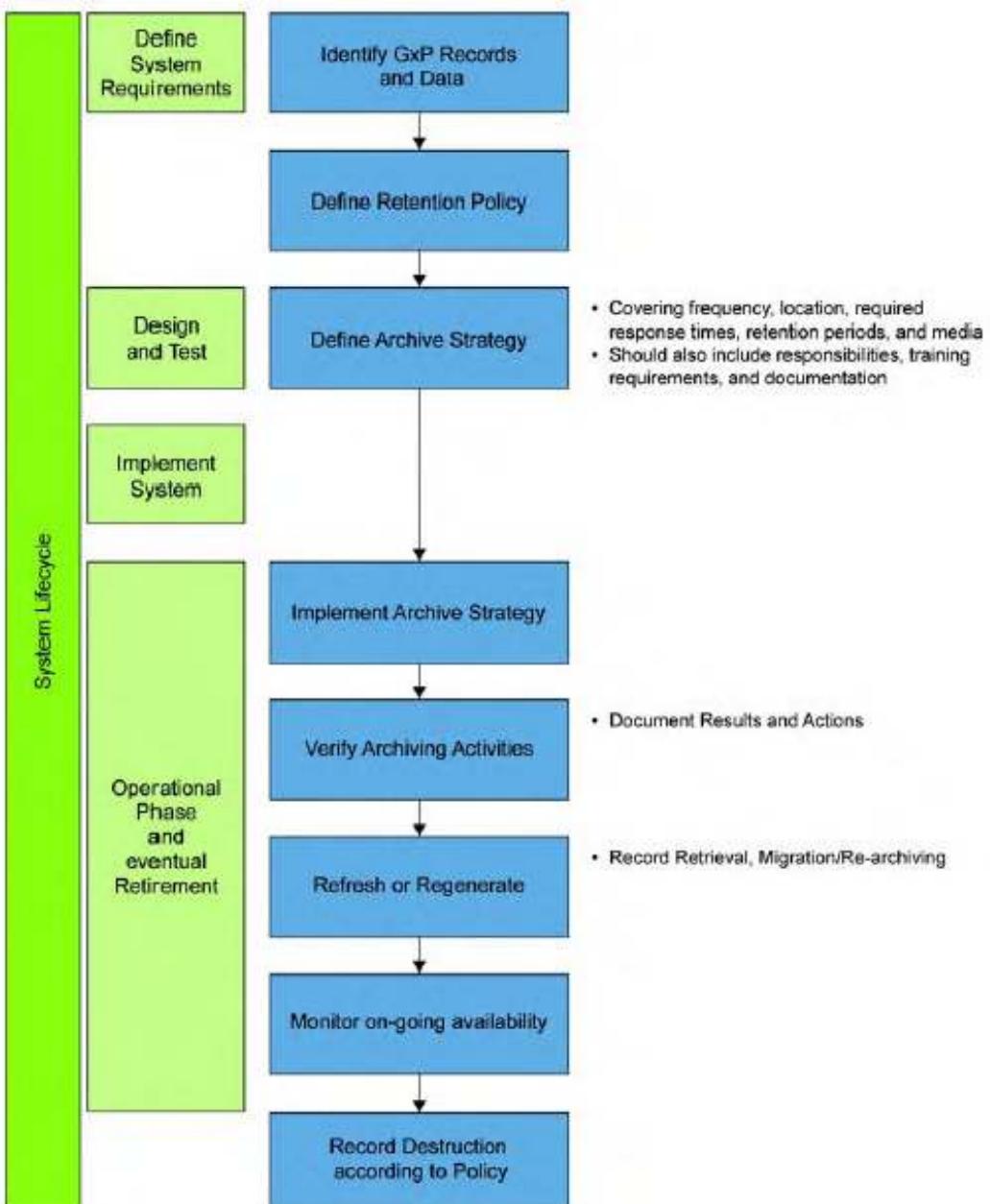
Stored records and data should be initially and then periodically checked for accessibility, durability, accuracy and completeness.

Archiving processes should ensure that record content and meaning are preserved.

Regulators should have reasonable access to GxP records during an inspection within a reasonable period of time for retrieval. Human-readable copies of archived records should be available on request.

3 Process

Figure O13.1



4 Guidance

4.1 General Approach

Archiving should be based on an appropriate archive strategy. It may be helpful to have a Standard Operating Procedure (SOP) which describes how to develop such a strategy.

Archiving processes should be verified to ensure that record content and (wherever appropriate) electronic signature content and meaning are preserved, and the ability to meet regulatory requirements is maintained.

The frequency of the periodic check for accessibility, durability, accuracy and completeness should be determined by risk assessment, taking into consideration storage type, media, and method of access.

Records with associated approvals required by GxP regulation should be subject to particular care to ensure that the validity of the approval is maintained through the archiving process.

More detailed guidance is available in the *GAMP Good Practice Guides: A Risk-Based Approach to Compliant Electronic Records and Signatures and Electronic Data Archiving* (References 34, Appendix G3).

4.2 Responsibilities

It is the responsibility of the process owner to ensure that an appropriate archiving process and procedure are in place.

It is the responsibility of the Quality Unit to assure that the process and procedure are followed.

The archivist is responsible for accepting the records to be archived from the user, maintaining the records in the state the records were received, and returning the records to the user in that same state.

The system owner is responsible for maintaining or updating the systems needed to access the records.

4.3 Scope

Archiving requirements are relevant to any regulated record that needs to be removed from operational systems before the end of its required retention period.

4.4 Policies and Strategy

The regulated company should have an established, documented policy on record retention that defines the types of records to be retained along with format and retention periods for each. The policy regarding the use of authenticated copies should be stated.

An Archive Strategy is recommended, which sets out the requirements and how they should be met. The strategy document can be applied to an organization, site, department or an individual Electronic Data Archive (EDA).

4.5 Archival and Retention

The chosen process should provide controls to:

- Ensure secure storage facilities
- Check and maintain archived records over the entire retention period, e.g., to manage aging media
- Provide indexing capabilities
- Detect the end of the intended retention period for specified records and notify management as appropriate
- Provide management with the option of extending the retention period
- Ensure any changes to the records are carried out under Change Control
- Securely destroy records given the necessary authorization
- Place a litigation hold on any scheduled destructions as appropriate
- Ensure that the technology to read archived records remains available throughout the retention period.

If the archiving process is computerized then that system should be specified and verified as fit for its intended use. Specifically, the automated process should:

- Ensure data is protected by backing-up at regular intervals. Backup data should be stored for the retention period, at a separate and secure location.
- Ensure the system and its contents are secure
- Allow for verification of record accessibility, accuracy, and completeness following changes to associated hardware or software
- Have the capability to keep track of changes to the records
- Ensure that content and meaning of records are preserved
- Consider the on-going availability of the devices and software needed to access the records

A process should be defined for periodically regenerating or refreshing the archive media based on the specification of the technology used. Electronic media degrade over time at rates that may vary based on the nature of the media. The use of media for archive should be in accordance with manufacturer recommendations for the practical lifetime of the media. In some cases, e.g., with magnetic tape, exercising the media may be necessary to achieve its maximum practical lifetime. The integrity of the data retained in archive should be reviewed periodically in accordance with manufacturer's specifications. In some cases it may be more straightforward to copy the data onto new media rather than to review the old one.

Facilities and environmental conditions should be selected to minimize the degradation of storage media that could result in loss of records. The use of fire-proof and off-site storage should be considered based on risk. Conditions such as temperature and humidity should comply with published standards or manufacturers recommendations.

Archiving should be subject to periodic internal audits.

4.6 Retrieval

Retained records should be readily retrievable for business or regulatory purposes. The retrieval process should be documented, and consideration should be given to the following:

- An authorization process to allow appropriate controlled access to records
- The ability to access both on-line and off-line (archived) electronic data, as applicable
- The ability to obtain clear human readable (e.g., printed) and electronic copies of electronically stored data
- The means for retrieval of any record required by regulation after retirement of a GxP regulated system
- The periodic exercise of the retrieval or verification process to verify its continuing operation

Alignment with ASTM E2500

1 Introduction

There is a requirement in several of the GxP regulations to validate those parts of computer and control systems that are critical for the health and protection of the patient. In some cases regulated companies have chosen to perform an inefficient process of installing and commissioning equipment, and then validating it in a separate exercise. This often resulted in wasted effort and repeated activities. Some of the documentation generated during the process did not add value in contributing to fitness for intended use. The principles and practices described in all the versions of the GAMP Guides have been aimed at cost reduction, but separate and duplicated activities are inefficient and unnecessarily costly.

New standards and guidance documents¹ are emerging that aim to make the implementation process for GMP manufacturing control systems more cost-effective and value-added, focusing only on those aspects of systems critical to the protection of the patient. These new standards and guidelines are based on a science- and risk-based philosophy that focuses on the risk to the patient in a combination with Good Engineering Practices (GEP).² If used correctly, the combination of:

- Good Engineering Practice
- a science- and risk-based approach
- understanding of the process
- the appropriate involvement of subject matter experts from relevant organizational areas

These can all be combined in a streamlined effort within an overall framework which meets all regulatory requirements.

These emerging standards have influenced GAMP 5, the associated Good Practice Guides and the terminology used, especially in the context of GMP process systems and equipment.

2 Focusing on Patient Risk

Whilst GAMP 4 and previous guides provided an overall life cycle framework for systems and controlled equipment, they recognized that the practicalities are different for different system types. As a result, a series of Good Practice Guides were produced to support the understanding of these differences and provide more practical detail.

Many pharmaceutical companies undertake complex, time consuming and expensive qualification practices. There are aspects of qualification that can add value in terms of ensuring the equipment and systems are fit for intended use, but there are other aspects that often do not add this value. Some of the prescriptive and rigid conventions and practices that surround qualification as often practiced can detract from its overall value. GMP regulations provide the basis for the activities that are called qualification, but no specific requirements that relate to how qualification is practiced.

¹ From ICH and ASTM (including the ASTM Standard E2500 "A Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment."

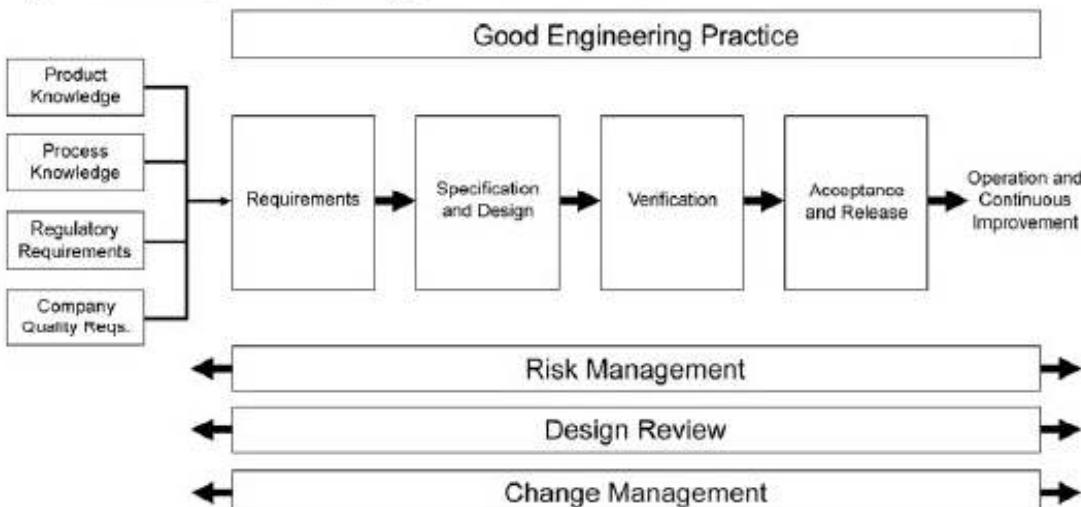
² GEP is defined as those established engineering methods and standards that are applied throughout the life cycle to deliver cost effective solutions that minimize risk to the patient.

By focusing on the risk to the patient and leveraging the expertise of the supplier and subject matter experts based on Good Engineering Practices, verification is considered as a set of integrated activities that can replace the activities previously called IQ and OQ. Regulated company IQ and OQ activities may then be omitted or limited to an assessment of the supplier's activities and documentation, and if necessary performing mitigation activities to close gaps. This eliminates much of the costly duplicated testing which does little or nothing to protect the patient. Finally the overall performance and fitness for intended purpose can be ensured through Performance Qualification or Verification, which focus on critical-to-quality attributes. Overall this will demonstrate that the equipment or system is performing satisfactorily for its intended purpose, the process with which it is involved is controlled, and the risks to the patient have been effectively managed, thus meeting the regulatory requirement for validation.

It is important to select the right tool for a specific need, such as design review, inspection or testing (e.g., Commissioning, Qualification, IQ, or OQ). The term verification is used in ASTM 2500 and aims to promote flexibility in choosing the right approach (See Figure S1.1).

A science- and risk-based approach is inherent in the thinking behind verification, where the level and extent of verification is based on scientifically assessed risk to the patient from specific processes, equipment and systems. This is directly in line with the principles described in ICH Q8, Q9 and the forthcoming Q10 documents for the development, quality risk management and quality management of pharmaceutical products throughout their life cycle.

Figure S1.1: The Specification, Design, and Verification Process



Reprinted with permission from *ASTM E2500-07 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment*, copyright ASTM International, 100 Barr Harbor Dr., West Conshohocken, PA 19428. A copy of the complete standard may be obtained from ASTM at www.astm.org.

It is, of course, still appropriate to create a plan describing and justifying the approach taken to ensure the equipment is fit for use in a GxP regulated environment, and to have a report available providing the necessary evidence to support this claim.

Performed in this way, the process for the specification, design, and verification of controlled process equipment meets all GxP regulatory expectations.

3 Different Types of Computerized Systems

For integrated manufacturing systems or equipment where a computer-based system is part of the overall functionality, a specific and separate computerized system validation may not be required.

For example, where the computer controlled equipment can be regarded as one component of a wider manufacturing or process control system the verification can be an integrated part of the overall process validation effort. The verification of fitness for intended use may be adequately demonstrated by documented integrated engineering or project activities together with subsequent Process Validation – and the overall approach may be defined based on each regulated company's policies and preferences.

Validation is the common term used in regulations worldwide to describe a process that demonstrates that systems are fit for intended use. Some computerized systems are intimately involved in many regulated business activities outside the manufacturing area, and are critical for the health and protection of the patient. Examples include the collection of clinical trials data, the management of donor details in blood collection, the recording of adverse events and complaints, the release of product for sale, and the recall of defective product.

Such IT systems have no direct correlation with the manufacturing and release of the product. Consequently there is no direct parallel with the manufacturing process and associated process validation. Acceptance of the system is dependent on the satisfactory completion of a functional test, such as the traditional OQ or equivalent tests, prior to a controlled cut over into the live environment. (Some further testing, e.g., stress or performance testing, may be necessary which some organizations call PQ but it is not an activity parallel to the PQ testing of controlled process equipment.)

The principles described in ASTM Standard E2500 should be interpreted with attention to the special characteristics of particular systems, and suitable verification that the critical-to-quality requirements of the system have been met should be completed before the computer system can be approved for use in a GxP-regulated environment.

The ideas that led to the development of ASTM E2500 are applicable to all computerized systems. In GAMP 5 we have tried to describe a process which follows the same principles:

- the requirements of the system should be clearly defined
- requirements critical to the health and protection of the patient (critical-to-quality requirements) have been identified and the risks identified and controlled
- the principles of GEP are applied throughout
- the testing carried out and documented by the supplier should be leveraged as much as possible
- the critical-to-quality requirements are appropriately verified and reported by the regulated organization in line with regulatory expectations

It is also recommended that a plan describing and justifying the approach taken, and a report supporting the claim that the system is fit for intended use, are created.

Performed in this way, the process described above for computerized systems meets all the GxP regulatory expectations for validation.

4 Terminology

Since GAMP 5 covers both systems involved in manufacturing of pharmaceuticals and systems for other critical types of IT applications this Guide uses terminology that enables appropriate selection of the relevant life cycle activities, depending on the specific context.

Some organizations have already taken the decision to adopt the term "verification" and apply it to both computer and control systems. Others have indicated that they will stay with the words "qualification", but adopt the principles described in the ASTM Standard E2500. Still others have changed to verification for controlled process equipment but retained "qualification" for computer systems.

The GAMP Community of Practice aims to strongly support and promote innovation. GAMP Guidance is neither mandatory, nor prescriptive, but aims at enabling innovation in a compliant and cost effective manner.

Descriptions of current industry practices should not be read as constraining in any way the development and adoption of other approaches. Individual companies should and will decide what terms and precise approach they will use.

GAMP 5, like previous versions of GAMP, is a guide that supports good quality management practices. The enhanced focus on science and the increased focus on risk to the patient are important to the future of the pharmaceutical industry. GAMP will continue to support evolving good practices for the pharmaceutical industry at large, its regulators and suppliers.

Electronic Production Records (EPR)

1 Introduction

This Appendix presents principles to facilitate the implementation and use of Electronic Production Records (EPRs) in GxP environments supporting quality processes required for real-time release or parametric release, and Process Analytical Technology (PAT). Two common types of EPR are Electronic Batch Record (EBR) and Electronic Device History Record (EDHR).

The implementation of electronic systems enables companies to better control manufacturing processes as well as automatically collect process data and equipment status as operations occur. The implementation of automated control and electronic production records can provide a high level of assurance that the product or device has been manufactured according to its specifications and standards. Reporting for review and disposition can be tailored to system capabilities in providing focused information to personnel in real time or post-production on the status and results of manufacturing process execution.

This Appendix may be applied to electronic and hybrid (combination of paper and electronic) systems for GxP regulated processes.

The ANSI-ISA-88.01-1995 standard provides a basis for establishing electronic equivalent terminology to paper-based batch record systems. This and additional terminology supporting the implementation of EPR is defined further in the glossary (see Appendix G2).

It should be noted that while this appendix specifically addresses EPRs, Review By Exception (RBE) can equally be applied to other regulated areas. One example is a temperature monitoring system in a GLP facility.

2 Review By Exception

2.1 Overview of RBE

Review By Exception (RBE) is a method whereby data from manufacturing-related operations is screened to create reports for review and disposition (e.g., release, quarantine, reject) that include critical process exceptions and reduce or eliminate the need for reviewing acceptable data and trends.

RBE is an extension of existing systems functionality, and therefore, is evolutionary not revolutionary in nature. Systems data is used for review and disposition, and RBE is a data screening and reporting function applied to this existing process.

The RBE Method:

- filters production data for batch or device history reports
- includes any critical exceptions or deviations to the process
- accepts normal operations data, events or alerts not required to support critical exceptions, and typically excludes them from disposition reports
- is applied to well-understood processes or portions of processes
- may be implemented in electronic or hybrid systems

Exceptions to Critical Process Parameters (CPPs) or Critical Quality Attributes (CQAs) are typically included in production reports for RBE.

The concepts underlying RBE have been part of the regulatory environment since the early 1980s. However, it is important to remember that the regulatory authorities may want to review and determine the acceptability of a company's RBE strategy.

The goal of RBE is to provide efficient manufacturing and quality review processes by dividing data review operations between human and systems functionality, leveraging the comparative strengths of each.

Modern automation systems generate a very large volume of data, and practical human review can only be based on statistical methods such as data samples, averages, or other processed summaries such as trend graphs.

Detailed review by personnel of data from validated computerized systems is considered a redundant operation that diverts human review efforts from more critical disposition activities.

2.2 Implementation of RBE

Implementation of RBE is based upon the following requirements:

- system functionality, accuracy, and reliability are clearly defined
- data that would be manually reviewed in non-RBE type reports is retained and can be presented in human readable form for the appropriate retention period
- the computerized means of review is at least as comprehensive and accurate as a manual review
- RBE functionality is appropriately specified, verified and periodically reviewed
- communications or other systems errors that could result in preventing a critical exception from being reported are noted in an RBE report, or otherwise made available to reviewers
- when no critical exceptions occur during operations, the associated exception report indicates that operations were completed without error

RBE may be implemented in a phased approach until complete production reports use the method. This approach provides data reports for segments of processes or equipment for which there is no current automated exception analysis and reporting capability, or for legacy systems that will not be upgraded in functionality before replacement. These individual reports may be used in conjunction with RBE reports where appropriate procedural and technical controls define methods to manage each report as part of an overall review process.

RBE can be applied to the execution of product recipes generating logical or physical inventory such as intermediate, product, sub-assembly or device, and non-product recipes such as asset preparation, which may include equipment selection, setup, cleaning, and sterilizing.

Exception instances in reports should include sufficient context information to allow reviewers to procedurally or automatically retrieve data associated with each exception in support of investigation and disposition processes. This may include actual data, or links and references to data sources.

RBE is enabled by the GAMP approach, where systems are appropriately specified and verified to ensure critical process parameters and overall systems operations are implemented correctly, and are appropriate to each process, process step or system function.

Following the GAMP approach should ensure the following:

- processes are maintained within defined tolerances
- data and events are accurately recorded
- process data are monitored and checked at appropriate rates for processes
- alerts and alarms are generated when tolerances or other operating constraints are exceeded
- electronic records are accurate, trustworthy and secure
- production reports for process/product review are accurate

3 Migration to Real-Time Release

With the implementation of electronic production records and RBE, quality assurance activities can be performed close to actual process execution. An example of an implementation migration is shown in Figure S2.1.

Figure S2.1: Implementation Migration

Electronic Control Recipe(s)

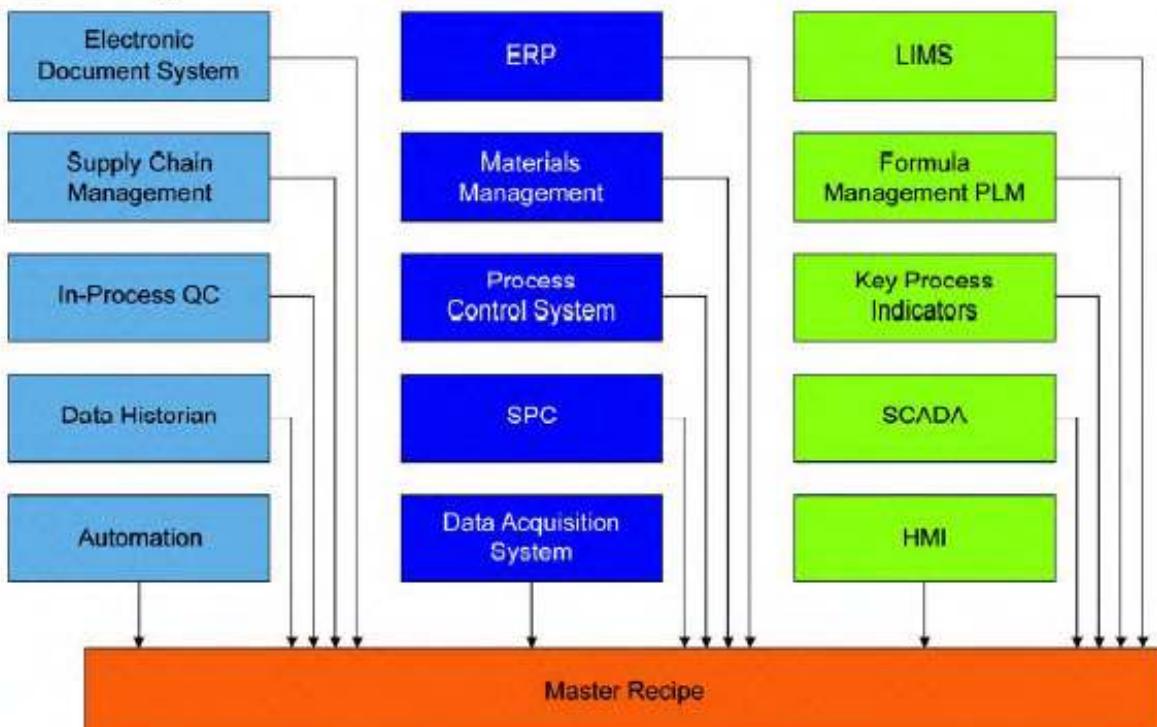
- Raw Materials (Incoming inspection)
- Weigh and Dispense
- In-Process Inspection
- Operator Work Instructions
- Environmental Monitoring and Control
- Process Monitoring and Control
- Product Inspection



4 Database Approach to EPRs

A manufacturing process may have master data such as material specifications, process parameters, alert and alarm limits, or process step sequences controlled by several systems (see Figure S2.2). Recipes combine master data from one or more sources either by direct entry or by links to systems, and deliver it to the production environment for execution. Systems design and/or procedural controls should ensure that the version of all master data is known and controlled, and can be demonstrated for any specific master recipe.

Figure S2.2: Typical Data Sources



It is the responsibility of the process owner to demonstrate that the design (from supplier or user configuration), implementation, and usage of data are accurate and under control, and that EPR data types and their associated use and retention requirements are documented.

End User Applications Including Spreadsheets

1 Introduction

This appendix gives guidance on the use of end user applications such as spreadsheets or small databases in a GxP environment.

Application tools are available for creating a wide range of end user applications, including customized statistical analyses, the creation of local databases, data mining, and multivariate analysis. These may be used for GxP regulated activities, and they present particular compliance challenges.

End user applications tend to be among the most under-documented systems used in GxP environments, for the following reasons:

- users regard them as part of the desktop
- the ease with which applications can be built without much training
- the data processing power that they can have

The flexibility and power of the spreadsheet allows users to create tools that range from performing simple calculations to sophisticated analysis of a major clinical study. Special emphasis is placed on spreadsheets in this appendix because PC users may have the opportunity and ability to create a spreadsheet application, and may use them to process regulated data.

The level and rigor of specification and verification applied to end user applications should be based on risk, complexity, and novelty. This appendix provides guidance to help users determine the appropriate approach. While the examples given in this appendix are mainly spreadsheets, the same principles can be applied to other end user applications.

2 Application Types

This section considers typical examples of end user applications found in the GxP environment.

2.1 Disposable spreadsheets

Spreadsheets may be used in the same way as a hand calculator. For example, ten output values from a laboratory test are input for the purpose of calculating a mean and standard deviation. In this scenario, the electronic copy is not retained.

This should be documented in the same way the use of a calculator would be documented, i.e., the values and result are recorded and signed. The results can be printed, labelled, and signed. It should be clear on the page exactly what arithmetic manipulation was done. This can be facilitated in most spreadsheet tools by printing a copy of the spreadsheet displaying the cell formulae. The paper becomes part of the GxP record.

Calculations used to process GxP data should be verified. This does not mean that algorithms used by native functions of the spreadsheet need to be checked for accuracy, but rather to demonstrate that they are the correct calculations. For example, $(a+b)*c$ is a very different expression from $a+(b*c)$, and errors like this are easily made. Verification of the algorithms can be accomplished by using the capability of most spreadsheet software to print the cell formulae, or by a third party review.

2.2 Spreadsheets Retained as Documents

In many cases, the way in which spreadsheets are used is more like a word processing document than a traditional application. The main difference is that the spreadsheet can be used to both record GxP data and to manipulate it. The flexibility of manipulation that makes spreadsheets useful makes it advisable to manage them as documents rather than applications. It is likely to be extremely difficult to establish that all subsequent saved copies are the same as the original. Calculations should, therefore, be verified and fully explained, as they would be in a text document. This should include proof that the intended formulae have been used, as described in Section 2.1 of this appendix.

Unless the spreadsheet is adequately controlled, it may be advisable to consider a paper printout as the master record. There are a variety of options for achieving adequate control, including:

- using the spreadsheet tool's internal security options, such as password protecting cells or sheets
- storing the spreadsheet in a secure directory
- managing the spreadsheet in an electronic document management system

Spreadsheets that are effectively documents should be managed in compliance with the applicable regulations. For example, a common use of spreadsheets is to manipulate and maintain laboratory data, where compliance with electronic record and signature regulations is a particular concern.

2.3 Spreadsheets as Databases

Another popular use of spreadsheets is as a simple database, i.e., to manage or store GxP data electronically. Data may be frequently updated, which may cause difficulty because spreadsheets lack the intrinsic controls possessed by many true databases that are necessary to ensure data integrity. For example, spreadsheets generally have limited or no capability to limit a user's ability to edit data, or to support audit trails where needed. If a compliant solution is to be developed using a spreadsheet, external controls should be developed to overcome these shortcomings. Users should, therefore, be fully aware of the limitations and weaknesses of spreadsheets when proposed as an alternative to a database application.

While there are commercially available products intended to provide audit trail capability to spreadsheets, as a general rule the use of spreadsheets where audit trails are required is inadvisable. Spreadsheet software typically is not designed to provide audit trail functionality and the use of a database with such capability intrinsic to the design is considered preferable.

2.4 Template Applications

A very common use of spreadsheets is the development of template solutions, where data can be subjected to a standard manipulation and the result saved as a unique document. Statistical analysis or data mining applications may also fit this subcategory. Templates may be used, e.g., in tabulating and processing data from a clinical study, or similarly, for QC test results prior to product release.

When developing such templates, users and developers should fully understand and document the required manipulation. This allows clear confirmation of design intentions against standard package features to be established and confirmed. The following should also be considered:

- calculations should be verified to be correct
- Will the template be running on a single workstation, or available for download from a single location? If not, how is it ensured that everyone is using the correct version? Version control should be established, supported by an effective change management process.
- How will access to the application and data fields by users and developers be controlled? Ideally, all cells other than data entry should be locked and inaccessible to users.
- How will functionality be configured? Is there a custom script requirement when using application wizards? A macro is custom software. Even when created by keystroke capture, there is a program in a language such as Visual Basic for Applications® (VBA) behind each macro.
- Will there be more than one module? Integration testing is appropriate in such circumstances. For spreadsheets this may involve direct cell links to other worksheets. These links can be affected by changes, and should be addressed as part of the change control process.
- Will data input be only via keyboard? External data feeds need configuration, and a spreadsheet may not be sophisticated enough to deal with unusual input (e.g., a character string that is too long).
- Will output be saved to file or only printed? Electronic record controls may be necessary if the document is retained electronically.

2.5 True Desktop Databases

Both proprietary and open source desktop databases offer superior solutions to managing large volumes of data compared to spreadsheets, but they still are often significantly less secure than more sophisticated database management systems developed to run in IT-managed server-based environments (e.g., Oracle®). This may present significant issues if the information in the database is GxP regulated. External controls may be required.

3 Risk-Based Approach

End user applications can vary significantly in risk and complexity. The following are, however, required for all applications:

- risk assessment and appropriate risk control measures to manage identified risks
- Appropriate specification and verification to determine that the application performs as intended.

The strategy for specification and verification of the application being built should be based on:

- system impact on patient safety, product quality and data integrity (risk assessment)
- system complexity and novelty (architecture and categorization of system components)
- appropriate security to mitigate the risk of unauthorized changes to data or the application

- management of the application under change control

Company policies and procedures should define their specific approach to achieving and maintaining compliance and fitness for intended use of end user applications.

This appendix:

- describes how the use of GAMP categories assists with understanding novelty and complexity
- provides advice on appropriate risk-based controls
- provides examples of typical approaches for different applications

3.1 Use of GAMP Categories

The product on which the application is built should be considered to be Category 1. Categories for spreadsheets and other end user applications should be viewed as a continuum that spans Categories 3, 4, and 5 (see Figure S3.1). Assignment of a category is a function of the complexity and novelty of the spreadsheet or application. Note, however, that a spreadsheet that merely makes use of the tabular editing power and does no calculations should be considered a document.

A spreadsheet that simply uses native functions to make calculations in place of a hand-calculator is typically Category 3. For example, a laboratory analyst might create a unique spreadsheet to do a calculation related to an "Out Of Specification" investigation. When the spreadsheet's arithmetic functions are used, the calculations should be fully explained, as they would be in a text document. This should include verification that the intended formulae have been used properly, and that the data being analyzed is the right data. Such verification could easily be documented by having another analyst or a supervisor examine the spreadsheet and approve it. No further verification is required, since there is no need to challenge the accuracy of the calculations.

When developing spreadsheets as templates, such templates could be Category 3 to 5, depending on complexity, see Section 2.4 of this appendix. For example:

- A template is used by analysts in a laboratory to do a routine calculation of averages and standard deviations of experimental results. This is a straightforward arithmetic operation with no configuration, so the template is Category 3.
- A spreadsheet template requires the user to input tablet strength, so that the application automatically branches to different cells to use strength-specific calculations based on this initial input. Such a simple operation would make the sheet Category 4, as it is effectively configured by the analyst before each use of the template.
- a spreadsheet application that employs custom macros or sophisticated or nested logic or lookup functions should be treated as Category 5

Figure S3.1: Continuum of Categories for End User Applications

	Spreadsheets	Personal Databases	Data Mining and Analysis Tools
Category 5	Custom Macros	Custom Macros	Custom Macros
	Sophisticated Lookup Functions	Multiple System Sources (e.g., ODBC Connectivity)	
	Nested Boolean Functions		
	Networked Spreadsheet Applications		
	Customized Functions		
Category 4	Simple Boolean Functions	Multiple Related Table Operations	
	Complex Template		Complex Analysis based on Labels
	Statistical Functions	User Defined Queries and Reports	
	Range Operations	Simple User Form Linked to Single Table	
Category 3	Cell Relationships		
	Simple Templates		Simple Analysis based on Preddefined Queries
	Arithmetic Operators Printing Functions		
Category 1	Spreadsheet Office Application	Personal DB Office Application	Package for Building SW Tool

4 Risk-Based Controls

GxP risk should be assessed. The following aspects should be considered:

- data integrity related to the control of data files, as most end user applications process data
- The complexity of the application, based on the assumption that undetected systemic errors are more likely in software not developed under a rigorous development method, and more complex applications have more opportunities for errors.
- potential impact on patient safety, product quality or data integrity.

Based on these risk assessments, controls should be established which focus on:

- degree of verification
- security control (for both the application code and any GxP records that are in the application)
- control of changes
- control of the infrastructure on which the end user application is built

4.1 Degree of Verification

The extent and rigor of verification should be based on risk, complexity, and novelty.

One level of testing may be appropriate for simple and low risk systems or several levels may be required.

Complex and higher risk applications require more rigorous testing. The amount of logical branching in the application is a good gauge for complexity; if many logic functions (IF, AND, OR, etc.) or lookup tables are used, complexity is higher. Although they are native functions, these introduce more potential pathways through the application, and such branching requires a more sophisticated test strategy.

Macros also increase complexity, because these are effectively embedded secondary applications. Even when created by keystroke capture, there is a program in a language behind it, although macros that simply automate a string of actions are less of a concern than ones that contain logical branches. Macros should be challenged in documented functional testing. Macros that include logical branches should be subject to greater rigor, with attention paid to multiple logic paths.

See Appendix D5 for further details on testing.

4.2 Security Control

Security considerations for end user applications are similar to those for server or web-based applications, such as access to the application, access to data through the application, and access at the operating system level to data or the application code. Security within the environment should be adequate for the type of information stored or processed.

For many end user applications, a combination of infrastructure controls (e.g., restricted access to directories) and controls available through the application (e.g., password protection of spreadsheet cells) can provide some security against unintentional change. These controls may, however, be ineffective in keeping the application author from making changes outside of a change control process, especially if the application resides on an individual workstation. In some cases it may be possible to improve security by running the end user application on a network drive on which the user's rights are limited, and which includes a regular scheduled back-up process.

Data is often saved within the application itself, especially in spreadsheets. Ensuring adequate data integrity held in spreadsheets requires the use of strict controls, including any required electronic record controls. Where spreadsheets are subject to edit, it is difficult to establish whether original data in subsequently saved copies has been edited. In such cases adequate control can be provided through the use of an Electronic Document Management System (EDMS). Alternatively, it may be necessary to maintain controlled copies in an unalterable format, e.g., PDF or hardcopy. In general, GxP data should not be saved to a non-secure, non-backed up local disk drive.

If the degree of security that can be provided is not adequate for the data being managed, consideration should be given to the use of applications that operate in a more robust environment.

4.3 Change Control

End user applications that process GxP data should be subject to change control. Version management is difficult for such applications. In some cases, especially spreadsheets, management of the application within an EDMS may be an appropriate solution, as an audit trail of application versions will be retained. Another solution is to use library tools that are often used by developers to manage code. These can be used to manage any type of file, can be effective and reasonably easy to implement, and are less expensive than an EDMS. The use of either approach may also control risks related to security of the environment.

As with any change control process, changes to end user applications should have a change record that includes a description of the change and an assessment of the impact. Where appropriate, associated testing should be documented.

4.4 Control of the Infrastructure

End user application environments are Software Category 1 (see Appendix M4). These tools provide an application environment for the spreadsheets, databases, programs, or scripts that are developed by users.

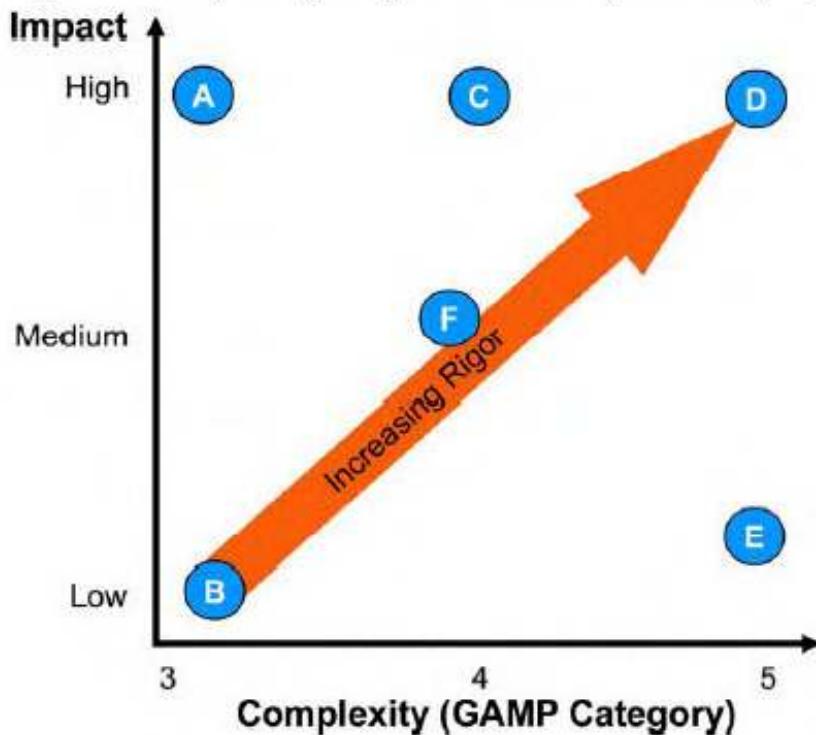
The installation of the environment should be verified and the environment should be managed under change and configuration management.

5 Examples of Typical Approaches

Figure S3.2 illustrates five different end user applications and a brief summary of potential approaches based on consideration of GxP impact and the complexity of the application. These examples are intended to be illustrative only, and not definitive.

The analysis is based on an assumption of a constant level of risk. If the risk for a particular application is high, then the rigor should be increased.

Figure S3.2: Examples of Typical Approach Based on Impact and Complexity



- A. simple spreadsheet template for arithmetic calculation for content uniformity test:
 - high impact, low complexity
 - recommended approach:
 - User Requirements Specification (URS), documented verification by a third party that the calculations are the right ones
 - security to ensure the sheet is protected against unauthorized change
 - security to ensure the users can access only the approved version
 - secure storage of electronic document
- B. spreadsheet record of training attendance
 - low impact, low complexity
 - recommended approach:
 - no specific functionality requiring specification and verification.
 - standard controls for electronic documents containing evidence for GxP compliance
- C. desktop database for analyzing toxicology study
 - high impact, medium complexity
 - recommended approach:
 - full Category 4 approach: validation plan, URS, Functional/Design Specification (may be combined), Traceability, Documented testing against predetermined acceptance criteria, validation report
 - security to limit access to authorized users
 - change control
- D. spreadsheet for statistical analysis of a clinical study, with VB macros
 - high impact, high complexity
 - recommended approach:
 - full Category 5 approach: validation plan, URS, Functional/Design Specification (may be combined), Traceability, Documented testing against predetermined acceptance criteria, validation report
 - security to limit access to authorized users
 - change control

- E. spreadsheet for statistical analysis of manufacturing data for purpose of statistical process control of parameters within validated ranges (includes complex logic and look-up functions).
 - low impact, high complexity
 - recommended approach:
 - documented verification by a third party that the calculations are the right ones
 - change control
 - security to ensure the sheet is protected against unauthorized change
 - security to ensure the users can access only the approved version
- F. desktop database tracking disposition of printed labels
 - medium impact, medium complexity
 - recommended approach:
 - abbreviated Category 4 approach: validation plan, combined URS/Functional/Design specification, documented testing against predetermined acceptance criteria, validation report
 - change control
 - security to limit access to authorized users

Patch and Update Management

1 Introduction

This appendix describes the compliance aspects to consider when planning security patches, hot fixes, or service pack upgrades.

There may be a frequent need for such patches and updates, for reasons including:

- Widely integrated and connected applications may be vulnerable on several levels to abuse and exploitation with malicious intent. Examples include:
 - theft of personal data or intellectual property
 - theft of computing power and bandwidth for malicious software agents
- Complex software may be released with defects. Such defects may affect critical processes, and require fixes to be issued by the supplier.
- periodic software updates from suppliers

Appropriate management of patches and upgrades is particularly important to maintain compliance and fitness for intended use of GxP regulated computerized systems.

2 Approach to Patch and Update Management

Regulated companies should develop an approach to patch and upgrade management that:

- provides criteria for determining enterprise threat levels, and thus the urgency for applying patches
- allows for flexibility in patch application that considers risks to both the enterprise and risks to the compliant status of regulated systems
- generates configuration records that show the version and patch level for a system at any point in its life cycle
- Generates change records that describe what level of testing was done. This may include general testing at the enterprise level and/or application specific tests. It may be determined by analysis of release notes that an application is unaffected and no testing is required.

There is a need to determine what effect applying (or electing not to apply) a patch or upgrade will have on the compliance status of GxP regulated computerized systems. Many patches are released by suppliers to address urgent security vulnerabilities, and exploits may already be known or may be imminent. The time required to evaluate and test all affected GxP regulated computerized systems prior to implementation of the patch may therefore increase the risk to the integrity of these systems and their data.

Regulated companies should develop a risk management approach for patch and upgrade management that considers both regulatory compliance and the level of threat to the system and the wider computing environment. The approach should ensure there is a requirement for clear communication at the appropriate times.

Application specific patches should be planned as part of normal change management procedures. Patches that must be applied enterprise wide are far more difficult to plan. Figure S4.1 illustrates some of the strategies that may be considered for such patches. The more aggressive options tend to minimize risk to the enterprise as a whole by expediting the fix, thus reducing exposure to the problem addressed by the patch. This has the side-effect, however, of increasing the risk to the compliance status of individual applications because the impact of the change has not been considered fully in the context of each application.

The Quality Unit should approve the process for risk evaluation of all patches. The evaluation should be performed by appropriate subject matter experts. The process should define the criteria and required approvals for selecting and following each defined strategy, such as those shown in Figure S4.1. Roles and responsibilities should also be defined.

Figure S4.1: Patch Strategies and Related Risk Levels

Risk to	Strategy
	<ol style="list-style-type: none">1. Patch or upgrade "pushed" to environment as soon as it can be configured; users notified afterward2. Patch or upgraded "pushed" to environment at a non-negotiable time with advanced notice to users3. Patch or upgrade built into planned ad hoc upgrade with users involved in planning4. Patch or upgrade built into user's normal scheduled upgrade cycle5. Patch or upgrade not applied

The selection of the strategy for applying the patch should consider the degree of risk reduction.

For example, a fix to an operating system level security problem that threatens a wide range of GxP regulated and unregulated systems it may appropriate to follow strategy 1 since this patch reduces risk to all of the applications.

Alternatively, the infrastructure group or other Subject Matter Experts (SMEs) may be able to assess a risk level as being very low, e.g., when a patch disables a software port that is typically unused by applications. In this example the risk evaluation may conclude that there is no risk to the applications and therefore any of the patch strategies in Figure S4.1 may be selected. Furthermore testing at the application level would not be necessary in this example based on knowledge of the application and the nature of the patch.

2.1 Configuration Management

Accurate and complete configuration management records support patch and update management in several ways, including:

- **Planning future patching activities:** Sometimes patches must be applied sequentially, so it is important to know the current patch level.
- **Interoperability:** If a system is running at multiple locations, there may be compatibility issues if different sites are at different patch levels. External applications may also require an interfaced system to be at a particular version and patch level.
- **Troubleshooting:** Thorough knowledge of a system's configuration is often critical to understanding what went wrong.
- **Data Integrity:** Application of a security patch may be crucial to data integrity, especially if exploits are widely published. It is important to be able to demonstrate that security gaps have been closed, and when this was achieved.

Configuration records for systems and infrastructure should be sufficient to show the current *as-built* state and when patches or upgrades have been applied.

See Appendix O6 for further details on these topics.

Managing Quality within an Outsourced IS/IT Environment

1 Introduction

Many regulated companies are outsourcing Information Systems or Information Technology services.

The outsourcing model can vary significantly in terms of:

- use of offshore, near shore or on-shore suppliers
- use of external supplier resources only
- use of external supplier computing environments

The controls required to manage the outsource service will be determined by the scope and criticality of the outsourced services and the outsourcing model employed. A quality risk management approach should be employed to ensure that adequate controls are in place and that patient safety, product quality and data integrity are not compromised.

Information Technology Infrastructure Library® (ITIL) is the most widely accepted approach to IT service management and can be used to assess supplier processes (Reference 36, appendix G3).

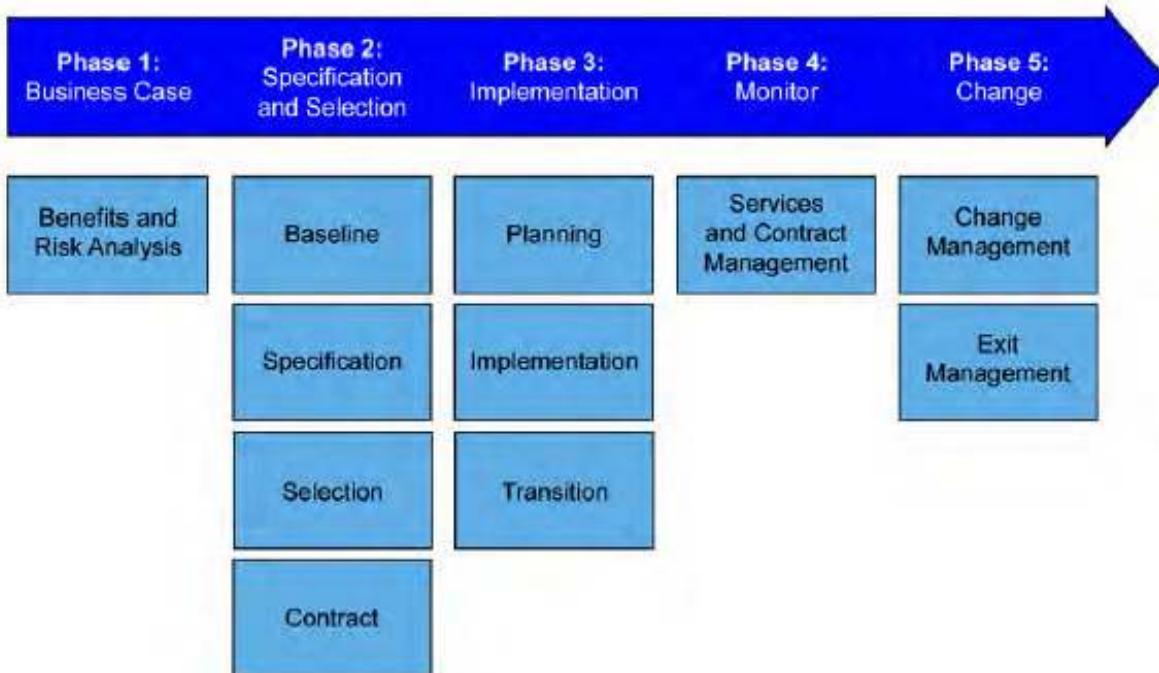
2 Outsourcing Process

Figure S5.1 shows a generic outsourcing process. This is divided into five phases:

1. initial business case
2. selection and specification
3. implementation
4. monitor
5. change

These phases are described in more detail below. Note that the phases described here are specifically for an outsourcing process and not the phases of a computerised system life cycle as described in the Main Body.

Figure S5.1: Outsourcing Process



2.1 Phase 1: Business Case

The benefits of outsourcing may include:

- focus on core, value adding business activities (product development and manufacture)
- cost optimization
- access to resources, capability and technologies
- optimise resource and asset utilization
- improved service portfolio and performance improvement
- simplified organization, supply chain
- improved quality standards

Quality considerations should be balanced against other benefits when defining the business case. The Quality Unit should be involved in developing and approving this aspect of the business case.

The following risks should be considered:

- misalignment of business objectives – quality versus cost versus volume
- loss of control and visibility of regulated services
- loss of intellectual property control

- constraints to business improvement, focus on maintaining the *status quo*
- loss of business knowledge base
- reduction in quality standards
- accountability and liability

2.2 Phase 2: Specification and Selection

2.2.1 Baseline Assessment

Prior to defining the outsource specification, the regulated company should be clear as to the current quality and compliance status of equipment and applications included within the scope of the contract, including:

- regulatory impact of applications, assets, services to be outsourced (GxP, Sarbanes-Oxley (SOX), privacy, etc.)
- current quality status
- current documentation and records management practices (of particular importance to outsourcing maintenance of existing applications, assets and services)

A key step in defining the baseline is to create a process map of activities that are under consideration for outsourcing with the associated roles and responsibilities. This map can be used to help develop the Service Level Agreement (SLA), identify any gaps in support, and aid in identifying any hidden costs that might be passed on to the customer.

This Guide provides guidance on supplier assessment (see Appendix M2) and the *GAMP Good Practice Guide: IT Infrastructure Control and Compliance* (Reference 34, Appendix G3) provides guidance for infrastructure assessment. The assessment should define the quality baseline that should be maintained and areas requiring improvement; both should be defined in the outsource contract. An important aspect of any supplier assessment is employee staffing. Employee qualifications, employee turnover and ratio of employee to customer(s) should all be carefully reviewed and addressed appropriately in the SLA.

If there are any gaps in service that supplier is unable or unwilling to provide then the regulated company should have a plan for filling such gaps. This may mean retaining or hiring the appropriate internal resources to support the missing or inadequate activities.

2.2.2 Outsource Specification

The Outsource Specification defines the services, assets and organizations to be outsourced. Table S5.1, identifies some important quality related considerations when defining the Outsource Specification.

Table S5.1: Outsource Quality Considerations

What are the Service Definition, Quality Requirements, and Performance Requirements?
What is the Quality Organization Structure and Relationships?
What are the compliance expectations against regulated company internal policies, standards and processes?
What is the definition of Quality Framework – Quality Management Objectives and Key Process Requirements, Regulated Company and Supplier QMS interfaces?
What are the training and education requirements?
Where are the Documentation and Information Responsibilities/Ownership defined?
What are the Performance Monitoring Expectations (e.g., SLAs) ?
What are the Auditing Requirements?
What are the Review and Approval Requirements?
What are the Quality Improvement Requirements?
What are the Security and Data Protection Requirements?
What are the Regulatory Inspection Support Requirements?
What are the Incident Reporting and Investigation?
What are the Alert and escalation procedures?
What are the Records management and retention requirements?
What outsource contract startup and transition controls are required?
What outsource contract change management and exit controls are required?
What is impact on existing service levels (a fall in service level is not always detrimental to GxP compliance)?
Implications of different business risks across the infrastructure e.g., GxP and non GxP?
Whose processes, procedures and systems will be used?
How will the regulated company's and the outsource company's processes, procedures, and systems be interfaced?
Will the outsource organization's processes, procedures and systems be transparent to the regulated company organization?
Which organization is responsible for defining, reviewing, authorisation and implementing changes to the outsource organization's processes, procedures and systems?
Whose information/documentation standards will apply?
Who will own documentation, are there any issues with shared documentation management responsibilities?
What will be the impact on regulated company staff, will they transition to the outsource company. Will they continue to be engaged in the provision of services to the regulated company?
How will local site issues be managed and prioritised within a global contract framework?
How are outsourced services accessed?
How will outsourced service quality be measured and reported?
What are the implications of a global outsourcing agreement involving multiple regulated company businesses e.g., manufacturing versus research and development and different regional approaches?

Table S5.1: Outsource Quality Considerations (continued)

How will the outsource organization work with different regulated company processes, procedures and systems across regions and sites?
How will different regulatory demands (GxPs, regional) be addressed?
How will total dependence on outsource company's processes, procedures and systems be avoided. In particular, how will the regulated company regain control of processes, documentation and information in the event that a new service provider is selected or services are taken back in house?

2.2.3 *Outsource Scope Considerations*

The scope of the outsource agreement will influence the complexity of the outsource strategy and the ability to achieve a consistent quality standard and service levels. Table S5.2 highlights some of the issues to be addressed when considering the various scope issues.

Table S5.2: Outsource Contract Scope Considerations

Scope	Consideration
Regions and Countries	Cultural differences
	Working practices
	Language
	Time differences (24/7 access)
	Processes and systems
	Legislation, regulations and industry influences
R&D, Manufacturing or Non-GxP	Different quality systems
	Different regulatory requirements
	Different quality organisations
	Different service expectations
All services versus selected services	Defining Boundaries and Interactions
	Defining Accountabilities (internal and external)
	Managing the Customer Interface
	Define whose processes, procedures and systems will be used
	Defining consistent service levels for internal and external services
Use of service provider assets or internal assets?	Data ownership
	Shared infrastructure with other regulated companies
	Open System issue
	Security policies
	Relationships between internal and external organisations

Financial details, warranties, liabilities and indemnities should also be covered. The contract may need to be structured to allow for regional or organizational variances to reflect local needs. The extent of such variance will impact the complexity of contract governance.

Data ownership should be made clear in the contract. Regulatory authorities will be interested in who is accountable for regulated processes and data.

Compliance is the responsibility of the regulated company, not the outsource organization. This means that accountability and liability for security remains with the regulated company.

Security related roles and responsibilities should be clearly and completely defined, including clear security objectives specified in the SLA for integrity, confidentiality, availability, accountability and control of use.

The regulated company should make provision for contract exit should the relationship with the outsource partner be unsatisfactory. Many regulated companies ask that systems be developed in accordance with their own standards and procedures so that if a change in outsource arrangements is required then they do not have the problem of converting documentation standards later.

2.3 Phase 3: Implementation

2.3.1 *Transition to the Outsource Company*

Transition to the outsource company usually occurs over a period of time, typically migrating less critical or complex services or applications first in order to gain learning before migrating more critical and complex services or applications. Plans should consider:

- when services, assets, applications will be migrated
- when people will transition to the outsource organization
- when, where and how the outsource partner should apply their own processes and procedures
- service disruption management
- knowledge transfer

During this period, potential problems arising from lack of trust, perceptions of falling services standards and employment fears should not be underestimated. An expert team comprised of experts from both organizations should be in place to address these issues.

2.3.2 *Governance*

The governance model for the outsource contract should be carefully defined. From a quality perspective alone, there may be several quality functions that could potentially interface with the outsource organization including Research and Development (R&D) quality management, manufacturing quality management, business quality assurance, and corporate audit groups.

Quality interfaces to the outsource organization should be streamlined. An internal committee comprising quality representation from all impacted organizations may be a useful way of communicating quality expectations and concerns and to understand improvement plans.

Business Management:

- assess outsourcing benefits and risks
- ensure intellectual property and critical data is identified and protected
- define relevant laws, regulations, licensing agreements and directives
- establish and communicate outsourcing and quality policies and standards

Contract Management:

- Establish and monitor conformance to Contract, Outsource Specification, and SLAs. Manage deviations.
- scope change management
- cost and performance management

Service and Quality Management:

- Establish and monitor conformance to contract, Outsource Specification, and SLAs. Manage deviations.
- scope change management
- cost and performance management

Customer/Supplier Relationship Management:

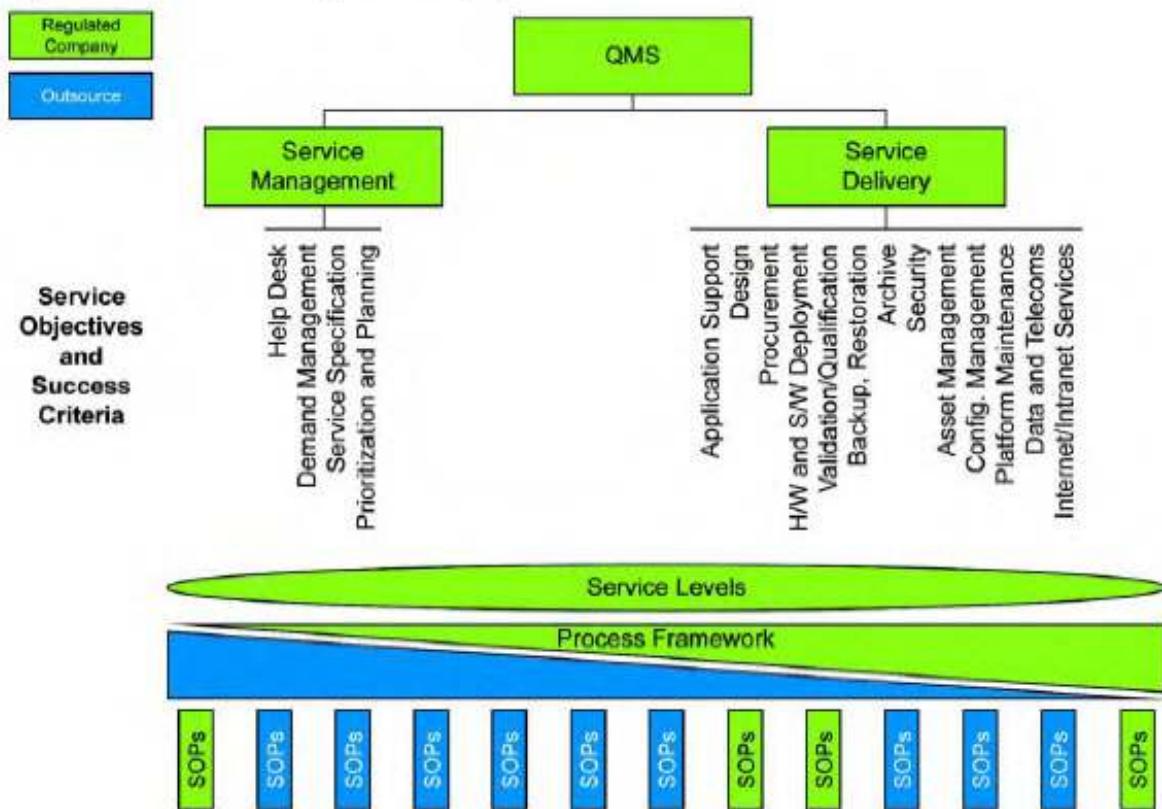
- regulated company/supplier working relationships
- effectiveness of regulated company/supplier interfaces and governance structures
- be sure that the supplier supports post-incident review

2.3.3 *Quality Management Systems*

The scope of the outsource agreement will determine the shape and content of Quality Management Systems (QMS) operated by the regulated company and supplier organizations. In a total outsourced agreement, regulated company quality systems should be focussed on defining minimum standards and outsource management processes; whereas supplier quality systems should be focussed on service/application delivery and support processes. It is essential that relevant processes are in place on both sides of the agreement and that interfaces between processes are clearly defined.

Figure S5.2 shows a typical relationship between a regulated company QMS and the outsource processes which define the external services to be provided.

Figure S5.2: Framework of Regulated Company and Outsource Processes



SLAs define the services to be provided, the mechanism for requesting and delivering services, service performance targets and relate service levels to the contract objectives.

Typical interface processes include:

- requirements and planning
- change management (technical and scope change)
- security management
- disaster recovery and business continuity
- assurance (incident reporting and review, audit, periodic review)
- dispute resolution and escalation
- performance reporting, monitoring and improvement
- training (including regulatory as appropriate)
- records management (retention, retrieval, access control, data integrity)
- risk management

2.3.4 Skill Considerations

Skills requirements and shortfalls should be addressed as part of the contract implementation and on an ongoing basis. One of the purposes of outsourcing will be to increase skills, typically technical skills but there are a number of other skills considerations.

Knowledge of the current application and asset configuration and documentation and records systems will reside in the regulated company organization. This knowledge may be transferred to the outsource organization by transferring resource to the outsource organization. Alternatively, knowledge transfer should be built into the transition plan. Even when resource is transferred to the outsource organization, resource turnover, redeployment and succession may cause knowledge loss.

A key benefit of internal resource is that they understand business needs and risks, including the regulatory and quality environment within which applications and services are delivered and maintained.

Quality skills and knowledge need to be transferred to the outsource organization. Quality knowledge includes:

- company policies, processes and systems/tools
- knowledge of GxPs, industry best practice (including document and record management practices)
- understanding of quality and regulatory related risks on both a local and regional basis
- understanding of documentation structures for existing applications and assets

2.3.5 Supporting Systems

A number of systems will be employed by the regulated company prior to migration to the outsource company. These systems will vary largely from organization to organization in terms of sophistication and integration. Further, there may be multiple different tools meeting the same objective if the scope of the outsourcing crosses organizational boundaries. Such tools include but are not limited to:

- help desk
- configuration management
- service management
- document management
- inventory management
- automated testing

Whether the existing internal systems, outsource company systems or a blend of both will be used is dependent on a number of factors. These factors include:

- standard tool set used by outsource supplier
- scope of services or applications outsourced
- standardisation of platform across organization

- compliance status, e.g., validation, electronic records and signatures, operational controls
- information migration issues
- ability to withdraw from the contract without data and documentation loss

2.3.6 *Information and Document Management Issues*

Responsibilities for document and information management should be defined by the contract. Some documentation will be jointly developed by the regulated company and the outsource company.

A key problem arising when outsourcing is that transparency of information and documentation is lost. Important documentation and records supporting regulatory compliance may not be easily accessible. Such records should be periodically audited to ensure application of defined quality and documentation standards. Further, the contract should define requirements for providing access to such records during a regulatory inspection.

2.3.7 *People Considerations*

Personnel issues and their impact on quality should not be underestimated when establishing an outsource agreement. Some of the issues faced by internal personnel include:

- loss of accountability and control
- fear of losing their job
- transfer to other organization
- change in employment drivers (commercial versus technical versus personnel well being)
- change in role (technical to supervisory)
- loyalty to customers
- new processes and standards

2.3.8 *Supporting Regulatory Inspection*

The contract should ensure that adequate support is provided by the outsource company during regulatory inspection. The regulated company remains accountable for the information supporting compliance and as such cannot abdicate responsibility due to the outsource arrangement. Inspections may take place at either the regulated company premises or the outsource company premises, or both. Regulated companies are likely to want to be present in helping to prepare and manage regulatory inspections at their outsource partner premises.

The outsource contract should define how outsource personnel are engaged during a regulatory inspection and appropriate inspection readiness and support training should be provided. The contract should define requirements for accessing people and documentation. Staff at outsource companies who could be called upon to present should be trained in terms of what to expect and etiquette during inspections. Provision of suitable translators who appreciate the technical aspects of systems should be planned if relevant.

Retention schedules and retrieval times for key documents need to be agreed. Consideration should be given to providing governing policies, standards, and processes in a language which can be understood by the regulatory authority without translation. Other documents do not necessarily need formal translations but should be readily available for immediate inspection such as:

- plans and specifications
- configuration information
- training records
- system data/records

Security arrangements for personnel and information should be clear as these are likely to be checked. These arrangements will include remote access to systems under local management of outsource company, security within outsource company to preserve confidentiality and integrity of regulated company information, and any information transfer (electronic or paper) between the outsource company and regulated company.

2.4 Phase 4: Monitor

Typically periodic reports are issued defining service performance against agreed service levels. Where global or major outsourcing agreements are in place, the reporting structure should not obscure significant quality and performance incidents at a site level e.g., a significant infrastructure outage or compliance shortfall at a site level should not appear to be insignificant at a global level.

Performance reporting should provide a combination of cost, quality and service volume metrics. The structure of the reports should consider the various stakeholders interests in cost, system outages, end user service satisfaction, and quality and compliance.

Audits should be conducted periodically in order to ensure that processes and standards are complied with. Typically, a central auditing group will conduct audits in order to ensure consistency from site to site and region to region. Where central audit functions are used all quality and compliance management stakeholders should be able to influence the audit scope and objectives. Central auditors should be aware of site and regional issues prior to conducting audits at that site or within that region.

2.5 Phase 5: Contract Change and Exit

Quality representatives associated with the outsource contract should be consulted prior to the change in order that changes to service levels and the quality framework can be evaluated and addressed.

In particular, consideration should be given to changes in the regulatory environment. It may be necessary to respond to regulatory changes mid contract. Contract provisions should ensure that suppliers are agile to changes in regulatory environment.

The greatest change that will occur is contract exit, either as a result of changing suppliers or on occasions bringing services back in house. All considerations of the original contract creation should be considered such as:

- availability of controlled and compliant infrastructure
- availability of business, technical and quality capability
- availability of suitable service and application delivery and maintenance policies, standards and processes
- ownership and migration of documentation and records to regulated company systems
- phased migration to ensure continuity of service and performance

Risks need to be carefully managed. When an outsource organization is being changed because of poor performance the level of assistance may decrease. Skilled staff are likely to be moved off the project and low priority given to necessary activities. The business continuity of the regulated company could be put in jeopardy. Contracts should therefore include provision for change due to poor performance, while safeguarding business continuity.

Organizational Change

1 Introduction

This appendix provides guidance on how to deal with organizational change.

There is a global trend towards consolidation and outsourcing, and this trend is likely to continue. This appendix considers the impact of such change on GxP regulated computerized systems, and provides guidance in terms of areas to be considered for ensuring continued compliance and system availability.

2 Initiators for Change

Reasons for organizational change may include:

- internal re-organization
- being acquired by another company
- divesting part of an organization to a third party (including activities such as offshoring and outsourcing)
- a supplier ceasing to trade

3 Scope and Impact of Change

The organizational change may apply to any aspect of the system supply chain, including regulated companies, system integrators and base product and infrastructure suppliers.

Organizational change can occur during any stage of a computerized system's life cycle, and the impact of the change will depend on the stage. When organizational change occurs aspects to consider include:

- changes in the business process that a computerized system supports.
- changes in how an existing system is used.
- moving systems from one location to another.
- new or different regulatory and compliance requirements.
- the impact on regulated records and any associated signatures.
- changes in how security (both physical and logical access control) is handled.
- clarification of where the master data is located.
- clarification of who the process and system owners are or will be.
- the timing and need to perform an audit of a reorganized supplier.

- the business relationships with the supplier.
- impact of the change on any service level agreements.
- the impact on company strategies with regard to preferred solutions.
- interim measures/solutions.
- maintaining expertise on systems (both with regard to the supplier and the regulated company).
- validity of any support contracts with suppliers.
- postponement or cancellation of existing system implementation projects
- acceleration or advancement of existing system implementation projects
- changes in personnel and/or individual responsibilities.

4 Organizational Factors

Organizational challenges include:

- maintaining multiple/parallel system for the same business process
- developing interfaces between these multiple/parallel systems
- the migration of data or subsets of data from one system to another
- maintaining data sets for third parties for (possibly significant) periods of time
 - Will all data be treated in the same manner?
 - Will the data remain in the same format?
 - Will some data be converted to paper/fiche records?
 - Will some data be discarded?
- systems likely to be retired
- the location of life cycle documentation (paper and electronic) and inspection support on an ongoing basis
- maintaining multiple/parallel compliance practices and documentation
- harmonization of compliance practices, documenting the rationale for change (and justify with regulator) and training in new practices
- in some cases the regulatory expectations will change and existing life cycle activities and documentation may have to be readdressed
- how change management and configuration management will be handled across the changed organizations

- ensuring that operation and maintenance activities are clearly identified and transitioned across to the revised organizations
- increased focus/profile of incident monitoring during the transition period

5 Outsourcing

Where the organizational change is associated with outsourcing then the following additional aspects should be considered:

- the decision as to whether the regulated company continues to own the equipment or whether this transfers to the outsource company
- whether the outsource organization Quality Management System (QMS) is used or the regulated company QMS
- the need to both initially and periodically audit the outsource organization (the audit scope should be both compliance and financial)

See Appendix S5 for further details.

6 Loss of a Supplier

Where the change is associated with a supplier ceasing to trade consideration should be given to:

- ensuring Business Continuity Plans are established and accurate for the related systems
- invoking any escrow agreements to gain access to application source code
- record and system migration options
- retrieval of any regulated company owned components, including hardware, software, records, and associated documentation retained from the supplier

7 Risk Assessment of Organizational Change

A risk assessment process to identify and rank risks should be executed in order to develop a plan. As part of the risk assessment process, projects should be considered as well as operational systems, the likely approach will depend on the nature of the change. Table S6.1 illustrates some possible scenarios:

Table S6.1: Possible Scenarios Resulting from Organizational Change

Project Status:	Company Acquisition	Company Merger	Supplier Insolvency
Not Started	Put on hold pending management review	Put on hold pending management review	Cancelled
In Progress Early in Life Cycle	Put on hold pending management review	Put on hold pending management review	Cancelled
In Progress Late in Life Cycle	Put on hold pending management review	Continued	Put on hold pending management review
Approaching Go-live (Decisions on these projects will be a priority)	Put on hold pending management review	Continued	Put on hold pending management review

8 Affected Stakeholders

Whether dealing with internal or external organizations, agreement has to be reached between all affected organizations on any decisions concerning the system(s), the data, and the documentation.

All affected stakeholders (from all organizations) should be involved, and where required should approve the strategy and decisions made.

Representatives from the following business areas typically would be involved:

- business process owners
- compliance/quality/regulatory
- legal
- IT and Engineering
- purchasing groups and in some cases finance

One of the key tasks for the business area stakeholders is to review and update as appropriate documentation affected by the organizational change. Some key documentation areas to be considered are listed below:

- business process documentation
- policies, procedures, work instructions, test methods (if applicable)
- training materials
- user manuals
- batch records (if applicable)
- archived records/data
- contracts (if applicable)

- system interfaces
- validation/qualification
- records retention schedules

Another important task for stakeholders is to ensure that training requirements are evaluated. This should be performed against any changes made to quality management systems, ways of working or documentation, and should be considered at both an organizational and a system level.

