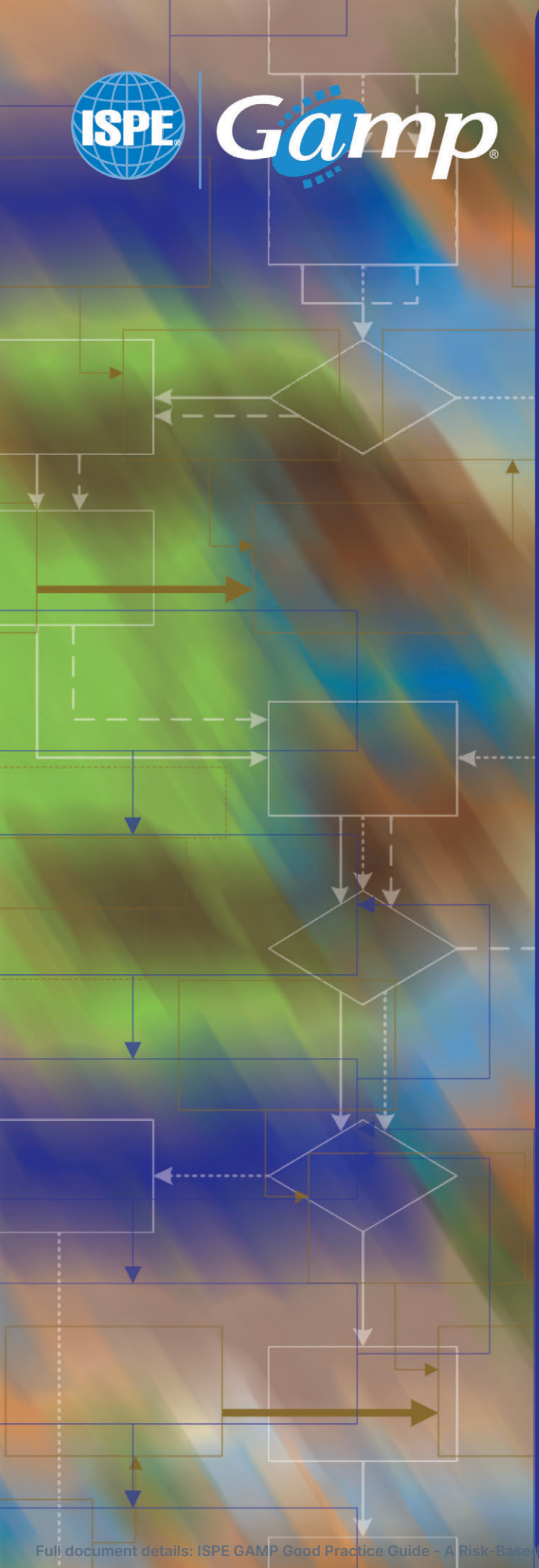


GAMP Good Practice Guide

A Risk-Based Approach to Testing of GxP Systems

Second Edition

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

What's your approach...

A leader in providing Computer Systems Implementation, Validation and Quality Assurance Services.



CQV (An Azzur Group Company) provides consulting services to the Life Sciences Industry. We offer system integration, compliance and validation services within the Quality Assurance, Laboratory, Clinical, IT/IM, Business Processes, Manufacturing, Operations, and R&D settings to our pharmaceutical, biotechnology and medical device clients.

With a depth of expertise in all facets of the system life cycle we are able to assist our clients within any phase to reach their goals of running a lean, efficient operation.

SERVICES AVAILABLE

- RISK-BASED LAB RELOCATION
- COMPUTER SYSTEMS VALIDATION
- INSTRUMENT IQ/OQ/PQ SERVICES
- LIFE CYCLE DOCUMENTATION
- LIMS SYSTEM QUALIFICATION
- IT INFRASTRUCTURE
- PROJECT MANAGEMENT

"...to achieve success?"

CQV (An Azzur Group Company) takes a holistic approach when working with our clients to provide the best service possible. We work hand in hand with each client to achieve success by ensuring that all goals are met and safe and effective products are delivered.

An Azzur Group Company

helping life sciences succeed

Tel: 800.726.0331 Email: info@azzurgroup.com www.azzurgroup.com

Documents
Document Sharing Hub

GAMP Good Practice Guide

A Risk-Based Approach to Testing of GxP Systems

Second Edition

Disclaimer:
This Guide focuses on functional, structural, and performance testing of GxP systems and is intended to assist regulated organizations and suppliers to work together to ensure sufficient test coverage to guarantee fitness for intended use, while minimizing any duplication of effort. ISPE cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

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

© Copyright ISPE 2012. All rights reserved.

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

All trademarks used are acknowledged.

ISBN 978-1-936379-51-4

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Preface

This document, the ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems, represents a revision of the first edition, ISPE GAMP® GPG – Testing and is intended as a supplement to ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems. This Guide focuses on functional, structural, and performance testing. It has been updated to align with the concepts and terminology of GAMP® 5 and regulatory and industry developments which focus attention on patient safety, product quality, and data integrity.

The ISPE GAMP® Community of Practice Document Task Team was asked to revise this Guide. The team consisted of representatives from regulated organizations, contract research organizations, suppliers of pharmaceutical systems and equipment, and consultants.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Acknowledgements

The production of the ISPE GAMP® Good Practice Guide: Risk-Based Approach to Testing of GxP Systems was initiated by the Testing Task Team at the request of the GAMP® Council.

The following members of the GAMP® Community of Practice (COP) Testing Task Team worked on one or more sections of this Guide and volunteered countless hours to attend meetings and review the many drafts. The members committed to, and achieved, a challenging timescale for this substantial revision and their exceptional efforts are much appreciated.

Chairs

Karen Ashworth	Karen Ashworth Consulting	United Kingdom
Charlie Wakeham	Pall Life Sciences	United Kingdom

Task Team Members

Kevin Ashley	Siemens Healthcare Diagnostics	United Kingdom
Karen Ashworth	Karen Ashworth Consulting	United Kingdom
Roger Buchanan	Lilly UK	United Kingdom
Jonathan Davey	Provalidus Ltd.	United Kingdom
Stephen Dawson	Eden Biodesign Ltd.	United Kingdom
Angille K. Heintzman	NHS Blood and Transplant	United Kingdom
Daniel G. Mewborn	Eli Lilly and Company	USA
Daniel Montgomery	Covance, Inc.	USA
Radha Ramesh	TCS	USA
Genni Sanders	Systematicity	United Kingdom
George Smerdon	Industrial Technology Systems Ltd. (ITS)	United Kingdom
Paul Smith	Agilent Technologies	United Kingdom
Kimberly Stanton	QPharma, Inc.	USA
David Stokes	Business & Decision Life Sciences	United Kingdom
Thanabalan Subramanian	GE Healthcare	United Kingdom
Matthew Theobald	Three Circles	United Kingdom
Steve Tinson	Scitech	United Kingdom
Simon Topham	Napp Pharmaceuticals Limited	United Kingdom
Anders Vidstrup	NNIT A/S	Denmark
Linda Waddick	Eli Lilly and Company	USA
Charlie Wakeham	Pall Life Sciences	United Kingdom

Within this highly professional and committed team, special thanks are due to David Stokes, Kimberly Stanton, and Steve Tinson for their expertise in innovative technologies and methodologies, and their dedication in formulating the guidance in these areas.

Contributing Members

The following contributors are members from the GAMP® COP US Automation SIG and GAMP® COP DACH Automation SIG. David Stokes coordinated the work of the Automation SIGs and integrated that work into the Guide as Appendix T11.

Peter Brandstetter	Arcondis GmbH	Austria
Konstantin Clevermann	IDS Scheer Consulting GmbH	Germany
Thierry Dietrich	Arcondis	Germany
Srinivas Gopanapalli	Cognizant	USA

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Andreas Hengstberger	Nycomed Austria GmbH	Austria
Bernhard Kausler	ITQ GmbH	Germany
Oliver Kieckhöfel	BTConsult GmbH	Germany
Stefan Münch (DACH Lead)	Rockwell Automation Solutions GmbH	Germany
Radha Ramesh (US Lead)	TCS	USA
Shweta Rangarajan	Celgene Corp.	USA
Ernst-Reiner Schäfer	Abacon GmbH	Switzerland
Jason R. Tepfenhardt	Genilogix	USA

The GAMP® Testing Task Team would like to acknowledge the support of their direct management and companies in this endeavor.

Particular thanks go to the GAMP® COP Editorial Review Board for their review and comment:

Winnie Cappucci	Bayer Healthcare (retired)	USA
Chris Clark (Chair)	Napp Pharmaceuticals Limited	United Kingdom
Gail Evans	ISPE	United Kingdom
Colin Jones	Conformity Limited	United Kingdom
Randy Perez	Novartis	USA
Sion Wyn	Conformity Limited	United Kingdom

The Leaders of the GAMP® Testing Task Team wish to thank GAMP® Council, GAMP® Europe Steering Committee, and the Guidance Documents Executive Committee (GDEC) for their contributions and commitment throughout the production of this Guide.



Connecting a World of
Pharmaceutical Knowledge

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

ISPE Asia Pacific Office
73 Bukit Timah Road, #04-01 Rex House, Singapore 229832
Tel: +65-6496-5502, Fax: +65-6336-6449

ISPE China Office
Suite 2302, Wise Logic International Center
No. 66 North Shan Xi Road, Shanghai, China 200041
Tel +86-21-5116-0265, Fax +86-21-5116-0260

ISPE European Office
Avenue de Tervueren, 300, B-1150 Brussels, Belgium
Tel: +32-2-743-4422, Fax: +32-2-743-1550

www.ISPE.org

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Table of Contents

1 Introduction 9
1.1 Overview 9
1.2 Purpose 9
1.3 Scope 10
1.4 Benefits 12
1.5 Objectives 12
1.6 Structure of this Guide 13

2 Key Concepts 15
2.1 Product and Process Understanding 15
2.2 Life Cycle Approach within a QMS 16
2.3 Scalable Life Cycle Activities 17
2.4 Science-Based Quality Risk Management 18
2.5 Leveraging Supplier Involvement 19

3 Regulated Organization and Supplier Relationship 23
3.1 Introduction 23
3.2 The Supply Chain 24
3.3 Quality Risk Management 25
3.4 Supplier Assessment 26
3.5 Leveraging Supplier Testing 28
3.6 Determining Appropriate Test Evidence 31
3.7 Ongoing Support 32
3.8 Commercial Issues 32

4 Appendix T1 – Test Practices 35
4.1 Introduction 35
4.2 Test Policies 35
4.3 Types of Verification 37
4.4 Determination of the Scope of Testing 58

5 Appendix T2 – Test Planning and Test Management 61
5.1 Introduction 61
5.2 Test Plan or Strategy 61
5.3 Test Metrics 81
5.4 Automated Tools for Planning and Management 88

6 Appendix T3 – Test Specifications, Cases, and Scripts 91
6.1 Test Specifications or Test Protocols 91
6.2 Test Cases and Test Scripts 92
6.3 Example Test Step Classification Scheme 99
6.4 Example Test Scripts and Cases 100

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

7 Appendix T4 – Test Environments 105
7.1 Introduction 105
7.2 Hardware Environment 107
7.3 Test Software 108
7.4 Test Data Sets 109
7.5 Test User Accounts 111
7.6 Test Documentation 111
7.7 Managing Test Environments 111
7.8 Automated Testing 114
7.9 Non-Linear Software Development Methods 114

8 Appendix T5 – Testing Execution 115
8.1 Introduction 115
8.2 Test Pre-Requisites 115
8.3 Test Execution 115

9 Appendix T6 – Test Results Recording and Reviewing 119
9.1 Test Evidence 119
9.2 Test Record Integrity 120
9.3 Post Execution Review 121
9.4 Test Evidence for Packaged Systems 122

10 Appendix T7 – Test Reporting and System Handover 125
10.1 Test Reports 125
10.2 Leveraging Supplier Testing 126
10.3 Determination of Residual Risk 127
10.4 Formal Handover and Release 127

11 Appendix T8 – Testing in the Operational Phase 131
11.1 Types of Change 131
11.2 Test Planning and Test Management 133
11.3 Testing Changes 134
11.4 Releasing a Change 138

12 Appendix T9 – Testing as Part of Data Management 141
12.1 Introduction 141
12.2 Data Migration 141
12.3 Data Verification 142
12.4 Manual Data Migration and Data Verification 145
12.5 Automated Data Migration and Data Verification 146
12.6 Data Management in the Operational Phase 149

13 Appendix T10 – Testing in Non-Linear Software Development Methods 155
13.1 Introduction 155
13.2 Non-Linear Software Development Life Cycles 155
13.3 Prototyping 157
13.4 Non-Linear Software Development Risk Scenarios 157
13.5 Testing by Phase 160
13.6 Team Roles 161
13.7 Test Documentation 162

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

14 Appendix T11 – Automated Test Execution and Computerized Test Management Tools 163
14.1 Introduction 163
14.2 General Benefits of Test Automation Tools 167
14.3 How to Use Test Automation Tools 168
14.4 Selection and Benchmarking of Computerized Test Tools 170
14.5 Assessment of Computerized Test Tools 175

15 Appendix E1 – Testing Configurable IT Systems 179
15.1 Introduction 179
15.2 What is special about these systems? – Risk Scenarios 180
15.3 Business Process versus Functional Process Testing 181
15.4 Typical Test Types and Phasing for Configurable IT Systems 185
15.5 Example ERP Test Script 186
15.6 Example Pharmacovigilance Test Script 189

16 Appendix E2 – Testing of Cloud Applications 197
16.1 Introduction 197
16.2 What is special about these systems? – Risk Scenarios 199
16.3 Typical Test Types and Phasing for Cloud Applications 206

17 Appendix E3 – Testing Analytical Instruments 209
17.1 Introduction 209
17.2 What is special about these systems? – Risk Scenarios 210
17.3 Typical Test Types and Phasing for Analytical Instruments 213

18 Appendix E4 – End User Developed Applications 215
18.1 Introduction 215
18.2 Core Package 215
18.3 Testing Approach 215
18.4 Management of Testing 215
18.5 What is special about these systems? – Risk Scenarios 216
18.6 Typical Test Types and Phasing for End User Developed Applications 217

19 Appendix E5 – Testing of Infrastructure and Interfaces 219
19.1 Introduction 219
19.2 What is special about these systems? – Risk Scenarios 223
19.3 Typical Test Types and Phasing for Infrastructure and Interfaces 226

20 Appendix E6 – Process Control Systems 229
20.1 Introduction 229
20.2 What is special about these systems? – Risk Scenarios 233
20.3 Typical Test Types and Phasing for Process Control Systems 236

21 Appendix E7 – Packaged Systems 241
21.1 Introduction 241
21.2 What is special about these systems? – Risk Scenarios 243
21.3 Typical Test Types and Phasing for Packaged Systems 244

22 Appendix E8 – Testing Systems Applying Process Analytical Technology 249
22.1 Introduction 249
22.2 What is special about these systems? – Risk Scenarios 253
22.3 Typical Test Types and Phasing for Systems Applying Process Analytical Technology 257

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

23 Appendix 20 – References 261

24 Appendix 21 – Glossary 263

24.1 Acronyms and Abbreviations 263

24.2 Definitions 265

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

1 Introduction

1.1 Overview

This Guide is a revision of the first edition of the ISPE GAMP® Good Practice Guide (GPG): A Risk-Based Approach to Testing of GxP Systems. It has been updated to align with the concepts and terminology of GAMP® 5 [1], associated GAMP® guidance, and recent regulatory and industry developments. These developments focus attention on patient safety, product quality, and data integrity.

GAMP® 5 and associated GPGs aim to provide guidance to achieve computerized systems that are fit for intended use and meet current GxP regulatory requirements, by building upon existing industry good practice in an efficient and effective manner. This Guide builds on the framework described in GAMP® 5, and provides detailed guidance on testing GxP systems.

GAMP® is an ISPE Community of Practice (COP). For further information, see www.ispe.org [2].

The approach and terminology used in this Guide are generally harmonized with the following industry guidance:

- International Conference on Harmonization (ICH) Guidance including Q8 [3], Q9 [4], and Q10 [5]
- ASTM Standard E2500-07, Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment [6]
- EU GMP EudraLex Volume 4 (Chapter 4) [7] and Annex 11 [8]

This edition of the Guide also has been aligned with advances in industry best practice, including:

- Increased adoption and implementation of Process Analytical Technology (PAT) and Quality by Design (QbD)
- Increased industry focus on risk-based approaches
- Increased use of non-linear development life cycles
- Increased use of automated test tools

Consideration should be given to the existing policies and procedures within a regulated organization and to other external industry standards and practices when applying the principles described in this Guide.

1.2 Purpose

This Guide has been written to provide regulated organizations and suppliers with pragmatic guidance on the testing of computerized and software based systems that impact patient safety, product quality, and data integrity. The key objective of this Guide is to encourage regulated organizations and suppliers to work together to ensure sufficient test coverage to guarantee fitness for intended use, while minimizing any duplication of effort.

The Guide seeks to identify the testing that should be performed and the associated level of documentation. Where suppliers' systems do not meet the expectations of a regulated organization, the Guide identifies suitable risk control strategies. These strategies can include the execution of additional testing, or the selection and use of alternative suppliers or products, by the regulated organization.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

This Guide intends to provide pragmatic answers to questions such as:

- Why should I test?
- What should I test?
- How much testing is enough?
- How should I conduct tests?
- How should I document my testing?

Specifically, this Guide is intended to take a risk-based approach to compliance of GxP computerized systems and provide practical advice on the application of this approach in the planning and execution of testing.

The Guide is intended to assist:

- Regulated organizations (the pharmaceutical customer or regulated user organization contracting a supplier to provide a product)
- Suppliers (usually external third parties, but also including "in-house" providers of IT services) including:
  - Suppliers of standard products
  - Systems integrators responsible for configuration and coding of standard product to create a specific application
  - Suppliers of control systems that are packaged with the process equipment
  - Service providers
- Regulatory agencies

The overall computer systems compliance approach recommended for regulated organizations is described in GAMP® 5. Suggested good practices for suppliers of GxP systems and services are described in Supplier Activities (Section 7) of GAMP® 5 [1].

1.3 Scope

The scope of this Guide is the testing of GxP regulated computerized systems, including 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)

AVA Documents
Document Sharing Hub

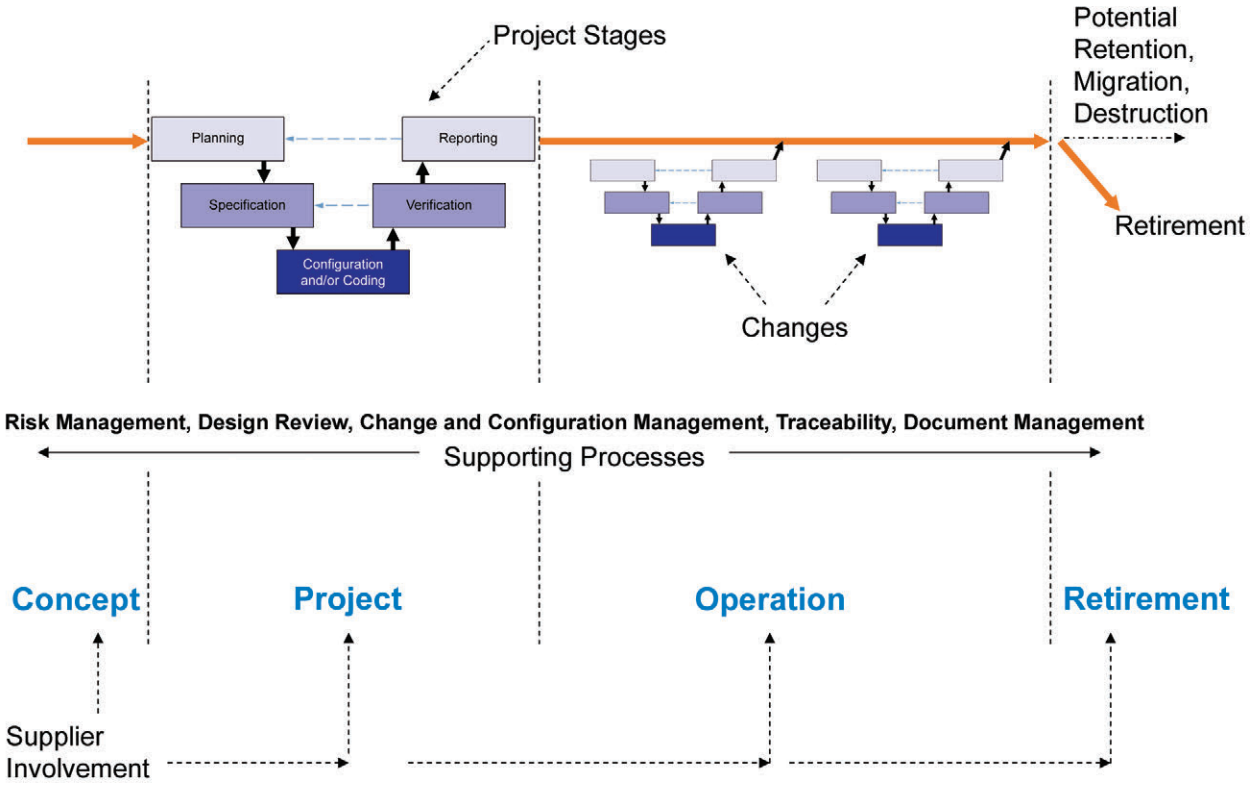
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

The Guide focuses on functional, structural, and performance testing. It also discusses other:

- Activities of the verification stage of the project phase of the life cycle
- Verification activities used to support or replace testing activities as a result of a risk assessment

Testing activities within the operation and retirement phases the life cycle are also considered. Other life cycle activities are out of scope.

Figure 1.1: GAMP® 5 Life Cycle



In the project and operation phases, verification should confirm that the regulated organization (or supplier) requirements and project specifications have been met. This can be achieved by applying an appropriate combination of:

- Design reviews
- Checking installation
- Reviewing configuration and data items, e.g., recipes
- Testing against specifications, e.g., module testing, integration testing, and functional testing
- Testing against requirements to ensure intended use will be consistently fulfilled
- Testing to ensure identified risk controls are in place and effective

This Guide will concentrate on the testing activities within verification.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

The focus of this Guide is GxP risk (i.e., risk to patient safety, product quality, and data integrity (and data confidentiality)); other aspects of testing (e.g., risks related to health and safety for personnel/caregivers or risks related to the environment) are out of scope of this Guide.

In the preparation of this Guide, the authors have deliberately chosen not to redefine testing good practice used in the wider software development and testing community. Focus is given to the pragmatic application of these practices to the testing of GxP systems and references for further reading are provided where appropriate.

1.4 Benefits

The main benefits from verifying systems include:

- Improved cost effectiveness from moving into the operational environment with systems that are fit for their intended use
- Ease of demonstrating compliance to regulatory requirements
- Improvement in patient safety, product quality, and data integrity as a result of control of identified risks

Insufficient or inappropriate testing may cause problems later in the system life cycle; these problems could be time consuming and troublesome to resolve.

Where there is pressure to implement systems in timescales that are unrealistic, there are several potential consequences:

- Reduction in the effectiveness and efficiency of the system at go live
- Increased maintenance and support costs
- A costly program of corrective actions may need to be implemented to correct faults and meet the original requirements
- A system that does not meet the basic user requirements is released into the operational environment

Effective testing will reduce the overall life cycle costs of implementing and operating the system, and prevent delays to the effective and efficient use of the system.

1.5 Objectives

Testing is concerned with identifying defects so that they can be corrected, as well as demonstrating that a system meets requirements. Testing computerized systems is considered a fundamental verification activity. Appropriate testing is a regulatory expectation. As stated in EU GMP Annex 11 [8]:

> *"Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered."*

This indicates a focus on careful choice of test strategy, including negative or challenge testing, intended to identify defects.

Verification should confirm that project specifications have been met. This may involve multiple stages of reviews and testing depending on the type of system, the development method applied, and the use of the computerized system. Regulated organizations should be prepared to justify the adequacy of their verification approach.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Appropriate testing should:

- Assure patient safety, product quality, and data integrity (and data confidentiality)
- Improve reliability and reducing system downtime; increasing user confidence in the system
- Reduce the cost of commissioning, start-up, and on-going support
- Protect business reputation and credibility

A science-based quality risk management process (e.g., using ICH Q9 [4]) should be used to determine the appropriate scope and rigor of system verification. Tests should be designed to demonstrate that all required risk controls are in place.

Failure to appropriately test functions which have high impact on patient safety, product quality, and data integrity appropriately may undermine the compliance and fitness for intended use of a system. Inadequate testing also may lead to regulatory citation and possibly further regulatory action.

Any proposed change to a system should trigger an impact assessment to determine the extent of any re-verification, including any regression testing required. Alterations to a system should be made only in accordance with a predefined procedure for change control and change management which should include provision for approving, implementing, verifying, and, if necessary, backing out the change.

1.6 Structure of this Guide

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



Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

1.6.2 Structure of this Guide

This Guide contains the following:

- Main body defining how the GAMP®5 Key Concepts [1] relate specifically to testing and outlining regulated organization and supplier considerations
- A set of “T” appendices giving detailed guidance on test practices, applicable across all phases in the life cycles unless explicitly stated otherwise
- A set of “E” appendices providing examples of special considerations involved in applying the test practices to different system types

Templates and examples are also included in the appendices to assist in the development of appropriate documents, suitable for planning, executing, and reporting on the testing of a GxP system.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

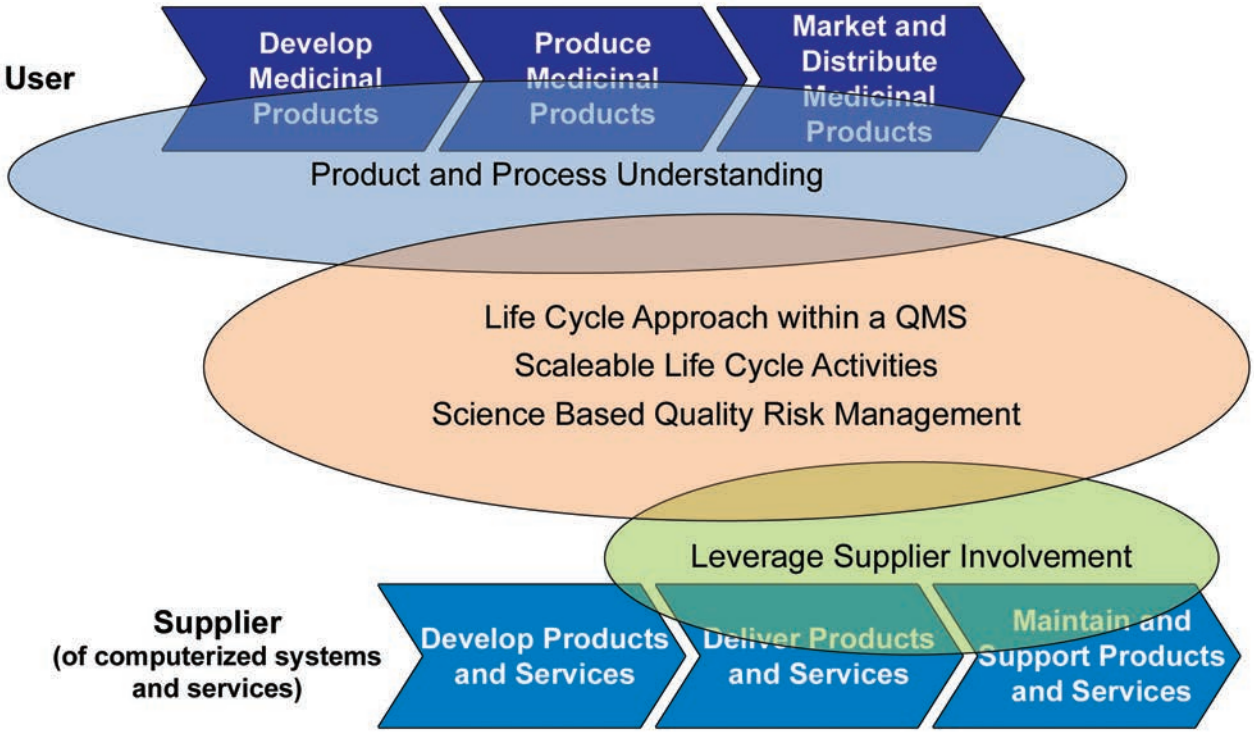
2 Key Concepts

Within this section, the key concepts from GAMP® 5 [1] are shown *italicized* and are followed by a discussion of the application of each concept to the testing of GxP systems.

The following five key concepts are described in GAMP® 5 [1].

- *Product and Process Understanding*
- *Life Cycle Approach within a Quality Management System (QMS)*
- *Scalable Life Cycle Activities*
- *Science-Based Quality Risk Management*
- *Leveraging Supplier Involvement*

Figure 2.1: GAMP® 5 Key Concepts



2.1 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.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Systems within the scope of this Guide support a wide range of processes, including clinical trials, toxological 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.

The understanding of both product and process (including business processes as well as physical processes) assists in determining appropriate test scope and strategy. It underlies the risk management processes that allow critical aspects to be identified and specified; therefore allowing those critical aspects to be verified as part of ensuring fitness for intended use. Traceability between requirements, identified risks, and test cases is an important part of demonstrating this fitness for intended use.

In the manufacturing arena where systems control critical process parameters, the testing of process controls should challenge both measurement and control systems to ensure that the process remains within acceptable limits. In an environment where process analytical technology is in use, testing also may need to include tests designed to challenge the process model and control model. Appendix E8 covers specific risk scenarios associated with the use of PAT and the ways in which testing can help to control these.

Where the process is not known, e.g., in a system designed to control a multi-purpose facility (such as is often found in contract manufacture or in Research and Development (R&D) pilot plants), testing should adequately verify the designed control capability.

Outside the manufacturing arena, risk management processes allow critical aspects to be identified (e.g., data processing functions that impact on a regulated organization's ability to support pharmacovigilance monitoring or to perform a product recall) so that testing can be appropriately focused to verify or challenge these aspects.

2.2 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.

Testing plays a vital role in the project, operational, and retirement phases of a computerized system life cycle:

- During all phases, the main purpose of testing is to discover defects; therefore, avoiding those defects being present in the operational environment

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

- Within the project phase, testing helps to demonstrate fitness for intended use by verifying the correct operation of GxP critical functions and effective implementation of controls identified during risk assessment
- Within the operational phase, risk-based testing may be required following a system change to demonstrate that:
  - Any new functionality is correct.
  - Remaining original functionality has not been adversely affected.
  - Required risk controls are still in place and effective.
- Within the retirement phase, testing of data migration and/or archive and retrieval methods may be required prior to decommissioning the system.

The adoption of a suitable life cycle means that testing has a context where previous life cycle activities provide inputs to the testing process (e.g., the generation of clear requirements and risk controls that tests can be designed to verify and challenge). Testing feeds into later life cycle activities (including iterative activities such as re-design and re-implementation under change control). An understanding of this context is vital to ensuring that testing is appropriately scaled and is focused on higher risk areas.

Appendix T10 describes how appropriate testing can be applied when using non-linear development methods and models.

2.3 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.

As with other life cycle activities, testing should be scaled according to system impact on patient safety, product quality, and data integrity, system complexity and novelty, and the outcome of supplier assessment. What types of test are required, and the scope and rigor of each test type, are determined in part by risk assessment. Tests may be grouped into test phases in a life cycle to reflect both the overall philosophy of testing and the practicalities of testing the particular system. Some types of test may be included in more than one test phase, e.g., functional tests could be present in both integration testing and user acceptance testing (or equivalent phases with alternative names, such as factory acceptance testing and site acceptance testing).

Scalable elements, based on a documented and justified risk assessment, include the following:

- Rigor of testing:
  - Some higher impact or more novel/complex functions may require structural testing as well as functional testing. Within the structural tests, some functions may demand full coverage of every possible path, while for others, covering each outcome of a decision once is sufficient. Other functions may be appropriately

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

verified with functional tests alone and still others may be appropriately verified by parameter or configuration checks. Scope and rigor of non-functional testing such as performance testing also can be scaled according to risk. Refer to Appendix T1 for further information on types of testing.

- Extent of testing:
  - Depending on the supplier assessment results, it may be appropriate to leverage the supplier's results entirely, perform sample checks focused on high risk functions, or perform a full, comprehensive set of tests. Refer to Section 3.4 for further information on Supplier Assessment and on optimizing testing done by the regulated organization.
- Test evidence:
  - Depending on the risk associated with the functionality under test, there may be a requirement (or not) for detailed manual recording of values or hard copy evidence. Refer to Appendix T6 for further information on appropriate methods for recording results
- Rigor of test incident management:
  - Rigor of problem resolution and tracking processes and the extent of regression analysis can be scaled based on the risk associated with the failed functionality and the phase of the life cycle. Refer to Appendix T2 for further information on the management of test incidents.
- Test review/approval:
  - Some tests may be reviewed/approved by an appropriate Subject Matter Expert (SME) while others require an additional input from the regulated organization management or quality unit. Refer to Appendix T2 for further information on test roles and responsibilities.

2.4 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.

Quality risk management should be applied when defining test strategy and designing tests that are intended to verify and challenge a system. The controls identified by the quality risk management process should form the basis for designing tests that verify and challenge the functions within the system; with each control being considered as a starting point for generating test cases. This allows critical aspects of a computerized system to be identified and tested adequately.

Tracing that all controls have been verified as effective is part of effective test reporting and determination of residual risk.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

2.5 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.

Testing is an area of the system life cycle in which there are potentially large efficiency gains to be made by the appropriate leveraging of supplier involvement; in particular through the:

- Avoidance of duplication in testing
- Leveraging of supplier test activities and evidence to the maximum practical extent whilewhile still ensuring fitness for intended use

Responsibilities should be defined between the regulated organization and the supplier, but the final responsibility for the system's fitness for intended use rests with the regulated organization.

Depending on the scope of the supply (see Section 3.1 of this Guide for types of supplier), testing may be performed by suppliers both during their own product development life cycle (as part of the release of a new standard product or function) and during the life cycle for developing the required end user application. Therefore, the testing of a system is a combination of:

- Testing conducted by the supplier during basic development of the standard product
- Testing conducted by the supplier (or integrator) during application-specific development, i.e., the development of a solution customized or configured to the customer's business process
- Testing conducted by the regulated organization

Where supplier(s) have been assessed and their quality management practices found to be appropriate, the regulated organization should seek to minimize the duplication of testing effort by:

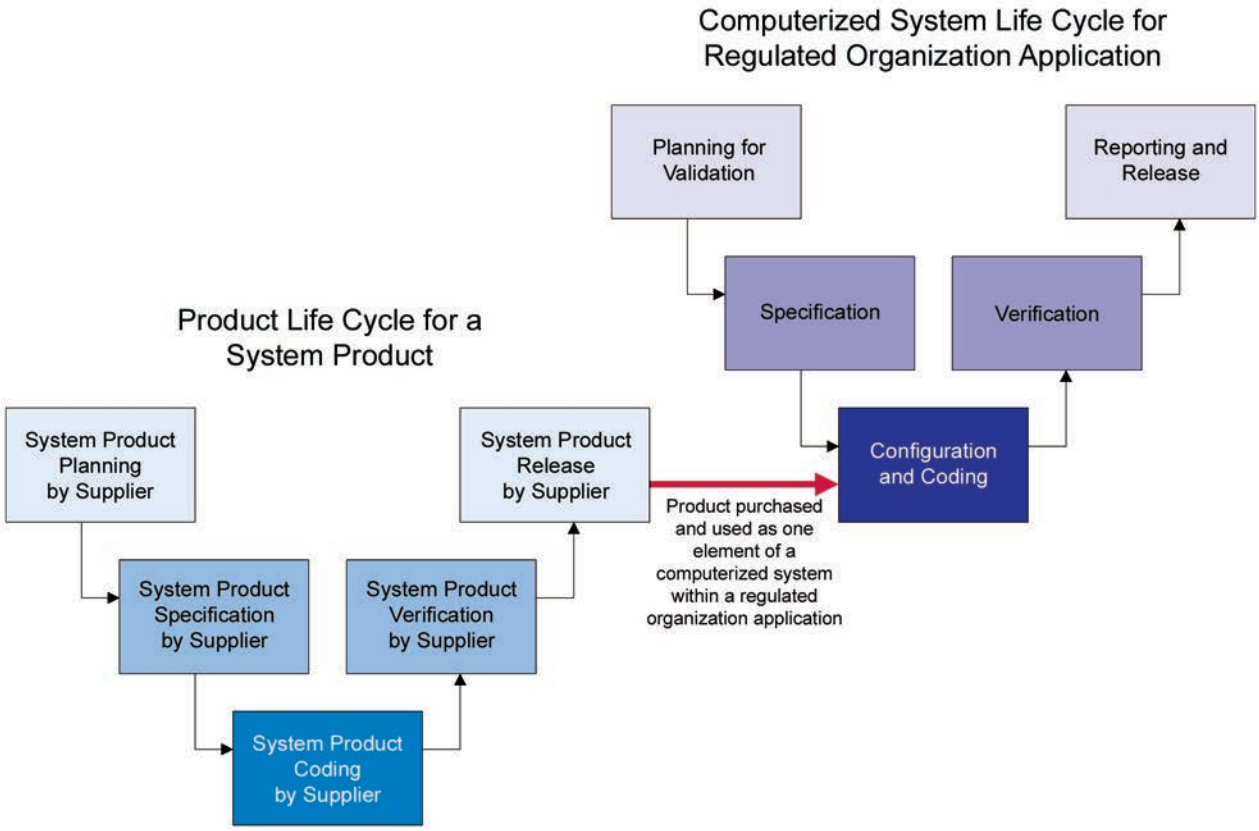
- Leveraging testing already performed as part of the development of the standard products being used (e.g., focusing on high risk and customized rather than low risk and standard)
- Leveraging testing already conducted earlier in the development of the specific application (e.g., repeating on site only those tests relating to functions that may have been affected by the move to the operational environment, not those that were successfully passed during factory testing and which are unaffected by the move)
- Leveraging testing previously performed on earlier instances of equipment where business processes allow repeat purchases of that equipment
- Ensuring that test planning does not result in unnecessary duplication between different suppliers (particularly where communication interfaces or interfaces between systems and processes are involved)

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

The supplier may minimize duplication of testing effort through robust configuration management and re-use of common modules across multiple application-specific developments.

The examples that follow show supplier and regulated organization development and test activities and are based on the specification and verification model described in GAMP® 5 [1]. Many suppliers may use alternative development methods and these may be perfectly acceptable.

Figure 2.2: Leveraging Work Already Done in the Supplier's Product Life Cycle



For example, where a non-configured product from an appropriately assessed supplier is used within an application, the verification element of the application life cycle may be limited to:

- Ensuring and recording correct installation (and parameterization if appropriate)
- Demonstrating and documenting fitness for intended use (against user requirements)
- Identifying any further tests required as a result of the quality risk management process

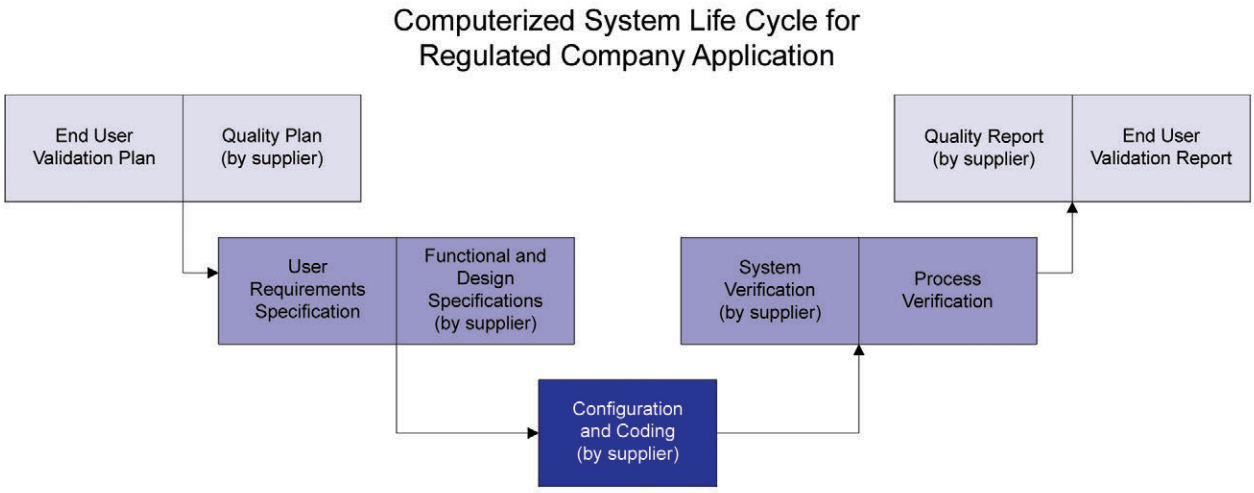
The structural level testing, functional testing, and challenge testing performed by the supplier during product development are leveraged rather than repeated.

Guidance on managing supplier test documentation is given in Table 3.4: Considerations for Determining Appropriate Test Evidence.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Figure 2.3: Leveraging Work by the Supplier during the Application Life Cycle



For example, where an assessed supplier is integrating a system for a regulated organization application, the verification steps should seek to avoid repeating tests relating to system installation and operation, referencing the supplier test results/reports instead.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

3 Regulated Organization and Supplier Relationship

3.1 Introduction

Ultimate responsibility for testing and confirming that the system meets its requirements lies with the regulated organization.

Where the regulated organization is not developing the application themselves, it is likely that they will be acquiring their system or service from one of the following sources:

- Product developer: developing a product or a custom system.
- Systems integrator: implementing a system specifically for the regulated organization and this work forms part of the regulated organization's life cycle. Their supply is likely to be based on commercial off-the-shelf products which they have configured for the particular regulated organization application, although there also may be some custom elements within the supply.
- Service provider: whose services require an element of testing, e.g., cloud computing providers, calibration outsourcing, etc.

The term *supplier* in this Guide encompasses all of the above.

In some cases, a supplier may fulfill more than one role, e.g., being both the product developer and system integrator (developing the regulated organization's application using their own organization's products). It also may be that the supplier is a division within the regulated organization.

The effort required by the regulated organization can be reduced if the relationship between it and the supplier allows for a thorough understanding by both parties as to their requirements on both a commercial and technical basis.

The regulated organization should ensure that the supplier fully understands the user requirements for the system and also how the system design, development, and implementation methods can impact the effort required by both parties. They also should ensure that the commercial aspects are clearly defined and that all the deliverables are defined and agreed in the contract for supply of the system.

The supplier should be prepared to work with the regulated organization to ensure that the supplier not only fully understands the user requirements for the system, but also the processes that will be necessary to verify the system for use. By understanding these processes and working with the regulated organization, significant savings may be achieved

A defined and agreed software development approach will help both parties during the development phase particularly with confirming that the system will meet the needs of the regulated organization. It also may enable the regulated organization to leverage the work conducted by the supplier . The effort saved can be particularly noticeable in the testing phase where, if the testing performed by the supplier has been completed to an acceptable standard and the results made available to the regulated organization, it may not be necessary for the regulated organization to retest those aspects of the system's functionality.

This leveraging of the work done by the supplier can not only save effort, but also can lead to an improved relationship between both parties with potential benefits for both.

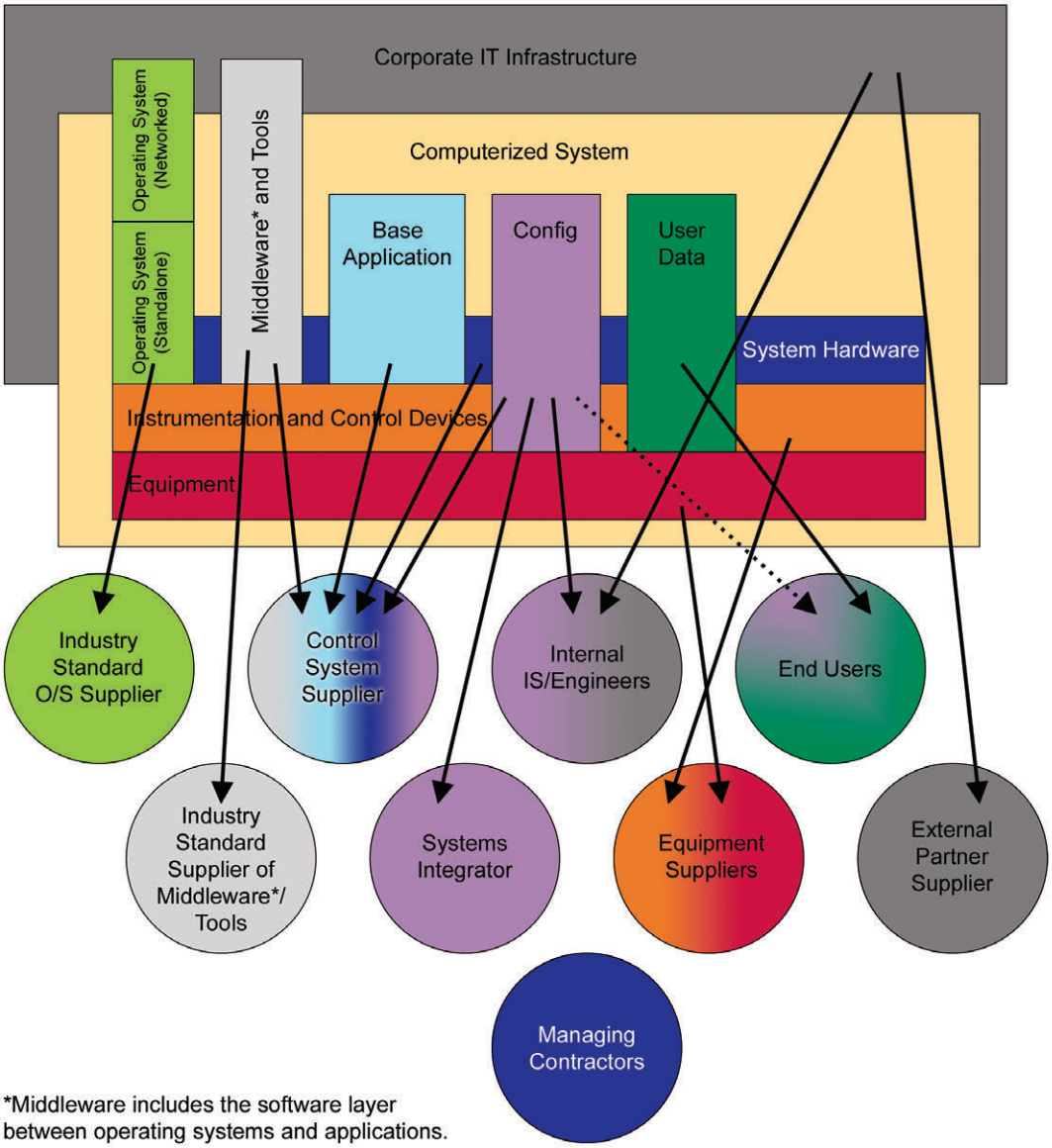
The following sections provide guidelines as to what considerations the two parties should give in maximizing the benefits in the area of system testing.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

3.2 The Supply Chain

Many suppliers may be involved. Figure 3.1 illustrates examples of the wide variety of potential sources of control system components. Similar supply chain considerations also may apply to other types of systems.

Figure 3.1: Source of Components of a System



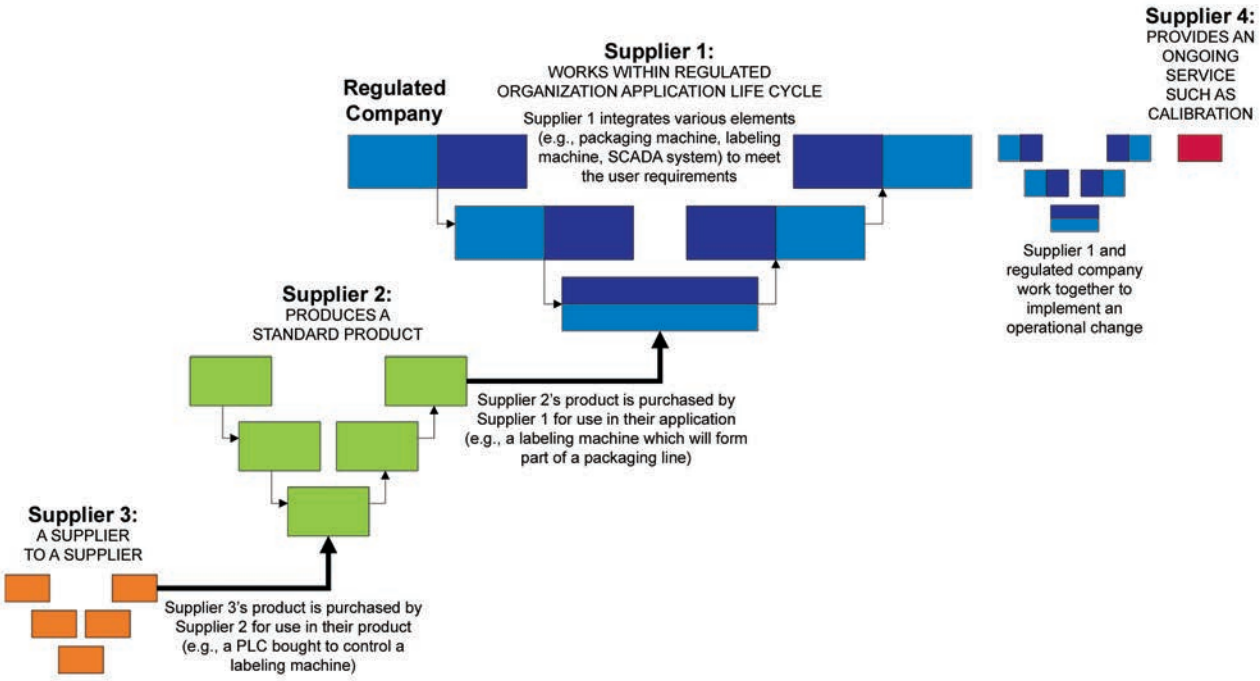
Within the supply chain, there may be suppliers to the regulated organization's supplier. These sub-suppliers should be taken into account when considering the overall supply chain.

Note: that there may be a series of sub-suppliers within the chain.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Figure 3.2: Successive Life Cycle Components of a System



3.3 Quality Risk Management

Table 3.1 includes regulated organization and supplier considerations on quality risk management.

Table 3.1

Regulated Organization Considerations	Supplier Considerations
GAMP® 5, Section 3 Quality Risk Management together with associated Appendices describes a risk management process. The regulated organization should undertake a risk assessment for the overall project. This may highlight some areas within the computer system that need particular attention and this needs to be taken in account by the regulated organization when determining the level of testing required on the computer system.	It is likely that a systems integrator will be involved in regulated organization risk assessment process and in risk-based verification activities within the application life cycle. A supplier of standard product will often take risk-based decisions (e.g., about scope and rigor of verification within own product) based on general marketplace understanding ("typical use") and may need to assume worst case impact for particular functions.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Table 3.1 (continued)

Regulated Organization Considerations	Supplier Considerations
The outcome of risk assessment will determine on which, if any, areas of the system the regulated organization should seek to perform additional testing. These may include those areas of the system that are perceived as: • Being critical to product quality and patient safety • Having a potential impact on data integrity • Complex or having novel features • Having been impacted by project specific configuration • Having a weakness in the supplier development life cycle, e.g., poor testing practices or poor test documentation • Having an unacceptable degree of risk following an assessment of the system and the supplier Having determined these areas, the regulated organization can then plan the testing of the system to focus appropriately.	Suppliers should use their own risk management processes in seeking to leverage the testing already executed by their own supplier(s), or testing conducted by themselves on identical systems or pieces of equipment.
The regulated organization should be wary of relying upon any risk assessment of the level of testing required carried out by the supplier in isolation. It is unlikely that the supplier will fully understand all the regulated organization's processes and all the critical aspects of the system. If the supplier has a thorough knowledge of the regulated organization's processes through a long standing relationship with them and the pharmaceutical market, this may be practical, but care should be exercised by the regulated organization.	Suppliers should be willing to share their "generic marketplace" risk assessment for a product, application, or service so that regulated organizations know the basis from which the assessment results were derived. Any differences between the assumed worst case impact and the actual risk severity associated with the end user application can then be analyzed and controlled.

3.4 Supplier Assessment

In order to decide what level of verification is appropriate, a regulated organization needs to consider the scope and rigor of testing that has already been executed on the functions that are critical to the specific application (and how well it was controlled and documented). This may be achieved through an appropriate type and rigor of supplier assessment. For further information on supplier assessments see Appendix M2 of GAMP® 5 [1].

Products that are widely used in pharmaceutical and other highly regulated industries are generally considered to have a lower likelihood of undiscovered software defects than new products or those developed for general markets and used infrequently in such regulated industries.

Suppliers who are experienced in the industry, who implement appropriate quality practices and have appropriate functionality, features, and documentation, will supply products more likely to meet the needs and quality expectations of regulated organizations.

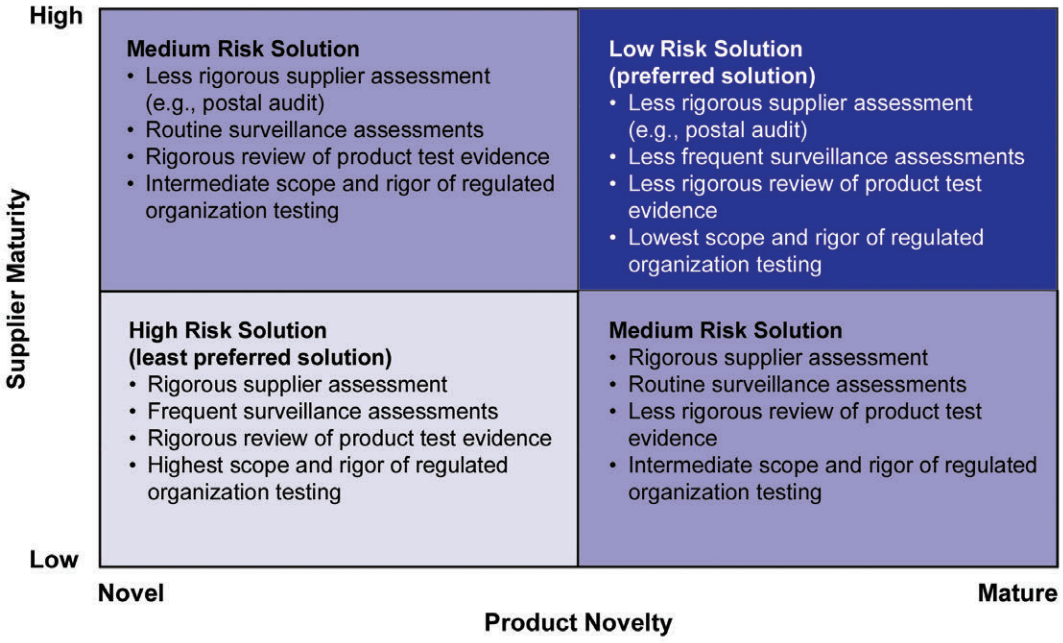
Market review and an initial supplier assessment should establish the relative maturity of a product and its supplier and this should include a consideration of supplier testing. Note this may need to cover more than one product and supplier for a given application and the regulated organization should, if applicable, take note of this throughout the risk management process.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

The following diagram gives an example approach to considering the relative risk associated with acquiring a solution (a specific computerized system from a specific supplier), and the level of assessment and review needed to be performed by the regulated organization, based on the maturity of the product and the supplier.

Figure 3.3: Example Supplier and Product Maturity Approach



Supplier maturity refers to regulated industry track record and appropriate quality management system. A mature product will have a history of good product quality with a high level of customer satisfaction in the relevant industry as opposed to novel, relatively unproven product.

Regulated organizations may choose to select products which fall into the High or Medium Risk Solution areas shown in the Figure 3.3, but this may result in an increase in assessment rigor (audit) and/or regulated organization documentation and testing to ensure that the risk is appropriately addressed.

Table 3.2: Specific Considerations for Supplier Assessment

Regulated Organization Considerations	Supplier Considerations
The regulated organization should confirm that the approach to testing being adopted by the supplier is appropriate to the product, application, or service being provided. If the system being supplied comprises a mix of categories, e.g., a largely configurable solution, but having some elements of custom “special to project” software, the regulated organization must take care to ensure that supplier testing is appropriate to the complexity and risk associated with each element and not simply to those categories that form the larger part of the system.	Suppliers should be willing to share the approach used for product development, application development, or service provision, and where necessary, explain how the testing relates to the novelty and complexity of the items being developed.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Table 3.2: Specific Considerations for Supplier Assessment (continued)

Regulated Organization Considerations	Supplier Considerations
The regulated organization should ensure that any sub suppliers to their main supplier have all been considered, risk assessments carried out as necessary, and where required, supplier assessments of appropriate rigor have been conducted. These should have been conducted by the regulated organization's supplier, or in turn their (sub) suppliers with any shortcoming or actions required being clearly documented with appropriate recommendations for closure. If there are any outstanding shortcomings or actions from the risk assessment, these should be minor in nature such that they will easily be closed out by the regulated organization's supplier (or sub supplier). Those with a good QMS are likely to have made this consideration already.	Where the supplier integrates third party software or hardware at any stage in their product development life cycle, they should consider the quality of their own suppliers and their suppliers' products when determining an appropriate level of testing. This Guide provides assistance to regulated organizations in the pharmaceutical industry as to how they should approach the testing of supplied systems. The same approach is recommended for adoption by suppliers when they make use of third party products. Suppliers should be in a position to verify that the products they use have been developed following good practice and that they have taken all possible measures to ensure this. This may involve, but not be limited to: • Assessment of developers of the third party products. This may be restricted to a postal audit, but consideration should be given to carrying out a full audit. • The specific testing of their use of these products, e.g., where specific configurations of automated tools are used, should be tested and documentary evidence provided of fitness for intended use. • Where third party products are considered to be a widely used standard product, suitable evidence should be available to support this statement.

3.5 Leveraging Supplier Testing

The regulated organization should be seeking to leverage supplier documentation and testing. Where the system has been appropriately tested, there is no value in the regulated organization repeating those tests. The need for additional testing should be based on the regulated organization applying a documented quality risk management process to ensure the supplier is adopting good quality practices toward testing.

The following diagram shows the differing levels of testing that the regulated organization should consider undertaking when using products from the preferred and least preferred option from the supplier and product maturity model outlined in the Supplier Assessment section as shown in Figure 3.3.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Figure 3.4: Relative Regulated Organization's Test Burden when using Preferred versus Least Preferred Solutions

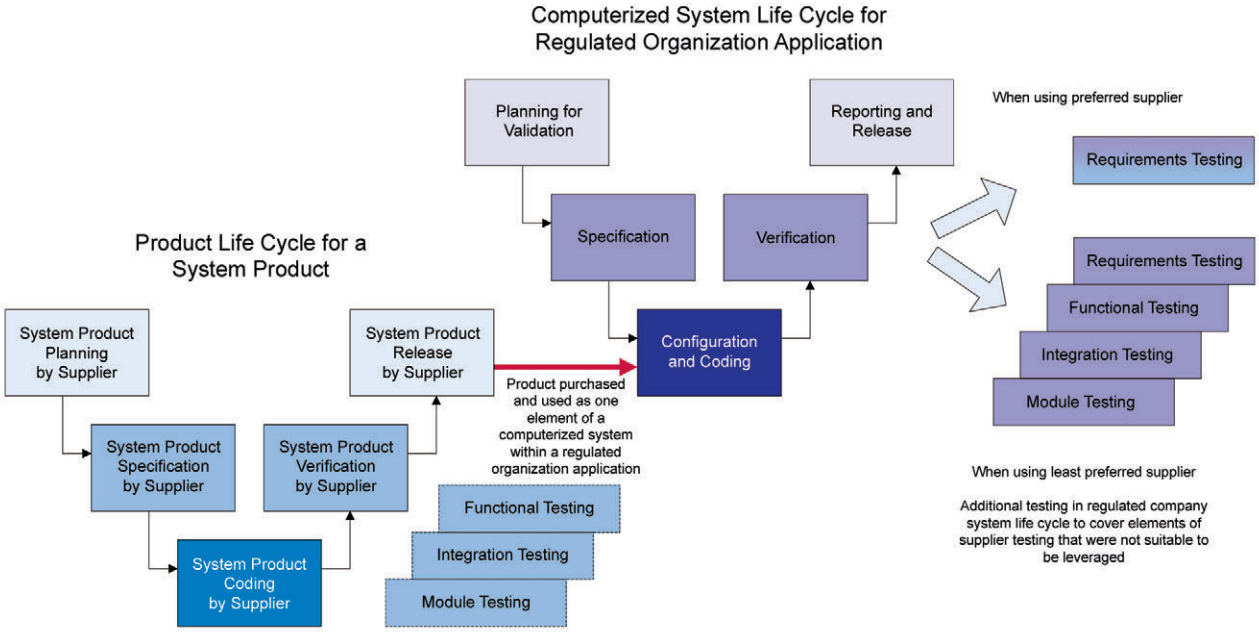


Table 3.3: Considerations for Leveraging Supplier Testing

Regulated Organization Considerations	Supplier Considerations
Supplier testing and associated documentation should be assessed and used if appropriate. The regulated organization can minimize the volume and rigor of testing required by: • Avoiding unnecessary customization, e.g., by modifying the business process, if this is practical, to match an off-the-shelf application • Seeking to leverage the testing already executed by the supplier or possibly by the regulated organization on identical systems or pieces of equipment	A systems integrator will be involved in risk-based verification activities within the application life cycle. A supplier of standard product or services needs to ensure their verification activities are suitable in scope/ rigor and are suitably controlled/documented so they can be leveraged by regulated organization. A supplier of standard product who then also acts as integrator (e.g., configuring each instance of product to meet specific customer requirements) needs to separate out what is "product development" from what is "application" as the verification evidence from the first will need to be made available to all customers (e.g., during supplier audit). The verification results from the second will accompany the delivered end user application.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Table 3.3: Considerations for Leveraging Supplier Testing (continued)

Regulated Organization Considerations	Supplier Considerations
In an ideal situation, regulated organization verification may be optimized at a level which confirms that the system meets their requirements and verifies the adequacy of previous testing. Where the business process and/or functionality are deemed high risk, the regulated organization needs to consider testing additional to that performed by the supplier.	The use of a defined and auditable software development method will potentially allow the regulated organization to make use of the supplier's test results in validating the system for use in operation. This can lead to savings for the regulated organization which may give the supplier a differentiator from other potential system suppliers. Section 7 Supplier Activities of GAMP® 5 [1] gives a good breakdown of what the supplier should be considering when seeking to supply to the life sciences industry. This guide follows the principles given in GAMP® 5 [1], and the methodologies given within this Guide will take a supplier through the testing considerations for systems to be supplied.
Where shortfalls in supplier testing processes are identified, the regulated organization needs to assess the impacts of these gaps and put in place actions to address or control them: • Deficiencies may be addressed in a one-off product or on a project basis as part of a plan of corrective actions agreed between the regulated organization and supplier, and this may include additional testing by the regulated organization. • Regulated organizations should encourage suppliers to address any shortcomings in their testing processes and documentation in a systematic manner. This may be done as part of a program of continuous improvement under the supplier's quality system and may include the introduction of an appropriate Testing Maturity Model. • The regulated organization may consider that where the systems are of a highly critical nature, it may be appropriate that corrective actions to the supplier's quality system have a suitable contractual basis. Where additional regulated organization testing does not appropriately control the risks resulting from inadequate supplier testing, it may be appropriate to consider the selection of alternate products and/or suppliers.	
Where it is not practical to conduct an assessment of the supplier (e.g., open source software or uncooperative suppliers) appropriate risk controls steps will need to be taken. This may include additional detailed testing depending upon the maturity of the product and the supplier or considering the selection of alternative products and/or suppliers.	

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

3.6 Determining Appropriate Test Evidence

Table 3.4: Considerations for Determining Appropriate Test Evidence

Regulated Organization Considerations	Supplier Considerations
Regulated organizations should define what level of test evidence should be in place before the system can be considered to be fit for intended use.	The supplier should consider what test evidence will be beneficial to the regulated organization's system verification exercise and endeavor to design their testing strategy to assist in this area.
When leveraging test results generated under the supplier's QMS, regulated organizations should ensure that they focus on the coverage and quality of test results rather than on the terminology or formats used. As long as the content and coverage is appropriate and good test documentation practices are followed (detailed elsewhere in this Guide), it is acceptable to leverage test documentation provided in the supplier's standard format.	The supplier may need to consider how these test results are recorded at the various stages of development and at each point of supply of the system. Development testing may be conducted under the supplier's own QMS with its particular methodology while testing at the point of supply, which may be factory and/or site testing, may be under the regulated organization's QMS or the supplier's own. Ensuring that whatever approach is adopted, the test results are of suitable quality for use by the regulated organization can save effort in the verification process.
Regulated organizations should define how long test evidence needs to be available. The value of such test evidence changes over time and the retention period can be determined by risk assessment. For example, the retention of detailed unit test scripts, with the results of the executed scripts, will facilitate subsequent regression testing if the custom software is still subject to change, but once the custom software is no longer subject to modification, the usefulness of retaining the test evidence can be assessed, results documented and appropriate actions taken.	The supplier should consider the period of test result retention and ensure that test results from the product development phase are retained throughout the product's life. A situation may arise when an established product/ supplier is acquired by a new supplier. The new supplier should ensure that relevant test evidence from the previous supplier is secure and available for audit.
Where possible, the regulated organization should build on evidence of testing provided by the supplier and aim not to duplicate test evidence. The ability of regulated organizations to leverage supplier testing may depend on suppliers allowing access to specific test evidence, e.g., during supplier assessment. This may need specific contractual agreement.	Where the supply is within the regulated organization's application life cycle, test evidence will be associated with that life cycle and available to the user as part of the application life cycle documentation. Where the system is to be generic, the supplier should consider what testing they will conduct during product development and what test results they will retain and be able to provide, if required, to the regulated organization as part of the overall supply. Where generic systems may be slightly modified for a given regulated organization, consideration as to how these will be tested and how these test results may be provided to as part of the overall supply will be of assistance to the customer.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

3.7 Ongoing Support

Table 3.5: Considerations for Ongoing Support

Regulated Organization Considerations	Supplier Considerations
Service Level Agreements covering not only spares and repairs mechanical aspects, but also backups, system software checks, and performance monitoring will help the regulated organization to ensure that the system remains in good working order.	The supplier should ensure that they have processes in place to provide long term support to the regulated organization. Being able to do this offers the supplier the opportunity to maintain a relationship with the regulated organization with the potential benefits this may bring them.
Service Level Agreements that cover the process for installing upgrades or patches to the system can help define the testing that will be required as part of this process.	Suppliers should consider the need for ongoing support of the system following its delivery and setting to work at the regulated organization's site – including requirements for installation or patches and upgrades and the appropriate level of regression testing.
Patches for fault rectification and/or updates to the system, while they may require some verification activities on the part of the regulated organization, can bring benefits such as improved efficiency, less down time, better user interfaces etc. Having a defined and structured approach to this activity can greatly assist the regulated organization and improve the status of the supplier.	The need for a rationale as to why the patch/update is being provided together with suitable testing evidence appropriate to the risks involved with the change can offer substantial benefits to the regulated organization and help in their decision as to whether to install the change. See Appendix T8 for more detail.

3.8 Commercial Issues

It is important that level of documentation, including design, development, and testing information to be supplied to the regulated organization is agreed at the earliest point in the project as possible, preferably before the contract is finalized.

Testing, particularly where there is any custom development, is often a milestone linked to a stage payment. Key points for success include:

- Agree and document early in the project the stages, scope, and rigor of the testing required – an assessment of the critical functions and risk impact to the regulated organization can assist with this.
- Agree test phasing and acceptance criteria for release, such as allowed levels of residual defects.
- If appropriate, ensure that a non disclosure agreement or similar is in place to enable the supplier to allow access by the regulated organization to sensitive information, test results etc., and vice versa.
- Ensure the test scripts are traceable to the various design specifications particularly those requirements specific to the life sciences market.
- Where appropriate, involve the supplier and regulated organization personnel in the review and approval of test scripts that are relevant to them. This should ensure that all parties understand the test objectives and should limit the effect of subsequent changes.
- Focus on the critical and high risk requirements carrying out full black box and stress testing for these areas and consider structural testing and code reviews if appropriate.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

- Reduced testing for the lower risk areas
- Document and agree the configuration management process and regression analysis being followed during the testing activities
- Ensure all equipment, including spare parts required for any disaster recovery testing, are available prior to the commencement of testing
- Ensure that time planned for document reviews factors in the expected size and complexity of the item to be reviewed
- Ensure all personnel are available when required, including system developers in case of a deviation occurring which requires a change to the system
- Prepare contingency and recovery plans

On completion of the testing, agreement on any outstanding actions or deviations should be reached between the supplier and regulated organization in order for the project to progress to the next stage.

Other commercial issues for consideration include:

- The retention period for the test documentation relative to the needs of the system and the business process
- Whether escrow agreements are required and in place for software and documentation
- Whether the regulated organization retains the right to audit supplier either at fixed intervals or in response to particular triggers

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

4 Appendix T1 – Test Practices

4.1 Introduction

This appendix covers the need for high level test policies within an organization, discusses the different types of verification activity that may be covered by such a policy, and goes on to define how the scope of testing for a particular project may be determined.

4.2 Test Policies

Regulated organizations should have consistent policies for testing computerized systems; particularly for GxP computerized systems. Test policies are usually defined at the corporate level. Policies may be established at site or department level if required by regional needs or to provide applicable procedures for specific types of software or systems. Regulated organizations should define the test policy within the context of their own computerized systems' QMS. The test policy may be included within a specific testing policy document or may be part of a validation policy document.

Test policies, dealing with the high-level approach across all systems, must not be confused with test strategies, which are defined at the system level and consider risks specific to business processes.

Test policies can be influenced by the risk philosophy of an organization, as testing is closely related to the risk management process. For regulated organizations, factors which can influence a corporate risk philosophy include:

- Positive and negative experiences with system suppliers
- The inherent product or process risk (potential for patient harm, poor quality product or loss of data confidentiality and integrity) and the level of product and process understanding within the organization
- Recent and historic regulatory inspection findings
- Corporate reputation in the market

Regulated organizations should seek to maximize supplier involvement throughout the system life cycle in order to leverage knowledge, experience, and documentation, including existing test documentation, to avoid wasted effort and duplication (see GAMP® 5 [1]). However, a risk-averse organization may choose to test lower risk functions with greater rigor, and may be reluctant to leverage supplier testing, preferring to repeat it under their own in-house control.

Key testing principles should be defined in either the test policy or a high level Testing Standard Operating Procedure (SOP). This should provide the flexibility to define how these principles will be applied to different types of system or within different life cycles. Specific SOPs or work instructions (which may be system, project, or model specific) should provide the detail of how these principles are applied. The test types needed will come out of the risk assessment, and what phases they will be done in will fit with where it is most efficient to do them.

Specified procedures for testing should help to provide consistency during execution of the testing process. These procedures should be based upon a common testing policy (which should apply to both manual and automated testing). A common testing policy may provide benefits, including:

- Common methodologies being adopted
- Common terminology (and less potential for confusion)

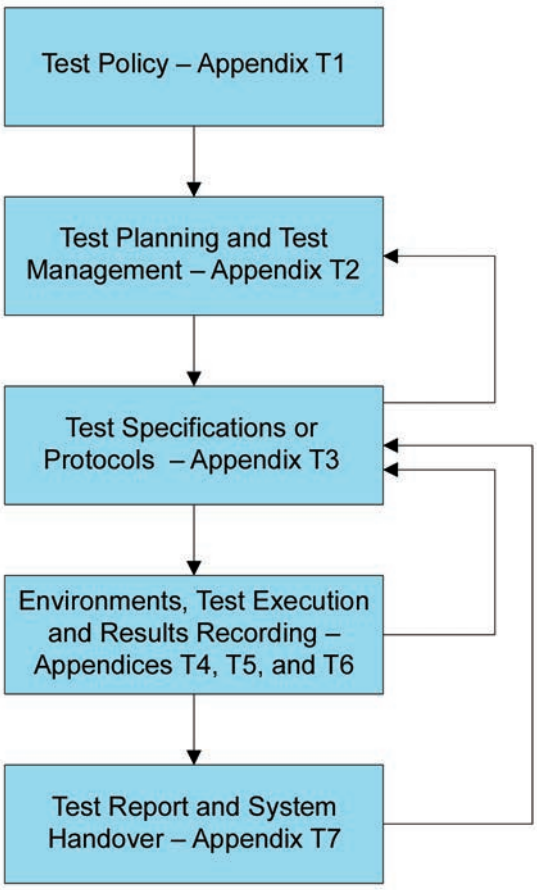
AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

- Common test documentation models
- Common risk management and analysis processes and documentation standards
- Use of common test documentation templates
- Provision for the use of computer based testing tools (see Appendix T11)
- Similarity in approach means testers are familiar with the process so reducing the duration of the learning curve
- Consistent testing processes throughout the organization
- Formal and well understood practice for efficiently managing defects, including defect resolution
- Faster and more consistent reviews

The test policy may need to address particular requirements for the situation where a system is being delivered in stages to ensure that changes made as a result of test incidents in one environment are promoted and backtracked as necessary into earlier or later test environments and the operational system.

Figure 4.1: Overview of Testing Process



4.2.1 Additional Considerations for Non-Linear Development Methods

Testing in non-linear development methods is discussed in detail in Appendix T10.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Key differences associated with non-linear development which should be addressed by a test policy include:

- The delivery of the system is usually in more than one stage, referred to as an increment or phase.
- Each iteration of an increment/phase includes cycles of:
  - Design
  - Development
  - Testing
  - Review
- Design and test documentation is not formally approved until the end of an increment/phase.

Where a prototype is to be further developed (an “evolutionary” prototype rather than a “throw away” prototype), the test policy should be clearly defined and should consider how the prototype will be baselined and tested before becoming part of the main development life cycle.

Points to address the risks of non-linear development life cycles for consideration in a test policy include:

- Definition of measures during an iteration to ensure that the resulting application is fit for purpose. These may include:
  - Regular regression testing (the use of automated test tools for this is a considerable advantage – see Appendix T11)
  - Source code reviews
  - Regular reviews of draft test scripts to ensure adequate test coverage
  - Maintenance of traceability
- Definition of periods or milestones when development documentation should be updated to reflect the current use of the system
- Definition of a formal test phase prior to deployment of the iteration which verifies the critical functions by execution of formally approved test scripts against the finalized and approved design
- Requirements added, removed, or modified can cause a need for requirements and impact analysis to ensure requirements are still consistent and do not contain non-conformities.

4.3 Types of Verification

This section discusses the types of tests that can be performed as part of product development and project testing.

The types of test that are required, and the scope and rigor of each type of test, are determined in part by risk assessment.

Some types of test may be included in more than one test phase, e.g., functional tests can occur in both integration testing and user acceptance testing.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

During the development of a project/system specific test strategy or test plan, each type of test should be considered in the context of the risks assessed and the test objectives, e.g.:

- Is positive case testing sufficient to demonstrate correct functioning of a low risk Category 3 system?
- Is it necessary to demonstrate the effective mitigation of high risks within a software Category 5 system using challenge, stress, and positive and negative case functional testing?

Each strategy or test plan should clearly define which types of tests are applicable to each test phase.

Tests may be automated using computerized test tools; this can benefit functional testing (especially regression testing) and performance (load) testing.

4.3.1 Static Testing

Static tests can be used to capture early coding errors and issues. Static tests include:

- **Design Reviews** (outside the scope of this Guide)
- **Source Code Review** – this provides a means for documenting the structural verification of a custom coded module. Source code review is normally performed before the start of formal module testing. It should include review against the:
  - Required coding standards
  - Design requirements
- **Static Analysis Tools** – these are commercially available test tools which evaluate a program in a non-runtime environment, e.g., to detect coding errors which may result in defects such as buffer overruns and resource leaks.
- **Configuration Testing** – for a configurable system, testing should verify that a package has been configured in accordance with the specification. This could take the form of inspections or a check of supplier documentation.

4.3.2 Structural Testing

4.3.2.1 Test Objective

The objective of structural testing (or white-box testing) is to ensure that each program statement performs its intended function. Structural testing identifies test cases, based on knowledge of the source code, detailed design specification, and other development documents. These test cases should challenge the control decisions made by the program and the program's data structures, including any configuration settings. Structural testing also can identify dead code that is never executed when a program is run.

Structural testing is recommended for requirements identified as having a high-risk priority (in addition to functional testing) because testing of all functionality defined by the user requirements does not mean that all software code has been tested.

In cases where a system is customized from Commercial-Off-The-Shelf (COTS) software, this type of testing can be employed on customizations. Customizations may include a program written for an interface or code written to follow a different workflow in the system. Structural testing requires careful planning to achieve complete coverage (see Section 4.3.2.2 of this appendix) efficiently; however, once structural tests have been developed, they may be automated for subsequent regression testing.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

4.3.2.2 Test Scope

The scope of structural testing should reflect the risk priority associated with a system or function. Structural test coverage may include:

- **Statement Coverage** – this criterion requires sufficient test cases to ensure each program statement is executed at least once; however, its achievement is insufficient to provide confidence in a software product's behavior.

- **Decision (Branch) Coverage** – this criterion requires sufficient test cases to ensure each program decision or branch is executed so that each possible outcome occurs at least once. It is considered to be a minimum level of coverage for most software products, but decision coverage alone is insufficient for high-integrity applications.

- **Condition Coverage** – this criterion requires sufficient test cases to ensure each condition in a program is executed, to test all possible outcomes at least once. It differs from branch coverage only when multiple conditions should be evaluated to reach a decision.

- **Multi-Condition Coverage** – this criterion requires sufficient test cases to exercise all possible combinations of conditions in a program decision.

- **Loop Coverage** – this criterion requires sufficient test cases for all program loops to be executed for zero, one, two, and many iterations, covering initialization, typical running, and termination (boundary) conditions.

- **Path Coverage** – this criterion requires sufficient test cases to ensure that each feasible path, from start to exit of a defined program segment, is executed at least once. As a result of the very large number of possible paths through a software program, complete path coverage is generally not achievable. The scope of path coverage is normally established based on the risk priority of the software under test.

- **Data Flow Coverage** – this criterion requires sufficient test cases to ensure that each feasible data flow is executed at least once. A number of data flow testing strategies are available [9].

The style of structural testing may depend on the type of algorithm/program under test. For example:

- Testing of a module implemented as flowchart style logic may need to focus on coverage of statements that make up each process within the flowchart and coverage of branches created by each decision.

- Testing of a module implemented as a state transition diagram may need to focus on coverage of the statements/actions which are supposed to happen in each state and of branches created by each possible transition criterion.

- Testing of a recursive or iterative algorithm may need (in addition to checking the logic carried out within each iteration and the correct passing of data from one iteration to the next) to focus on areas such as correct interpretation of the finish condition and exit from the recursion/iteration, correct behavior when a boundary condition is encountered, whether there is a possibility to end up in an endless loop and whether there is the possibility that a local optimal solution may be found and the algorithm exit without finding the correct global solution.

- Testing of a program split into modules or objects may need (in addition to checking the logic carried out within each module) to focus on data and messages passed between these modules or objects.

When executing business process based testing of COTS applications, the principles of structural testing also can be used to ensure that every process path (i.e., normal, alternate, and exception) is tested and that every step in the process (i.e., every system transaction) is tested. Note: if the required functionality matches that provided as standard by the COTS package, this level of coverage may already have been addressed in full by the supplier and it may be possible to leverage the supplier's results rather than repeat test effort.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Complete coverage testing requires a careful analysis of the software design to determine for the branches:

- Normal case (the expected path through the code)
- Alternate case (an unusual, but anticipated path through the code)
- Exception case (an exceptional or error condition)

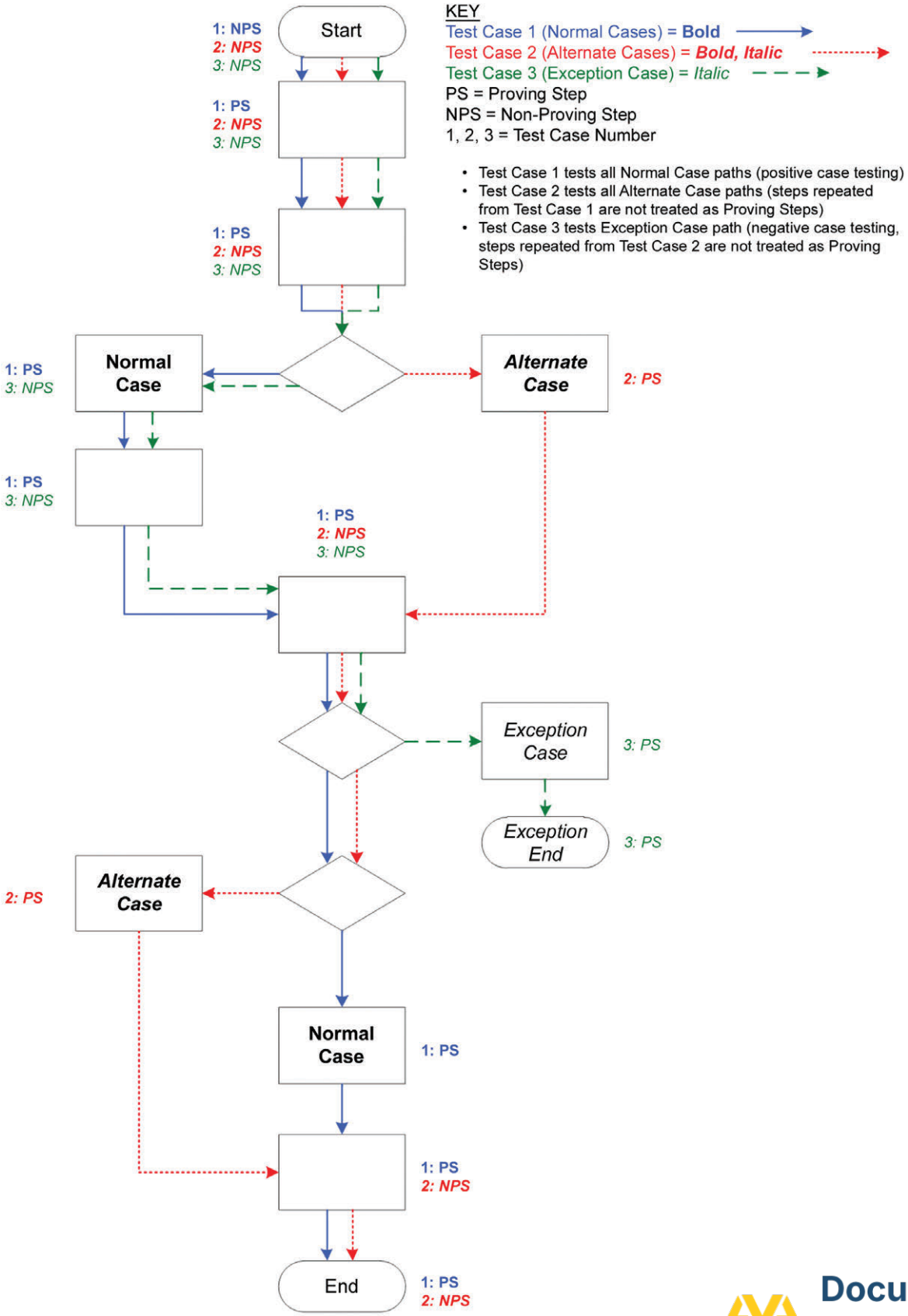
In many cases, careful analysis of the software design means that it is possible to test a number of paths/branches with a limited number of test cases, i.e., multiple paths can be tested by a single test case. In other cases, steps that need to be executed to reach a specific branch can be treated as non-proving steps for that test case if they were treated as proving steps in an earlier test case.

An illustrative example of this approach is shown in Figure 4.2. It applies the example test step classification scheme described in Appendix T1.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Figure 4.2: Branch and Path Coverage by Test Cases



Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

This example shows that:

- Test Case 1 executes all normal case paths. The Start step is a non-proving (set-up) step, but all other steps are proving steps, see Appendix T3. Note that this single test case exercises two normal case paths.

- Test Case 2 executes all alternate paths and the single test case exercises two alternative case paths. The initial steps executed in Test Case 1 should be repeated in order to arrive at the branches at which the alternate cases are tested, but because these initial steps were proved during Test Case 1, they are considered to be non-proving steps for Test Case 2.

- Test Case 3 executes the single exception case path. The initial steps executed in Test Case 1 should be repeated in order to arrive at the branch at which the exception case is tested, but because these initial steps were proved during Test Case 1, they are considered to be non-proving steps for Test Case 3. Only the steps that test the exception case are considered to be proving steps for Test Case 3.

In this example, it is also possible to define the repeated steps from Test Case 1 as test pre-requisites or set-up steps for Test Case 2 and 3 and thereby reduce the size/complexity of these latter test cases.

Using this approach, it is possible to assure complete branch coverage testing with an optimal number of test cases, but this requires careful analysis and detailed test planning.

4.3.2.3 Test Positioning within the Life Cycle

Structural testing is performed primarily within the unit or module test phase.

4.3.3 Functional Testing

4.3.3.1 Test Objective

The objective of functional testing (or black-box testing) is to evaluate the compliance of a system or component with specified functional requirements. Functional testing therefore identifies test cases based on the definition of what the software is intended to do. These test cases challenge the intended use or functionality of a program, and the program's internal and external interfaces.

Functional testing is required in addition to structural testing because testing of all of a program's code does not necessarily mean that all required functionality is present in the program.

Functional testing also requires careful planning to achieve complete coverage efficiently. Significant benefit can be gained by automating functional tests for subsequent regression testing, but not all functional tests lend themselves to automation. The automation of invalid case tests requires specific attention to the design of the automated scripts.

4.3.3.2 Test Scope

Functional testing usually should cover all specified functional requirements. For a particular requirement; however, the number and types of functional tests performed may reflect the risk priority associated with the system or function.

Note: although a project may include a test cycle called functional testing (see E Appendices for examples), from the perspective of test types, functional testing may include:

- Black box testing of individual software objects (e.g., conducted by a regulated organization, following white box structural testing by a supplier)

- Coverage of functional requirements in an appropriate test cycle (e.g., conducted by a supplier and/or regulated organization in test cycles typically called system test, functional test, or operational qualification)

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

- Coverage of user requirements in an appropriate test cycle (e.g., conducted by the regulated organization in a test cycle typically called user acceptance testing or performance qualification)

Some common types of functional tests include:

- **Normal Case (Positive Case) Testing** – testing to show that a system does what it is supposed to do in response to the usual and expected inputs (e.g., checking that a calculation gives the correct result in response to expected inputs). By itself, normal case testing does not provide sufficient confidence in the dependability of a software product.

- **Invalid Case (Negative Case) Testing** – testing to show that a system does what it is supposed to do in response to specified invalid inputs (e.g., giving the correct error message in response to an out-of-range input).

- **Business Process Testing** – testing, possibly using a test harness, to challenge the different branches and paths of the business workflow.

- **Special Case Testing** – testing to show that a system does what it is supposed to do in response to inputs at the limit of the permitted domain (boundary or limit condition testing) or to inputs which form a special case or exception (e.g., checking that a calculation produces the correct result for the maximum and minimum values of each input, or checking that a zero input is handled without leading to a "divide by zero" error).

- **Output Testing** – choosing test inputs to ensure that all software outputs are generated at least once during testing (and if relevant that the outputs are exercised at the limits of their allowed range).

- **Input Combination Testing** – testing combinations of inputs to ensure correct outputs. The input combinations can be selected at random from the possible range of inputs or selected specifically because they are considered likely to reveal faults.

An example of this is shown in Table 4.1.

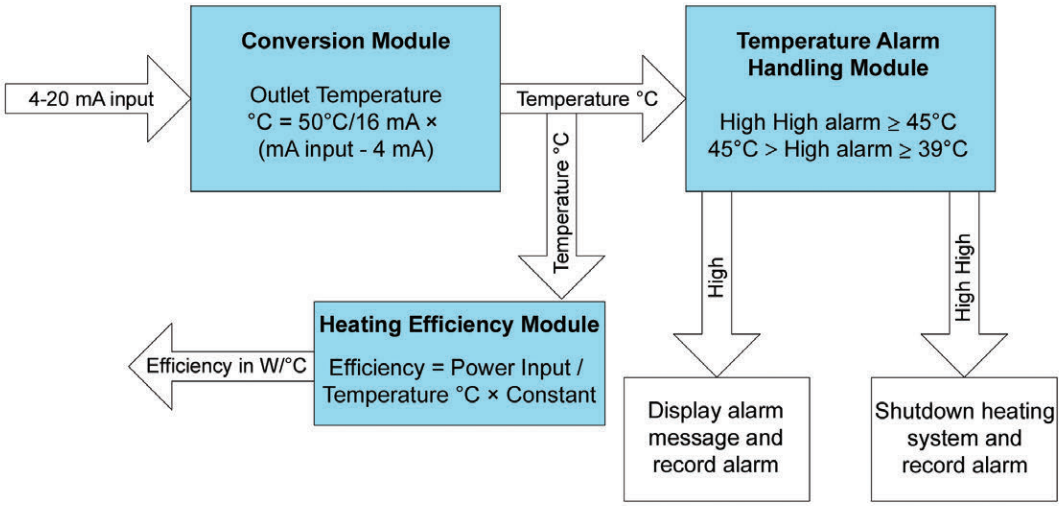
Table 4.1: Example Extract from Risk Assessment

Risk No.	FS ref.	Potential Failure Mode	Potential Effect of Failure	Severity	Probability	Detectability	Risk Priority	Required Action
41	6.12.5	Temperature incorrectly calculated	M	M	M	L	H	Test temperature conversion limits
42	6.12.5	Temperature exceeds upper limit	M	M	M	M	M	Test High alarm and normal operating condition
43	6.12.5	Aggregates form – drug becomes toxic	H	M	M	M	H	Test High alarm boundaries

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Figure 4.3: Process Control Modules under Test



By injecting the input values listed below using a loop calibrator or other simulator, with power input artificially fixed at 100W for simplicity, output testing can be achieved by a combination of negative and positive case testing, to verify the functionality of the temperature, temperature alarm, and efficiency modules.

Table 4.2

Input	Temperature Displayed	Efficiency Displayed	Expected System Response
0	Error	Error	Wire broken alert message displayed and recorded
4.00 mA	0.0°C	Error	Unable to calculate parameter message displayed and recorded
15.84 mA	37.0°C	2.70	None
16.48 mA	39.0°C	2.56	High temperature alarm displayed and recorded
18.37 mA	44.9°C	2.22	High temperature alarm displayed and recorded
18.40 mA	45.0°C	2.22	Heating system shutdown and alarm recorded
19.97 mA	49.9°C	2.00	Heating system shutdown and alarm recorded
20.00 mA	50.0°C	2.00	Heating system shutdown and alarm recorded
20.01 mA	Error	Error	Out of range error displayed and recorded

4.3.3.3 Test Positioning within the Life Cycle

Functional testing may be performed during all phases of software testing, from unit or module testing to system level testing.

4.3.4 Performance Testing

4.3.4.1 Test Objective

The objective of performance testing is to evaluate the compliance of a system or component with specified performance requirements. These may include non-functional user requirements (e.g., speed of response to operator input).

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

4.3.4.2 Test Scope

Performance testing should normally cover all stated performance requirements. Use of automated performance (load) test tools which can simulate the load usually generated by a significant number of users and which also can measure and monitor system performance in real time can be beneficial. For a specific requirement, the number and type of performance tests executed may reflect the risk priority associated with the system or function. Types of performance tests include:

- **Environmental Tests** – testing to show that a system is capable of operating reliably in the specified environment (e.g., under specified temperature conditions). Testing performed by the supplier is normally leveraged. Where the operating environment falls outside the supplier's specification for the product, additional testing may be necessary.

- **Accuracy Tests** – testing to show that the system is capable of meeting the required accuracy of measurement or control (e.g., controlling temperature to within a specified range).

- **Repeatability Tests** – testing to show that a system is capable of repeatedly meeting the required performance (e.g., by running repeated trials using the same recipe to check that the product is always within specification).

- **Timing or Response Tests (also known as Latency Tests)** – testing to show that a system is capable of meeting the required timing, throughput or response (e.g., responding to operator requests within a specified period).

- **Load Tests or Capacity Tests** – testing to show that a system is capable of meeting the required performance while operating under realistic high load conditions (e.g., with a high number of concurrent users of a database). Load testing can be a complex area. For further information, see Section 4.3.4.4 of this appendix.

- **Usability Tests** – testing to evaluate the combined performance of a system and user (e.g., checking that the user is able to access and respond to information in a timely fashion via a menu system). Usability testing may be either structured (e.g., to check every menu option in sequence) or unstructured (which allows the operators to "play" with the system in a realistic manner, in order to detect any issues which may not arise through the use of formally scripted tests).

4.3.4.3 Test Positioning within the Life Cycle

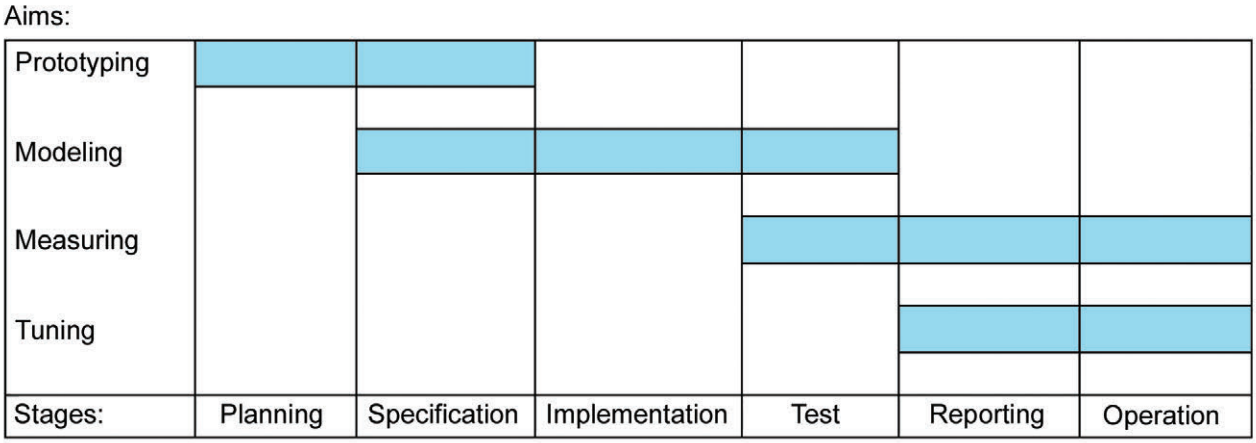
Performance testing is usually performed during the factory and site acceptance test phases or before operational release. Performance testing also may be used to verify that hardware meets user requirements. Where possible, performance tests should be built into to earlier stages of testing to help to detect performance issues such as memory leaks. It may be possible to assess performance at an earlier stage using prototypes or theoretical models or by scaling up results from unit or module test phases. Where differences exist between the test environment and the operational environment, it also may be necessary to perform some performance monitoring and tuning within the operational environment.

Figure 4.4 provides an example of different stages where performance testing may be conducted using one or more of the types above. This shows that performance testing can be used to assure the robust performance of a system at various stages within a project.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Figure 4.4: Performance Testing in System Life Cycle



4.3.4.4 Load Testing Considerations

The goal of load testing is to show that a system works as expected at specified operating limits (within the standard range of operation). During load testing, the system is operated under high load conditions. In addition, load testing can be used to prove the design of the software architecture and to support operations throughout the life of a system through scalability or load balancing.

Where it is necessary to conduct load testing on systems with a large number of users, the use of automated performance test tools (load generation tools) can be advantageous in terms of reducing the number of staff required to generate the necessary load profile. This can be particularly beneficial in reducing the time required for full scope regression testing of web-based applications.

Potential issues with load testing include:

- Potential system limits being difficult to foresee during system development
- Costs for load testing being relatively high due to resource-consuming processing
- The generation of data for high volume tests

In addition, a proper definition of the expected load may not be available or may be unrealistic.

Typical problems that are detected during load testing include:

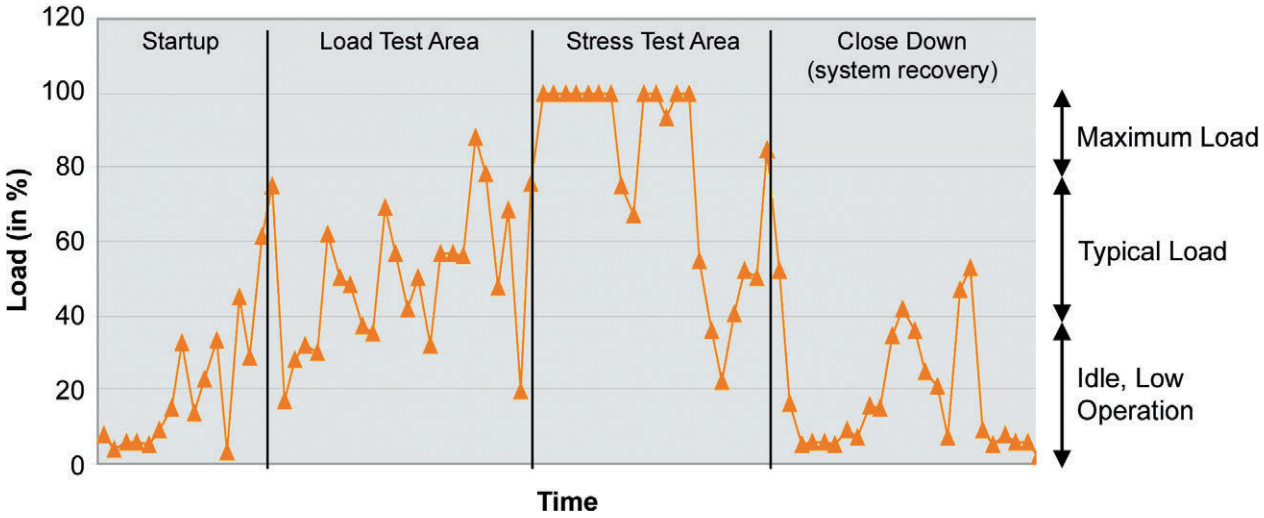
- Data transfer fails due to long processing times
- Memory leaks
- Long response times due to large number of concurrent users
- Poor response times due to heavy load on the system caused by audit trail generation on databases or software implemented encryption algorithms
- Scalability of an architecture is limited by network bandwidth
- Maintenance periods exceeded due to long batch processing runtimes

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

The phases and the load profile of a typical load and stress test (see Section 4.3.5 on Challenge Testing for details of stress testing) are shown in Figure 4.5.

Figure 4.5: Load and Stress Test Profile



The load test in this case addressed high volume tests specified to use between 40% and 80% of the available system capacity. A stress test then followed where an attempt was made to operate at maximum load.

In general, the more complex a system and the more data volume processed, the more difficult it is to predict the behavior of a system under load. Where system behavior is difficult to predict, formal load testing is recommended.

Load testing requires clear definition of expected operating conditions that define the normal operating condition. User requirements related to the expected behavior of the system should be available. These non-functional requirements should be measurable. An example is shown in Table 4.3.

Table 4.3: Examples of Loading Requirements

Metric	Performance Counter/Units	Definition/Example
Data throughput	Bits/second	Data transfer, bandwidth
Data volume	Mbyte, GByte	Database size, transferred data
Transaction rate	Transactions/second	Database transactions
Requests rate	Requests/second	Application server load, web server (hits per seconds)
Response time	Seconds	Expected average system response time to a user request
Number of concurrent users	Number	Number of users concurrently using a system, e.g., accessing a server in parallel
Processing time	Seconds	Allowed runtime for batch processes, e.g., report generation time

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012

Load test scenarios should be based on critical business processes such as:

- Data migration, e.g., of production databases. For further information on testing data migration, see Appendix T9.
- Concurrent user system access, e.g., production start-up or month end accounting runs
- Batch processes, e.g., generation of reports
- Maintenance operations, e.g., database backup

It may be beneficial to measure system parameters during a load test, as well as measuring the performance against stated requirements. An example is shown in Table 4.4.

Table 4.4: Examples of System Parameters to Monitor during Load Testing

System Property	Performance Counter/ Units	Definition
Memory	Available Bytes/Bytes	The amount of physical/virtual memory in bytes available to processes running on the computer.
Disc I/O	Disk Read (write)/sec	The rate of read operations on the disk, e.g., database cache writes
	% Disk Time	The percentages of elapsed time that the selected disk drive is busy servicing read or write requests.
	Avg. Disk Queue Length	The average numbers of both read and write requests that were queued for the selected disk during the sample interval.
CPU	% Processor Time	The percentage of time that the processor is executing a non-idle thread. This counter is a primary indicator of processor activity doing useful work.
	Processor Queue Length	The number of threads in the processor queue. There is a single queue for processor time even on computers with multiple processors. A sustained processor queue of greater than two threads generally indicates processor congestion.
Network	% Network Utilization	Percentage of network bandwidth in use on a network segment.
	Bytes Sent (received)/sec	The rate at which bytes are sent (received) on the interface, including framing characters.
Database	Number of Commits and Rollbacks/sec	Rate of database transactions commits and rollbacks.
	Avg. Time per Transaction	Average time per database transaction.
	Number of Cache Misses	Measures the efficiency of data access and storage.
	Size in GByte	The size and the growth of the database, e.g., physical available and allocated table size.
	Database Locks	Number of tables or data locked due to modification of data.
	Number of Active Database Sessions	Measures concurrent access onto database.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Testing of GxP Systems 2012