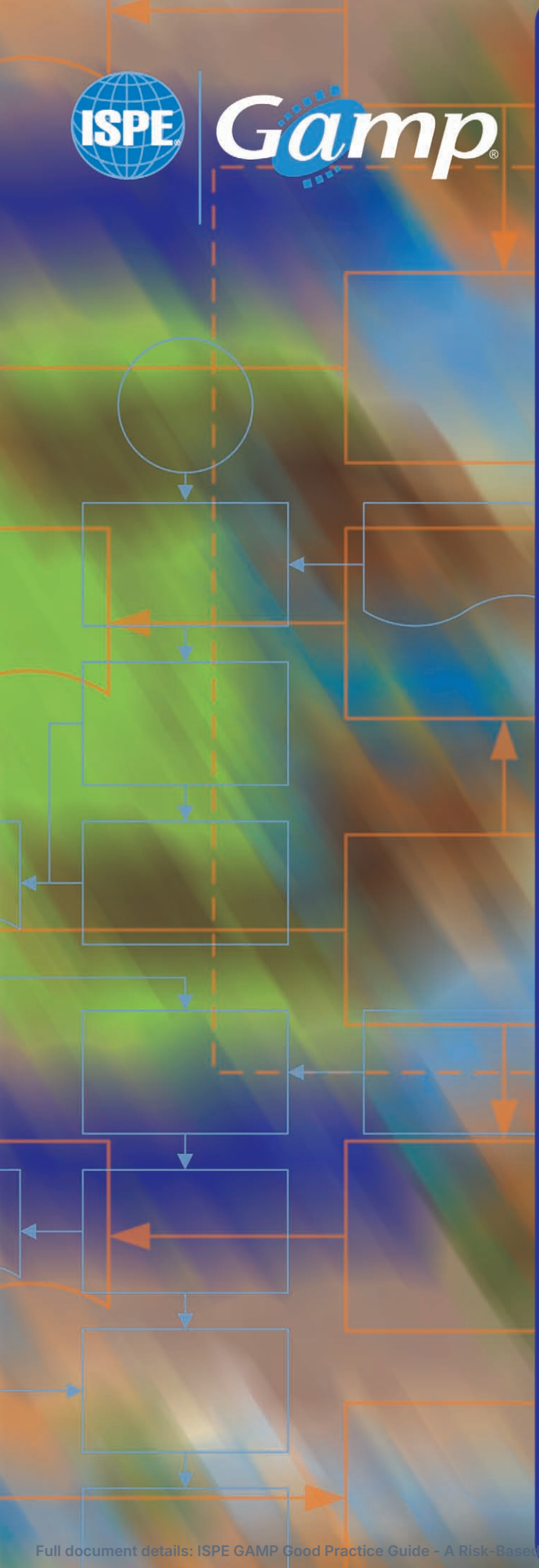


GAMP Good Practice Guide

A Risk-Based Approach to Operation of GxP Computerized Systems

A Companion Volume to GAMP® 5

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009



GAMP = Generally Anticipated Mountains of Paper

But computer systems validation doesn't have to be an Everest-scale marathon.

We design and implement practical, risk-based validation solutions that won't cost the earth.
Or a lot of trees.

PharmOut offers FDA, TGA & PIC/S regulatory compliance consulting and training to pharmaceutical and medical device manufacturers throughout the Asia Pacific.
To support your GMP compliance & validation needs visit www.pharmout.com.au/csv

PharmOut Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

GAMP Good Practice Guide

A Risk-Based Approach to Operation of GxP Computerized Systems

A Companion Volume to GAMP® 5

Disclaimer:
This Guide is meant to assist pharmaceutical organizations in determining a common understanding of the concept and principles of operation of GxP computerized systems.The International Society for Pharmaceutical Engineering (ISPE) cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

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

© Copyright ISPE 2009. All rights reserved.

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

All trademarks used are acknowledged.

ISBN 1-931879-68-0

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Preface

Regulated computerized systems should be maintained in a demonstrable state of control and in accordance with regulatory requirements. Maintained regulated data and records should be complete, accurate, and secure. Some regulated data and records need to be retained after system retirement.

For regulated organizations, the Return On Investment (ROI) for the significant time and resources expended in implementing new computerized systems is achieved during the Operation Phase. Recovery from a failure to maintain control of a regulated system during the Operation Phase can be both time-consuming and expensive, and increase the risk to data integrity, product quality, and patient safety.

The purpose of this ISPE GAMP® Good Practice Guide, a Risk-Based Approach to Operation of GxP Computerized Systems, is to provide detailed information to enable organizations to support their systems more effectively during the Operation Phase of the system life cycle.

It provides comprehensive guidance for maintaining control of regulated systems throughout their operational life (including acceptance and release, system handover, through to system retirement and decommissioning). When applied as intended, this Guide can provide detailed direction on the required control processes which form a substantial part of an appropriate Quality Management System (QMS).

This Guide focuses on achieving effective and efficient business processes aligned with regulatory expectations, by providing generic principles which can be applied to regulated systems using a systematic and scalable approach.

This Guide addresses the operational and support processes that need to be established to receive regulated computerized systems into the Operation Phase of their life cycle and to maintain them in a state of compliance throughout their operational life, through to system retirement.

It is applicable to systems consisting of hardware and software of all GAMP® categories.

Guidance provided is scalable and can be applied to a range of systems, including:

- laboratory systems
- process control systems
- IT applications

Whereas GAMP® 5 is primarily concerned with strategic approaches and planning of operational activities, this Guide contains more detailed information, including:

- a fuller consideration of process scope
- risk-based scalability considerations
- the appropriate assignment of roles and responsibilities
- identification of associated records
- example procedures

Process flow diagrams provided are intended to assist in making the process steps and their interrelationships clear and accessible. Wherever possible a common terminology has been adopted to describe the required management processes, to allow the guidance to be accessible to as wide a readership as possible.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Acknowledgements

This Guide was developed by a team under the **co-leadership** of **Kate Samways** and **Rob Stephenson**.

Section Writers and Reviewers

This Guide was produced by a dedicated team of subject matter experts from across the industry. The leaders of this Guide would like to recognize the following participants who took lead roles in the authoring of this document.

Karen Alexander	Pfizer Limited	United Kingdom
Winnie Cappucci	Bayer HealthCare	USA
Pam Lawrence	Perceptive Informatics	United Kingdom
Scott Lewis	Eli Lilly and Company Limited	United Kingdom
Christopher Loscombe	Eli Lilly and Company Limited	United Kingdom
Munya Mafemba	Johnson & Johnson	United Kingdom
Chris Reid	Integrity Solutions Limited	United Kingdom
Elizabeth Harrison	GSK	United Kingdom
Kate Samways	KAS Associates	United Kingdom
Genni Sanders	Systematicity Limited	United Kingdom
James Stafford	Business & Decision Limited	United Kingdom
Rob Stephenson	Pfizer Limited	United Kingdom
Simon Topham	Napp Pharmaceuticals Limited	United Kingdom
Charlie Wakeham	Pall Corporation	United Kingdom

Special thanks go to Sam Brooks (Novartis) and Chris Clark (Napp Pharmaceuticals Limited) for their editorial contributions, coaching, and tireless support of this Guide.

Many other individuals reviewed and provided comments during the preparation of this Guide; although they are too numerous to list here, their input is greatly appreciated.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009



ISPE Headquarters
3109 W. Dr. Martin Luther King Jr. Blvd., Suite 250, Tampa, Florida 33607 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 Operation of GxP Computerized Systems 2009

Table of Contents

1 Introduction 9
1.1 Overview 9
1.2 Purpose 9
1.3 Benefits 11
1.4 Key Concepts 11
1.5 Structure of this Guide 12

2 Overview of the Operation Phase 13

3 What Organizations Should Do 17
3.1 Introduction 17
3.2 Capture of Operational Control Requirements 18
3.3 Design of Operational Processes 18
3.4 Verification of Processes 19
3.5 Deployment of Processes 19
3.6 Verification of the Effectiveness of Processes 19

4 Process Relationships 21

5 Handover 23
5.1 Introduction 23
5.2 Scope 23
5.3 Roles and Responsibilities 23
5.4 Handover Process Flow Diagram 25
5.5 Process Narrative 26
5.6 Procedural Guidelines and Considerations 27
5.7 Records and Record Content 29
5.8 Scalability 32

6 Establishing and Managing Support Services 33
6.1 Introduction 33
6.2 Scope 33
6.3 Roles and Responsibilities 33
6.4 Establishing and Managing Support Services Process Flow Diagram 35
6.5 Process Narrative 36
6.6 Procedural Guidelines and Considerations 38
6.7 Records and Record Content 40
6.8 Scaleability 44

7 Performance Monitoring 45
7.1 Introduction 45
7.2 Scope 45
7.3 Roles and Responsibilities 45
7.4 Performance Monitoring Process Flow Diagram 46
7.5 Process Narrative 47
7.6 Procedural Guidelines and Considerations 49
7.7 Records and Record Content 52
7.8 Scaleability 53

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

8 Incident Management 55
8.1 Introduction 55
8.2 Scope 55
8.3 Roles and Responsibilities 55
8.4 Incident Management Process Flow Diagram 57
8.5 Process Narrative 58
8.6 Procedural Guidelines and Considerations 60
8.7 Records and Record Content 63
8.8 Scalability 64

9 Corrective and Preventive Action 65
9.1 Introduction 65
9.2 Scope 65
9.3 Roles and Responsibilities 65
9.4 Corrective and Preventive Action Process Flow Diagram 67
9.5 Process Narrative 68
9.6 Procedural Guidelines and Considerations 70
9.7 Records and Record Content 71
9.8 Scalability 72

10 Operational Change and Configuration Management 75
10.1 Introduction 75
10.2 Scope 75
10.3 Roles and Responsibilities 76
10.4 Operational Change Management Process Flow Diagram 78
10.5 Operational Change Management Process Narrative 79
10.6 Configuration Management Process Flow Diagram 86
10.7 Configuration Management Process Narrative 87
10.8 Procedural Guidelines and Considerations 89
10.9 Records and Record Content 94
10.10 Scalability 97

11 Repair Activity 101
11.1 Introduction 101
11.2 Scope 101
11.3 Roles and Responsibilities 101
11.4 Repair Activity Process Flow Diagram 102
11.5 Process Narrative 103
11.6 Procedural Guidelines and Considerations 104
11.7 Records and Record Content 105
11.8 Scalability 105

12 Periodic Review 107
12.1 Introduction 107
12.2 Scope 107
12.3 Roles and Responsibilities 107
12.4 Periodic Review Process Flow Diagram 109
12.5 Process Narrative 110
12.6 Procedural Guidelines and Considerations 111
12.7 Records and Record Content 115
12.8 Scalability 117

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

13 Backup and Restore 121
13.1 Introduction 121
13.2 Scope 121
13.3 Roles and Responsibilities 121
13.4 Backup and Restore Process Flow Diagram 123
13.5 Process Narrative 124
13.6 Procedural Guidelines and Considerations 125
13.7 Records and Record Content 128
13.8 Scalability 129

14 Business Continuity Management 131
14.1 Introduction 131
14.2 Scope 131
14.3 Roles and Responsibilities 132
14.4 Business Continuity Management Process Flow Diagram 134
14.5 Process Narrative 135
14.6 Procedural Guidelines and Considerations 137
14.7 Records and Record Content 140
14.8 Scalability 143

15 Security Management 145
15.1 Introduction 145
15.2 Scope 145
15.3 Roles and Responsibilities 145
15.4 Security Management Process Flow Diagram 147
15.5 Process Narrative 148
15.6 Procedural Guidelines and Considerations 153
15.7 Records and Record Content 154
15.8 Scalability 155

16 System Administration 157
16.1 Introduction 157
16.2 Scope 157
16.3 Roles and Responsibilities 157
16.4 System Administration Process Flow Diagram 159
16.5 Process Narrative 160
16.6 Procedural Guidelines and Considerations 161
16.7 Records and Record Content 163
16.8 Scalability 164

17 Data Migration 167
17.1 Introduction 167
17.2 Scope 167
17.3 Roles and Responsibilities 167
17.4 Data Migration Process Flow Diagram 169
17.5 Process Narrative 170
17.6 Procedural Guidelines and Considerations 174
17.7 Records and Record Content 175
17.8 Scalability 178

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

18 System Retirement, Decommissioning, and Disposal 179
18.1 Introduction 179
18.2 Scope 179
18.3 Roles and Responsibilities 179
18.4 System Retirement, Decommissioning, and Disposal Process Flow Diagram 181
18.5 Process Narrative 182
18.6 Procedural Guidelines and Considerations 186
18.7 Record and Record Content 186
18.8 Scalability 190

19 Appendix 1 – RACI Roles and Operational Processes 191
19.1 RACI Terms 191
19.2 Grid Showing Operational Process versus RACI Role 192
19.3 Roles 192

20 Appendix 2 – Mapping of Operational Processes to ITIL® and COBIT® 195

21 Appendix 3 – List of Control Records 201

22 Appendix 4 – References 205

23 Appendix 5 – Glossary 207
23.1 Acronyms and Abbreviations 207
23.2 Definitions 209

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

1 Introduction

1.1 Overview

For regulated organizations, the Return On Investment (ROI) for the significant time and resources expended in implementing new computerized systems is achieved during the Operation Phase. The Operation Phase is usually significantly longer than the time spent in developing and delivering the system to the user community.

Regulated computerized systems should be maintained in a demonstrable state of control and in accordance with regulatory requirements. This applies to all components of the system (e.g., hardware, software, infrastructure, documentation, and personnel) throughout the system life cycle, from concept to retirement. Maintained regulated data and records should be complete, accurate, and secure. Some regulated data and records need to be retained after system retirement. Organizations should ensure that their integrity is assured for any required trending, re-evaluation, or inspection purposes within the defined retention period.

During the operational life of a GxP system, regulators usually focus on the integrity, consistency, and completeness of controls required to maintain compliance.

Recovery from a failure to maintain control of a regulated system during the Operation Phase can be both time-consuming and expensive, and increase the risk to data integrity, product quality, and patient safety.

Operational management controls should be established prior to acceptance and release and maintained throughout the Operation Phase of the system life cycle. Incidents and changes to systems should be managed effectively and efficiently, and the required records produced and retained.

These controls are similar to those employed to comply with the Sarbanes-Oxley (SOX) Act, the Federal Information Security Management Act (FISMA), and other regulations. All share common elements with ISO 20001 (ISO 17799) (Reference 4, Appendix 4).

1.2 Purpose

The purpose of this ISPE GAMP® Good Practice Guide, a Risk-Based Approach to Operation of GxP Computerized Systems (OGCS), is to provide detailed information to enable organizations to support their systems more effectively during the Operation Phase of the system life cycle.

It provides comprehensive guidance for maintaining control of regulated systems throughout their operational life (including acceptance and release, system handover, through to system retirement and decommissioning). When applied as intended, this Guide can provide detailed direction on the required control processes which form a substantial part of an appropriate Quality Management System (QMS).

This Guide focuses on achieving effective and efficient business processes aligned with regulatory expectations, by providing generic principles which can be applied to regulated systems using a systematic and scalable approach.

Risk-based controls should be implemented at a level of formality and complexity appropriate to an organization and system.

This Guide addresses the operational and support processes that need to be established to receive regulated computerized systems into the Operation Phase of their life cycle and to maintain them in a state of compliance throughout their operational life, through to system retirement.

It is applicable to systems consisting of hardware and software of all GAMP® categories.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Guidance provided is scalable and can be applied to a range of systems, including:

- laboratory systems
- process control systems
- IT applications

Whereas GAMP® 5 (Reference 7, Appendix 4) is primarily concerned with strategic approaches and planning of operational activities, this Guide contains more detailed information, including:

- a fuller consideration of process scope
- risk-based scalability considerations
- the appropriate assignment of roles and responsibilities
- identification of associated records
- example documentation and record content

Table 2.1 links each operational process described in this Guide and the related GAMP® 5 Appendix.

The process flow diagrams provided are intended to assist in making the process steps and their interrelationships clear and accessible. Wherever possible, a common terminology has been adopted to describe the required management processes, to allow the guidance to be accessible to as wide a readership as possible.

This Guide is intended to be of interest to:

- Process Owners
- System Owners
- Subject Matter Experts (SMEs)
- Quality Unit Representatives
- End Users
- Support Organizations
- Suppliers
- Other Stakeholders

For further information, see Section 19 of this Guide (Appendix 1: RACI Roles and Processes).

This Guide is based on the output of a GAMP® Community of Practice (COP) Special Interest Group initially concerned with the topic of ‘Maintaining Control during Operation’ of regulated computerized systems. The material presented in this Guide has developed and evolved in parallel to guidance provided in GAMP® 5 and is intended to align with and supplement that guidance.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

1.3 Benefits

This Guide aims to increase the awareness of the importance of the Operation Phase and to assist in the development, implementation, and maintenance of efficient, cost-effective, and compliant processes and procedures.

This Guide seeks to:

- provide a better understanding of both the individual operational processes and the interrelationships between them
- help organizations to assign clear roles and responsibilities to required activities throughout the Operation Phase
- embed scalable risk-based approaches into the definition and management of those internal and external operational processes

This Guide aims to help regulated organizations to achieve regulated computerized systems that are fit for intended use and compliant with applicable regulations.

1.4 Key Concepts

This Guide describes an integrated approach to the management, maintenance, and control of regulated computerized systems. GAMP® 5 (Reference 7, Appendix 4) terminology and key concepts are applied to the Operation Phase.

These GAMP® 5 key concepts are:

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

Product and process understanding is essential to the selection of appropriate and scalable controls and procedures. This focus also gives alignment with the ISPE Product Quality Lifecycle Implementation (PQLI) Initiative.

The application of a Quality Management System based approach is aligned with ICH Q10 (Pharmaceutical Quality System) (Reference 6, Appendix 4). A quality risk management approach aligned with ICH Q9 (Quality Risk Management) (Reference 5, Appendix 4) is applied.

The opportunities for leveraging supplier resource and expertise to provide support throughout the Operation Phase are considered. The Guide also takes into account the increased use of computerized systems to support the main operational processes.

The Guide applies the widely used RACI terminology to ensure that roles and responsibilities are identified, defined, and understood (see Appendix 1 for more information).

The Guide has been aligned wherever possible and appropriate with the IT Infrastructure Library (ITIL® V3) (Reference 10, Appendix 4) and Control Objectives for Information and related Technology (COBIT®) (Reference 9, Appendix 4) approaches and terminology. (See Appendix 2 which maps the operational processes described in this Guide to ITIL® and COBIT®).

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

1.5 Structure of this Guide

This Guide consists of a Main Body, including introductory sections, detailed operational guidance, and sections on data migration and system retirement.

The introductory sections consist of:

- **Introduction:** Overview, Scope, Purpose, Benefits, Key Concepts, and Structure of this Guide
- **Overview of the Operation Phase**
- **What Organizations should do:** how to implement the guidance

The detailed operational guidance sections have each been structured in the same way to present the information in a consistent and accessible manner:

- **Introduction:** the purpose of the Operational Process being described
- **Scope:** the scope of the guideline for the Operational Process being described
- **Roles and Responsibilities:** a table in system role order summarizing the RACI assignments for the operational process and detailing main responsibilities for each role related to the operational process being described.
- **Process Flow Diagram:** representation of the Operational Process as a workflow diagram identifying critical process steps, interactions with other operational processes, decision points, and required records. Shading is used to indicate activities and records directly related to the operational processes and is reflected in the associated process narratives.
- **Process Narrative:** a tabular representation of the process flow diagram with additional guidance specific to each process step.
- **Procedural Guidelines and Considerations:** a section providing further guidance information regarding any additional considerations relating to establishing and maintaining the operational process.
- **Records and Record Content:** a list of the expected evidential records for each of the operational processes with their expected content.
- **Scalability:** a risk-based consideration of how the operational process can be appropriately scaled depending on the impact of the system on patient safety, product quality, and data integrity, and on the business impact of the system.

Three Appendices discuss RACI Roles, processes and their relationship to ITIL® (Reference 10, Appendix 4) and COBIT® (Reference 9, Appendix 4), and provide a list of control records.

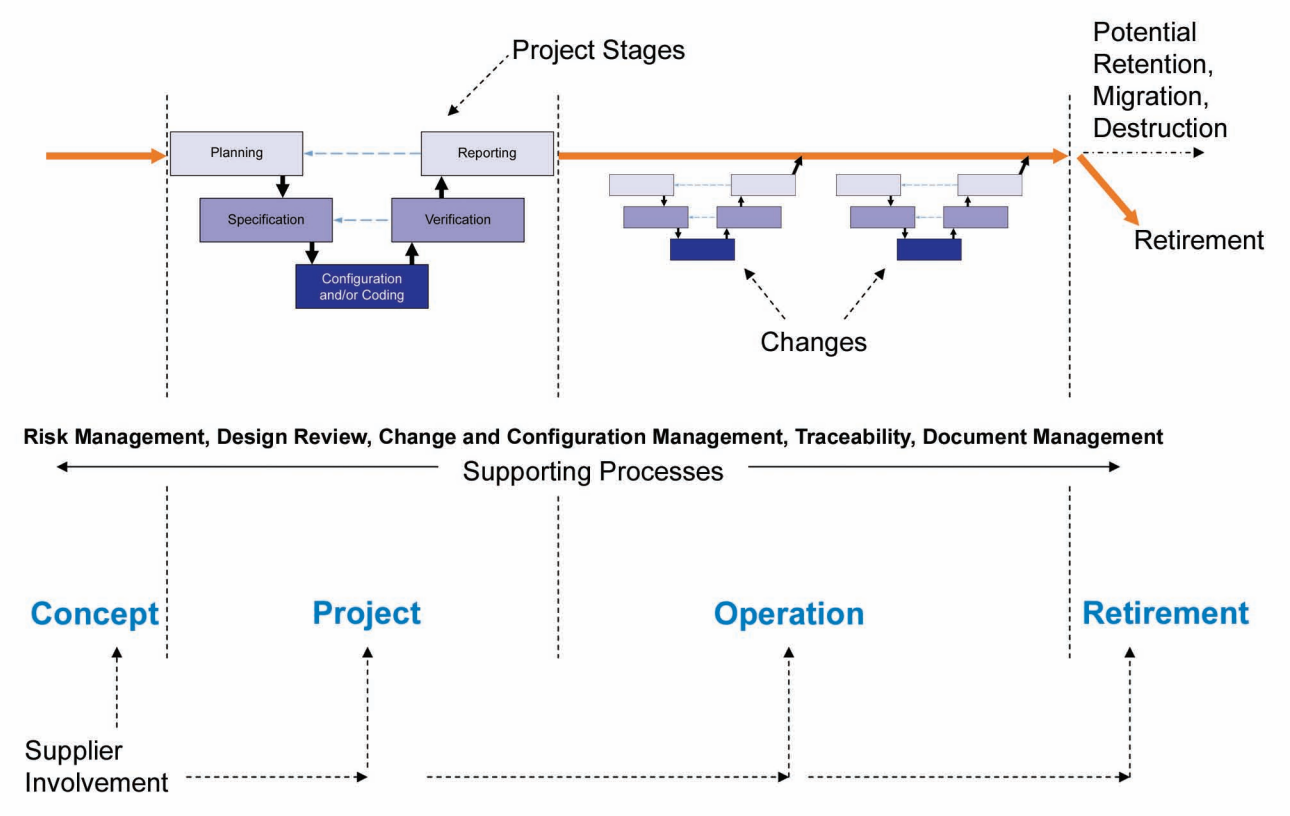
Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

2 Overview of the Operation Phase

Figure 2.1 (from GAMP® 5) shows the Operation Phase in the context of the complete system life cycle.

Figure 2.1: Life Cycle Phases Highlighting the Operation Phase



Organizations should ensure that appropriate operational processes, procedures, and plans have been implemented and are supported by appropriate training, in preparation for acceptance and release, and system handover. Suppliers may be involved in support and maintenance activities.

Compliance and fitness for intended use should be maintained throughout the Operation Phase. This may be achieved by the use of documented procedures and training that cover use, maintenance, and management.

The Operation Phase of a system may last many years, and may include changes to:

- software
- hardware
- system configuration
- business process regulatory requirements

The integrity of the system and its data should be maintained and verified as part of periodic review. Data life cycle considerations are inherent in the operational, support, and management processes described.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Opportunities for process and system improvements should be based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures. Information from Incident Management and Corrective and Preventive Action (CAPA) processes can provide significant input to the evaluation.

Change management should provide a reliable mechanism for rapid implementation of technically sound improvements following the approach to specification, design, and verification described in GAMP® 5 (Reference 7, Appendix 4). The rigor of the approach, including the extent of documentation and verification, should be based on the risk and complexity of the change and the risk to patient safety, product quality, and data integrity.

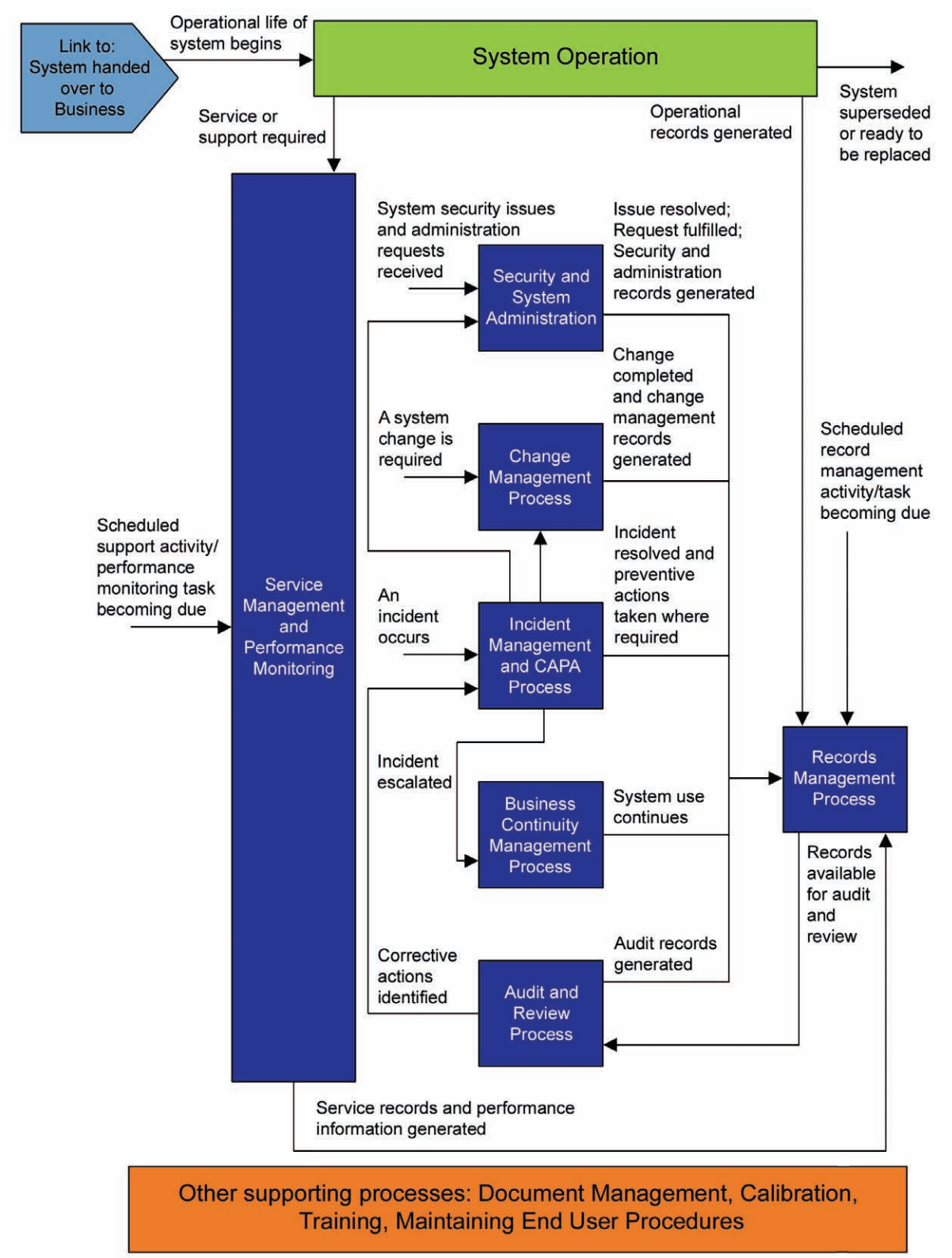
Maintaining system compliance during operation requires the performance of interrelated activities and the approach taken should be scaled according to the nature, risk, and complexity of the system. Figure 2.2 gives an overview of the major relationships between related groups of these activities.

Groups may contain several individual related processes, procedures, and plans (see Table 2.1).

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Figure 2.2: Major Information Flows between Operational Activities



Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Table 2.1: Grouping of Operation Phase Processes

Group of Processes	Process	This Guide Section	GAMP® 5 Appendix
Handover	• Handover Process	5	O1
Service Management and Performance Monitoring	• Establishing and Managing Support Services • Performance Monitoring	6 7	O2, S5 O3
Incident Management and CAPA	• Incident Management • CAPA	8 9	O4 O5
Change Management	• Operational Change and Configuration Management • Repair Activity	10 11	O6 O7
Audits and Reviews	• Periodic Review • Internal Quality Audits	12	O8 -
Business Continuity Management	• Back Up and Restore • Business Continuity Planning (includes Disaster Recovery Planning)	13 14	O9 O10
Security and System Administration	• Security Management • Systems Administration	15 16	O11 O12
Records Management	• Archiving and Retrieval[1]	-	O13
Plus the following processes included in the scope of this Guide:			
Data Migration	• Data Migration	17	D7
System Retirement	• System Retirement, Decommissioning, and Disposal	18	M10

These operational processes are supported by QMS activities, such as document management training management, calibration management, and the maintenance of end user procedures. For further information, see GAMP® 5 and ISPE GAMP® Good Practice Guide: Calibration Management (Reference 8, Appendix 4).

For further information on the individual support and maintenance processes required to maintain the compliance of regulated computerized systems during operation, see the sections of this Guide listed in Table 2.1.

[1] For a more detailed discussion of archiving and retrieval, see ISPE GAMP® Good Practice Guide: Electronic Data Archiving (Reference 8, Appendix 4).

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

3 What Organizations Should Do

3.1 Introduction

To ensure compliance with regulatory expectations organizations should be able to demonstrate that the maintenance and support needs for each system have been reviewed. Appropriate procedures, processes, and records should be established. This evaluation should be performed during the Project Phase; specific elements may be addressed in the Operation Phase.

Operational processes may be generic in nature, system specific, or generic with system specific schedules attached.

Table 4.1 shows how operational processes are related and how they may trigger other operational processes or support processes.

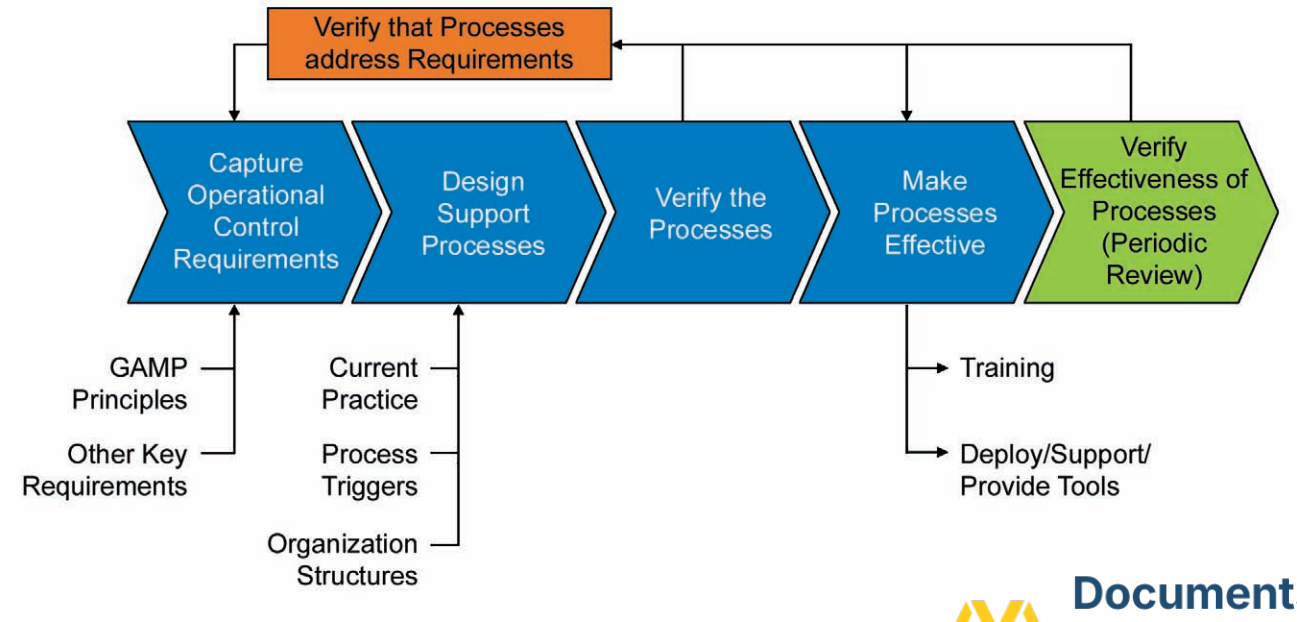
A possible approach to establishing operational control is discussed.

The key steps of this approach include:

- capture operational control requirements (ideally, during the Project Phase)
- design operational processes (ideally, during the Project Phase)
- verify the processes (ideally, during the Project Phase)
- deploy processes
- verify effectiveness of processes

The relationship between these steps is shown in Figure 3.1 and described in this section. These relationships can be subject to ongoing change. It is particularly important to ensure that the processes continue to address requirements and that any updates are managed under change control.

Figure 3.1: Establishing Operational Control



Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

3.2 Capture of Operational Control Requirements

Organizations should be able to demonstrate that processes to achieve operational control requirements are established and that records are maintained for the required retention period, to demonstrate that controls are effective.

The interrelationships between these processes should be considered, to ensure that operational incidents and changes to systems during their operational life cycle are effectively managed, and that the security and integrity of critical records and processes are maintained.

A consistent approach to addressing should be established. Business and regulatory requirements should be considered, e.g.:

- Environmental, Health and Safety regulations
- Sarbanes-Oxley (SOX) controls
- Privacy and Data Protection regulations (such as Health Insurance Portability and Accountability Act (HIPAA)
- Industry specific regulations, such as Payment Card Industry Data Security Standards (PCI DSS)
- local regulations

3.3 Design of Operational Processes

Current practices for the operational management of existing systems within the organization need to be understood before developing a detailed plan for the implementation of operational controls. There may be a significant number of support and review processes established, which already may have been subject to audit and review.

Where there are existing processes a gap analysis can be developed against the operational control requirements statements in order to identify improvement activities.

Controlling procedures which describe the processes should be practical. A definition of the current processes should be produced by consulting those involved. It is generally better to improve and simplify existing processes rather than to create new procedures.

Where a gap is identified and there is no current process supporting a set of key requirements, a new process will need to be designed and implemented. The need to understand how the various processes interrelate is critical to maintain operational control; process design should consider how other processes may be triggered and responsibilities for each process step should be clearly assigned.

A critical consideration in the design of processes and the creation of procedures is the organizational structure of the enterprise; this will determine who has overall responsibility for each process and who is responsible for task steps within the process. For small organizations some of these controls may be achieved through the consistent application of written procedures. For larger organizations, electronic systems may be used to assign roles and permissions, keep track of critical records, and ensure that activities are notified to the correct individuals or teams and escalated appropriately, e.g., in the case of service or control failures. Paper-based systems may be adequate.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

3.4 Verification of Processes

Once the processes have been established, procedures documented, and personnel trained, they should be verified to ensure that the required level of control is in place. Subsequent amendments to the processes should be managed under change control.

3.5 Deployment of Processes

Once processes have been verified, they should be deployed consistently throughout an organization. This may be achieved by a deployment plan which should include a communication plan, the roll-out of training, where appropriate, and provision of the necessary resources, e.g., record forms and log books, personnel.

3.6 Verification of the Effectiveness of Processes

For regulated systems, the Quality Unit should be involved in the review and approval of operational processes. The scope and depth of involvement of the Quality Unit depends on the impact of a system on patient safety, product quality, and data integrity, and should be documented. Opportunities to combine with other compliance testing of internal controls may be considered, e.g., SOX audits.

The Quality Unit should verify effectiveness of operational processes by audit and review using internal assessment tools and Periodic Review.

Appropriate metrics can help to ensure key performance indicators are being met and to support investigation or improvement initiatives.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

4 Process Relationships

Table 4.1 shows the interrelationships and dependencies between operational processes and other related processes.

Table 4.1 is intended to help organizations implement a comprehensive set of operational processes and records in a structured way by:

- ensuring completeness: showing which processes should be supported by controlling procedures
- providing an aid to navigation: supporting users when undertaking an impact analysis to establish which other processes may be triggered

Table 4.1: 'Triggers and Checks'

For each process in the top row, the vertical column indicates those processes that potentially trigger another process (t) or are part of a checking process (c). E.g., **O7 Repair Activity** may trigger **O6 Operational Change and Configuration Management**; **O1 Handover** may check that an **O7 Repair Activity** process is in place.	O1 Handover	O2 Establishing and Managing Support Services	O3 Performance Monitoring	O4 Incident Management	O5 Corrective and Preventive Action	O6 Operational Change and Configuration Management	O7 Repair Activity	O8 Periodic Review	O9 Backup and Restore	O10 Business Continuity Management	O11 Security Management	O12 System Administration	D7 Data Migration	M10 System Retirement, Decommissioning, and Disposal
O1 Handover														
O2 Establishing and Managing Support Services	c		t		t			c						
O3 Performance Monitoring	c	t		t	t			t/c		t				
O4 Incident Management	c		t/c					c			t			
O5 Corrective and Preventive Action	c		t	t				t/c						
O6 Operational Change and Configuration Management	c		t	t	t		t	c		t				
O7 Repair Activity	c	t	t/c	t	t			c		t				
O8 Periodic Review			t	t	t									
O9 Backup and Restore	c	t		t		t		c		t			t	t
O10 Business Continuity Management	c			t	t			c						
O11 Security Management	c			t	t			t/c						
O12 System Administration	c	t		t	t			c						
D7 Data Migration						t		c						t
M10 System Retirement, Decommissioning, and Disposal		t	t	t				t						
• Training	c	t	t	t	t	t		c		t				
• Calibration	c		t		t		t	c						
M9 Document Management	c				t	t		t/c						t
• Application Specific Operational Use SOPs	c				t	t		c						
• SDLC Processes and Procedures	c				t	t		c						
• Validation Processes	c				t	t		c					t	t

Note: Archiving and Retrieval (O13) is not included in this table as a more detailed discussion of this topic is included in the ISPE GAMP® Good Practice Guide: Electronic Data Archiving (Reference 8, Appendix 4).

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

Notes:

The O, D, and M numbers in Table 4.1 and throughout this Guide refer to specific appendices in GAMP® 5. For example, O1 refers to Appendix O1 *Handover* in GAMP® 5 (Reference 7, Appendix 4).

Topics in the Table 4.1 with no number, e.g., Training and Calibration, do not have a dedicated Appendix in GAMP® 5, but are covered in appropriate sections of GAMP® 5.

Table 4.1 provides an indication of where 'triggers' and 'checks' may be appropriate. As organizations may arrange or scope their business processes differently or use different terminology, Table 4.1 is subject to interpretation.

- A 'trigger' is intended to represent the concept that one process may initiate the use of another process.
- A 'check' is intended to represent the concept that one process may seek to assure that another process has been defined, approved, and is in place.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

5 Handover

5.1 Introduction

The Handover process defines the controls required for the transition of a computerized system from a project into the Operation Phase. The process ensures that the environment into which the system is to be received is prepared, to ensure that the system can be used and supported in a controlled manner. The Handover process should ensure that:

- Project (including license and warranty agreements) and project validation activities are complete.
- Configuration items (software, hardware, documentation) are transferred to user and support organization.
- Document management and archiving controls are established and required documentation is archived.
- Operational and support organizations are established and roles defined.
- System management, use, administration, and operational processes are established.
- Support services are defined.
- System users, administrators, and support organizations are trained.
- Data setup is complete (including cutover activities).
- Security setup is complete.
- Residual risks and issues are transferred to user and support organizations.

Note: other processes may be responsible for delivery of the listed activities and creation of the listed documentation, e.g., several of these activities may be included in the verification tasks within the scope of the Validation Plan. The handover process should ensure that the listed activities have been completed and appropriately documented.

This section is related to Appendix O1 of GAMP® 5 (Reference 7, Appendix 4).

5.2 Scope

This process applies to the transition of systems from the Project Phase to the Operation Phase. The principles of this process apply to computerized systems; it can be scaled according the complexity of the system and organization. This process also can be applied when upgrading systems or when changing support organizations.

5.3 Roles and Responsibilities

Table 5.1 provides an indicative example. Organizations should allocate roles and responsibilities based on organizational structure and the specific system.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

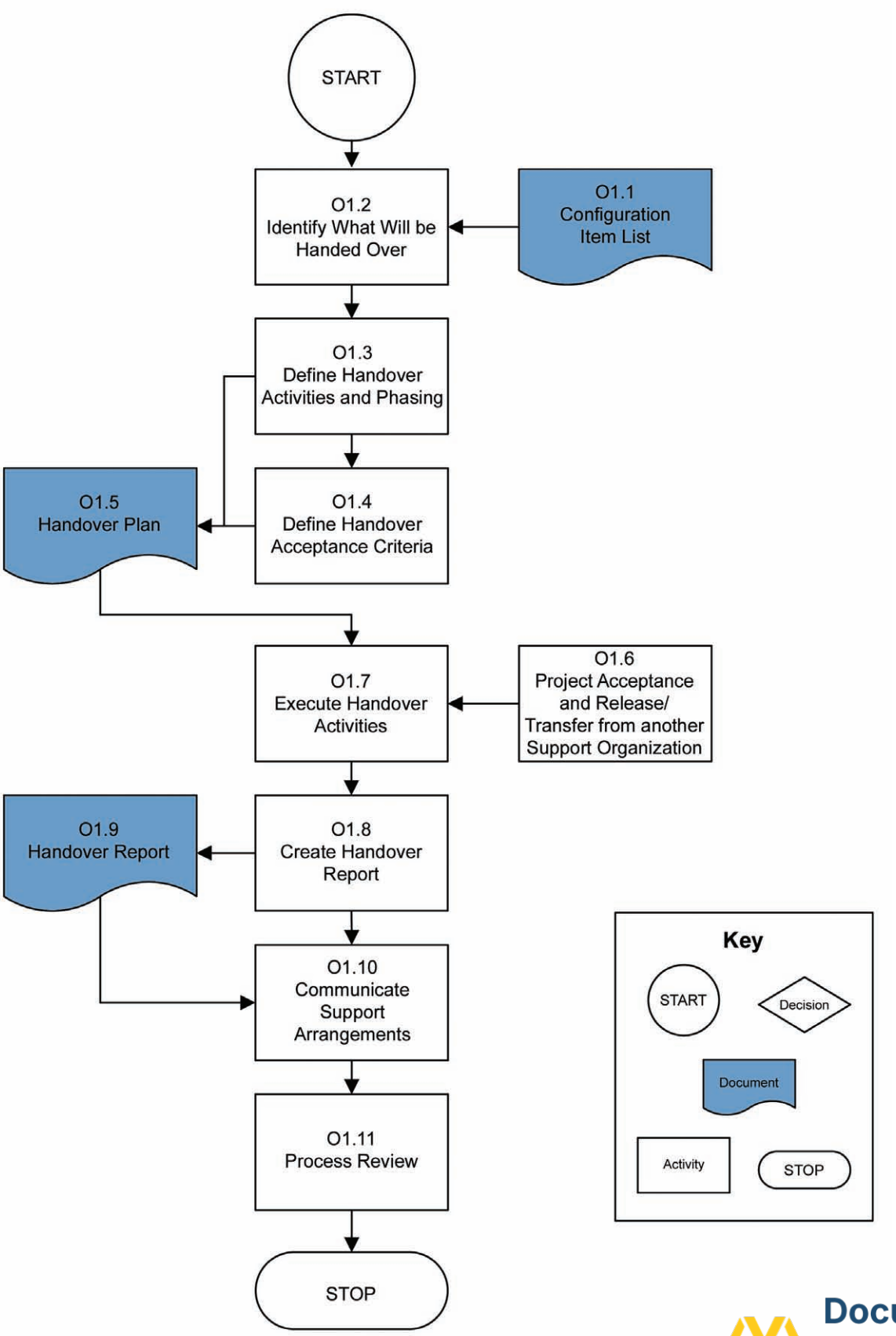
Table 5.1: Roles and Responsibilities for Handover

Role	RACI Role	Responsibilities
Process Owner	R	• takes responsibility for accepting the system into operation • takes responsibility for resolution of residual system issues and risks following acceptance and release
System Owner	R	• takes responsibility for the availability and support and maintenance of a system and for the security of data residing on that system • ensures that system documentation, Standard Operating Procedures (SOPs), system manuals, support agreements, and training are delivered prior to completion of Handover • shares responsibility for resolution of residual system issues and risks following acceptance and release
Project Manager	A	• ensures that Handover activities are incorporated into project plans • ensures that residual issues and risks are communicated and accepted by the Process Owner and System Owner • ensures that acceptance and release decision mandates that Handover activities and documentation are delivered
End User	I	• provides input into development of SOPs and training • attends system and SOP training • works to established operational procedures
Quality Unit	C	• reviews validation report and compliance with quality standards/procedures to ensure control and any residual risks are acceptable for acceptance and release
Platform Support (SME)	R	• takes responsibility for technical platform documentation • establishes Service Level Agreements (SLAs) where required • provides input into development of SOPs and training • attends or delivers training, provides system support, and technical requirements • supplies 'as built' system documentation
Application Support (SME)	R	• takes responsibility for technical application documentation • establishes SLAs where required • provides input into development of SOPs and training • attends or delivers training, provides system support, and technical requirements • supplies 'as built' system documentation
System Administrator	R	• responsible for technical/data setup and administrative procedures (e.g., security administration, maintenance, backup, and restore)
Supplier	C	• provides input to a client SLA or provides a standard supplier SLA • attends SOP/support training if involved in support • delivers training, system support, and technical requirements • supplies or makes available 'as built' system documentation and software
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

5.4 Handover Process Flow Diagram



Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

5.5 Process Narrative

Process Step/Decision/Record	Description
O1 Handover	**A risk-based process by which a Project Team (or other support organization) transfers a system into the Operation Phase.**
O1.1 Configuration Item List	This list should be generated in the Project Phase under the **Configuration Management** process and should include system components and documentation.
O1.2 Identify What Will be Handed Over	The Handover process should transition system components, accountabilities, knowledge, documentation, procedural controls, and support agreements to relevant organizations. Such organizations include Process Owners, System Owners, SMEs (Platform Support, Application Support, etc.), End Users, Supplier Organizations, Document Management, and Quality Units. Process and System ownership, roles and responsibilities, and documentation ownership should be explicit.
O1.3 Define Handover Activities and Phasing	Handover is a series of activities required to transfer a system into Operation. These activities should be defined and agreed by the transferring and receiving parties. **Note:** specific Handover activities may not be completed before system acceptance and release. There should be an explicit action plan for undelivered Handover items before acceptance and release within the context of a risk and impact analysis.
O1.4 Define Handover Acceptance Criteria	Acceptance criteria may be used to define the basis by which Handover activities are deemed complete, e.g., approved training records are in established; SLAs have been created, reviewed, and approved.
O1.5 Handover Plan	The Handover Plan should document the tasks, responsibilities, timing, and acceptance criteria to establish when Handover is complete. The Handover Plan should be approved by the transferring and receiving parties. The Handover Plan may be a separate document or may be incorporated within relevant project documentation.
O1.6 Project Acceptance and Release/Transfer from another Support Organization	The deliverable/technical aspect of the Handover process, can start only: • when a project team completes the Project Phase and hands over the system for operational use • when the support of a system already in operation is handed over from one support provider to another Planning for Handover should be initiated at an earlier stage to ensure that the Handover is managed effectively.
O1.7 Execute Handover Activities	The Handover Plan should be executed. Meetings between transferring and receiving groups should be scheduled, as appropriate, to ensure that progress is made to complete agreed activities.
O1.8 Create Handover Report	The Handover Report should summarize Handover activities against the Handover Plan. Deviations should be assessed for impact and appropriate action should be taken.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

5.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O1.9 Handover Report	The Handover Report should document completion of all agreed activities and acceptance of any items that are not complete (may be covered by Validation or Project Report). Approval by Project Manager and System Owner signifies acceptance of the system into the Operation Phase. The Handover Report may be an input to O1.10 Communicate Support Arrangements.
O1.10 Communicate Support Arrangements	Support organizations, processes, and agreements are communicated to system users. This may be undertaken by the System Owner with support from the Project Team.
O1.11 Process Review	Following Handover a review should be conducted to identify any lessons learned and any opportunities for improvement in the Handover process. This may be undertaken by the System Owner with support from the Project Team. The process review also may be scheduled to coincide with the review of SOPs. (This is independent of a review of the project.)

5.6 Procedural Guidelines and Considerations

5.6.1 Project Acceptance and Release or Transfer from another Support Organization

Handover planning should be considered when transferring a new system into the Operation Phase, when implementing significant system modifications or upgrades, or when changing support organizations or end user groups.

The Handover process should ensure that the system is fit for Handover and that the operation and support organizations are ready to take ownership of system use and management (roles defined, operational processes and procedures in place, residual risks accepted and support organizations in place to maintain compliance). Accountability and responsibility for the system (hardware, software, documentation, and data) is transferred from the project organization to the Process Owner and System Owner, respectively.

External support organizations may be used, e.g., where expertise or resources are not available within the user organization. Where support services are provided for systems which may have a high impact on processes or where the scope of external support services provided is high, a supplier assessment should be considered in consultation with the Quality Unit.

5.6.2 Define Handover Plan

Handover activities can be broken down into several areas and should ensure that:

- Project (including license and warranty agreements) and Validation Activities are complete.
- Configuration Items (software, hardware, documentation) are accessible to user and support organizations.
- Document Management and Archiving controls are in place and required documentation is archived.
- Operational and Support Organizations are in place and roles defined.
- System Management, Use, Administration, Operational and Support Processes and SOPs are in place.
- Operational and Support Services are defined and organizations in place.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

- Skills and knowledge are transferred, including training of System Users, Administrators and Support organizations.
- Data Setup is complete.
- Security Setup is complete.
- Residual Risks and Issues are handed over to user and support organizations.

Section 5.7.1 provides an example structure and content of the Handover Plan.

Documentation should be in an "as built" state. Handed over documentation should be under document management control and stored in secure electronic or physical document repositories. Documents which require ongoing maintenance (e.g., design documents) should be accessible by support organizations to allow maintenance under configuration management. Documents which do not require ongoing maintenance (e.g., executed test documentation) should be accessible for information purposes and archived for historical access.

Handover may be phased and activities may be scaled according to the complexity of a system, in regard to:

- geographic distribution of the system
- number of sites
- consistency in intended use
- use of third party support organizations

Other considerations for a phased Handover include whether the system is to be implemented vertically (e.g., system supports complete business process in one area, site, or division) or horizontally (e.g., functionality is provided to support an aspect of a business process across several areas, sites, or divisions).

Handover Plans should be agreed by Project Managers, Support Organizations, and User Organizations, including Quality Units.

For complex projects, a Handover manager may be beneficial in coordinating between the project team and the operating organization.

5.6.3 Define Acceptance Criteria

Acceptance criteria should be established to ensure that the providing and receiving organizations are able to determine clearly that a Handover activity is complete. Criteria may include:

- 'as built' documentation available and approved
- validation summary report approved (confirming satisfactory specification, design, and testing of the system)
- training records updated for all planned training
- user and support organization roles defined
- review and monitoring processes are in place
- instrumentation added to calibration schedules

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

- availability of maintenance schedules with defined responsibilities
- SLAs approved and issued
- number of critical errors encountered in the first defined period of use

5.6.4 Completion of Handover Activities

Handover is considered complete when all activities in the Handover Plan are complete and all defined acceptance criteria have been met.

Project managers (or Handover managers) should monitor a Handover Plan regularly.

5.6.5 Communication

A Handover Report should be created to define the outcome of Handover activities. For less complex systems and projects, this may be summarized in a Validation Summary Report.

During Handover, Project Managers should communicate progress and discuss issues with Process Owners, System Owners, and Support Organization leaders.

5.7 Records and Record Content

5.7.1 Handover Plan

The Handover Plan (which may be incorporated into another document, e.g., the Validation Plan) should include:

- Purpose and Scope
- Operational Organization:
  - define roles and responsibilities of receiving organizations:
    - > process and system owner
    - > internal support organizations (application and platform)
    - > external support organizations
    - > quality unit
    - > documentation control and archiving organizations
- Configuration Items (refer to configuration item list)
  - system software components including version and build number (and licensing)
  - system hardware components
  - technical documentation (specifications, certificates, and manuals)
  - user documentation (user requirements, test documentation, plans, reports)

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

- system, design and configuration documentation, including security matrix

• Activities

- confirmation of project and validation activities
  - > validation summary report approved
  - > performance qualification completed and post implementation monitoring planned or performance qualification incorporated into post implementation monitoring
- handover of configuration items
  - > system hardware and software installation
  - > system software and configuration archiving
- document management and archiving
  - > update documentation to “as built” state
  - > system use documentation handover activities
  - > support documentation handover activities
  - > document archive activities
  - > document storage and access requirements
- operational and support organizations
  - > Process Owner
  - > System Owner
  - > applications support organization
  - > platform support organization
  - > external support organization(s)
- process and procedures
  - > performance monitoring
  - > incident management
  - > CAPA
  - > change management (including configuration management)
  - > repair
  - > periodic review

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

  - > business continuity management and disaster recovery
  - > backup and restoration
  - > security management
  - > archive, refresh, and retrieval
  - > retirement and decommissioning
  - > document management
  - > training
  - > calibration
  - > system use
- support services
  - > SLAs
  - > support service governance structure
  - > updates to system Inventory
  - > calibration schedules and relevant certificates
  - > maintenance schedules
  - > provision of spare parts
- training
  - > users
  - > administrators
  - > support organizations
  - > management
  - > ongoing training (ownership, responsibilities, procedures)
- data setup
  - > data migration (for further information see Chapter 17 of this Guide)
  - > data setup
  - > isolation of test data from runtime environment
- security setup

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

    - > manage users, e.g., add new users, change user profiles, disable users
  - risk and issues handover
    - > residual risks handed over from project risk management process
    - > pending changes
    - > known issues (including minor deviations)
    - > active work-arounds
- Schedule of Handover Tasks, Sequence, and Responsibilities to incorporate any phased Handover associated with the complexities of the system implementation (see Section 5.6.2 of this Guide)
- Acceptance Criteria
  - Criteria defined for each handover activity. Used to determine when activity is complete.

5.7.2 Handover Report

The Handover Report should provide a summary of completion of Handover Activities and acceptance criteria. The report should demonstrate that acceptance criteria have been met. Handover Reports may include:

- Handover Activity
- Planned Completion
- Actual Completion
- Acceptance Criteria
- Reference to evidence of Acceptance Criteria
- List or Reference to List, of Handover Documents
- Outstanding items (e.g., bugs, functionality gaps, deviations) and how they will be tracked to completion (e.g., via a CAPA unique ID)

5.8 Scalability

A separate System Handover Plan may be required, depending on the competence of suppliers (determined by an appropriate risk-based approach, e.g., use of the appropriate level of supplier assessment), the size and complexity of the system, and the size and complexity of the receiving operation and support organizations.

For less complex systems, a Handover Plan may be integrated into Project Plans or the Validation Plan. A checklist pro-forma also may be used. Handover Reports may be incorporated into Validation Summary Reports.

A Handover Manager may be appointed for large and complex systems, particularly for multi-site or global roll-outs.

The criticality of systems has only limited impact on the scalability of Handover Plans; large, complex systems with low to medium impact may benefit from Handover planning.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

6 Establishing and Managing Support Services

6.1 Introduction

This guidance aims to define the process by which internal and external support services are defined, agreed, and managed to ensure that:

- Services are defined clearly.
- Roles and responsibilities, and interfaces between or within organizations, are defined clearly.
- Service delivery controls are established.
- Appropriate skills are established.
- Document and record ownership are defined clearly.
- Escalation procedures are established.
- Service performance can be monitored.
- Quality requirements are defined.

This section is related to Appendix O2 of GAMP® 5 (Reference 7, Appendix 4).

For further information on outsourced IS/IT environments, see GAMP® 5, Appendix S5 Managing Quality within an Outsourced IS/IT Environment.

6.2 Scope

This process applies when establishing internal and external support services. This guidance covers the identification of support services, creation of SLAs, delivery of support services, and the monitoring of performance against agreed service levels.

6.3 Roles and Responsibilities

Table 6.1 provides an indicative example. Organizations should allocate roles and responsibilities based on organizational structure and the specific system.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

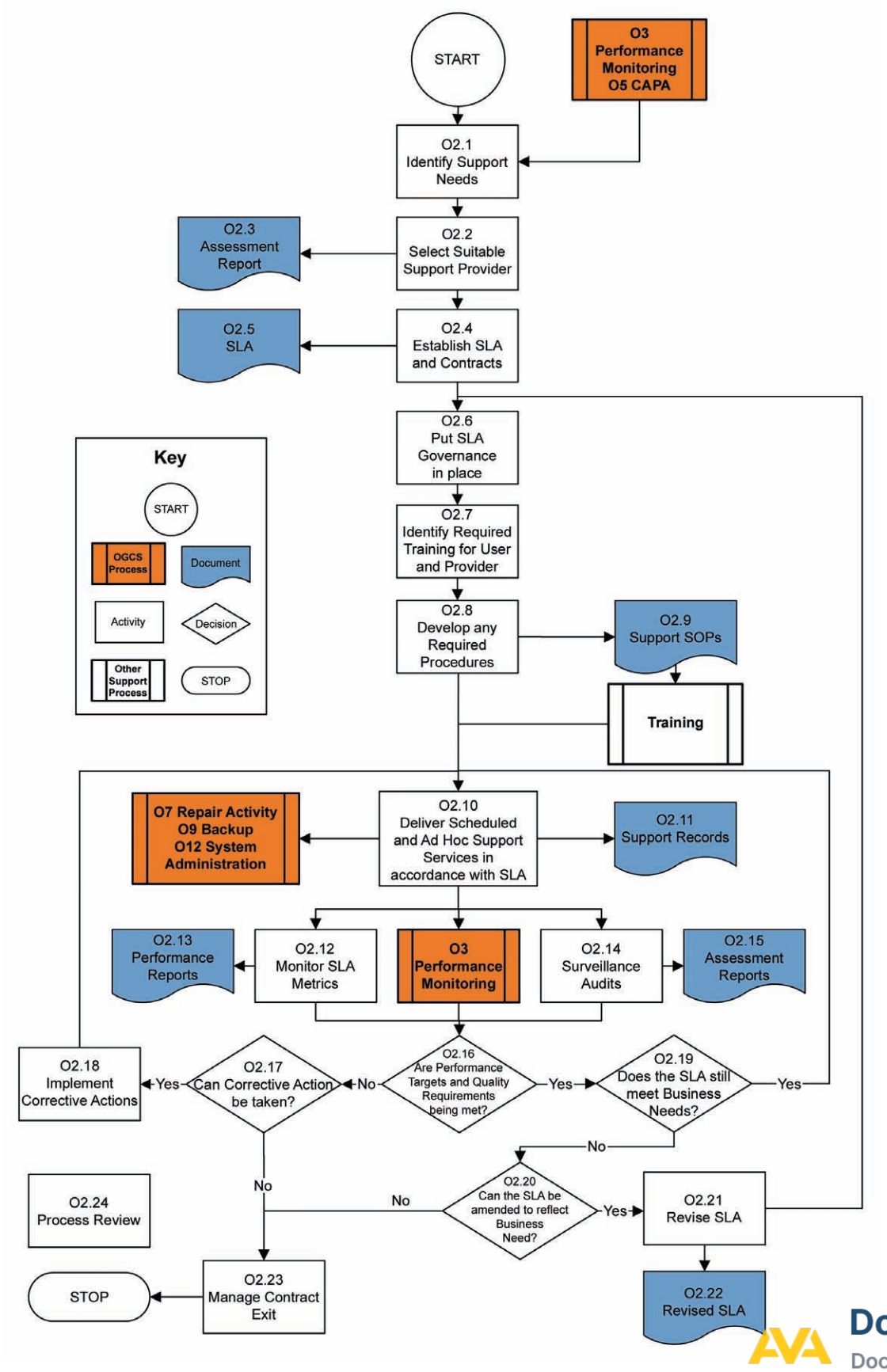
Table 6.1: Roles and Responsibilities for Establishing and Managing Support Services

Role	RACI Role	Responsibilities
Process Owner	C	• supports the determination of system impact and criticality of support service requirements • supports the determination of whether internal or external support organizations should be used
System Owner	A	• ensures that appropriate service providers are identified and evaluated • ensures that SLAs are in place • monitors the performance of services provided against agreed metrics • manages the service contract • defines the interfaces between user and support organizations • ensures that training in technical requirements and user procedures is provided to the support organization (where required) • ensures that the handover process has provided required procedures, documentation, skills, roles, etc., to enable effective support to be delivered • owns the support records
Project Manager	R	• ensures that SLAs are established prior to Handover (where required)
End User	I	• is made aware of support services and means of accessing support services • follows defined procedures and SLAs when accessing support services
Quality Unit	C	• evaluates external and internal support organizations • ensures that regulatory and quality requirements, e.g., audit, documentation standards, procedural controls, record keeping, and training are defined within support contracts and SLAs • reviews effect of deviations from agreed service definition and levels
Platform Support (SME)	R	• provides support (or manages external support) in accordance with agreed SLAs
Application Support (SME)	R	• provides support (or manages external support) in accordance with agreed SLAs
System Administrator (SME)	R	• provides support (or manages external support) in accordance with agreed SLAs
Supplier	C	• provides support in accordance with agreed SLAs
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

6.4 Establishing and Managing Support Services Process Flow Diagram



Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

6.5 Process Narrative

Process Step/Decision/Record	Description
O2 Establishing and Managing Support Services	**An operational process for ensuring that maintenance and support contracts are appropriately specified and managed.**
O2.1 Identify Support Needs	Process Owner and System Owner identify support required for a system from both internal and external support organizations. A review of support requirements may be triggered by the operational processes **O3 Performance Monitoring** and **O5 Corrective and Preventive Action**.
O2.2 Select Suitable Support Provider	Appropriate support organization is identified. If provider is an external supplier and services are high impact an audit or other means of supplier assessment should be considered. Internal reviews may be less formal, but necessary checks should be performed.
O2.3 Assessment Report	Prior to agreement, Assessment Report is created and observations addressed (where possible). The Assessment Report should include an evaluation of any risk factors identified.
O2.4 Establish SLA and Contracts	SLA is established, reviewed, and approved by both parties. Where there is a contractual element this should be included in Contract documentation.
O2.5 SLA	SLA defines support services required, governance requirements, tools and procedural controls, resources, training requirements, escalation procedures, metrics, etc. (For further information on proposed SLA content, see Section 6.7.1 of this Guide).
O2.6 Put SLA Governance in Place	Governance organization is established. Roles and communications processes are defined in the SLA.
O2.7 Identify Required Training for User and Provider	Training needs are identified. Support and maintenance services providers should be competent to perform their required tasks. This includes GxP training where necessary (e.g., external providers).
O2.8 Develop any Required Procedures	SOPs required to control the support service are established by required parties. SOPs controlling interfaces between receiving and supplying organizations should be defined.
O2.9 Support SOPs	Required support SOPs are established, reviewed, and approved by relevant parties. Once in place these trigger training activities.
Training	Training in user organization or provider organization procedures or systems may be required. Training will be delivered by relevant party. Training records are established to document training.
O2.10 Deliver Scheduled and Ad Hoc Support Services in accordance with SLA	Scheduled and ad hoc support requests are processed and delivered in accordance with agreed procedures. These procedures are reflected in other operational processes, other support processes, and in related processes, such as validation.
O2.11 Support Records	Records documenting delivered support should be established. Records are determined by the type of support provided.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

6.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O7 Repair Activity **O9 Backup** **O12 System Administration**	Other operational processes, relating to the specific service provided are invoked to control the service.
O2.12 Monitor SLA Metrics	User and Supplier organization report and review performance of user and supplier organization against agreed support metrics. Deviations are reviewed and risks mitigated in accordance with their priority.
O2.13 Performance Reports	Performance reports document actual performance against SLA metrics.
O3 Performance Monitoring	The operational process **O3 Performance Monitoring** is triggered once support services are delivered.
O2.14 Surveillance Audits	Audits are conducted periodically to ensure that agreed quality systems are being adhered to.
O2.15 Assessment Reports	Assessment Report is created and observations addressed, including those where no action is required.
O2.16 Are Performance Targets and Quality Requirements being met?	Where there is a deviation from performance targets or surveillance audits, deviations from stated standards are identified; action needs to be taken to address the problem. The Root Cause of the problem should be evaluated and relevant preventive and corrective actions taken to address the deviations, where possible.
O2.17 Can Corrective Action be taken?	Root Cause assessment will determine what actions can be taken to address deviations from agreed service levels or quality requirements. It may not be possible to address a problem or problems may be recurring. In such cases, it may be necessary to change the scope of the services provided or seek an alternative service provider (internal or external).
O2.18 Implement Corrective Actions	Corrective action is taken to address deviations from stated service levels and quality requirements. This may include changing service levels, implementing new processes and procedures, additional training, or changes in resources, etc.
O2.19 Does the SLA still meet Business Needs?	The defined support service may be meeting SLA performance requirement and quality requirements; however, business needs may have changed resulting in a change to the SLA or exit from the contract.
O2.20 Can the SLA be amended to reflect Business Need?	SLA is modified to reflect new business requirements. This may lead to changes in governance structure, service levels, SOPs, and training.
O2.21 Revise SLA	SLA is modified, reviewed, and approved to reflect revised services and service levels.
O2.22 Revised SLA	SLA is revised to reflect new business requirements.
O2.23 Manage Contract Exit	An alternative support provider may be required (internal or external) or a system may have been retired. Contract exit should be considered when establishing an SLA to ensure that full control can be regained of the support service. Documentation and record ownership should have been identified at the outset of the contract.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

6.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O2.24 Process Review	From time to time, a review should be conducted to identify any lessons learned and any opportunities for improvement to the process for Establishing and Managing Support Services. This may be undertaken by the System Owner. This type of process review may be scheduled to fall in line with the review of SOPs for currency.

6.6 Procedural Guidelines and Considerations

6.6.1 Identify Support Needs

Process Owners and System Owners, with in-house support (SMEs), should determine the scope of required support services and identify potential suppliers.

6.6.2 Select Suitable Support Supplier

Process Owners and System Owners should consult with the Quality Unit to determine the need for Supplier Assessment. The need for assessment will be determined by a number of criteria, including:

- scope of services to be provided
- criticality of services to be provided (business and regulatory impact)
- previous history of the supplier
- use of own or supplier quality processes

If required, supplier evaluation should be conducted and documented in accordance with GAMP® 5 Appendix M2: Supplier Assessment (Reference 7, Appendix 4) or other in-house supplier assessment processes and procedures.

The output of the evaluation determines whether the supplier can be used, the adequacy of existing service management and delivery controls, and any additional controls that may be required.

For internal organizations, an assessment should be conducted to ensure that appropriate service management and delivery controls are established.

Where shortfalls are identified, these should be reported and a remediation plan established.

6.6.3 Establish Service Level Agreement and Support Contracts

SLAs should be established to define the scope of services to be provided, controls to be used, training needs, service performance metrics, and roles and responsibilities. For further information see Section 6.7.1 of this Guide. There may be a hierarchy in the provision of support, e.g., first level support is provided by local IT, second level support is provided by a global organization collecting solutions and managing supplier relations.

A Quality Unit should ensure that quality controls, such as training, GxP record keeping, documentation standards, and ongoing audit program are defined.

SLAs will be needed for each support organization.

Procurement and legal departments should be consulted when drawing up external SLAs and contracts.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

For each support organization, service performance metrics and escalation procedures should be defined.

Interfaces between client and supplier organizations should be defined clearly, including:

- how services are accessed
- whether or how remote access is permitted
- how upgrades should be managed
- how file transfers are achieved

The definition of interfaces should include access to quality documentation and records, including SOPs, contact numbers, use of call logging systems, roles and responsibilities, etc.

A governance structure should be established for managing the provision of services. Governance considerations include:

Business Management

- ensuring Intellectual Property and critical data are identified and protected
- ensuring Non-Disclosure Agreements are in place, where necessary
- defining relevant laws, regulations, licensing agreements, and directives
- identifying policies and standards impacting support services

Contract Management

- establishing and monitoring conformance to contract and SLAs
- managing deviations
- scope change management

Quality Management

- surveillance audits for the quality of the service provision, monitoring quality controls
  (This is distinct from Performance Monitoring. See Chapter 7 of this Guide, which focuses on how the system itself is performing.)

Customer/Supplier Relationship Management

- effectiveness of client/supplier interfaces and governance structures
- adherence to commitments

6.6.4 Training

User organization and supplier organization personnel may need to be trained prior to commencing services. Training should consider:

- GxP requirements (GLP, GCP, GMP, GDP) as appropriate

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

- user and supplier procedures, (including system administration, handling back-end access, data ownership, and management)
- requirements of SLAs
- system and technical documentation
- security requirements (where necessary)
- any other relevant regulations, (e.g., data associated with personally identifiable information)

6.6.5 Standard Operating Procedures

SOPs may need to be developed to control the services being provided. Where there is an interface between user organization and supplier organization procedures, this should be addressed.

Procedures should be part of a user's and a supplier's quality management system. It should be clear which procedures are to be used.

6.6.6 Routine and Ad Hoc Support

Routine and ad hoc support should be provided in accordance with the agreed SLA and support procedures. All support activities (including any validation activities) should be documented using service reports, change control records, maintenance records, or other relevant records as defined by governing support service SOPs and SLA.

6.6.7 Service Performance Monitoring and Periodic Audits

Service performance should be monitored against agreed SLAs. Deviations from agreed SLAs should be evaluated and appropriate corrective actions taken. Where there is a quality impact from a deviation, relevant Incident and CAPA processes should be employed.

Periodic quality audits should be conducted (if deemed necessary by the scope and criticality of the services provided). Observations should be reviewed with the service provider and appropriate action taken to address an observation.

The root cause of any deviations from an SLA should be determined. Decisions regarding changes to service management and delivery controls, additional training, changes to metrics or in certain cases change of service provider may result.

6.7 Records and Record Content

6.7.1 Service Level Agreement Content Considerations

Content to be considered when developing SLAs includes:

- Scope:
  - system scope (what system is to be covered by the service)
  - service scope:
    - > system upgrades

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

> backup and restoration

> archiving and retrieval

> data maintenance

> disaster recovery

> fault feedback, fault diagnosis, and rectification (fault reporting, workarounds, patches, and service releases, etc.)

> documentation maintenance

> product updates

> maintenance spares and consumables

> routine testing and calibration

> system management and housekeeping

> handling of technical queries

> information security management

> security administration

> change management

> access for diagnostic purposes (e.g., remote login)

> ownership of off-line test facilities/tools/temporary licenses

> hardware repairs

> calibration

> software escrow

> database performance monitoring, database capacity monitoring (hard disk capacity), network (LAN and WAN) velocity, memory usage, etc. For further information, see Section 7 of this Guide.

- service performance targets (for in scope services):

  > response and resolution times

• Governance:

- roles (as appropriate) with contact details (as necessary):

  > Process Owner

  > System Owner

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

> client QA

> supplier QA/QM

> service access points (e.g., service desk/call management)

> SMEs (e.g., Engineering, IT, etc.)

> service users

> contract manager

> service manager

> third parties

- Tools:
  - service desk
  - asset management
  - maintenance management
  - backup and restore
- Documentation and Records:
  - types of documents and records required:
    > system documentation to be kept up to date:
      -- requirements and design specifications
      -- test specifications
      -- operating and maintenance manuals
    > audit trail of tasks executed to the system:
      -- service requests and reports
      -- fault reports
      -- maintenance schedules and records
      -- calibration schedules and records
      -- change control/configuration records
    > service manual
    > service performance metrics

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

> training records

> archiving of documentation

- Ownership and responsibility for:
  - configuration management
  - document distribution management
  - documents and records during service provision
  - documents and records following contract exit
  - format of documents and records (electronic /paper)
  - document templates
  - retention periods for service/support records
- Resources:
  - client and supplier resource requirements:
    > management and supervision (on-site and remote)
    > service delivery, including hours of operation
    > contract management
    > service management
    > quality and security
    > physical resources
    > IT Infrastructure
    > storage
    > offices
- Escalation and Complaints:
  - dispute, resolution and arbitration procedures
  - escalation procedures
  - complaints procedures
- SOPs and Training:
  - What SOPs are needed to manage/deliver the support services within the user and supplier organizations?

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

- How do SOPs interface?
- What training is required to manage/deliver the services within the user and supplier organizations and how often?

• Service Management and Service Performance Monitoring:

- review meetings
- report requirements
- service performance metrics
- service performance incentives and penalties
- audit requirements
- onsite management and supervision requirements
- remote access requirements
- service continuity requirements

6.8 Scalability

The level of definition in the SLA and the complexity of the governance model may be scaled according to the scope, complexity, and impact of the services provided. The scalability of each support service is described in the relevant process section.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

7 Performance Monitoring

7.1 Introduction

GAMP® 5 defines Performance Monitoring as "that part of overall preventive maintenance that obtains performance data that is useful in diagnosing system problems. It provides trends that may indicate performance problems, which can be used as part of CAPA to reduce application or system down time."

The purpose of monitoring performance is to enable the delivery of a consistent and timely service to system users; this aligns closely with ITIL®, which looks at Performance Monitoring as a sub-process of Performance Management in the context of the continuous improvement of Capacity Management (see Appendix 2).

Planning for Performance Monitoring may have commenced during the Project Phase (e.g., during specification and verification, which would incorporate the definition of critical process parameters).

This section is related to Appendix O3 of GAMP® 5(Reference 7, Appendix 4).

7.2 Scope

The scope of this guidance applies to business critical and GxP regulated automated systems.

7.3 Roles and Responsibilities

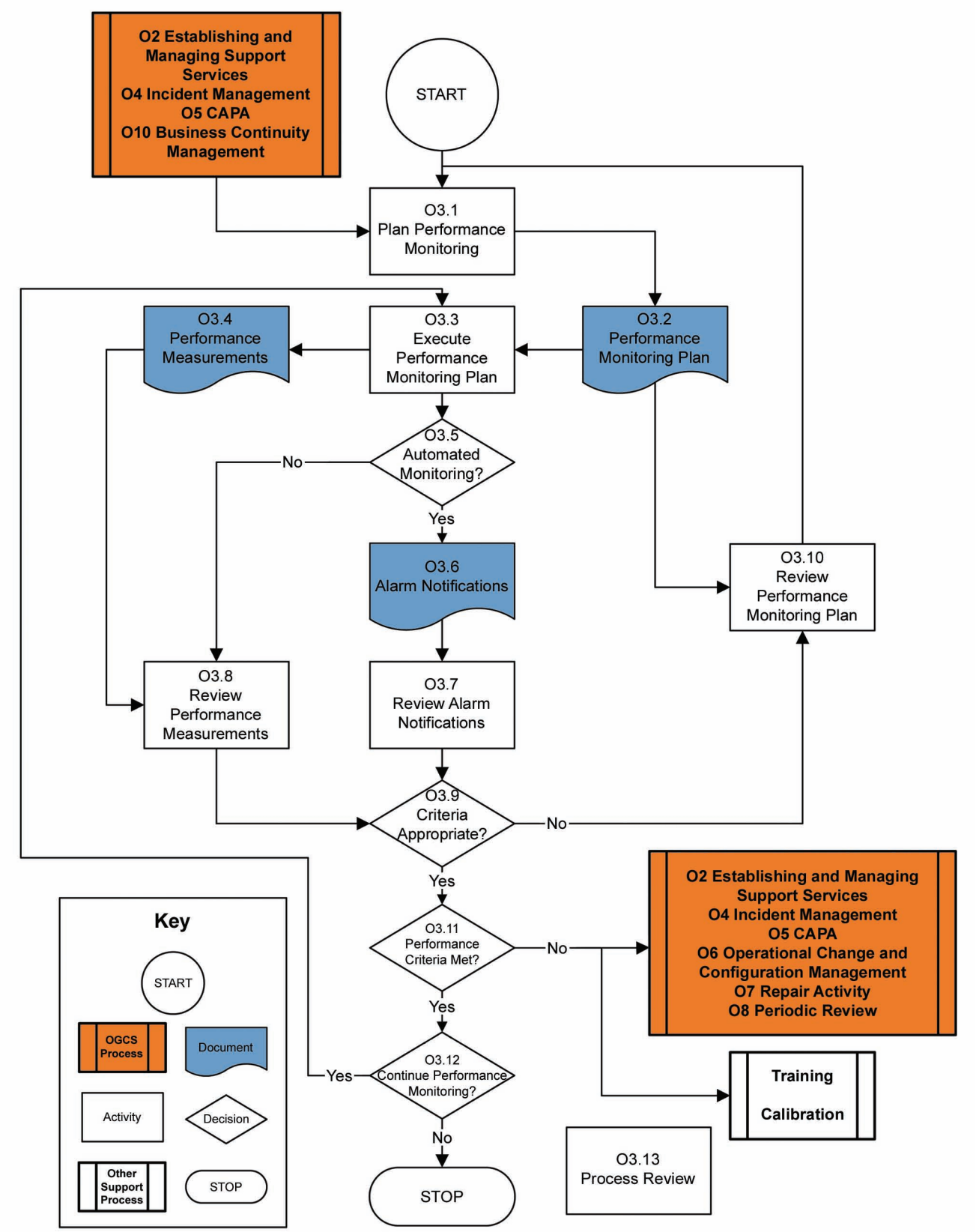
Table 7.1 provides an indicative example. Organizations should allocate roles and responsibilities based on organizational structure and the specific system.

Table 7.1: Roles and Responsibilities for Performance Monitoring

Role	RACI Role	Responsibilities
Process Owner	I	• informed of issues with the computerized system highlighted by the performance monitoring process
System Owner	A	• accountable for the application of the Performance Monitoring Process as applied to system(s) under their ownership • accountable for analysis of performance metrics • accountable for the reporting of performance issues
Platform Support (SME)	R	• responsible for collection of performance metrics • responsible for responding to alarm signals
Application Support (SME)	R	• responsible for collection of performance metrics • responsible for responding to alarm signals
System Administrator (SME)	R	• responsible for collection of performance metrics • responsible for responding to alarm signals
Supplier	C	• consulted when establishing performance metrics • informed about performance metrics results in order to drive supplier CAPA processes
Where R=Responsible, A=Accountable, C=Consult, I = Inform		See Appendix 1 for definitions.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

7.4 Performance Monitoring Process Flow Diagram



Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

7.5 Process Narrative

Process Step/Decision/Record	Description
O3 Performance Monitoring	**An operational process which is part of overall preventative maintenance that obtains performance data that is useful in diagnosing system problems.**
O2 Establishing and Managing Support Services **O4 Incident Management** **O5 CAPA** **O10 Business Continuity Management**	Operational processes which may trigger **O3 Performance Monitoring**.
O3.1 Plan Performance Monitoring	Determine and document how **O3 Performance Monitoring** is to be conducted, which performance metrics are to be monitored, and how the metrics are to be interpreted to provide indications of process performance over time. The system or process parameters selected for measurement should be decided by assessing the potential risk to patient safety, product quality, or data integrity if the component fails or exhibits deteriorating performance. Risks to data integrity (reliability and authenticity) and availability also should be considered in relation to product quality or patient safety. The output is the Monitoring Plan. The performance requirements should have been defined in the Requirements Specification and should differentiate between GxP and non-GxP metrics. Performance monitoring may be triggered by **O2 Establishing and Managing Support Services, O4 Incident Management, O5 Corrective and Preventive Action,** and **O10 Business Continuity Management**.
O3.2 Performance Monitoring Plan	The Monitoring Plan is the agreed mechanism by which performance metrics will be gathered and processed. Where real-time warnings of performance deviation are required, the Monitoring Plan may be automated. For manual systems, the Monitoring Plan will detail a schedule of process performance reviews. This may be a separate document or part of a broader plan.
O3.3 Execute Performance Monitoring Plan	Depending on whether the monitoring process is automated, execution of the plan will either initiate automatic collection of performance metrics or schedule reviews of Performance Measurements in order to gather required metrics.
O3.4 Performance Measurements	Records of measured parameters can occur in many formats, depending upon the nature and frequency of measurement. Records vary from system generated logs of measured values to manual records maintained in control logs or equipment logbooks. Data can be the original observations or derived.
O3.5 Automated Monitoring?	If monitoring is automated, alarms are automatically triggered by the monitored parameter deviating from preset limits. If monitoring is not automated, then parameters are monitored manually.
O3.6 Alarm Notifications	Automated alarm notifications can take many forms, e.g., audible or visual alarms, message on system console, emails, text alerts, printed lists, or logs of alarm conditions.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009

7.5 Process Narrative (continued)

Process Step/Decision/Record	Description
O3.7 Review Alarm Notifications	This activity reviews alarm notifications, i.e., all instances of deviations from preset limits. The purpose is to determine whether the alarm frequency is predictive of performance deterioration, and therefore, whether preset criteria are adequate for intended purpose based on practice.
O3.8 Review Performance Measurements	The purpose of the review is to summarize raw performance data to facilitate detection of trends in the data that may be useful in predicting process performance deterioration or process or service interruption.
O3.9 Criteria Appropriate?	Criteria should be sufficiently sensitive to process variability in order to be capable of providing an early warning of potential performance problems. Sensitivity should not be sufficiently high to yield a high level of false warnings.
O3.10 Review Performance Monitoring Plan	If the performance criteria are inadequate for purpose, e.g., insensitive to process or service deterioration or failure, the Performance Monitoring Plan should be reviewed in order to confirm purpose and suitability of performance metrics. The Performance and Monitoring Plan should be revised, as required.
O3.11 Performance Criteria Met?	If the performance metrics are fit for purpose and performance criteria are met, then the process or service is considered to be operating as intended. If the performance criteria are not met then depending upon then process affected external processes are triggered to manage a solution to resolve performance deterioration.
O2 Establishing and Managing Support Services **O4 Incident Management** **O5 CAPA** **O6 Operational Change and Configuration Management** **O7 Repair Activity** **O8 Periodic Review**	Operational processes that could be triggered by process step O3.11
Training **Calibration**	Other support processes that could be triggered by process step O3.11
O3.12 Continue Performance Monitoring?	Decision whether to continue with **O3 Performance Monitoring**. If no, the process stops. If **yes**, the process feeds back into step O3.3.
O3.13 Process Review	Reviews should be conducted to ensure that the process is operating as expected.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Operation of GxP Computerized Systems 2009