

GOOD PRACTICE GUIDE:

Global Information Systems Control and Compliance

Second Edition



GOOD PRACTICE GUIDE:

Global Information Systems Control and Compliance

Second Edition

Disclaimer:

This Guide is intended to provide a risk-based approach to implementing and supporting regulated global information systems. ISPE cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability

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

© Copyright ISPE 2017. All rights reserved.

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

All trademarks used are acknowledged.

ISBN 978-1-936379-92-7

Preface

This document, the *ISPE GAMP® Good Practice Guide: Global Information Systems Control and Compliance (Second Edition)*, is intended to be used in conjunction with *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems* and other ISPE GAMP® guidance documents. It considers major issues related to multi-site computerized systems, and provides guidance on effective and efficient control and compliance of globally deployed IT systems throughout their life cycle.

This Second Edition is aligned with the Quality Risk Management and life cycle approaches defined in *ISPE GAMP® 5*. It reflects the move away from client-server application architecture, which was prevalent at the time of publication of the First Edition. This edition also covers Software as a Service (SaaS) and other cloud solutions, which can be economical options for global systems.

Acknowledgements

The Guide was produced by a Task Team led by Arthur (Randy) Perez (Novartis (retired)). The work was supported by the ISPE GAMP Community of Practice (COP).

Core Team

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

Winnie Cappucci	Bayer Healthcare (retired)	USA
Colin Jones	Conformity Limited	United Kingdom
Randy Perez	Novartis (retired)	USA

Other Contributors

The Team wish to thank the following individuals for their significant contribution to the document.

Chris Clark	TenTenTen Consulting	United Kingdom
Gail Evans	Technical Writer/Editor	United Kingdom
Christopher White	Alexion Pharmaceuticals	USA
Sion Wyn	Conformity Limited	United Kingdom

Subject Matter Expert Input and Review

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

Lorrie Vuolo-Schuessler	GlaxoSmithKline	USA
David Stokes	Convalido Consulting Limited	United Kingdom

Special thanks also goes to Lynda Goldbach, ISPE Guidance Documents Manager, for the layout and design of this Guide.

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

Company affiliations are as of the final draft of the Guide



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

www.ISPE.org

AVA **Documents**
Document Sharing Hub

Table of Contents

1	Introduction	7
1.1	Background	7
1.2	Purpose.....	8
1.3	Scope.....	9
1.4	Structure of this Guide	10
2	Specific Challenges of Global Information Systems.....	11
3	Application of <i>ISPE GAMP® 5</i> to Global Information Systems.....	19
3.1	Product and Process Understanding	19
3.2	Ownership and Other Key Roles	19
3.3	Life Cycle Approach within a Quality Management System.....	20
3.4	Science-Based Quality Risk Management.....	20
4	Global Information Systems Life Cycle.....	23
4.1	Concept.....	24
4.2	Project Phase.....	31
4.3	Operation	38
4.4	Retirement	50
5	Appendix 1 – Project Phase Activities.....	53
5.1	Define Global Business Processes.....	54
5.2	Establish System Ownership	55
5.3	Establish Project Organization.....	57
5.4	Pilot Projects	60
5.5	System Architecture	60
5.6	Validation Planning	62
5.7	User Requirements Specification.....	69
5.8	System Specification and Design Review.....	70
5.9	Traceability Management.....	70
5.10	Environments	72
5.11	Testing.....	73
5.12	Validation Reporting.....	75
6	Appendix 2 – Operation Phase System Management Processes	77
6.1	Operational Change Management.....	77
6.2	Configuration Management.....	84
6.3	Incident Management	86
6.4	Service Desk.....	86
6.5	System Security	87
6.6	Performance and Capacity Planning	88
6.7	Performance Monitoring.....	88
6.8	Backup and Recovery of Software and Data	88
6.9	Record Retention, Archive, and Retrieval	89
6.10	Business Continuity and Disaster Recovery	90
6.11	Periodic Review	91

7	Appendix 3 – Architecture Design Considerations	93
7.1	Centralized System.....	93
7.2	Distributed System.....	94
7.3	Software as a Service.....	95
7.4	Risk Management Considerations Driven by Architecture Choices.....	96
8	Appendix 4 – Application Architecture Effects on Validation Strategy	99
8.1	Potential Validation Strategies	100
8.2	Application Architecture and Test Strategy	101
9	Appendix 5 – Example Case Studies.....	105
9.1	Global MES Implementation	105
9.2	Global ERP Implementation.....	108
9.3	Global Chromatography Data and Control System.....	112
9.4	Global Drug Safety System Implementation	116
9.5	Global Electronic Document Management System	118
9.6	Global Clinical Data System	121
10	Appendix 6 – Quality Risk Management Approach.....	123
11	Appendix 7 – Global Project Management Considerations	127
11.1	Cultural.....	128
11.2	Funding.....	133
12	Appendix 8 – Supplier Management and Good Practice	135
12.1	Supplier Good Practice – Development and Support	135
12.2	Supplier Quality Management System.....	137
12.3	Supplier Quality Planning.....	138
12.4	Sub-Supplier Assessments	138
12.5	SaaS Supplier Evaluation Considerations	139
13	Appendix 9 – Data and Record Management Life Cycle.....	141
13.1	Data Management Planning	142
13.2	Business Process Requirements	142
13.3	Life Cycle Considerations	144
13.4	Data Quality	145
13.5	Data Migration.....	146
13.6	Record Management	147
13.7	Data Destruction	148
14	Appendix 10 – Converting a Local System into a Global System	149
14.1	History.....	149
14.2	Business Process	149
14.3	Supporting Documentation	149
14.4	System Design and Technical Architecture.....	150
14.5	System Support	151
15	Appendix 11 – References.....	153
16	Appendix 12 – Glossary	155
16.1	Acronyms and Abbreviations	155
16.2	Definitions	156

1 Introduction

1.1 Background

Since the publication of the first edition of this Guide in 2005 there has been a continuing trend towards factors that complicate the landscape. Among the most significant are:

- Globalization in the life-science industries. This includes consolidation through mergers, outsourcing, and a trend toward fewer manufacturers making specific products, intermediates, and raw materials.
- The use of cloud technologies
- Expansion of applications to cover many areas that used to be managed by dedicated systems, e.g., Enterprise Resource Planning (ERP) systems that include a Laboratory Information Management System (LIMS) module

As organizations find themselves operating from multiple sites worldwide, with groups and departments split between multiple locations in a country, or even using third party distributors, the challenges of information sharing become more complex. There are many competitive advantages to efficient and effective information sharing. Research and development activities often cross international boundaries. Integrated activities can be achieved only with excellent communication between everyone involved, and this means that the ability to share electronic information effectively is a primary concern.

With escalating drug development costs, time to market is a significant factor in recouping investment, and ineffective information sharing can become a major cost factor if it slows down approval to market.

There are many ways to share information. An interface between applications can be a major requirement for different systems that facilitate integrated business processes. For processes that are conducted at multiple sites, however, there are clearly advantages to all participants using the same suite of software systems.

The implementation of multi-site computer systems can be difficult. Regulatory compliance creates an additional challenge for regulated systems such as a clinical database or an ERP system. This Guide considers major issues that confront organizations implementing and operating a regulated multi-site computerized system.

1.1.1 Drivers

The technical and regulatory landscape has also changed since the publication of the first edition of this Guide. In addition to the issues noted above, important factors include:

- The move away from client-server application architecture, upon which the first edition was based, but which is far less common today
- The substantial improvements in the power of applications
- The growth of outsourced services
- Beyond the simple use of cloud-based infrastructure, web-based Software as a Service (SaaS) can be a cost-effective option for global information systems
- The revision of EU GMP Annex 11 [1] and EU GMP Chapter 4 [2] (both adopted for wider use by PIC/S [3])
- The Quality Risk Management and Specification and Verification approach, such as that defined in *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems* [4]

- Increased regulatory focus on the wider aspects of data integrity

This update will address current state-of-the-art thinking with the above factors taken into account. It will help the healthcare and life sciences industry understand viable approaches to using new technology, e.g., cloud computing, in a manner that will facilitate global use of applications while at the same time meeting compliance expectations of international regulators.

1.2 Purpose

This Guide aims to assist in the following aspects of widely used, regulated global information systems:

- Development
- Implementation
- Validation
- Management
- Maintenance

It is intended to provide an understanding of the issues faced by teams that are tasked with completing a global deployment. In particular, this Guide aims to provide some insight into addressing issues of control and regulatory compliance efficiently and effectively. The Guide provides:

1. A consistent document that guides stakeholders to take advantage of current good practices in the field to achieve compliance with applicable regulations
2. Guidance on good practice for unique aspects of computerized systems implemented on a global basis

This Guide is intended to be used in conjunction with *ISPE GAMP® 5* [4] and other ISPE GAMP® guidance documents [5]. References are provided to supporting information available in other ISPE GAMP® guidance documents [5]. Where additional information is not available in *ISPE GAMP® 5* [4], this Guide provides more specific detail.

The intended audience for this guidance covers both corporate and local groups within an organization, and includes:

- Project Management
- Business Process Owners
- Suppliers
- Validation Team
- Quality Assurance
- IT System Owners and application support teams

Particular benefits of taking a global perspective for a global system implementation include:

- Achieving maximum collaboration in central and distributed validation effort
- Effective focus on objectives and deliverables throughout the entire life cycle

- Minimal overlap in documentation
- Efficient handling of audits, inspections, and assessments

A basic understanding and knowledge of the principles and framework of *ISPE GAMP® 5* [4] is considered helpful to the use of this Guide.

1.3 Scope

For the purpose of this Guide, a global information system is defined as any computer system that is used at multiple sites within an organization. These sites can be very close together or in different countries.

This Guide addresses compliance with relevant international regulations and guidelines for global information systems. It covers:

- New systems and expanded use of existing ones
- Existing validated systems
- Systems that are being implemented by extending the scope of an existing local system

A wide range of healthcare and life sciences requirements related to computerized system control and compliance have been taken into account, including:

- Good Manufacturing Practice (GMP)
- Good Clinical Practice (GCP)
- Good Laboratory Practice (GLP)
- Good Distribution Practice (GDP)
- Good Pharmacovigilance Practice (GVP, also known as GPvP)

The following regulations and guidelines have been specifically considered in drawing up this document:

- US Federal Food and Drug Administration (FDA) regulations and Compliance Policy Guides [6]
- Relevant sections of EU GMPs, e.g., Annexes 11, 15, and 18 [7]
- PIC/S Guidance [3]
- Health Canada GMP regulations [8]
- ICH Guidelines [9]

The Guide covers systems that are to be used in more than one site, state/province, or country.

While not within the scope of this document, it is recognized that aspects such as business criticality, health and safety, and environmental requirements may also require specific assessment and control.

1.4 Structure of this Guide

The Guide has been structured to meet the needs of various readers, and contains increasing level of detail through the main body of the Guide and into the appendices.

Section 2 and Section 3:

- Provide an overview of challenges specific to global information systems, along with a high level overview of how to address them.
- Along with Appendix 8, these sections also provide information relevant to suppliers of global information systems.

Section 4 and Section 5:

- Provide further information on how to apply the *ISPE GAMP*® 5 [4] life cycle and Quality Risk Management (QRM) approach to global information systems.

Appendices:

- Appendices are based on specific areas of interest and responsibility and provide more detailed “how to” guidance for developing and supporting global information systems
- The example case studies reflect a wide variety of typical global information systems and are intended to be useful when applying the guidance provided to specific situations.

2 Specific Challenges of Global Information Systems

This section addresses the different and specific aspects of global information systems that require specific consideration and action. The following table does not provide a full analysis of the issues. Table 2.1 refers to other sections within this Guide that provide more comprehensive discussion and guidance on these topics.

Table 2.1: Challenges Related to Management of Global Information Systems Development and Operation

Topic	Particular Considerations for Global Information Systems	For Further Information, see
Project Team (global)	There may be sensitivity to having to adopt a standard in which an organization has not been given any opportunity to provide input. This may be especially true when local, unique software is being replaced. An effort should be made to demonstrate that the global project team is composed of personnel from several sites (not just headquarters) who can understand local processes and requirements.	Appendix 1, Section 5.3
Project Team (local)	<p>The need for a local project team will vary depending on the architecture of the global information systems solution, but it can be helpful to have a local project team which is familiar with local business processes. The local project team should have authority to alter local business processes, if necessary, based on business or regulatory drivers.</p> <p>If the global information system has been piloted at another site, the local project team will need to lead the implementation applying the lessons from the pilot and any intervening installations.</p> <p>A local project team can also be helpful supporting training and rollout.</p>	Appendix 1, Section 5.3
Project Team (project manager)	<p>Project managers should have the ability to understand and deal with a variety of local cultural issues. These issues can be linked to national or regional customs, and the Project Manager needs to be sensitive to these differences.</p> <p>There can also be significant cultural differences between sites within the same country. For example, a manufacturing site may have a different culture from corporate headquarters.</p> <p>A site may be asked to adopt a standardized practice as part of adopting a global solution and there may be resistance to this, if there is a perception that the standardized practice is different. Project managers should be able to identify where there is an actual difference that needs to be addressed.</p>	Appendix 1, Section 5.3.4

Table 2.1: Challenges Related to Management of Global Information Systems Development and Operation
(continued)

Topic	Particular Considerations for Global Information Systems	For Further Information, see
Project Steering Committee	<p>A global project Steering Committee should understand the business process and have authority to make decisions and to drive those decisions to completion.</p> <p>The Steering Committee should include both executives and personnel who understand the affected business processes. Other persons who should be on the Steering Committee include:</p> <ul style="list-style-type: none"> • The future global information System Owner (they may be a good candidate to chair this committee) • The business process owner for the pilot site • Quality Assurance (QA) <p>After the pilot, there may be a benefit to retaining the System Owner from the pilot. The System Owner should be involved in ongoing subsequent implementations, as an ad hoc member of the Steering Committee while the project is ongoing.</p> <p>Following the pilot, there should be local Steering Committees for implementations. This team should be structured along the same lines as the global team, and should include:</p> <ul style="list-style-type: none"> • The local Process Owner • The System Owner • QA • A representative from a Center of Excellence (CoE) • A local Subject Matter Expert (SME) (if possible) <p>Local project teams should provide regular reports that are reviewed by the global project team.</p>	Appendix 1, Section 5.3.2
Project Management and Training	When implementing a global solution various local and global teams need to have a common understanding so that actions taken produce consistent results that meet all expectations. They should be trained in the implementation methodology.	Appendix 1, Section 5.3.5
Project Communication	<p>Global and local project teams should work from a common glossary, which may need extra emphasis if cultural differences are an issue. Global teams should stay up-to-date with the work occurring locally, so that deviations are recognized and adjustments made, if necessary.</p> <p>Communication can help to gain buy-in from various sites. It can help to prepare staff for change. Seeking feedback from staff can help to make them feel that they are contributing to the project.</p>	Appendix 7, Section 11.1.1.5 Appendix 7, 11.1.2.1
Project Change Management	<p>Changes made to global information systems during the project phase can result in implementations at different sites that result in differences between those implementations. This could result in the inability to share information. Major changes should be brought to the attention of the Steering Committee. Changes that are considered necessary at a local level should be vetted at the global level to see if they have a global effect. If there is a global effect, the global project team should decide whether to:</p> <ul style="list-style-type: none"> • Accept the local change and propagate it to other sites • Accept the difference at the one site • Tell the local project team that the change is unacceptable <p>Local changes may be proposed to globally defined business processes during the project, and these should be vetted before being accepted.</p>	Appendix 1, Section 5.6.5.1

Table 2.1: Challenges Related to Management of Global Information Systems Development and Operation
(continued)

Topic	Particular Considerations for Global Information Systems	For Further Information, see
Business Process	<p>Business processes that have been local may have to be adapted to meet a globally defined standard. Departments may be required to adopt new ways of working that are compatible with the new system.</p> <p>This may become more complicated if different local processes have generated a variety of data in different systems that need to be migrated to the new common global information system.</p>	Appendix 1, Section 5.1
System Ownership	<p>System ownership is a concept that has evolved since the first edition of this Guide. What was termed "System Owner" is now termed the "Business Process Owner" to ensure clarity of the responsibilities of the owner. The responsibilities of the Business Process Owner should be clear and placed appropriately within the business, i.e., not IT (unless the business process belongs to IT).</p> <p>There may need to be two separate Business Process owners:</p> <ol style="list-style-type: none"> 1. Local Business Process Owners who are responsible for the business process and the data 2. A global Business Process Owner who has overall accountability <p>The global Business Process Owner should have sufficient authority to ensure that cross-organizational decisions are consistent.</p>	<p>Section 3.2</p> <p>Appendix 1, Section 5.2</p>
User Requirements	<p>Unique local processes maybe justified. Reasons for this could include, e.g.:</p> <ul style="list-style-type: none"> • Local laws • The requirements for special handling provisions for a product produced at a site <p>This should be captured when collecting user requirements. Failure to make this adjustment could put the project at risk.</p> <p>Collaboration between local and global project teams can be a strong contributor to assurance of good user requirement specifications.</p>	Appendix 1, Section 5.7
System Architecture	<p>The choice of system architecture can either simplify or complicate global projects and operational support. Infrastructure as a Service (IaaS), Platform as a service (PaaS), or SaaS approaches delegate varying degrees of responsibility to suppliers. They also limit the degree of control that a regulated company has relating to changes. It may also limit the ability for sites with unique needs to modify a global information system to their situation.</p> <p>System architecture can also have an effect on operational needs such as backup and recovery, business continuity, or down time for service or upgrade.</p>	<p>Section 4.1.3</p> <p>Appendix 1, Section 5.5</p>
Interfaces	<p>Interfaces, (input and output), are a source of vulnerability for data integrity.</p>	<p>Appendix 1, Section 5.7</p> <p>Appendix 1, 5.11</p> <p>Appendix 5</p>
Software Selection	<p>Selecting a software supplier for a system that is to be deployed around the globe requires attention to specific issues, e.g.:</p> <ul style="list-style-type: none"> • Does the supplier have the ability to support all locations? • Is the software available in local languages? <p>These and other questions should be addressed as part of the selection process.</p>	Appendix 1, Section 5.6.4

Table 2.1: Challenges Related to Management of Global Information Systems Development and Operation
(continued)

Topic	Particular Considerations for Global Information Systems	For Further Information, see
Validation Planning	<p>Validation planning for a global information system is more complex than for local system. Issues that require consideration include:</p> <ul style="list-style-type: none"> • Implications of the architecture choice • What can be done centrally versus what needs to be done locally • Piloting the application • Phased global implementation • Documentation management 	Appendix 1, Section 5.6
Legal and Regulatory	<p>Applicable laws and regulations for delivering a compliant solution should be understood. A global information system will need to comply with all rules.</p> <p>Conflict between GxP requirements and other national laws is a possibility. For example, a privacy law requiring deletion of all personal data when an employee leaves a firm may conflict with a GxP expectation to retain a training record. Such conflicts should be resolved by Legal and QA authorities and the decision documented. There should be a shared interpretation of global regulations.</p>	Appendix 1, Section 5.6.1
Supplier Assessment and Management	<p>Suppliers should be assessed, e.g., suppliers of:</p> <ul style="list-style-type: none"> • Software suppliers • Integrators • Developers • Managed services • PaaS suppliers • SaaS suppliers <p>Suppliers should be evaluated for their capability to provide support globally. If development activities involve access to data, privacy issues may become significant.</p>	Appendix 1, Section 5.6.4
Testing	<p>Testing should be planned to allow centralized execution, where possible.</p> <p>Some level of local testing may be needed. Tests that need to be executed locally, may be designed, written, and approved at a global level. This can reduce the resources needed.</p> <p>If no local testing is intended, there should be a review of global testing by locally responsible individuals.</p> <p>The use of a test tool can be beneficial. A test tool can:</p> <ul style="list-style-type: none"> • Make local testing easier • Assure that everyone has access to the tests and results • Facilitate offshore testing <p>Test records should be available to support audits or inspections at all sites where needed.</p>	Appendix 1, Section 5.11

Table 2.1: Challenges Related to Management of Global Information Systems Development and Operation
(continued)

Topic	Particular Considerations for Global Information Systems	For Further Information, see
Data Management Planning	<p>Data management issues may vary, ranging from privacy protection to retention requirements, depending upon the nature of the global information system.</p> <p>Conflicts may arise between different jurisdictions, e.g., for data retention requirements. One approach is to plan to retain all records for the length of time required by the most restrictive laws or regulations. However, this may be problematic, because while country A may require a record to be kept for forty years, country B may require that it is deleted when the employee leaves the company. The legal department should be involved in discussion of such issues. If it is a GxP record, QA should also be involved in the discussion.</p> <p>Potential conflicts need to be recognized during requirements gathering. Business rules for managing the data should be designed. Data standardization should be implemented where possible.</p>	<p>Section 4.1.4</p> <p>Section 4.2.3</p>
Pilot Projects	<p>Pilot projects may be helpful for global information systems. For projects like ERP, it may be possible to run simultaneous pilots, e.g., manufacturing support at one site and finance at another.</p> <p>Pilot projects should be well documented, as the global project team are not usually at every site throughout the implementation.</p>	<p>Appendix 1, Section 5.4</p>
Support (Centers of Excellence (CoE))	<p>For a global information system with implementations in multiple sites around the world, centralized support with fulltime dedicated staff is recommended. The CoE concept is an approach that can provide help to users for both IT and business support problems in a way that accounts for the needs of all sites. This might include support in multiple languages.</p>	<p>Section 4.2.4.1</p> <p>Section 4.3.2</p>
Support (“follow the sun”)	<p>A support model that provides acceptable service to all sites may require “follow the sun” access to SMEs and technicians, i.e., support tasks may be passed around daily between work sites that are several times zones apart.</p> <p>This should be considered for support provided both by the CoE and by the supplier.</p>	<p>Section 4.3.4</p>
Support (down time)	<p>Consideration should be given to when a support performs maintenance and upgrades. These usually need system down time at night. This may not be acceptable for global information systems, because one site’s night is another site’s prime business hours.</p>	<p>Section 4.3.4</p>
Configuration Management	<p>Effective Configuration Management should be applied to global information systems to help to maintain communication and data sharing between sites. This should be a specific consideration for older architectures like client-server or for scenarios where a site has a slightly different configuration.</p>	<p>Appendix 2, Section 6.2</p>
Change Management	<p>Change Management needs to be coordinated between sites, and should have central oversight by a CoE or similar group. Change Advisory Boards need to understand local and global impacts when evaluating proposed changes. For global SaaS applications, changes need to be evaluated and approved quickly, so that they can be executed locally in time to meet the suppliers release schedule.</p> <p>Companies may have separate processes for managing business and IT changes. If so, a link needs to be established to minimize unintended consequences.</p>	<p>Appendix 2, Section 6.1</p>

Table 2.1: Challenges Related to Management of Global Information Systems Development and Operation
(continued)

Topic	Particular Considerations for Global Information Systems	For Further Information, see
Incident Management	<p>Incident management can benefit from centralized management by a CoE. Second level support (i.e., support requests that cannot be handled by the service desk) at the CoE is in position to recognize whether incidents are local in nature or global, and can initiate global changes if required to remediate a problem.</p> <p>A “follow the sun” approach can be used for managing incidents for global information systems, in order to ensure that issues are handled in a timely manner regardless of user location.</p>	Appendix 2, Section 6.3
Security Management	<p>Security policy can be managed globally and security groups can be developed at a global level. Access granting and revocation, along with periodic review of access, should be handled at a local level.</p> <p>Access to various data groups may need to be restricted to comply with privacy laws. A company may decide that intellectual property in specific locations may inadequately protected under local laws. Encryption may help solve such issues. These issues could affect where data can be stored and where system administrators can be based. GxP data integrity expectations may need similar measures.</p> <p>Small sites may have problems complying with expectations of the segregation of duties. The segregation of key security and system administration roles should be maintained.</p>	Appendix 2, Section 6.5
Backup and Recovery	<p>For a global information system, a mechanism to facilitate backup that also allows access to the database in other time zones should be implemented.</p> <p>A request to restore the database to a prior state needs to consider potential impact to the rest of the organization.</p>	Appendix 2, Section 6.8
Disaster Recovery and Business Continuity	The architecture of global information systems can make managing Disaster Recovery (DR) and Business Continuity Planning easier, because users can default to another instance if a local instance fails. However, there needs to be sufficient capacity on the other server so that its performance is not affected.	Appendix 2, Section 6.10
Data Management (synchronization)	<p>The global information systems and data may be on multiple servers to distribute processing load and to facilitate business continuity. Synchronization of these servers should be performed in real time. Business rules should be developed around:</p> <ul style="list-style-type: none"> • When and how often synchronization occurs • The rights of users who do not normally use the global information system on synchronized servers 	Appendix 9, Section 13.2
Data Management (time stamps)	The assignment of time of creation, editing, or deletion of records in a global information system should be managed. An agreed format for date and time stamps should be addressed.	Appendix 9, Section 13.3
Data Management (ownership)	Decisions regarding data destruction need to comply with local laws. Appropriate ownership of the data should be determined, especially if the Data Owner bears responsibility for data destruction decisions.	Appendix 9, Section 13.2
Data Management (access)	It may be illegal for personal information of some countries to be accessible in other countries. In some cases, this may be overcome using approved processes.	Appendix 9, Section 13.2

Table 2.1: Challenges Related to Management of Global Information Systems Development and Operation
(continued)

Topic	Particular Considerations for Global Information Systems	For Further Information, see
Data Management (storage)	Data should be stored in regions that are considered to have adequate protection for personal data or intellectual property, especially if data is unencrypted.	Appendix 9, Section 13.2
Data Management (destruction)	Data destruction needs to account for all local laws and for all locations that reference that data. Retention requirements may differ by jurisdiction, or there may be a litigation hold on some data in some countries. On rare occasions there may be conflict between applicable laws.	Appendix 9, Section 13.7
Data Management (regulatory and legal compliance)	Many of the aspects of global data management require an understanding of multiple jurisdictions. In general, QA departments are familiar with rules for one or two jurisdictions (often local and FDA regulations); legal departments are usually locally focused, and are extremely reluctant to make decisions related to other jurisdictions. This places significant responsibility on the Data Owner and the project teams to ensure that they understand the aggregate requirements related to records maintained in a global information system.	Section 4.1.4
System Retirement	With global information systems, the decision to retire an application should not compromise the ability of other sites to operate. For example, support elements need to remain in place until the last site retires the application.	Section 4.4
Merger and Acquisitions Considerations	Integrating information from a merger partner, or segregating and migrating data to another company, to whom a business entity was sold, should be carefully managed.	Section 4.1.4
Record Life Cycle	Record life cycle phases may be different based on regional considerations: <ul style="list-style-type: none"> • Record creation – occurs at multiple locations • Active records – some records may be active at only one site • Semi-active records – records that are kept on-line or near-line but are not frequently used. These may be retained in such states to support audit or inspection (not all companies define a semi-active status). • Inactive records – typically in archive and almost never referenced. These are usually retained in order to meet company and/or legal/regulatory retention requirements. • Destruction – should not occur without verification that the record is not in a hold status to support litigation. When a record is destroyed, distributed copies should also be destroyed. 	Appendix 9

3 Application of *ISPE GAMP® 5* to Global Information Systems

The approach described in this Guide is based on *ISPE GAMP® 5* [4].

3.1 Product and Process Understanding

In order to determine global information systems requirements, the intended use and intended user-base, and the global business processes to be supported should be understood. Existing business processes may need revision in order to gain most benefit (see Appendix 1, Section 5.1). Process understanding is also the basis for QRM. Where such processes are defined globally, proposed changes to any aspects, including ones which are entirely local, should be evaluated for their effect on both the overall global business process and on the validation approach.

3.2 Ownership and Other Key Roles

System ownership and several other key roles should be handled differently for global information systems. This reflects the fact that decision making processes need to occur at two levels, or three levels for SaaS solutions. Table 3.1 summarizes this. This table is not comprehensive. It focuses on roles that merit consideration for global information systems.

Table 3.1: Important Roles in the Development and Management of Global Information Systems

Role	Description and Discussion
Application Support Manager	This is the IT role responsible for system management, i.e., configuration management, change management, backup and archive management, etc. This should not be confused with the business process ownership role.
Business Process Owner (global)	This is the individual within the business community who is responsible for the overall business use of the system. Care should be exercised in naming this person, as there are some actions required. It is probably not advisable to appoint top leadership to this role. Similarly, the global business owner does not always have to be in corporate headquarters; it could be assigned to a local owner (see below) at one of the larger user sites.
Business Process Owner (local)	This is a site-level position, parallel to the global owner. This person is responsible for all ownership activities that do not impact other sites. This role is not mandatory, although it is advisable to have a local owner for distributed systems or for any system where there are locally unique aspects of the business process that are managed through the system.
Center of Excellence	This is a group of SMEs that provide IT and business support to the business community. It may include both global team and core team members, along with other ad hoc SMEs. They are generally the primary interface with the supplier of the computer system. They generally provide second level support working with the help desk. The Application Support Manager is frequently a member of the CoE.

Table 3.1: Important Roles in the Development and Management of Global Information Systems (continued)

Role	Description and Discussion
Quality Assurance	<p>Administrators have elevated privileges within the application. Different types of administrators should have different privileges. For example, a Business Administrator whose role is to enable role-based system access for users should not have the ability to manipulate the data at a database table level. Conversely, a Database Administrator (DBA) should not be able to alter business roles of users within the application.</p> <p>In general, administrative privileges should be controlled, and the number of people in administrative roles should be kept to the minimum necessary to support the smooth conduct of business. Administrative privileges for outsourced systems may be more difficult to control, as suppliers may want to allow a wider distribution of privileges in order to maximize the flexibility of their staff. This can increase the risk to data integrity and, if possible, suppliers should be asked to minimize the number of system administrators.</p>

Note: This table is not comprehensive. It focuses on roles that merit consideration for global information systems.

3.3 Life Cycle Approach within a Quality Management System

The life cycle should define the necessary activities to manage the development and support of global information systems in a systematic way from conception to retirement (see Section 4).

Life cycle activities should be scaled according to:

- Impact on product quality, patient safety, and data integrity
- Complexity and novelty of the system
- Assessment of any suppliers

For further information, see Appendix 1, Section 5.6.

3.4 Science-Based Quality Risk Management

QRM is a systematic process for the assessment, control, communication, and review of risks. Application of QRM enables effort to be focused on critical aspects of a Global Information System.

This document provides a QRM approach in Appendix 6, based on that described in *ISPE GAMP® 5* [4]. The approach is intended to be applicable to any Global Information System with a potential impact on patient safety.

The QRM approach is intended for use throughout the life cycle from concept to retirement. Aspects of risk management applicable to each life cycle phase are described in Section 4.

3.4.1 Sources of Risk Specific to Global Systems

While Global Information Systems share many of the same risks that are common to any software system, there are additional potential sources of risk, because of the typical scope and complexity of such systems. These can include:

- Varying legal requirements
- Multiple user languages and cultures
- Business process variants
- Synchronization of data
- Complex support structures

3.4.2 Leveraging Supplier Involvement

Regulated companies should try to leverage supplier knowledge, experience, and documentation throughout the life cycle, subject to satisfactory supplier assessment.

For example, suppliers may assist with:

- Requirements gathering
- Risk assessments
- The creation of functional and other specifications
- System configuration
- Testing
- Support
- Maintenance

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

Some suppliers offer “validation packages” which may include supplier managed testing. The final responsibility for all aspects of validation and testing rests with the regulated company, regardless of how much supplier help they may choose to use.

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

Supplier assessment is described in Appendix 1, Section 5.6.4.

4 Global Information Systems Life Cycle

Compliance with regulatory requirements and fitness for intended use may be supported by adopting a life cycle approach following good practice, such as that as defined in *ISPE GAMP® 5* [4].

The life cycle should define the necessary activities to manage the development and support of global information systems in a systematic way, from conception to retirement. The life cycle of data captured or generated and maintained should also be considered.

The system life cycle described in this Guide for a regulated company is for global information systems. This is different from a defined approach or method for software development, which is typically the responsibility of the supplier.

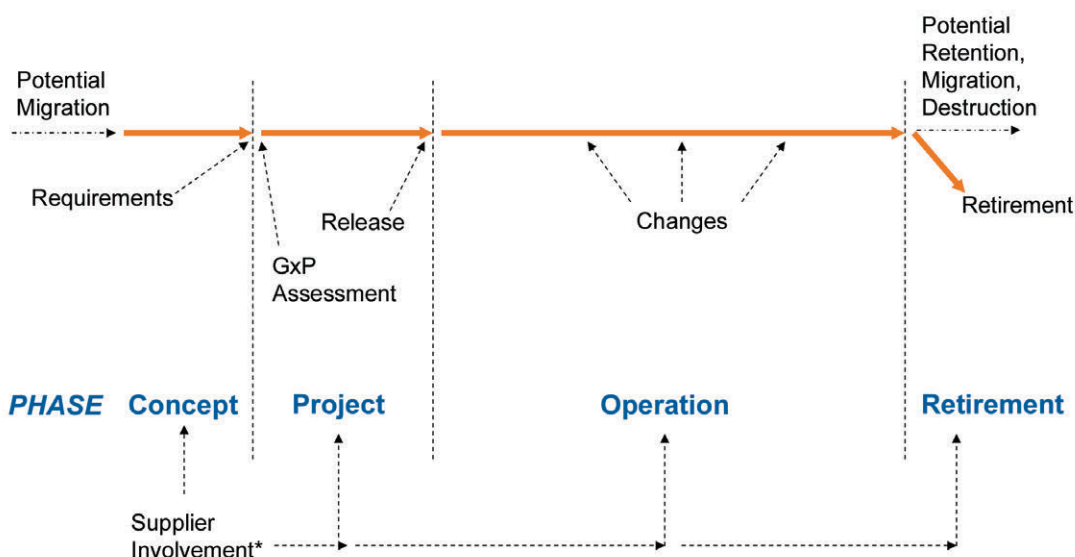
Good practices for suppliers of global information systems are described in Appendix 8. Supplier activities support regulated company activities.

This Guide uses diagrams to represent the life cycle. These diagrams may present relationships in a linear representation, but this is not mandating a waterfall approach. This is not intended to constrain the choice of development methods and models. Suppliers should use the most appropriate methods and models, which may include iterative approaches like piloting or prototyping.

Figure 4.1 shows the system life cycle as described in *ISPE GAMP® 5* [4], consisting of four major phases:

1. Concept
2. Project
3. Operation
4. Retirement

Figure 4.1: Life Cycle Phases



- * - This could be a complex supply chain.
- Supplier may provide knowledge, experience, documentation, and services throughout lifecycle.

During the **Concept** phase:

- An initial risk assessment is performed
- Initial quality planning is performed
- Initial requirements are defined

The **Project** phase involves further planning, supplier assessment, and selection (where the system is not being developed internally by the regulated company), various levels of functional and design specification, coding, and verification leading to acceptance and release for operation.

Operation is typically the longest phase and can present a significant risk. Data security and integrity, maintaining fitness for intended use, and compliance of the system are key aspects. Changes of different impact, scope, and complexity should be managed during this phase. System failures should be appropriately managed.

The final phase is **Retirement** of the system. This phase involves decisions about data retention, migration or destruction, and the management and enforcement of these processes.

4.1 Concept

4.1.1 Key Concept Phase Activities

The Concept phase covers the initial activities leading to initiating and justifying project commencement. These activities will depend on individual company approaches, but should cover:

- Business objectives
- Business case
- Business and cost benefits
- Overall budget
- Organization (roles and responsibilities)
- Resourcing
- Scope and rationale
- Key requirements

The information is used to gain senior management commitment to proceed with the project and to provide adequate resources.

4.1.2 Planning for the Project

During the Concept phase a documented initial risk assessment should be performed. The appropriate SMEs should perform the assessment, in conjunction with the regulated company quality assurance and/or regulatory affairs representatives.

The risk assessment should evaluate whether any GxP processes are supported by the global information system and determine the relevant risk level. Applicable guidance and regulations should be consulted for all jurisdictions where the global information system is to be used. A comprehensive list of possible regulatory considerations and guidance is provided in Appendix 1, Section 5.6.

Key factors for the successful delivery of the proposed global information system should be identified and understood as early as possible. These include:

- Possible cultural and language differences that will require careful management throughout the Project phase and into Operation
- Successfully developing global business processes
- Understanding and implementing the appropriate technical architecture (see Section 4.1.3)
- Network and hardware capacity
- Establishing an effective project organization
- Identifying business process, system, and data ownership
- Use of pilot projects and lead implementation sites
- Data management planning (see Section 4.1.4 and Appendix 9)

These topics should be considered during the Concept phase and developed further during the Project phase. These topics are covered in more detail in Appendix 1.

4.1.3 System Architecture

Factors to consider for the system architecture of a global information system include:

- Design
- Administration
- Environments
- Security
- Performance (including speed, capacity, availability, and reliability)

These aspects are addressed in this Guide within the phase of the system life cycle most affected. The impact of architecture decisions taken in the Concept phase on the global information system solution should be understood.

Architecture decisions are at the core of the automation solution and should, therefore, be made early in the implementation process, typically following business process definition and requirements gathering.

The selection of the type of system architecture should be made early in the Concept phase:

1. Centralized data architecture
2. Distributed data architecture

3. Blending of the two approaches (e.g., a central database with local elements for process control or data acquisition)

See Appendix 3 for a discussion of the advantages and disadvantages of centralization versus distribution.

4.1.4 Planning for Data Management

Data architecture can have a significant impact on data planning, see Appendix 3.

Data management for global information systems should be considered during the Concept phase. Data should be owned by Business Process Owners. The Business Process Owners should develop, or agree to, a data management strategy in support of the data life cycle for the system(s) involved in the project.

1. The data management strategy should be defined as early as possible in the Concept phase.
2. Data standardization should be a high priority goal.

Failure to address either of these two aspects can increase the risk of data integrity problems.

Many of the life cycle activities for global information systems may be under the control or influence of a diverse and geographically distributed group of individuals, so a well-defined data life cycle should be followed. This should cover:

- Planning
- Acquisition
- Organization
- Presentation
- Data use
- Data archival
- Data destruction

The aggregate requirements related to records maintained in a global information system should be understood. Global data management usually requires an understanding of multiple jurisdictions. Data owners and project teams should understand **all** applicable requirements:

- QA departments are usually familiar with rules for one or two jurisdictions (e.g., local and FDA regulations)
- Legal departments are usually locally focused

From the perspective of development and administration of a data management strategy, the data life cycle and the system life cycle should be viewed in parallel, at least as far as maintaining quality throughout both life cycles is concerned.

Stakeholders should be involved early in the Planning and Concept phase. The data management strategy should identify those individuals appointed to take on the policy setting and administration roles. These individuals should be adequately trained in global regulatory requirements as they relate to managing data and information.

The applicability of standards, procedures, and guidelines to best practices should be confirmed.

Decisions made during the Project phase that relate to data management and data integrity should be linked to new or existing operational processes.

4.1.4.1 Data Integrity

Decisions regarding product quality and patient safety are based on data that is recorded and reported. Data integrity issues may not be easy to detect, regardless of how data is recorded.

The use of computerized systems may require additional tools and expertise to identify data manipulation. Controls should be implemented and validated to mitigate the risk of data manipulation.

If any aspect of the Data Management Strategy is outsourced, the supplier management program should include an assessment of the potential risk to data integrity. Employees and suppliers should understand the accountability and traceability requirements for the recording and retention of data, and the consequences of any compromise to data integrity.

Training should be provided to help to ensure that documentation which records what happened is created at the time it occurred, in order to help to ensure product quality and patient safety. This documentation should include information about the personnel who performed it, along with clearly documenting changes and investigating deviations.

4.1.4.2 Accountability and Data Ownership

Data should be owned. A Business Process Owner with accountability for data and its management should be identified, allowing for the possibilities of central or distributed data, or a combination of both. While data may be locally distributed and have a local Data Owner, someone should be globally accountable to ensure that the global data life cycle requirements are met. This includes defined responsibilities for all applicable aspects described in this list.

4.1.4.3 Adherence to defined Corporate Retention Management Processes

Global processes for managing records should be followed. For a global information system, this includes understanding the various local legal and regulatory requirements (which may differ based on jurisdiction). Rules for managing data destruction, including who needs to approve the destruction, should be agreed. For further discussion of record retention, see Appendix 2.

4.1.4.4 Verification of the Appropriateness of Enterprise IT Control Processes

Processes such as IT backup and restore need to be verified as being compatible with the business model.¹

4.1.4.5 Rules of Archives

If data is to be archived, the nature and timing of the archival and rules for access to the archived data should be defined.

4.1.4.6 Security

Globally distributed information environments create an increased need for managing the security of the data effectively so that there is reduced risk of:

- Exposure of confidential data

¹ For example, if a system is only used for a brief period annually (e.g., to close out yearly activities), a monthly backup process that recycles media every fourth month is not appropriate, as corruption of the data could occur early in the year and be propagated to all backup copies before it is discovered.

- Unauthorized changes to data
- Accidental or intentional misuse of data
- Loss of data

Data management should ensure that the right people have access to the right data in an appropriately timely manner.

4.1.4.7 Data Migration

Data migration activities should be addressed during the Concept and planning phase. Key stakeholders should make the decisions as to what data will be migrated and from what existing systems. The members of the team handling this activity should be identified during the Concept and planning phase and work should start immediately. Data migration can often take longer than the entire project of system implementation.

When deploying new systems, it may be necessary to put a freeze on data collection in the predecessor system. This should be defined in the Data Migration Plan, including scope, i.e., whether the freeze is global or local. For changes to existing systems, this will more likely be a brief shutdown of the system while the change is implemented.

4.1.4.8 Unmigrated Data

It may be appropriate to archive rather than migrate some data that has not yet reached the end of its retention period. Not migrating the data could affect ease of access and/or the ability to reprocess it. Such decisions should be taken and justified based on a risk assessment.

4.1.4.9 Merger and Acquisition Considerations

Where a site or division using a global application is sold, the data (including metadata and supporting documentation) relevant to that business unit should be isolated and transferred to the new owner. This can be difficult to manage, but it can be made easier if the metadata is appropriately designed initially. Integrating information from an acquisition is a more standard data migration challenge.

4.1.5 Planning for System Management

For non-global information systems, most aspects of setting up operational system management processes typically form part of the Project phase. For global information systems, structures that need significant organizational planning might need to be created. This should be started as early as possible.

Issues that should be considered in parallel with initial project planning include:

- Accountability
- Communication
- Configuration management and version control
- Change control
- Security management
- CoE concept

4.1.5.1 Accountability

Most companies make someone responsible for system management, but assigning accountability is also important. This is especially important when responsibility may fall to local organizations. Someone should be globally accountable for consistent good practice across all locations. A local data center may be responsible for backup and archiving, but there should be accountability to ensure that changes and activities thought to be purely local do not compromise other sites.

4.1.5.2 Communication

Many aspects of system management require communication between sites and with global users. Language and cultural issues can impact effective communication.

4.1.5.3 Configuration Management and Version Control

Defined processes are imperative to keeping sites synchronized. This is especially true for distributed systems. It is inadvisable to permit sites to have different configurations, as managing this can be very difficult and can be a source of possible problems.

4.1.5.4 Change Control

Global systems require a change control infrastructure at both global and local levels. Proposed changes need to be evaluated for both global and local impact. Updates and patches need to be managed and applied in a controlled manner that minimizes negative impact on the business. Coordination is important, but so is sensitivity to local issues that may impact scheduling decisions.

4.1.5.5 Security Management

Central management of security reduces the number of security administrators needed, but communication with local sites is considered essential to ensure that access control reflects current needs based on defined role profiles. This may include differing requirements based on legal or regulatory jurisdictions, and a well reasoned, risk-based approach to security controls can be much more challenging in such circumstances.

People are one of the biggest risks to security and the roll out of effective security training to users in all geographies is equally important.

4.1.5.6 The Center of Excellence Concept

While several models for global system management can be envisioned, this Guide describes one strategy that can help, i.e., the establishment of a global "Competency Center" or CoE. This model can efficiently and effectively address many of the issues noted above and this Guide assumes the establishment of a CoE.

For very large systems, multiple regional CoEs may be considered. The general concept behind these organizations is to establish a concentration or focus of expertise in one place. If multiple CoEs are established, the most common and probably the most effective approach, is to designate one CoE as primary CoE, and the others as secondary CoEs. While all will participate equally in support tasks, the primary CoE can be the focus for strategic decisions.

The CoE concept provides several advantages for global management:

1. Common resources for problem resolution:
 - Significant collaboration can be achieved if many of the problems with the system can be addressed centrally.

2. Service or Operational Level Agreements:

- Service Level Agreements (SLAs) or Operational Level Agreement (OLAs) can be established that define expectations for the global information system for both internal and outsourced services. Depending on how support is to be provided, this may be a combination of local and global agreements.

3. Management of future global validation issues:

- Maintaining the validated state can be assured by CoE review and, where appropriate, CoE management of changes.

4. Documentation management:

- Responsibility should be established for managing both the global system management and validation documents.

See Section 4.3.2 for a more detailed description of the CoE model.

4.1.6 Typical Concept Phase Risks

Risks typically become noticeable during the project and operational phases of the system. Consideration of risks during the concept phase can help to mitigate significant issues and failures later. Typical concept phase risks for global systems are summarized in Table 4.1.

Table 4.1: Typical Concept Phase Risks

Issue Type	Hazard	Risk	Mitigation
User	Inadequate understanding of impact of new system	Inadequate resourcing or insufficient funding	Scope and impact of system fully defined as part of Business Case and communicated clearly to senior management in order to gain their commitment.
	Unclear objectives	Delayed or unsuccessful project	Objectives clearly defined and understood by senior management, Steering Committee, and Project Management.
	Cultural differences	Misunderstandings and issues during the project and beyond	Project Management identifies possible cultural differences and implements working practices and measures to ensure effective communication and co-operation between core and local team representatives.
	Inadequate resources or funding	Unrealistic timelines or failure to meet all requirements	Reconciling available resources and funding at Steering Committee level.

Table 4.1: Typical Concept Phase Risks (continued)

Issue Type	Hazard	Risk	Mitigation
User (continued)	Flawed user requirements	Flawed design or a system that does not meet the business needs	User Requirements Specification (URS) development involving all interested parties and is subject to rigorous review.
Technical	Invalid technical assumptions	Flawed design	Ensuring technical decisions taken by appropriately qualified and experienced specialists, based on: <ul style="list-style-type: none"> • Sufficient understanding of business processes to be automated • Consultation with suppliers • Defined and approved requirements
	Inappropriate choice of architecture	Operational limitations or inadequacies	Ensuring technical decisions taken by appropriately qualified and experienced specialists, based on: <ul style="list-style-type: none"> • Sufficient understanding of business processes to be automated • Consultation with suppliers • Performing cost benefit analysis • Defined and approved requirements
Regulatory and Legal	Not all regions covered by system have common understanding of regulatory requirements and expectations	<ul style="list-style-type: none"> • Inappropriate record retention • Lack of data integrity • Inappropriate use of data • Failure to address and meet regulatory requirements of all regions where system is used 	Reviewing and understanding local requirements. Involving all relevant QA and Legal departments in this process.

4.2 Project Phase

4.2.1 Key Project Phase Activities

The Project phase consists of the following activities within the overall project:

- Planning the validation strategy, taking into account possible pilot/lead implementation site approach
- Implementing project procedures, e.g., change control, configuration management
- Defining global business processes

- Establishing system ownership
- Defining project organization (roles and responsibilities)
- Finalizing and documenting both global and local user requirements, including any piloting, prototyping, and evaluation activities. Ensuring that they are:
 - Clear
 - Complete
 - Testable
 - Unambiguous
- Assessment, selection, and management of suppliers, e.g., contracted off-shore software development
- Translating user requirements into:
 - Appropriate system architecture
 - Functional or configuration specifications
 - Design specifications
- QRM activities:
 - The regulated company should ensure that an acceptable Quality Management System (QMS) is in place and is appropriate to the project
 - Responsibility for quality lies with the regulated company
- Performing design reviews
- Creating and maintaining traceability information
- Producing and managing the code for the system
- Documented software testing – ensuring the developed system is adequately verified
- Developing user documentation, instructions, and training in both a common and, as needed, local languages
- Operational system management planning, e.g., change control, security, backup and recovery
- Validation reporting
- Releasing the system for use

These activities are described in more detail in Appendices 1 and 8.

Successful delivery of a compliant and validated global information system normally requires effective project organization and management. The Project Manager should be responsible for managing aspects typically surrounding global information system projects. Further guidance is given in Appendix 7.

4.2.2 *Design Considerations*

Architectural aspects of global information systems should be considered and addressed appropriately within the project. This can involve negotiation with the responsible infrastructure support groups (which may include cloud or other outsourced providers). Architectural aspects may include:

- Need to use minimum standards for hardware and software across the global implementation
- Compatibility of applications running on the same platforms
- Need to interface local applications with global system
- Compatibility of local applications on the same platform
- Description and visual mapping of the system
- Clock synchronization. (This can be significant for time stamps on electronic records. A master clock server should be designated, as system clocks are usually controlled by infrastructure support.)
- Security, access controls, availability, integrity, confidentiality, and authentication
- Network availability and stability, including availability of internet connections where needed (applies to cloud solutions and to applications that have interfaces relying on the internet)
- Testing of contingencies involving cross-site communications
- Business continuity and disaster recovery

Several local infrastructure groups may need to be involved, depending upon the organization of the IT function in the regulated company. Architectural aspects should be addressed when contracting with outside service suppliers.

Architecture decisions should be included in determining the appropriate strategy for formal testing. For further information, see Appendix 4.

4.2.3 *Planning for Data Management*

Initial planning undertaken during the Concept phase should be further developed during the Project phase. There should be a well defined and documented data definition, to develop user requirements that adequately support good data management, including:

- The meaning of the data, including an understanding of the metadata needed to keep the data meaningful
- What is data quality (integrity, appropriate precision, and accuracy)?
 - **Note:** data quality is a business responsibility outside of the realm of IT responsibility
- How the data will be used
- Possible local legal requirements that may supersede global retention plans, e.g., for management of Personally Identifiable Information (PII)
- How long the data needs to be retained. (This can have a significant IT impact; for data retained for three to five years, proprietary formats are not likely to be problematic. There may be significant issues for data that needs to be retained for a decade or more.)

- Establishing the degree of standardization, including local versus global definitions and naming conventions for data. Implications of multi-language needs for prompts and data entries should also be considered.

The data definition should be agreed to by the data creators, owners, managers, and users.

To increase data consistency and integrity the following should be considered when developing data user requirements:

- Utilizing technical solutions to minimize human error and increase error detection, e.g.:
 - Dropdown menus
 - Data dictionaries
 - Field formatting
 - Range checking
- Required fields should be clearly identified to ensure that incomplete records are not allowed
- Audit trail data should be defined:
 - Expectations for audit trail availability should be defined. For example, there may be personal information that should be restricted to those with a legitimate business need to see it.
 - Consideration should be given to whether some simple audit trail queries should be developed. This might make audit trail review (as part of the business process simpler). It might also help to protect sensitive information.

An archiving strategy should be defined as a user requirement if the:

- Expected volume of new data, and of the data to be migrated, is significant
- The data needs to be retained for a long time

Data availability requirements should be defined.

For more information on data management requirements see Appendix 9.

4.2.4 Planning for System Management

Operational system management processes considered during the Concept phase should be established and finalized during the Project phase.

4.2.4.1 Centers of Excellence

If the decision has been made in the Concept phase to use the CoE model, building the first CoE should be started during the Project phase. The SME who will head the CoE is usually involved with the project. Consideration should be given to selecting the CoE head from the business side, as business impact of any actions by the CoE need to be understood.

A “follow the sun” model can ensure that at least one CoE is open at any time of day. This is usually appropriate for a large global information system with significant business risk.

CoEs are typically small in terms of staff, although they may have demands on other IT or business resources to execute system management or troubleshooting processes.

If multiple CoEs are to be established, this will probably be a phased project, with a subsequent CoE established when geographically justified. It is advisable to draw on experienced staff from the first CoE to build and train the staff for the second CoE.

Regulated companies may elect to outsource their CoE. This may work well for support of purely IT issues; however, it can make addressing issues that cross over into the business realm more complicated. Where a CoE is outsourced, handling the process interface should be considered. It may be advisable to build extra communication channels and expectations into the SLA with the outsourced CoE.

4.2.4.2 Definition of System Management Processes

Decisions are needed regarding where the various processes will be performed, in conjunction with developing the CoE. Processes may be:

- Entirely local:
 - Local processes are easily monitored by the most directly affected people, but care should be taken to ensure that nothing done locally creates risks or inhibits operations at other sites.
- Entirely global:
 - Managing a process globally can ensure consistent application, but it might not meet the needs of a unique, local situation.
- Hybrid

Planning and implementing these processes should include input from **all** involved parties.

Adopting a globally standardized service management methodology, e.g., ITIL®² [10] or ISO 20000 [11], can provide an effective approach to defining processes that can work globally. This can help to facilitate consistent system management, and should be adopted by CoEs.

Adopting a standard approach can help to ensure that system management meets consistent standards. This means that the high degree of confidence in the validated global information system is preserved throughout the Operational phase of its life cycle and in all locations. If a regulated company is considering an outsourced CoE, it is advisable to ensure that the company being engaged to manage the CoE follows one of these highly structured methodologies. A consistent and well defined processes can prevent potentially serious support problems.

Some processes, such as change control and incident/problem management, can have global implications, even if the change or incident appears to be entirely local. This can make the organization more complicated, as there needs to be a mechanism for escalation of problems to global teams, when needed. Typically, this escalation mechanism involves defining what can be managed locally. Anything outside of the defined boundaries needs global evaluation, probably by the CoE. Where an organizational infrastructure already exists, the project team needs to integrate the new global information system into the mechanism. If the global teams are not already set up, substantial work may be needed to build them.

² ITIL® (Information Technology Infrastructure Library) [10] is a methodology developed in the UK that has become a de facto global standard for IT service management. It has evolved since its introduction in the 1990s, with the current edition as of this writing having been published in 2011. Many of the processes described in ITIL® are good practices that form a base for effective system management. Much of the terminology used in this section is derived from ITIL®.

4.2.4.3 Configuration Management

In addition to managing the configuration of the global information system under development, the global information system development team should set up the process for managing it during operation. Part of the work of the global information system development team should be to define the Configuration Items (CIs) for the global information system, including the attributes and relationships for these CIs. (**Note:** the development team, not the validation team, should be responsible for this activity, although validation needs to verify that a configuration baseline is established.) CIs include configurable software settings and hardware components, common infrastructure components like servers and networks³, software components, and documents. For more information, see the *ISPE GAMP® Good Practice Guide: IT Infrastructure Control and Compliance (Second Edition)* [12].

4.2.5 Typical Project Phase Risks

Typical project phase risks for global information systems are summarized in Table 4.2.

Table 4.2: Typical Project Phase Risks

Issue Type	Hazard	Risk	Mitigation
Technical	Complex system architecture	<ul style="list-style-type: none"> Data configuration is not managed effectively Synchronization of data across sites/regions may be lost, threatening the ability to view up to date data, or to share or exchange data 	<ul style="list-style-type: none"> Employing suitably qualified staff Implementing clear data configuration and synchronization procedures and provide training
	Different versions of operating systems, middleware and applications to be supported	Appropriate compatibility is not maintained, which could lead to system failures	Minimizing the number of different versions in use where possible, enforce configuration and change management.
Supplier	Use of inappropriate or not suitably qualified or experienced supplier(s)	Software product or customer application is developed in an informal manner, without the rigor of a formal QMS, leading to the system not being fit for purpose	Performing supplier assessment to verify standards, agree and monitor corrective action, which may include added validation activities, where required.
	Insufficient staffing impacting quality related decision making	Software is developed and released without appropriate assurance that it meets the defined requirements	Project management to allocate staffing resources based on planned activities and deliverables, then monitor and adjust as necessary.

³ It should be noted that the ideal situation would have common infrastructure components already listed in a Configuration Management Database (CMDB), and that the global information system would list dependencies to existing CIs. It is not practical to expect those responsible for a single application to assume Configuration Management responsibility for infrastructure outside their control.

Table 4.2: Typical Project Phase Risks (continued)

Issue Type	Hazard	Risk	Mitigation
Supplier (continued)	Inexperience	While inexperience of either the regulated company or of the supplier introduces risk, the risk is multiplied when both are inexperienced	Preferably, an inexperienced company should work with an experienced supplier. If it is unavoidable that both are inexperienced, strong consideration should be given to hiring an experienced system implementation partner.
	Inadequate documentation management	Formal, controlled, documentation is not available to verify and demonstrate that the system is fit for intended use	Performing supplier assessment to verify standards, agree and monitor corrective action where required
Project Organization	Lack of system ownership	Functionality is not compatible with business processes	Identifying owner with sufficient knowledge and authority
	Insufficient local site representation	Insufficient local ownership and increased likelihood of a global solution that is not acceptable to one or more remote sites	Ensuring local site representation on project team
	Inadequate interaction between global team and designated local representatives	Insufficient local ownership and increased likelihood of a global solution that is not acceptable to one or more remote sites	Defining communication and feedback mechanism within project team
	Inadequate change management	<ul style="list-style-type: none"> Inadequate or invalid testing Project delays due to late or trivial changes Scope creep 	Defining rigorous risk-based change management procedure effective for whole project.
	Inadequate configuration management	Release and handover of flawed system	Defining configuration management procedure appropriate covering core and local elements.
Regulatory and Legal	Lack of understanding of applicable laws and regulations (e.g., GxP, Data Privacy)	Failure to comply with laws and regulations putting companies at risk of legal and regulatory action	Reviewing and understanding local requirements. Involve all relevant QA and Legal departments in this process.
	Inadequate knowledge of applicable regulations relating to electronic records and signatures	System does not provide the technical controls required to enable compliance with electronic record and signature requirements	Reviewing and understanding applicable regulations. Involve QA in this process.

4.3 Operation

Once the global information system has been accepted and released for use, there is a need to maintain compliance and fitness for intended use throughout its operational life. This can be achieved by the use of up to date documented procedures and training that cover use, maintenance, and management. Clear ongoing ownership of the business process(es), system, and data throughout the Operation phase is considered essential, see also Appendix 1 Section 5.2.

The Operation phase of a global information system may last many years, and may include changes to:

- Data (structure or content)
- Software
- Hardware
- Business process
- Regulatory requirements

The integrity of the system and its data should be maintained and verified as part of periodic review.

As experience is gained during operation, opportunities for process and system improvements should be obtained, based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures. Information from the Incident Management and Corrective and Preventive Action (CAPA) processes (or other mitigation process such as defined in ITIL® [10] or ISO 20000 [11]) can provide significant input to the evaluation.

Established operating procedures for global information systems should cover:

- Change and configuration management
- Incident and problem management
- Release management
- Security management
- System administration
- Data management
- Data retention, migration, or destruction
- Globally defined training requirements and curricula
- Data backup and recovery
- Business continuity and DR
- Supplier management, including the SLA
- Periodic review

System architecture will impact the Operational phase of a global information system. For example, a centralized system can have a mostly centralized support structure. A service desk that needs to be able to “follow the sun” can be centralized and staffed in shifts. A distributed system, however, needs some level of support to be local to the servers, e.g., for hardware maintenance. When support is being handled outside of the local area, support staff should be able to communicate in a language understood by the users who need help.

System architecture will also affect the approach to specific operational activities such as backup, business continuity planning, disaster planning, incident management, and user account management (see Appendix 2).

4.3.1 *Maintaining the Validated State*

Global information systems should be maintained in a validated state. This can be more complicated if a system is managed differently (or to different standards) at different sites. A globally standardized service management methodology, e.g., ITIL® [10] or ISO 20000 [11], can help to facilitate consistent system management.

Regulated companies should consider adopting a standard approach to ensure that system management meets consistently high standards so that the high degree of confidence in the validated system is preserved throughout the Operational phase of its life cycle and in all locations.

4.3.2 *Managing a Global Information System through a Center of Excellence*

CoEs can be an effective method for delivering key elements of system management. The CoE should have the responsibility for managing the global information system core, including:

- Configuration (including patch management)
- Global change controls process
- Possible involvement in local change control processes
- Application level security (but not user account management)
- Incident management referrals for solution of “Level 2” or higher problems (those not soluble by the front-line Help Desk)

The CoE can be used to negotiate an OLA with the Business Process Owner. The OLA should define what expectations users should have for performance and availability. The CoE also can also manage agreements with internal suppliers (e.g., for network support) and with external suppliers (e.g., the application supplier’s help desk).

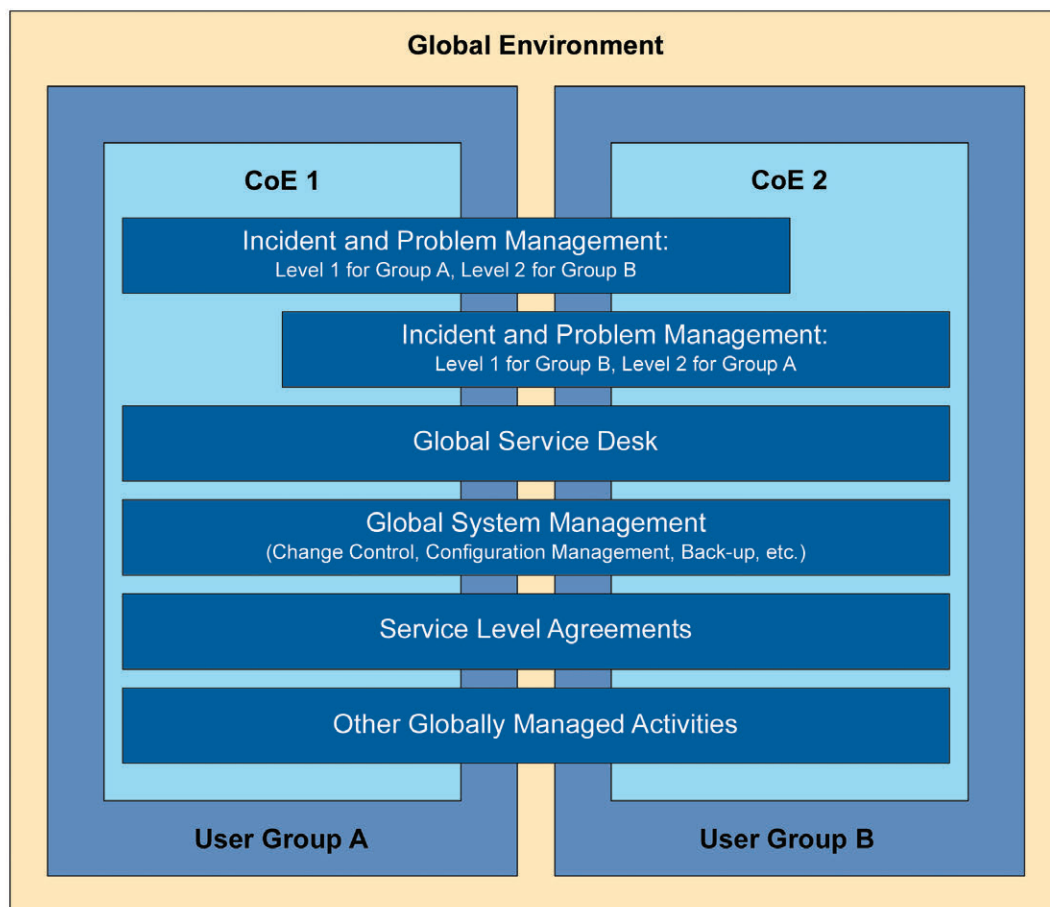
In cases where there are multiple CoEs, problem management may be shared to support off-hours work. The CoE(s) may also be given responsibility in relation to:

- Backup
- Archival
- Disaster recovery
- Training

Sites should not all be off-line at the same time in distributed scenarios.

Figure 4.2 shows a graphical representation of the CoE concept with more than one CoE. In this model CoEs “1” and “2” are located in different time zones. The Service Desk⁴ interacts fully with both CoEs. Incident management can be based either on geography or on which CoE is within normal business hours at the time the incident is escalated. For emergencies, the call should always go to the active CoE.

Figure 4.2: Center of Excellence Concept



High risk or high priority issues may involve work by a second CoE in cooperation with the first, e.g., during the off-hours of the first CoE. Both CoEs should assume full responsibility (and accountability) for compliance with critical processes such as Change Control and Configuration Management (see Appendix 2). A single OLA or SLA may tie user expectations together; however, business practices at different sites may make multiple OLAs or SLAs desirable.

Where multiple CoEs are involved, close and frequent communication should occur between the CoEs.

Where smaller companies do not have the capability (or the need) to support a separate CoE, consideration should be given to creating a “virtual CoE”. This should identify appropriate IT and business resources to address global problems and issues. Personnel assigned to a virtual CoE should have this role formally defined as part of their job responsibilities. The proper level of commitment should be made clear in their job objectives. A virtual CoE may not be as available and as responsive as a dedicated team.

⁴ It does not matter if the service desk is a centralized function or distributed in this model.

4.3.3 Establishing Risk-Based System Management Practices

The scope of global information systems means that the risks related to such a system may be subject to regional variation.

For example, countries with very strong privacy protection laws present challenges to the way that data is managed. This may potentially include conflicts with the requirements of health authority regulations and particularly health authority regulations from outside the country. These challenges can affect system management practices in areas such as backup management and record retention. Mitigation measures may help to alleviate some risks, but regulated companies may need to select a path of least harm. It is advisable to involve all relevant Legal and QA departments in such decisions.

The concept of weighing risk to the overall enterprise versus local risk is magnified for global information systems. Isolating global information systems within their own environment can be used to “protect” smaller GxP systems from relatively frequent infrastructure changes. This isolation technique can make it easier to delay infrastructure changes, in order to deal with them as packages releases. It may not, however, be possible to isolate global information systems within their own environment. Global business process owners and system administrators may not be able to delay an operating system or database patch because the overall risk to the company is too great. In these circumstances, the CoE should be able quickly to decide risk to the system to feed it into the enterprise risk calculation.

For outsourced solutions, the CoE may not be making the risk-based decisions. These decisions would usually come from the supplier, but the CoE still need to understand the risks and may need to initiate planning for mitigation activities.

Typical risks related to system management and possible approaches to mitigating them are summarized in Table 4.3.

Table 4.3: Risks Related to System Management Processes

System Management Area	Hazard	Risk	Mitigation
Service Levels	Unclear accountability for resolving incidents	<ul style="list-style-type: none"> Incidents go unresolved for too long Decisions are made but buy-in is not universal 	Assigning a single globally accountable individual (e.g., a CoE head) who can nominate locally responsible individuals.
	Poor communications with local users and managers	<ul style="list-style-type: none"> Questions are either not asked or not answered Local buy-in is not obtained 	Defining communication processes for different types of incidents based on risk and business impact, e.g., dashboards or performance metrics.
	Local expectations do not align with global priorities	<ul style="list-style-type: none"> Dissatisfied users Local business processes not aligned with system capabilities 	Establishing a CoE and developing OLAs or SLAs with local organizations which define promised service level and clear Key Performance Indicator (KPIs).

Table 4.3: Risks Related to System Management Processes (continued)

System Management Area	Hazard	Risk	Mitigation
Service Levels (continued)	Some users are underserved because of large time zone differences	<ul style="list-style-type: none"> Dissatisfied users Failure to meet OLA or SLA with a user segment Business impacted 	Establishing satellite CoE(s) which can provide first and second level support during all business hours should be considered, where the organization can support it. This scheme can also support extended work on major global problems.
Change Management	Global changes do not work for all sites	<ul style="list-style-type: none"> Dissatisfied users Business impacted Application drift if rollback is done only at affected sites Desired changes not implemented if rolled back globally 	Evaluating differences in all local infrastructures, interfaces, business practices, and laws and regulations when planning changes at the CoE. The CoE may need to consult multiple groups or sites to obtain the complete business and regulatory picture.
	Inadequate QA evaluation of local regulatory impact	<ul style="list-style-type: none"> Failure to comply with regulation Required successful change not implemented due to compliance 	Ensuring QA representative on the Change Advisory Board (CAB) is sufficiently knowledgeable to recognize when a local QA opinion is needed.
	Change schedule does not allow adequate time to address local validation issues	<ul style="list-style-type: none"> Changes not implemented as planned Changes implemented without complying with full change process 	Ensuring change is planned and communicated far enough in advance to allow local time to react. If possible, schedule staggered implementation to provide more time to address local problems.
	Local infrastructure changes not adequately evaluated for effect on the global application	<ul style="list-style-type: none"> Unexpected application failure Drift from global norms 	Establishing a local CAB for this purpose, with a direct communication channel to the global CAB.
	Misuse of emergency change processes	Regulatory risk that changes are not adequately evaluated prior to implementation	Creating Standard Operating Procedures (SOPs) defining what constitutes an emergency.

Table 4.3: Risks Related to System Management Processes (continued)

System Management Area	Hazard	Risk	Mitigation
Release Management	The number of releases overwhelms the local ability to address validation issues	Regulatory risk that changes are not adequately evaluated prior to implementation	Strictly limiting the number of delta or emergency releases and adopting a package release strategy with scheduled delivery dates. This can allow the local organization to plan resource allocation accordingly.
	Failed changes disrupt local business processes	<ul style="list-style-type: none"> Dissatisfied users Business impacted 	Defining rollback strategy for any change release. Establish a process for evaluating the relative risk and impact to the enterprise as a whole, if a change is to be rolled back because of one local problem.
Change Records	Inadequate or inconsistent documentation	<ul style="list-style-type: none"> Greater potential for records to negative audit findings Subsequent changes evaluated incorrectly Uncertainty about whether a change was actually implemented Configuration records not correct 	Change management SOP defining documentation requirements including: <ul style="list-style-type: none"> Update specifications, if appropriate All approvals obtained timely All associated records (e.g., testing) available Changes closed appropriately, even if not implemented
Configuration Management	Incompatible local and global tools and processes	<ul style="list-style-type: none"> Configuration records not correct Higher risk of failed changes 	Single CMDB owned globally, with CIs defined, including unique local CIs. Effective communication channels between local and global entities.
	Configuration records drift and become inaccurate	<ul style="list-style-type: none"> Higher risk of failed changes Regulatory exposure 	Defining an owner for every CI. Not all CIs need to be owned globally. Change management procedures at all levels define when the CMDB needs to be updated.
Incident Management	Local incidents do not get adequate global attention, or global incidents are a surprise to local organizations	<ul style="list-style-type: none"> Dissatisfied users Business impacted 	Regular communications between local and global organizations. Risk-based processes for determining which incidents need to be communicated.

Table 4.3: Risks Related to System Management Processes (continued)

System Management Area	Hazard	Risk	Mitigation
Security Management	Inadequate local security	<ul style="list-style-type: none"> Unauthorized users have access Unauthorized changes to data Data integrity questionable by regulators 	Defining minimum security requirements at the global level and cascade them locally. Follow accepted global security standards such as ISO 27001/27002 [13, 14] or the National Institute of Standards and Technology (NIST) [15] standards.
Performance Monitoring	Failure of global organization to appreciate local performance issues	<ul style="list-style-type: none"> Dissatisfied users Business impacted 	Planning for anticipated capacity and growth. Establish performance KPIs and track them at each site.
Backup and Recovery	Global backup processes do not align with local needs	<ul style="list-style-type: none"> Data at increased risk Dissatisfied users if backup interferes with work day Business impacted 	Local authorities need to evaluate the global process to ensure it fits business practices. If not, local authorities either need to establish compensating controls or drive a change to the global process.
	Backup management does not comply with local laws (e.g., for managing private data)	<ul style="list-style-type: none"> Data at increased risk Legal exposure to fines or other penalties Regulated company reputation at increased risk if a breach occurs 	Ensuring relevant laws are well understood and tailor processes to comply.
Record Retention and Archiving	Global retention policies do not take local law into account (e.g., for managing private data)	<ul style="list-style-type: none"> Legal exposure to fines or other penalties Company reputation at increased risk if a breach occurs 	Local organizations should make legal requirements known to the global organization.
	Conflicting international rules (e.g., GxP versus local data privacy law)	Legal exposure to fines or other penalties	Involving local and global legal and QA departments in developing a strategy for a least-harm approach.
Business Continuity	DR fails to account for local needs at all sites	<ul style="list-style-type: none"> Data at risk Increased business impact of disaster 	DR plan needs to be risk-based and accommodate highest-value restoration first.
	DR strategy of restoring at alternative live data center seriously impacts business at the site that did not have the disaster	<ul style="list-style-type: none"> Dissatisfied users Data at risk Increased business impact of disaster 	When preparing the DR plan, ensuring that alternative hot or warm sites have the capacity to take on the load for the affected site.

Table 4.3: Risks Related to System Management Processes (continued)

System Management Area	Hazard	Risk	Mitigation
Business Continuity (continued)	Not all resources needed for global DR effort are identified and ready	<ul style="list-style-type: none"> • Dissatisfied users • Data at risk • Increased business impact of disaster 	Ensuring that local personnel needed for a global DR exercise are listed and informed. Periodically review this list. Execute periodic recovery exercises.
Periodic Validation Review	Local and global alignment inadequate	<ul style="list-style-type: none"> • Data integrity at risk • Regulatory exposure 	Ensuring that global processes involve local assessments where appropriate. Provide global support for local reviews.

4.3.4 Service Level Management

Global information systems usually rely on multiple suppliers. These can be internal suppliers or a combination of internal and external suppliers. Suppliers bear some responsibility for keeping the global information system running smoothly. Both the Business Owner of the global information system and those supporting it should understand and agree expectations, e.g., for support hours by the IT group. For further information on the “follow the sun” model, see Section 4.2.4.

The Owner of the global information system is accountable for defining required service levels and funding their fulfillment. The CoE can have responsibility for monitoring and reporting on service levels.

This Guide references ITIL® [10]. ITIL® is a widely accepted approach to IT service management, and provides a cohesive set of best practice drawn from the public and private sectors internationally.

4.3.5 System Management Processes

4.3.5.1 Operational Change Control and Management

Operational Change Control is covered in *ISPE GAMP® 5, Appendix O6* [4] and more extensively in Chapter 10 of the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [16].

Change control is connected with configuration management, as most of the changes that need to be managed in conjunction with a computer system involve changes to the configuration. Managing change for global information systems needs a wide evaluation of potential effect and the coordination of release management processes. This emphasizes the need for a well-defined change control process that stresses thorough and effective planning, a clear understanding of risk management (risks may not be the same everywhere), and robust communication.

The challenge is to developing a process that routes the change requests appropriately, as evaluating all changes globally can introduce complexity and subsequent delays.

For further information on change management for global information systems, see Appendix 2.

4.3.5.2 Configuration Management

The complexity of the system architecture can affect how challenging configuration management is for a global information system. The more components there are that are managed locally, the greater the risk of configuration drift and the possibility of problems with compatibility.

One of the goals of configuration management is to ensure that different sites using the global information system do not lose the ability to share data and to produce consistent results. Listing documentation and software versions and hardware models as CI attributes, along with the relationships noted, may help to facilitate this.

For further information on configuration management for global information systems, see Appendix 2, Section 6.2.

4.3.5.3 Incident Management

The approach to incident management will depend upon the structure of the system. Whether a centralized or distributed system, a documented procedure should be considered. This should define suitable global communications (both to and from the CoE) and should take into account local implications. Risks related to an issue should be considered in regard to how communications related to the incident are handled, both to users and between support organizations.

For further information on incident management for global information systems, see Appendix 2, Section 6.3.

4.3.5.4 System Security

Consideration should be given to accepted international security standards for a global information system, e.g., ISO 27001 [13] and 27002 [14] or the NIST cybersecurity framework⁵ [15]. The specific challenges for global information systems are to distribute security management responsibilities to ensure the most effective and efficient processes while providing adequate logical security protection of data integrity. Adherence to global security standards, such as those in the ISO 27000 series [17], is recommended to ensure that all sites manage security in the same way.

For further information on system security, see *ISPE GAMP® 5, Appendix O11* [4].

Physical security for global systems should be a local responsibility.

For further information on security for global systems, see Appendix 2, Section 6.5.

4.3.5.5 Performance Monitoring

For further information on performance monitoring, see *ISPE GAMP® 5, Appendix O3* [4] and the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [16].

Performance of global information systems should be monitored effectively, rather than referring to benchmark sites. For example, an application may be performing satisfactorily at the site where the CoE is situated, but could be unacceptably slow at another site. This could be because of several conditions ranging from undersized servers to network latency, or competition for bandwidth during peak usage.

For further information on performance monitoring for global information systems, see Appendix 2, Section 6.7.

⁵ <http://www.nist.gov/cyberframework/>.

4.3.5.6 Backup Recovery of Software and Data

Impact on the business associated with backing up databases should be weighed against the cost. This should include the risk of not meeting business or regulatory requirements if data is irretrievably lost or otherwise compromised, as in the case of a catastrophic system failure or breach of security. This may affect the timing and frequency of backup operations. For distributed systems, the requirements for each site should be assessed when deciding whether a local copy of the backup is required.

For further information on backup and recovery for global information systems, see Appendix 2, Section 6.8. Backup and recovery of software and data are also discussed in *ISPE GAMP® 5, Appendix O9* [4] and the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [16].

4.3.5.7 Record Retention, Archival, and Retrieval

Record retention, archive, and retrieval are considered in *ISPE GAMP® 5, Appendix O13* [4] and in the *ISPE GAMP® Good Practice Guide: Electronic Data Archiving* [18].

Special challenges related to archival of global information systems include navigating different and occasionally conflicting legal requirements for record retention. For example, training records required under US GLP regulations [19] might be required under a local privacy law to be deleted when an employee leaves the company. Legal and QA advice is a requirement when deciding how to manage such records.

Some GxP systems may also have overlap with financial regulations, e.g., the Sarbanes-Oxley Act of 2002 [20].

See Appendix 2, Section 6.9, for a more detailed discussion of archival for global systems.

4.3.5.8 Business Continuity and Disaster Recovery

Business continuity and disaster recovery is considered in *ISPE GAMP® 5, Appendix O10* [4] and in the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [16].

Regulated companies should have enterprise disaster recovery plans. These should include recovery of a specific global information system. Enterprise disaster recovery plans should identify recovery sites and priorities. Business Process Owners of global information systems need to ensure that their business needs, i.e., that of all global users, are considered within the enterprise plan. Considering business continuity and disaster recovery during requirement planning can help to ensure business needs can be met. Identifying details such as “hot sites”, can be done later in the life cycle.

For further information on business continuity and disaster recovery for global information systems, see Appendix 2, Section 6.10.

4.3.5.9 Periodic Review

The purpose of periodic review of validated, global information systems is to assess the continued overall effectiveness of the GxP related systems and to maintain their validated and compliant status.

QA should be involved in the review process and should approve the final report. If deviations from expectations are found, the report should include an action list and target dates for remedial activities.

For further information on periodic review for global information systems, see Appendix 2, Section 6.11.

Periodic review is discussed in *ISPE GAMP® 5, Appendix O1* [4].

4.3.6 Data Management

This section describes the activities related to executing data management tasks. For data management planning, see Section 4.1.4.

4.3.6.1 Data Management Policies

The policy setting and administration roles should operate in a global context to ensure:

- Provision of data management policies, strategies, standards, and guidelines across locations and regulatory jurisdictions
- Promote data quality as an enterprise activity
- Identify appropriate training to ensure compliance and controls can be met and are demonstrable

4.3.6.2 Data Life Cycle

This is the policy-based approach to managing a computerized system's data from acquisition/creation and initial storage/use to the time of archival and eventually destruction.

A well-defined data life cycle should be followed, from planning, and used from data creation/collection through to data destruction and destruction as shown in Figure 4.3.

Figure 4.3: Data Life Cycle

