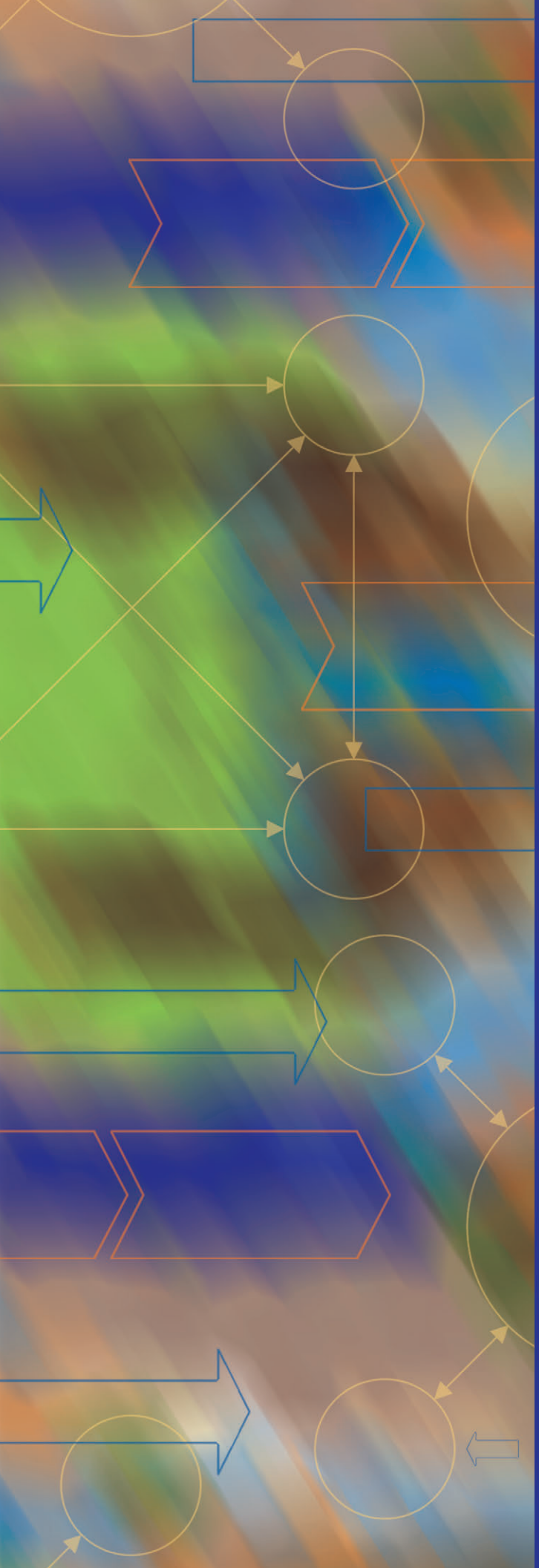


ISPE | GAMP

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.

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

Table of Contents

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)	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. 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. A local project team can also be helpful supporting training and rollout.	Appendix 1, Section 5.3
Project Team (project manager)	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. 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. 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.	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	A global project Steering Committee should understand the business process and have authority to make decisions and to drive those decisions to completion. 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: • 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) 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. 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: • The local Process Owner • The System Owner • QA • A representative from a Center of Excellence (CoE) • A local Subject Matter Expert (SME) (if possible) Local project teams should provide regular reports that are reviewed by the global project team.	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	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. 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.	Appendix 7, Section 11.1.1.5 Appendix 7, 11.1.2.1
Project Change Management	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: • 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 Local changes may be proposed to globally defined business processes during the project, and these should be vetted before being accepted.	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	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. 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.	Appendix 1, Section 5.1
System Ownership	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). There may need to be two separate Business Process owners: 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 The global Business Process Owner should have sufficient authority to ensure that cross-organizational decisions are consistent.	Section 3.2 Appendix 1, Section 5.2
User Requirements	Unique local processes maybe justified. Reasons for this could include, e.g.: • Local laws • The requirements for special handling provisions for a product produced at a site This should be captured when collecting user requirements. Failure to make this adjustment could put the project at risk. Collaboration between local and global project teams can be a strong contributor to assurance of good user requirement specifications.	Appendix 1, Section 5.7
System Architecture	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. System architecture can also have an effect on operational needs such as backup and recovery, business continuity, or down time for service or upgrade.	Section 4.1.3 Appendix 1, Section 5.5
Interfaces	Interfaces, (input and output), are a source of vulnerability for data integrity.	Appendix 1, Section 5.7 Appendix 1, 5.11 Appendix 5
Software Selection	Selecting a software supplier for a system that is to be deployed around the globe requires attention to specific issues, e.g.: • Does the supplier have the ability to support all locations? • Is the software available in local languages? These and other questions should be addressed as part of the selection process.	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	Validation planning for a global information system is more complex than for local system. Issues that require consideration include: • 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	Applicable laws and regulations for delivering a compliant solution should be understood. A global information system will need to comply with **all** rules. 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.	Appendix 1, Section 5.6.1
Supplier Assessment and Management	Suppliers should be assessed, e.g., suppliers of: • Software suppliers • Integrators • Developers • Managed services • PaaS suppliers • SaaS suppliers Suppliers should be evaluated for their capability to provide support globally. If development activities involve access to data, privacy issues may become significant.	Appendix 1, Section 5.6.4
Testing	Testing should be planned to allow centralized execution, where possible. 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. If no local testing is intended, there should be a review of global testing by locally responsible individuals. The use of a test tool can be beneficial. A test tool can: • Make local testing easier • Assure that everyone has access to the tests and results • Facilitate offshore testing Test records should be available to support audits or inspections at all sites where needed.	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	Data management issues may vary, ranging from privacy protection to retention requirements, depending upon the nature of the global information system. 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. 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.	Section 4.1.4 Section 4.2.3
Pilot Projects	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. Pilot projects should be well documented, as the global project team are not usually at every site throughout the implementation.	Appendix 1, Section 5.4
Support (Centers of Excellence (CoE))	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.	Section 4.2.4.1 Section 4.3.2
Support ("follow the sun")	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. This should be considered for support provided both by the CoE and by the supplier.	Section 4.3.4
Support (down time)	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.	Section 4.3.4
Configuration Management	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.	Appendix 2, Section 6.2
Change Management	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. Companies may have separate processes for managing business and IT changes. If so, a link needs to be established to minimize unintended consequences.	Appendix 2, Section 6.1

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
Incident Management	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. 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.	Appendix 2, Section 6.3
Security Management	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. 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. 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.	Appendix 2, Section 6.5
Backup and Recovery	For a global information system, a mechanism to facilitate backup that also allows access to the database in other time zones should be implemented. A request to restore the database to a prior state needs to consider potential impact to the rest of the organization.	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)	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: • 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: • 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	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. 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.

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.

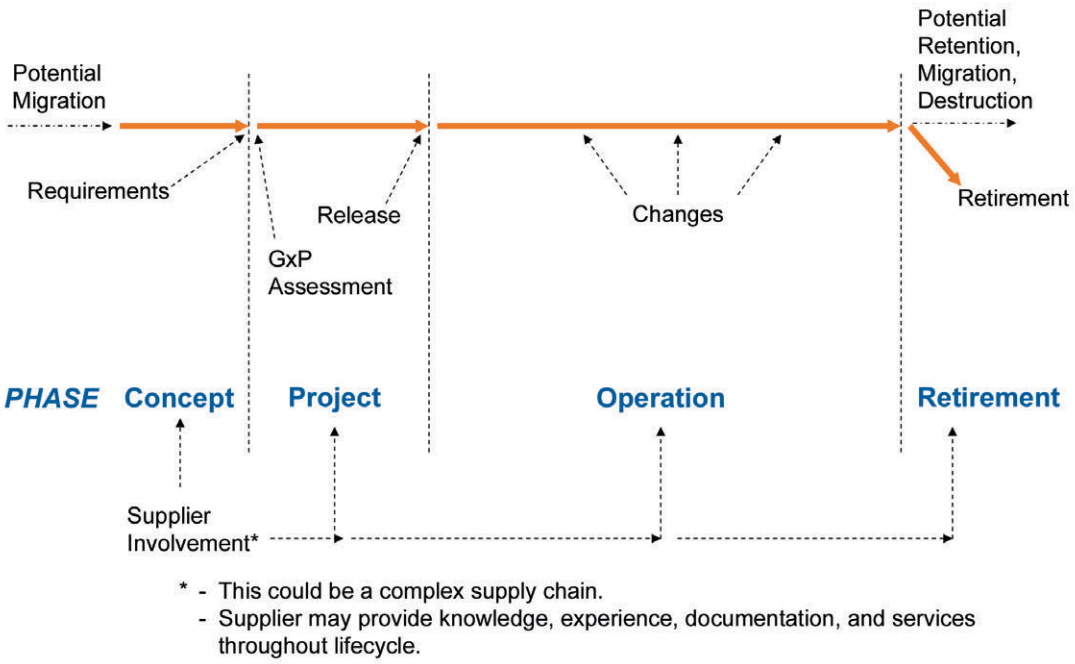
Good practices for suppliers of global information systems are described in Appendix 8. Supplier activities support regulated company activities.

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



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: • 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: • 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	• 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 networks[3], 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	• 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	• 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	• 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).

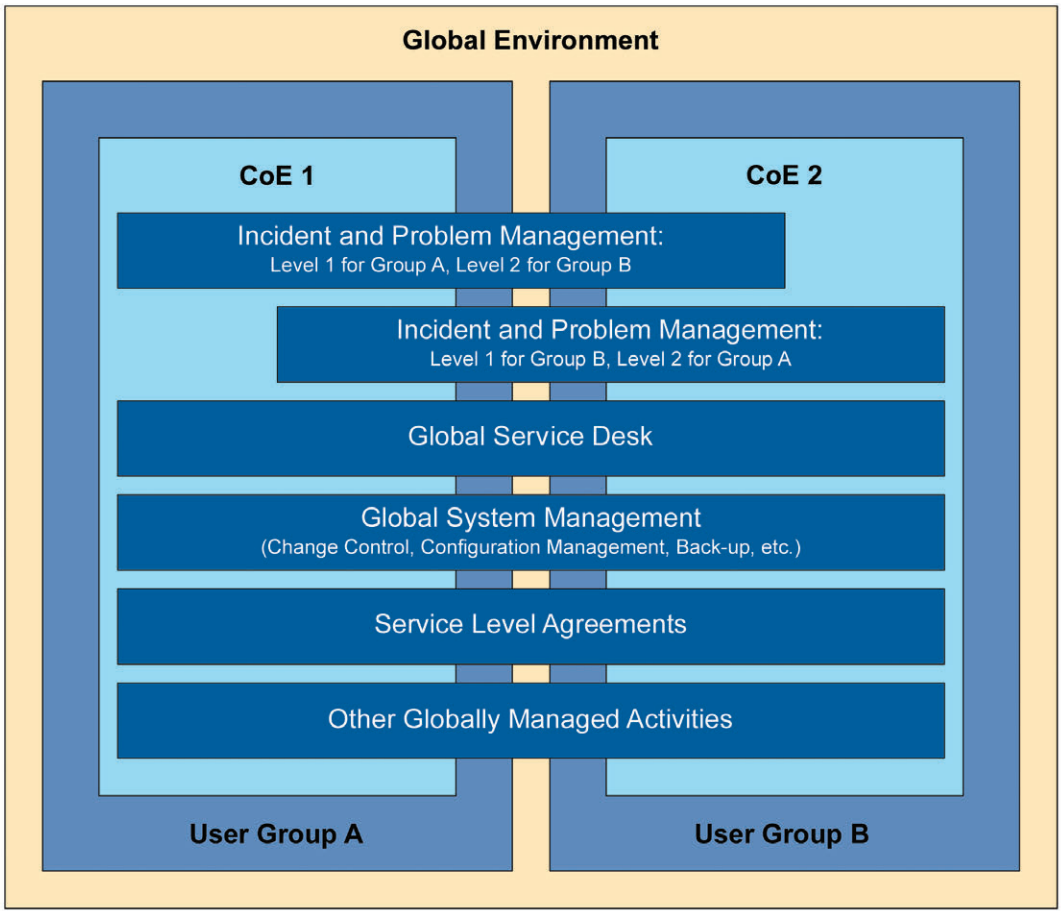
In cases where there are multiple CoEs, problem management may be shared to support off-hours work. The CoE(s) may also be given responsibility in relation to:

- 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 Desk[4] 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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	• 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: • 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	• 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	• 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	• 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	• 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	• 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	• 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)	• 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)	• 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	• 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	• 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	• 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	• 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 framework[5] [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:

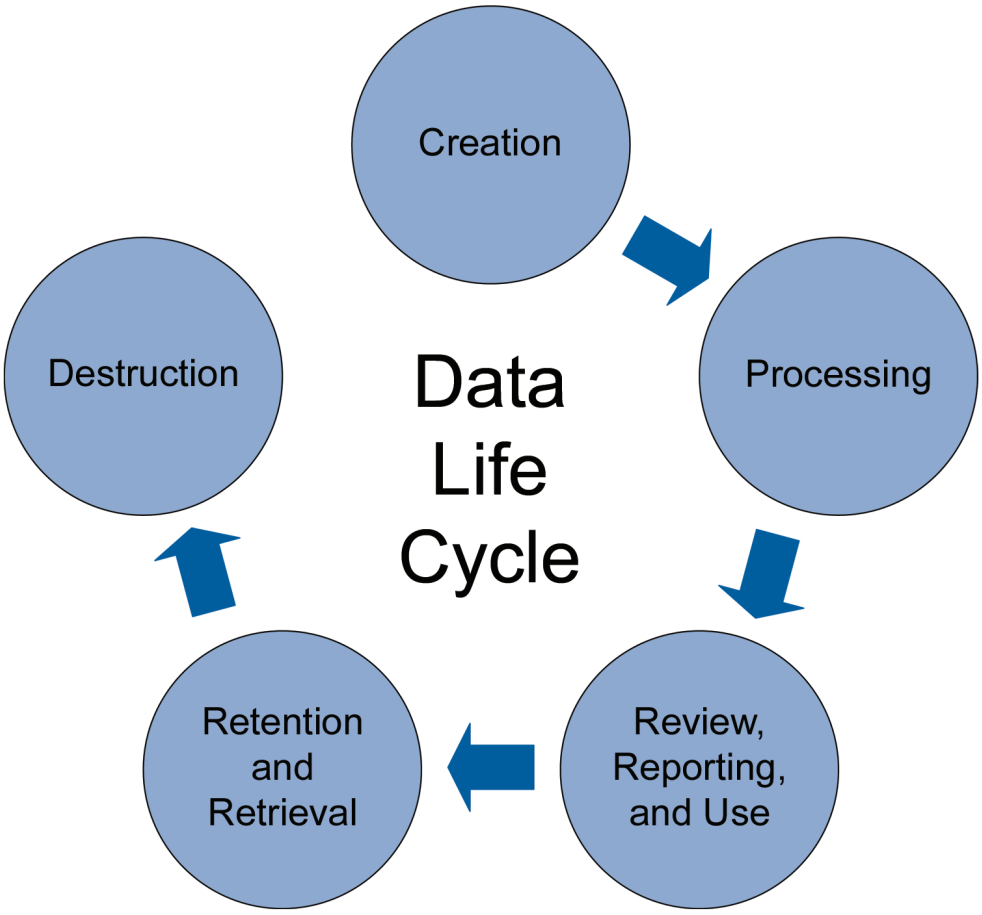
- Provision of data management policies, strategies, standards, and guidelines across locations and regulatory jurisdictions
- Promote data quality as an enterprise activity
- Identify appropriate training to ensure compliance and controls can be met and are demonstrable

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



Where a SaaS application is used, the planning of the data life cycle should include removal of data and/or application from the cloud (also known as de-clouding). This may be driven by a desire to:

- Archive
- Termination of the business partnership with the SaaS provider
- Other business needs

This will involve mapping within the supplier infrastructure to understand where the data resides. Typically, de-clouding will involve the same issues as data migration, e.g., handling metadata, possible data cleanup. Timing of de-clouding activities may be dependent on the provider.

4.3.6.3 Data Quality

Principles governing data quality are both operational and procedural. In terms of the principles, data should:

- Follow the ALCOA principle:
  - Attributable
  - Legible
  - Contemporaneous
  - Original
  - Accurate
- Have appropriate precision, be clear, and be complete
- Be consistent, relevant, and conform to agreed standards:
  - Standards are considered particularly important for global information systems
- Be secure and their integrity should be maintained
- Be assessed for value, cost, business benefits, and regulatory needs

4.3.6.4 Data Availability

Data availability requires a data management environment. This should allow users to find the data they need when they need it, at a required level of performance. OLAs or SLAs between the responsible and affected parties can be useful for defining what data is to be made available, at what level, and at what cost.

4.3.6.5 Data Access

A global information system increases the complexity of managing data access entitlement and permissions.

The security of data management systems should be integrated into the overall security fabric of the enterprise. Corporate data management policies, standards, and procedures should specify what can be provided to users, and how and when that access should be provided. These policies and procedures can be enforced via the management and timely maintenance of user permissions.

Data access management should help to control data risk. It is dependent on role-based permissions with in the global information system. It is more complex than general system access. Role-based permissions should be developed as a part of the business processes.

4.3.6.6 Data Administration

Administration roles (data managers and database administrators) with global responsibilities should ensure that:

- Data is administered in a consistent manner across sites and regions
- There are tools for data modeling and data administration
- There are coherent, consistent, stable, and secure database environments and architectures
- Data copy or replication practices meet business requirements
- There is an effective, compliant, and controlled infrastructure

4.3.6.7 Risk Mitigation

There should be policies, strategies, standards, and procedures to reduce risks related to:

- Data storage and replication (including backup)
- Data retention
- Management of source/raw data
- Data change management

4.4 Retirement

The retirement, replacement, or withdrawal of a global information system should be performed in accordance with an established process or plan. This plan should take into account potential risk to users should they lose access to the system or data. Technical functionality needed for retirement (e.g., data migration) should be considered and addressed during the Project phase, if possible.

The retention, migration, or destruction of data associated with a global information system should be performed in accordance with an established process or plan, taking into account applicable regulatory and other legal record retention requirements.

Retirement can be a major task for global information systems, due to the volumes of data and records involved. Consideration should be given to:

- Establishing procedures covering the retirement of the global information system, including withdrawal, decommissioning, and disposal, as needed
- Documentary evidence to be retained, including actions taken during retirement of the global information system
- GxP records to be maintained, their required retention periods, and which records can be destroyed
- The need to migrate records to a new global information system or archive. The method of verifying and documenting this process

- Ability to retrieve migrated records on a new global information system or from an archive
- Identification of personnel who should have access to migrated or archived records

Users should be provided with sufficient notice of retirement of a system and the replacement arrangements. Any expected supplier actions associated with retirement (e.g., transfer of data, software, or equipment to the regulated company) should be defined.

4.4.1 Typical Retirement Phase Risks

The approach to retirement of a global information system is dependent on its architecture. Planning in the Concept phase should consider potential concerns at the end of the life cycle of the global information system. If it is anticipated that retirement might need to be accomplished simultaneously for all users, then a distributed solution may not be optimal. Phased retirement coupled with a phased implementation of the next solution is considered more suitable for distributed systems, even if the follow-on application is centralized.

The end of the system life cycle is not usually the end of the record life cycle. Global applications usually contain records that need to be accessible after the servers are shut down. This could have a significant effect on choices for application architecture. If a record needs to be retained for forty years, the global information system should use a standard database rather than a custom tool that will be difficult to migrate or retain in a readable archive.

4.4.2 Typical Retirement Phase Risks

Typical risks associated with the retirement phase are summarized in Table 4.4.

Table 4.4: Risks Related to Retirement of Global Information Systems

Issue Type	Hazard	Risk	Mitigation
Technical	Inadequate technology	Retrieval of data not possible throughout the retention period	Developing and budgeting for archive strategy that accounts for technology change. If this is not possible, develop a strategy that preserves essential information but not all functionality.
	Ineffective mechanism for removing system from use in a coordinated manner	Continuing use of system leading to invalid data updates	Planning a global exit strategy and ensure compliance with that strategy.
Supplier	Support of archival technology is terminated	Retrieval of data not possible throughout the retention period	Developing an alternative strategy to preserve information even without functionality, e.g., print to PDF.
	Inadequate retention and archival processes	Loss or corruption of data	Developing a viable and sustainable archive strategy. Periodically verify access to archived records.
User	Equivalent access controls not maintained after data migration	Inappropriate use of data	Applying the same criteria for protection of the archive as for the system, e.g., encryption, access control review.
	Inadequate data migration process	Loss or corruption of data	Validating data migration. Retaining a copy of the data prior to migration.
Regulatory and Legal	Lack of understanding of local regulations and laws	Applicable regulations are not met, e.g., data is not retained to meet specific local requirements	Reviewing and understanding local requirements. QA and Legal should be involved in this process.
	Conflicting international rules (e.g., GxP versus local data privacy law)	Applicable regulations are not met	Reviewing and understanding local requirements. QA and Legal should be involved in this process.

5 Appendix 1 – Project Phase Activities

The Project phase involves the refinement and finalizing of the business processes and their associated requirements, which should be reflected in the system user requirements.[6]

Business processes and associated requirements can include:

- Validation planning
- Risk assessment
- Supplier assessment and selection
- Various levels of specification
- Design
- Coding
- Verification leading to acceptance and release for operation

Supporting activities may include:

- QRM
- Traceability
- Design review

The Software Development Life Cycle (SDLC) that is to be followed by project teams should be defined and agreed at the earliest possible time, in order to ensure that the project phase is completed in a controlled and consistent process at all locations.

Pilot or prototype systems may be created and evaluated until a final design is identified that meets established requirements. Requirements, specification, and design may be assessed continuously and refined (revised) until an appropriate, complete, and consistent design configuration is achieved.

During system development, an established process for change management should be applied to specification and design deliverables (see *ISPE GAMP® 5* [4]). Project change control should be implemented at a suitable point, based on the methodology. For example, if the approach involves prototyping, change control cannot be applied effectively to changes to the prototypes. Doing so could cause significant and unacceptable delays, without providing tangible benefit.

While developing the global core, once a design is agreed it should be managed under project change control.

Changes made during a local project that can affect the global core should be governed by the operational change control procedures for core functionality.

[6] **Note:** that while the defined business processes are the governing factor, the final system design may not fully support the business processes; therefore, the business processes should also be supported via non-system based that activities. The processes and user requirements can remain the same.

In addition, if a local project team wants to modify global business processes, changes should be assessed appropriately (including approval) from a global standpoint. The evaluation of such changes needs to include consideration of the impact on validation, as it could make a portion of the global validation package inapplicable at the site wanting the change.

The specification and design process should be integrated with the QRM process (Appendix 6). The required controls identified during risk assessments should be captured in the appropriate documentation. Risks that are not sufficiently mitigated through system design should be noted and referenced for external mitigation (e.g., through internal procedural controls, service provider controls).

Specifications and designs should be reviewed and approved and the code placed under change control, before formal system testing activities begin.

A pilot or prototyping approach can allow for testing of individual modules before all design activities are complete, provided the design for the module being tested has been approved. Specification documents should follow established document control and change management procedures. Specifications should be updated as necessary when existing requirements need modification, or when requirements need to be added or deleted.

The aims and objectives of the pilot/prototype should be clearly defined in order to be effective. The pilot/prototype should be evaluated against these to ensure that the objectives are met. How information gained can be incorporated in a controlled manner into specifications for the final system should be defined. This requires version control and segregation of the pilot/prototype and final software.

Project phase activities may be shared between the supplier and the regulated company and should involve the key stakeholders associated with the development of the system.

Use of contracted off-shore software development, implementation, and/or testing should be carefully assessed and planned, to ensure that supplier standards are understood and acceptable, and that documentation produced meets the regulated company requirements.

For global information systems, care should be taken to ensure that any supplier audit results are acceptable globally, in order to avoid multiple audits.

5.1 Define Global Business Processes

A team should be established to develop new global business processes or to modify existing global business processes. This business process team should be composed of management and key users from critical locations. The team leader should be a senior manager. This team should form the controlling factor for the project scope and end goal:

1. This team's role is the development of a business concept exempt from any technical tool considerations.

2. IT/technical personnel do not have a role to play on this team.

3. This team may have to make some adjustments to business activities in order to use the system to meet the business process requirements.

The output from the business process team should form the framework/context that the user requirements team will use to develop the detailed business requirements and the Request for Proposal (RFP). IT/technical personnel can be of help in an advisory role.

The detailed business requirements should be developed from the global business process.

One or more members of the business process team should also be a member of the requirements team in order to:

- Keep them on track
- Prevent scope creep
- Clarify issues
- Help set the prioritization of the detailed business requirements

Changes to defined business processes should be made only by the business process team and only under formal change control documentation.

Defined business processes should have a designated process owner.

The output from the business process team can help to identify requirements for product evaluation, e.g.:

- The business process should be workflow controlled
- Multiple language support is required in all or specific areas of the business process
- Electronic signatures will be used for some of the business activities
- Specific reporting needs for different countries
- Minimum number of security levels needed

Members of the business process team should also be members of the URS approval group.

The business process team should develop role and security profiles. This information can be used to generate job descriptions for the global business process and for training materials. It can also be used to configure security profiles in the system.

The combination of defined business processes and role profiles can be used for proof of concept during prototyping or a pilot stage of the project.

Training needs to be globally consistent and it should reflect globally defined roles. The business community using a global information system should be able to demonstrate that they understand and follow the global business process which the system supports. The system should not go-live until this has been demonstrated by all levels users.

The business process team, or some of its core members, may become the change control team for the global information system. This can help to maintain alignment between business processes and the system configuration/ functionality.

5.2 Establish System Ownership

System ownership should be established at the beginning of the project. During the project, delegation of some decisions to someone in an operational role may occur. However, system ownership should be defined throughout the project, as many decisions require robust business input, including:

- Development and approval of user requirements
- Selection of the solution

- Most in-project risk assessments
- User acceptance testing
- Ensuring that appropriate training and SOPs are developed and/or established
- Approval of key validation documentation
- Final acceptance of the solution
- Approval of service levels
- Business continuity and DR planning

Data ownership should be clearly identified and understood. Business representative(s) should assume leadership and accountability for global information systems. Ownership of global business processes being managed should be identified.

5.2.1 Global Business Process Owner

The global Business Process Owner:

- Should have global authority
- Needs to have an operational understanding of business processes
- Is responsible for the:
  - Availability of the system
  - Support and maintenance of the system
  - Security of the data residing on that system

The global Business Process Owner is ultimately responsible for ensuring that the global information system and its operation is in compliance and fit for intended use in accordance with applicable SOPs.

5.2.2 System Ownership Team

The membership of the System Ownership Team should be kept at a minimum to ensure accountability. Membership could be based on function, such as R&D, manufacturing, and/or by geographical grouping, and will be dependent upon company structure, etc.

Typically, System Ownership Team members, other than the leader, focus on the:

- Local system access
- Implementation
- Maintenance
- User training

Regardless of membership, the ability to act should be aligned with predefined responsibility. Some ownership activities can be handled locally.

Where global information systems are developed to serve multiple and diverse business processes, ownership may be assigned to several parties. A formalized relationship should be established to ensure that the system develops and evolves simultaneously with the business processes. In addition, any potential conflicts of interest involving QA, as the global information system or Business Process Owner, should be clarified.

Formalized relationships, roles, and responsibilities should be documented, e.g., in an organization chart, and referenced from the Validation Plan, in order to maintain accountability. This should be updated in a timely manner when system ownership changes.

The concept of a CoE should be considered as part of establishing system ownership. For further information, see Section 4.3.2.

Whilst ownership should be internal to the business, third party involvement in support services or operations is becoming more frequent. However, even for SaaS solutions, a senior business authority needs to take accountability for the way the system is used and managed, as well as owning the relationship between the business and the supplier. In such cases, careful consideration should be given to any agreements regarding documentation, validation, availability of service, and maintenance.

5.3 Establish Project Organization

Using an established project management methodology can be beneficial. The following subsections discuss specific aspects of project organization that should be considered.

5.3.1 Stakeholders

An understanding of key representatives within an organization should be established at the beginning of a project. This should include individuals who have a direct interest in project drivers or are directly impacted by business objectives.

Engaging only with stakeholders located at the largest in-scope site may not be effective. An effort should be made to include a representative sample of stakeholders from as many sites as possible, Representatives selected should have the correct background, i.e., they should understand business processes.

On going communications regarding updates and progress should be managed in line with stakeholder requirements, along with a clear understanding of scope and funding.

5.3.2 Steering Committees

On global projects, the role of the global project Steering Committee is to ensure the timely and cost effective completion of the project in multiple venues on behalf of the regulated company. This may include building effective regulatory compliance mechanisms and processes.

The Steering Committee is typically made up of senior company management usually from some or all of the following areas:

- Project sponsor
- Global Project Manager
- Global Business Process Owner
- Key technical areas, e.g., Information Technology or Engineering

- Quality Assurance
- Representation of user stakeholders

The global project Steering Committee should plan to meet regularly. Meeting times should be related to the duration and milestones of the project, to help to meet project timelines. The global project Steering Committee should understand and consider local needs. It should be as globally diverse as possible, i.e., it should include stakeholders from user sites, not just headquarters.

The following agenda points should be included:

- Project progress
- Financial status
- Validation status
- Key implementation and/or technical issues with proposed solutions
- Facilitation of resource allocation for global and local tasks (this may apply to both the global and local Steering Committees)
- Resolution of conflicts between local/global or local/local priorities
- Resolution of other issues

Relevant decisions should be communicated to all stakeholders, both globally and locally, throughout the organization.

Depending upon the nature of the project and how much work is needed locally, local Steering Committees also may be appropriate. These should have the authority to manage the above issues if they are purely local in scope; otherwise they should involve the global Steering Committee. Local Steering Committees should serve as the escalation point for issues that need global attention in order to be resolved.

5.3.3 Project Structure

A choice exists between hierarchical and matrix project structures.

Hierarchical structures provide clear communication and line management control, but can have disadvantages where large projects and diverse disciplines are involved in a global project, due to locations and time zones causing communication difficulties.

Matrix structures draw resources from within a regulated company's normal functional organization and provide the Project Manager with the structure to manage by influence. A matrix structure capitalizes on an individual's motivation to achieve local needs, while being able to contribute to global solutions.
The matrix structure may need local project management representatives in order to operate effectively.

5.3.4 Project Manager

The role of the project manager depends on how the project is organized. Consideration should be given to deputies to support language, validation/compliance, or local needs, especially if a project manager's responsibility includes regions where the local language is different.

The project manager should recognize and be equipped to deal with cultural issues that may arise during the life cycle of a global project. Project managers should be able to anticipate potential cultural complications. See also Appendix 7.

5.3.5 Project Team

Members of the project team should be representative of the global interests of the project, including:

- Business
- Technical
- Quality Assurance
- Compliance
- Security
- Geographical
- Functional

The various disciplines and complexities surrounding the business processes and technologies should be considered when assembling the project team. Face-to-face meetings of the team are recommended at the beginning of the project to help to enhance teamwork.

Consideration should be given to establishing:

- A core team with overall responsibility for delivery of the global information system
- Local project teams familiar with local business processes and with the authority to alter them, if necessary, based on business or regulatory drivers

Typically, the local project team will lead site implementation and apply the lessons from the pilot and any preceding installations. Local project teams can also be helpful in supporting training and rollout. A global resource with experience implementing and validating the application at another site should also be involved. This may be someone from a CoE, although someone who had worked on another local implementation could also fill this role.

Global and local teams should be given the same training in project standards and methodologies, so that all project teams can produce deliverables that are acceptable globally.

Smaller regulated companies may not have the capability (or the need) to support separate local teams. In such cases, local input should be collected. Local resources may be brought onto the global team, temporarily.

5.3.6 Supplier Involvement

Suppliers can be involved in projects in various ways, e.g.:

- SaaS suppliers who own, validate, and manage an application
- Implementation partners who may manage part of the project
- Specialists who work only on the validation and compliance
- Contracted programmers or testers

The level of responsibility and accountability of suppliers should be recognized; however, regulators will hold the regulated company accountable for any irregularities or violations of regulation.

When using off-shore resources, project managers should be aware that some processes that work well locally can be more challenging when done remotely. For example, validation testing using a paper-based process can work adequately if performed locally, but can be more challenging to manage if testers are based several time zones away. The availability of test automation tools can be beneficial. See the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition)* [21].

5.4 Pilot Projects

Pilot implementations are usually planned for most global projects, because of the associated level of complexity. This allows the project team to:

- Gain experience with the process of implementing the system
- Build expertise within support organizations
- Understand the effect of the transition on the business area

Selecting a smaller site for a first pilot can reduce possible negative effects and may improve the speed of fixing any problems, because of the smaller affected population. A very small site may not be suitable for a pilot, however, as it may not be representative.

The availability of resources should also be considered in selecting a pilot site. Pilots may be run at a headquarters site is because it is where IT resources are concentrated. Cost savings and ease of support should to be balanced against size considerations.

For very large projects (e.g., an ERP system) global resources may be leveraged, in order to do multiple pilot projects, such as implementing the first manufacturing support implementation at Site A while at the same time piloting the finance modules at Site B. This can be an effective approach, as it simultaneously involves both IT and user groups that do not typically support the same area.

There also may be secondary resource considerations. For example, if the same data center supports both it might be beneficial to stagger the target dates, so that data center staff are not overwhelmed by simultaneous demands.

5.5 System Architecture

The architecture choice has a significant effect on the approach to the implementation project, and on both the nature and ownership of validation work. Different architecture options are discussed in Appendix 3 of this Guide.

If the approach is to use IaaS or PaaS, the project could be managed in a similar way to other implementations. For example, if a global implementation of a customer call center management application were to be built on a specific SaaS platform, the project would usually be managed in a similar way to an internal project that builds an application around a commercially available database engine. At the highest level, both approaches are building business software around a database. There are, however, differences because the former is almost entirely outsourced and the regulated company has little, if any, control over the development processes.

Another major high-level difference for both IaaS or PaaS approaches comes in designing the support processes. For example, a SaaS supplier may have a quarterly update process that is not optional, and some of those updates may cause an unexpected effect on the application, which may in turn drive an unanticipated change. IaaS may have fewer issues of this type, but they exist because of events such as operating system upgrades.

SaaS is different in that the application will be built, managed, and owned by a third party. This generally means that supplier resources will be key for implementation. Consideration should be given to having a supplier project manager as part of the implementation team. This could be critical for a pilot implementation. Some access to supplier expertise will still be needed, although team membership may not be necessary for subsequent implementations.

Project planning for a SaaS implementation may be simpler, as there is no need to set up support processes. Support processes are owned by the supplier and should already be operating effectively. The support processes should be evaluated to ensure that they are adequate to support regulatory requirements.

5.5.1 System Architecture Validation Considerations

SaaS suppliers should own the validation, so that change control processes at the supplier accept a large portion of the validation burden. This should be one of the principle considerations when negotiating a contract with a SaaS supplier. There should be serious reservations about adopting a GxP solution without such ownership.

Note: although the SaaS supplier may own validation as a task, the regulated company is accountable for it. The regulated company should, therefore, review supplier generated validation documentation and take action where appropriate.

5.5.2 Supporting SaaS Validation

The regulated company should set up support processes to deal with system updates, even if the SaaS supplier accepts validation ownership, because updates are inevitable and there will probably not be an option to decline to accept them. Some suppliers that are focused on life science and healthcare may offer the option to defer updates, but this is exceptional rather than the rule for SaaS suppliers. This could be a factor in supplier selection.

The lack of an option related to updates means that if the supplier is on a quarterly schedule, validation resources need to be available:

- When the updates are released
- At the global level
- Possibly at the local level

It is unlikely that there will not be flexibility for timing of updates.

The contract or SLA with the supplier should include a provision requiring a brief validation summary report with scheduled releases. The requirement at the regulated company would be to assess the change and decide whether and how much of their own testing and documentation is needed, based on the way the system is configured and used. The need to generate validation documentation at the regulated company is unlikely to be removed by a supplier validation report. For example, testing at the supplier will be based on data that may not reflect actual business data, and this may require some level of User Acceptance Test (UAT) with validation impact.

5.5.2.1 SaaS Validation – Setting Expectations

If a regulated company decides to adopt a SaaS solution without any supplier ownership of validation, processes similar to those described in this Appendix should be designed, but on a much larger scale. Validation work could be substantially more extensive and complex, but timelines are unlikely to grow correspondingly. Planning should ensure that adequate resources (manpower and financial) are included that reflect this. It is also necessary to consider what will be done if validation reveals a flaw in the release and the supplier is either unable or unwilling to fix it immediately. If backing out the change is not an option, the application business owner may need to decide at what point to discontinue using the global information system and disrupt the business process.

Regulated companies may have internal validation policies that reflect the validation of systems that they own and control. These may not be entirely applicable for all architectures. The validation plan, and possibly the project plan, should acknowledge any inconsistencies and should detail the approach to addressing such problems.

5.6 Validation Planning

Validation planning should commence as soon as practical after the start of a project. Validation activities make take longer when multisite considerations are taken into account.

5.6.1 Regulations

While global regulations are reasonably consistent, they are not completely identical. Differences exist between GxP communities and between the regulations of some geographical regions and countries. A risk-based global review of applicable regulations and de facto standards should be performed and agreed early in a project life cycle, as these can impact the global information system design. For example, the degree of formality of electronic signatures for approval of project specific documentation should be addressed throughout the project.

Other regulatory areas and topics that should be considered are listed in the Table 5.1.

Table 5.1: Regulatory Topics for Consideration

Topic	Concern	Issues Unique to Global Information Systems
Audit Trails	Data Integrity	Minor differences in health authority expectations may drive a more rigorous global process in order to satisfy all regulatory expectations. Need to carefully and clearly define policy for audit trail review (EU GMP Annex 11 [1] requirement).
Backup	Data Integrity Business Priorities	There may not be a convenient and appropriately long window to run backups while the system is idle.
Change Control	Data Integrity Validated State	If there are local instances, inadequate or uncoordinated management of change can result in drifting, to the point where the instances are not equivalent.
Configuration Management	Data Integrity Validated State	If there are local instances, inadequate or uncoordinated management of configuration can result is drifting, to the point where the instances are not equivalent.
Security	Data Privacy	Data protection laws vary greatly between jurisdictions. The solution has to be robust enough to meet them all.
Business Continuity/ Disaster Recovery	Data Integrity Business Operations	Different locations may have significantly different sensitivity to business interruption. Sites may also be dependent on data drawn from other locations.
Document Management	Data Integrity Audit Response	Paper records can be difficult to share internationally. Electronic documents are easier to share but have to comply with regulatory expectation for control.
Facilities	Data Integrity Business Operations	Data centers need to be able to accommodate expected growth, and they should be able to provide adequate incident response for all time zones they support.
Incident Management	Data Integrity Business Operations	Incidents should be easily reportable for all sites, potentially in various languages. Service levels need to account for timely response to incidents in all supported venues.

Table 5.1: Regulatory Topics for Consideration (continued)

Topic	Concern	Issues Unique to Global Information Systems
System Performance	Business Operations	Servers should be sized to support intended loads. Attention should be paid to periods of high usage, e.g., mornings in North America/afternoons in Europe.
Network Performance	Business Operations	Bandwidth should be adequate to support all sites, especially at times of heavy network traffic. Network latency should be a considered during planning.
Personnel	Data Integrity Business Operations Data Privacy	Personnel require training relevant to all applicable jurisdictions. Staff size needs to be adequate to support at peak demand.
Quality Management	Data Integrity Validation Integrity Business Operations	Principles of QRM should be applied considering global risk. For example, if an application is relevant to drug safety tracking in only one of ten sites, this consideration needs to be included in overall planning and may impact processes at all sites.
Raw Data	Data Integrity	Raw data should be defined and understood in a global context, and processes to secure the raw data may be impacted globally based on the needs of one site.
Record Retention	Data Integrity Compliance with Predicate Rules	Retention requirements vary significantly based on jurisdiction. This is especially true for private data. The rules for each applicable jurisdiction need to be understood, and business rules for managing that data need to be developed. The application needs to be designed to meet the relevant laws. In some cases, various laws may be in conflict. The Project Manager needs to engage the appropriate resources (e.g., legal, QA) to define what processes should be developed.
Security Management	Security Data Integrity Data Privacy	Processes for granting, disabling, and revoking accounts need to be consistent and follow a globally defined standard. If encryption is appropriate it must be compatible with all local infrastructures.
Risk-based Compliance	Risk Management	Risk-based compliance decisions should take into account the compliance needs of the global business community, i.e., the strictest regulatory expectations should be the basis for risk decisions.
Signatures	Electronic Records/ Electronic Signatures (ER/ES) Compliance	Electronic signature processes, if used, should be compliant with all relevant jurisdictions.
Supplier Evaluation	Validation Integrity	If a supplier is supplying goods or services out of multiple locations globally, the assessment should verify that the same processes are used at all locations or evaluation of separate locations is probably necessary. It is generally the supplier's responsibility to qualify subcontractors, and it may be desirable to request evidence that they have done so.
System Retirement	Data Integrity Business Operations	The system may not be retired globally all at once. Provisions during a phased retirement need to allow for continued support at sites still running. Data migration to a new system needs to be managed while the old one is still running.

A Risk Management approach should be taken, based on the global requirements.

Conflicting requirements that arise from the variety of perspectives in a global review process should be addressed with agreed requirements and documented, e.g., in the URS.

Where a regulated company anticipates business in new geographical areas, corporate policies regarding regulations and de facto standards should be reviewed and updated.

5.6.2 Validation Approach

Planning should cover all required activities, responsibilities, procedures, and timelines. Activities should be scaled according to:

- System impact on patient safety, product quality, and data integrity
- System complexity and novelty
- Outcome of supplier assessment

The global information system owner should be able to manage both the system and validation documentation. The adoption of a single standard for a SDLC and validation for a global information system can be helpful in this regard. Uniform templates or document structures can simplify the process and transferability of the documentation can also simplify the regulatory audit process.

A review of critical global project success factors (cultural, regulatory, architectural, and procedural) as they relate to validation should be performed. Unresolved issues from overall project planning need to be addressed quickly during validation planning, to assure the project does not lose momentum. Validation planning should start with the involvement of a validation representative during initial project planning. Validation planning should reflect and support a pilot/prototype or lead implementation approach to the system.

A determination should be made regarding whether the global information system will be centrally or locally managed. There may be local elements or considerations for a project, even if the system is centralized. Generally, there will be some level of core validation activities. Core validation teams and local validation implementation teams are usually separate. Occasionally, core validation work can be completed by a local validation team, in which case their site is known as the host or sponsor site. Considerations when using a host validation team include:

- Level of attention that should be given to ensure that the core work would support basic validation requirements of other sites. If other sites are not satisfied with the work of the sponsor site, it is likely that they will redo the core validation in addition to their site validation activities, which will increase time and cost.
- Sponsor site should be in a position to complete the core validation activities prior to the planned rollout to other sites to maintain project momentum.

5.6.3 Validation Plan

The Validation Plan should focus on aspects related to patient safety, product quality, and data integrity. It should summarize the entire project, identify measures for success, and clearly define criteria for final acceptance and release of the system. The plan should define:

- Activities required
- How activities will be performed
- Responsibilities (including a clear definition of global versus local versus supplier responsibilities)

- Expected outputs
- Acceptance criteria
- How compliance will be maintained for the life time of the system

The level of detail in the plan should reflect the risk, complexity, and novelty of the system.

The Validation Plan should specify whether the core validation team members will assist the implementation team or whether there will be a formal technology transfer between groups. The role of the core validation team, implementation teams, local validation departments, and various quality departments needs to be defined. It should be understood and agreed that validation documentation generated should satisfy the local requirements at each site deployed, including those related to format, approval process, and authorization, to implement requirements that may be specified in local procedures. See Appendix 4 for additional information.

Particular attention should be given to the coordination of signatures and a clearly understood strategy should be defined in the Validation Plan for timely approval of key deliverables. Supporting tools, including the use of electronic signatures maybe considered. In addition, effort should be made early in the project to plan the verification strategy both for efficiency and, if using the development system for formal testing purposes, effectiveness.

Other Items to be considered include:

- **Approvers:** should include the author, the Business Process Owner, and QA, with the plan having a detailed review by project team members. Global plans should be signed by people with global authority, local plans should be signed by people with local authority. It can be beneficial to require at least one global approval on a local plan in order to ensure consistency with the global vision. This can be a member of the CoE.
- **Distribution:** controlled versioned copies of the global plan should be made available for each local site or end user group. The CoE should have a copy of each local plan.

For further guidance on validation planning, see *ISPE GAMP® 5* [4].

5.6.4 Supplier Assessment and Selection

Suppliers, including those for IaaS or PaaS components of the system, should be assessed to establish their quality capability. This is typically performed by an SME and may involve an audit of the supplier depending on risk, complexity, and novelty. The assessment may find that a supplier has either a well-established, formal, QMS, or has attained a recognized third party certification, such as ISO 9001 [22]. The strategy should take account of assessment conclusions.

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

Suppliers should not be forced to use company templates, as these often require context and specific knowledge that may seem trivial within the regulated company, but could be confusing or ambiguous to suppliers. If the supplier asks for such templates extra effort may be needed from both parties to ensure the documents generated using them meet expectations.

The capability of the supplier to provide expected support should be part of the assessment. This should include support expected globally, with particular attention to their ability to deal with the demands of sites outside of their time zone. If there are sites with local differences in the implementation of the system, the supplier's ability and willingness to support them should be evaluated (see Appendix 8).

For further information on supplier assessment, see *ISPE GAMP® 5* [4].

5.6.5 Procedural Considerations

Generally, when conducting a global information system implementation, more planning is required for system management procedures than might be considered normal for a purely local project. Differing local needs, resources, availability of appropriate expertise, and the desire of global management to standardize can pull otherwise straightforward procedures in opposing directions.

The following list includes key areas to address for global information systems:

- Change control
- Configuration management planning
- Security management
- Training
- Backup and restore
- Archive management
- System documentation management
- Periodic review

5.6.5.1 Change Control

There are two levels of change control that should be planned for:

1. Project change control
2. Operational change control

Managing change globally is one of the most challenging aspects facing a global project team and a global information system owner. Failure to do this well can lead to project delays, software bugs, and regulatory compliance problems.

Project Change Management

The project team should manage the scope and keep resources focused on value adding tasks. In this regard, version control is a principle concern for project specifications and supporting documentation. Co-ordination of groups working across multiple sites with a common objective is considered key. For example, if a developer changes a variable name in a module, but neglects to post the new version, colleagues on other sites may have great difficulty integrating it with their module. Similarly, if a user requirement is changed but not communicated then it will not be reflected in the delivered software.

Project teams should define a procedure for evaluation, relevant approvals and communication of changes along with retention and separate archiving of superseded versions. This definition should include the start and end points for project change control. For example, changes during prototyping activities could be a significant burden if change control were required without significant benefit. The point at which project change control should be superseded by operational change control should be selected to ensure that the integrity of testing is preserved.

While the level of formality of project change control need not be as rigorous as operational change control, change should be managed and controlled. This includes recognizing that changes made at a global level can have unintended effects at a local level. For example, a change in the approach to data management at a global level could result in noncompliance with a local data privacy law.

For further information, see *ISPE GAMP® 5* [4].

Operational Change Management

Project planning should include consideration of how changes will be managed after a system goes into production. One of the prerequisites for placing the system into production should be a change control SOP. One or more existing change control processes may need to be assessed in the context of the new application, both in terms of whether they will meet the technical needs for the system and in terms of whether they will meet the global organizational and regulatory needs. An enterprise change control SOP that defines core processes should be in place. A system specific SOP may be needed where the enterprise change control SOP does not adequately cover aspects of managing the changes globally.

The concerns discussed relating to project change control are still valid issues, but more formality is required around approvals and documentation. Many operational changes will require approval from a delegated QA representative, in addition to the System Owner (or designee). A global change control process should be established, to help with approvals and with notification of the appropriate people. Notification may need to extend to the global business community, if the change affects how they use the application.

For further information, see Appendix 2, Section 6.1 and *ISPE GAMP® 5* [4].

5.6.5.2 Configuration Management Planning

Configuration management is interconnected with change control, both during the project and in the operational lifetime of the application. It is advisable to plan a process that places the configuration data at one location (logical or physical). An individual should be designated as responsible for the data. While there may be some local differences due to diversity of local operating environments, such a measure makes it easier for the globally responsible persons to manage the overall configuration listing, with noted deviations. Rigorous configuration management should be applied where coding occurs at multiple locations.

5.6.5.3 Security Planning

Global information systems should adhere to a global minimum security standard and security planning should reflect this. Enterprise security standards should be established in the context of the global information system. Where existing minimum standards are not adequate, appropriate standards should be defined. If applicable local data privacy law sets minimum security (e.g., an encryption requirement) standards, the global information system should meet or exceed the most rigorous of each local requirement. Issues that should be managed to such standards include:

- Password format, complexity, and expiry
- If merited by risk, automated logoff after a designated idle period
- Restriction of administrative rights to those with a legitimate need
- Requesting, granting, modifying user accounts
- Role-based security, as appropriate. For global information systems, this can be managed using Active Directory or Lightweight Directory Access Protocol (LDAP) services. Use of Single Sign-On (SSO) technology can relieve the service desk of covering password reset requests.

- Measures to ensure that access rights are revoked for personnel who no longer require access to the system
- Electronic or digital signature standards, if applicable
- History of access rights
- Security policy

These factors can all be managed centrally. Some factors, such as the authentication of new users or revocation of access rights for former employees, have components that may be managed more effectively locally. Planning should reflect this, so that these factors can be incorporated into operating procedures and local/central coordination established.

5.6.5.4 Training

Training can adopt the following approaches:

- A small group of expert users can be trained in order to train all other users. Such a group should take into account local cultural issues and needs. While this group can often be drawn from users who help with user testing (e.g., UAT), care should be taken to ensure that anyone drawn into training activities is actually an effective trainer. Technical expertise does not always include an ability to communicate that expertise to others.
- A train-the-trainer approach, training a representative from each location or local grouping, drives a consistent approach but requires global monitoring of local trainer quality and expertise. **Note:** this approach can present a risk of knowledge drop-off, as knowledge transfer may not be entirely effective. This can be mitigated by developing appropriate training materials and providing the trainers with ongoing rapid response support.
- Outsourced training to companies with global resources to provide consistent training at several locations, which also requires global monitoring.

It is beneficial to consider the medium to be used, as communications such as web-based training, can be efficient. These should be supported by appropriate additional local or accessible central expertise.

A comprehensive set of user manuals and procedures, which are maintained and readily available, should be included as part of the process for training new users after a global information system has gone live and the project team has been disbanded.

5.6.5.5 Periodic Review

The need for a periodic review of a global system, particularly for distributed systems, is greater than for single-sited systems and should be planned at the implementation stage. For further information, see Appendix 2, Section 6.11.

Periodic review should be conducted as often as warranted, normally at least every three years.
Consideration should be given to a shorter time frame if the system is subject to frequent change or its proper operation is problematic and has associated business risks.

It may be necessary, as a result of a periodic review, to reinforce validation with additional work or to revalidate the global information system in its entirety (in unusual and extreme cases where control has been lost). For further information on the periodic review process, see *ISPE GAMP® 5* [4].

Periodic reviews should result in formal reports with the same approvers as the original validation report (minimally the author, Business Process Owner, and QA). This should include global personnel for the global elements, and local signers if a local review is warranted. Copies of the local review should be provided to the CoE so that they can ensure that local drift is not a problem.

5.7 User Requirements Specification

A commercial software tool should be considered in order to manage requirements, as a global information system is usually large and complex. This can also make using a traceability tool easier, see Appendix 1, Section 5.9.

The first step in the specification of global user requirements is to define the scope of the business processes. The presentation of this in a flow diagram format can be useful in cross cultural, multi-lingual projects. It can be valuable to indicate which processes and desired functionality are regulated (e.g., GxP, privacy, Sarbanes-Oxley Act of 2002 [20]). Overall scope should be defined at the local and corporate (integrated) levels and common processes extracted into a standard global business process. Differences should be detailed in local level process definitions.

Where legal and/or regulatory considerations impact requirements, a globally accepted common interpretation of applicable regulations is considered essential. If there are any local differences intended, they should be:

- Defined
- Analyzed for possible unintended consequences
- Carefully documented
- Approved

When defining business processes, data requirements may be neglected or gathered separately. However, when defining global business processes, particular attention needs to be given to setting standards for data that is shared. The requirements for interfaces, both input and output, need to be well understood and well documented, as this is a particular vulnerability for data integrity problems. Latency, both between peripheral devices, such as barcode scanners or instruments, as well as global network latency, needs to be understood and addressed as necessary.

Integrated multi-site, multi-discipline business processes may be too complex to define in a single model. The core business process should be presented at a sufficiently high level that all key integration points are identified. Subsequent levels of detail can be expanded upon, once defined. This may be managed in multiple requirements documents, or in a single multi-tiered document.

The Business Process Owner can take the responsibility for all the regional business process definitions or establish a guideline format for individual sites to use. The business process team needs to agree on where the core business process definition ends and where the local business process definitions starts. Formalizing this decision can help to avoid miss-communications.

Business process definitions should form the basis of, or be referenced from, the overview section of the URS.

The URS should include the definition of global processes against local requirements, which should be aligned and harmonized before attempting their automation.

For global information systems, the comprehensive requirements list should:

- Aid in the understanding of requirements, both local and global
- Expedite the URS approval process
- Reduce the risk of conflicting requirements

A substantial portion of the user requirements can be written directly from a review of well-defined business processes using, e.g., flow diagrams.

Regulated companies may also have templates of typical requirements by system type that relate to, e.g., security and other common elements.

Fully represented user involvement is strongly recommended throughout and should be included in an approvals process, but without making the process unduly bureaucratic. User involvement should include SMEs from different disciplines, e.g., privacy experts can help by reviewing GxP functionality. This can minimize the risk of compliance issues being overlooked, and may help to improve the URS by ensuring that it is clear and comprehensible.

For further information, see *ISPE GAMP® 5* [4].

5.8 System Specification and Design Review

The review of specifications and architecture should evaluate whether the design adequately addresses the mitigation of previously identified risks. It may be possible to mitigate some risks by design.

Core and locally specified functionality and/or design should be identified. A globally consistent naming or numbering system for traceability and subsequent testing should be implemented. This can help to ensure that all key elements are reviewed and tested.

Defining the system architecture should consider factors such as:

- Design
- Administration
- Environments
- Performance

For further information on supplier assessment, see Appendix 1, Section 5.6.4.

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

For further information on Functional and Design Specifications and on Design Review, see *ISPE GAMP® 5* [4].

5.9 Traceability Management

There are different mechanisms that exist, both administrative and tool-based, that can be used to demonstrate traceability. One such mechanism that illustrates the principles related to global information systems is considered in this section.

A primary issue with a global information system is maintaining consistency between local and global modifications, and maintaining traceability. While a traceability matrix managed in a spreadsheet can be a viable method for small systems, it may not be feasible for a large global system. In general, an electronic tool may a better solution for any large and complex system, especially when managing numerous one-to-many or many-to-one relationships.

The need for comprehensive system documentation to control a system is driven by personnel turnover and changes to a system. Traceability is an integral component of this system documentation. When combined with procedures and training from the start of the project, traceability can help to ensure the integrity of the system.

The topology of the global information system needs to be considered when:

- Developing the traceability solution
- Designing the business processes to maintain that traceability solution

For a global information system shared across a network that is maintained in one location, traceability can be handled through a core team leading to limited additional complexities over a single site system. In this case, it is important to have clear ownership of the tool and to ensure for the transfer of responsibility when the owner is changed.

For a global information system where local customizations are permitted, robust procedural controls are necessary to assure ongoing integrity and consistency of traceability and related documentation. An organization of local, core and global traceability tool owners should be documented and described in a procedure. The procedure should also document the process to maintain the tool. Management issues of staffing and training need to be addressed, to ensure continuity of responsibilities and proper coverage at all locations.

A global information system can be used in many different cultures. Documentation should be understandable within those cultures without the assistance of the project team. This requires a naming and numbering convention for the documentation that is easy to administer and well documented, so others can easily learn and apply the convention. This can be beneficial in creating a meaningful traceability matrix.

The approach used should ensure ongoing compliance across multiple languages and personnel changes that may occur over an extended timeframe. Information that should be traceable can include:

1. URS Reference Number:
    - All user requirements should be tracked.
2. Description:
    - This can be optional; however, including the full URS section, or a brief reference, can be helpful when using the tool. Including key words that identify specific types of critical functionality, e.g., security, audit trails, calculations should be considered.
3. Scope of Requirement (local, core, or global):
    - The scope that the URS section affects should be listed, such as global, core, or local. This scope will also identify which area has responsibility for maintaining this section of the tool. When there are multiple local areas, the specific local area that the URS section affects should be included.
4. GxP or regulatory impact:
    - If there is a GxP, or other regulatory impact (e.g., Sarbanes-Oxley Act of 2002 [20] or data privacy), then there should be a test reference, or a reference showing how this requirement was verified.
5. Functional or Configuration Specification Reference:
    - This links the URS to the way in which a user requirement is met. If the URS section will not be satisfied by the system, this should be made clear by an appropriate notation, such as “Not Met”; or an SOP reference that is used to procedurally satisfy the URS. Some requirements may be met by means other than software, and verified by means other than testing.

6. Design Specification Reference (for internally developed software elements only):

    - For a bespoke system the Design Specification that defines how the Functional Specification is met should be included.

7. Test or Verification Reference (e.g., installation, integration, acceptance test):

    - A reference to a specific test should be included where there is GxP impact. It can be beneficial to include this information where there is no GxP impact, to assist in testing to requirements.

8. Comments:

    - Comments that add information, particularly where reference needs to be made to additional testing or requirements that have arisen as part of this exercise, should be included.

The numbering convention needs to accommodate the parallel activities and allow for each area to update their sections independently from other areas, as the total system traceability will be the integration of the global core and local traceability.

Documentation numbering conventions should provide sufficient detail to allow traceability from specific requirements to executed test scripts. Definitions with examples should be developed to train personnel on the conventions and to describe how the detailed requirements will be traced.

Global project managers may consider developing global documentation traceability that clearly indicates governance at global or local levels and how the documentation cascades down.

For further guidance, see *ISPE GAMP® 5* [4].

5.10 Environments

The use of development, testing, and production environments and their synchronization and relationships are potentiality more complex when they are to be made available on a global basis. The intended approach should be established during the project phase. From the standpoint of control and simplicity the ideal case is that everyone works in the same environments; however, some regulated companies will elect to provide local flexibility in that regard.

Issues to be considered when environments are set up and established include:

- The level of customization of the software to be allowed locally will dictate the scope, boundaries, and degree of control to be exercised by the centralized development and testing team.

- The level of similarity with the production environment should be managed, as the test environment may not be an exact copy of the actual production system, due to the complexity of the system. Test and production environments need to be effectively identical.

- The level of testing that can be performed on test and production environments should be managed and coordinated. Generally, functional testing should be conducted on a centralized and controlled testing environment, with consideration given to "whole system" testing in a production environment or a mirrored preproduction environment with databases refreshed from production.[7] One useful technique can be to test during shutdown periods with subsequently refreshed databases.

[7] **Note:** while copying production data to test environments can solve some problems, it may create others, e.g., the need to manage privacy-relevant data appropriately might require encryption of test databases and additional controls for managing test data. This becomes more complex when laws and regulations for multiple jurisdictions have to be considered. Masking or scrambling data may be a necessity in order to comply with relevant legislation.

- Deployment of software from a global testing location to local sites should be addressed. Effective planning and establishment of controlled procedures can help to resolve potential communication and timing issues along with any additional retesting that may be required as a result. Communication and timing are considered critical issues if parallel testing is to be performed at multiple sites.

- Virtualization can be leveraged for several reasons that can make system development and management easier, e.g., simplification of management of development and test environments. This may be how SaaS providers supply test or sandbox environments.

Once deployed and operational, clearly defined procedures covering development and testing at both centralized and local levels should be developed. It may be necessary to maintain a dedicated team of developers and testers to support continually the system.

5.11 Testing

Careful analysis should be performed when planning testing to determine the functionality that can be tested centrally. Generally, core system functionality will fall into this category, while any parameters that may depend on unique local configuration will need to be tested locally.

In general, testing of the core functionality should be done centrally with subsets of testing for confidence to be considered locally, along with any local installation or functionality testing. Local sites may require testing for connectivity, such as in integration testing. Risk assessment can play a major part in directing test effort to focus on key functions and processes.

Performance testing should be defined with the relevant parts conducted centrally and locally. For distributed systems, this may be executed locally. Different sites or departments of a regulated company may use different versions of a browser, or different browsers, to access a global application. Verification of the proper function of all authorized versions of all authorized browsers should be included in testing. Performance testing should also verify that latency, both network and potentially with peripheral data sources, does not compromise data integrity.

Considerations for test planning include:

- Standardization of documentation
- Automated test tools
- Deviation handling
- Test script error handling
- Handling of test failures
- Review of test results
- Change management
- Regression tests

In addition, global information systems will tend to have a greater number of interfaces to consider, although the issues are similar as for other system interfaces. Application architecture effects on validation strategy are covered in Appendix 4 of this Guide.

Regulated companies have an opportunity for synergy and cost savings in regard to documented testing of a global information system. These savings can result from the distributed use of test results done centrally or at one of the user sites. The various local sites need to have confidence in both the people and the process, however, in order to take advantage of this.

For further guidance on all aspects of testing, see *ISPE GAMP® 5* [4] and the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition)* [21].

5.11.1 Standardizaton of Documentation

Defining test templates on a global basis can:

- Help to ensure that local testing is conducted in a consistent manner, which complies with global practices
- Help to give a more seamless appearance to the local validation package, which should be a combination of global and local documents
- Present a uniform appearance to regulators who may evaluate the system at one or more local sites

5.11.2 Automated Test Tools

While the initial work of developing the automated scripts can be several times more than is required for manual scripts, the payback from using automated test tools can be substantial, including frequent reuse and assistance in improving the overall quality of regression testing on a global basis.

The core team should, therefore, consider the likely level of change and the need for regression testing when determining the use or need of automated test tools, especially throughout the operation phase.

Automated test management tools can be useful in managing the distributed test effort and making the output and status visible.

5.11.3 Deviation Handling

Deviations from the planned test process that have purely local effect should be handled locally and according to the established deviation management process. Some deviations may have more significant effects; therefore, all deviations should be reported and recorded to allow a global impact analysis and appropriate monitoring and closure to occur. For example, if a module that was planned to be tested as part of the core cannot be so tested, this may mean that all of the local sites need to execute the testing, or that a portion of the core testing will be shifted to another site. Such deviations should be communicated to all of the local project teams that may be affected. This is generally accomplished via the existing communication channels between the core team and local teams.

A local deviation could have global significance. In all cases the local team should communicate the deviation to the core team and should also solicit advice for how to deal with the deviation in a manner least disruptive to other sites.

5.11.4 Test Script Error Handling

Errors found in test scripts need to be communicated quickly to all potentially affected sites so that the impact can be evaluated. Sites that have already executed the testing need to determine whether the error was found there, whether it was missed, and what the implications are regarding the validity of the test results for that script. Sites that have not yet executed the test need to decide whether the script needs to be changed before the test is carried out.

5.11.5 Handling of Test Failures

For tests that failed to meet acceptance criteria and the cause of failure is not attributable to the test script, a documented evaluation needs to be done to determine whether the problem is local or due to problems with the core. A local investigation should be executed, and the results documented and reported to the global team, even if the cause was purely local. This may help another site avoid a similar problem later. If the local team decides the problem is due to part of the core, a documented analysis will have to be done to determine the cause of the problem, find a solution, and decide to what extent the validation is affected. When the determination has been made, the core team should notify local teams if there is further required remedial action on their parts and a timeline for this work to be completed and agreed.

Test failures should be handled in accordance with approved change control or configuration management procedures.

5.11.6 Review of Test Results

Test results should be reviewed by an appropriate SME. In general, this can be a global SME for globally managed testing, and a local SME for local testing. This can be reversed if either party deems it desirable.

5.11.7 Change Management

During local or global testing, control over testing environments should be managed and maintained. The process should be fully defined and well understood, so that changes to core software do not impact local testing or vice versa.

5.11.8 Regression Testing

Where changes are made to core software during and after initial implementation there should be an impact assessment that identifies the need for additional or repeated core testing. Additional testing may also be required locally. Careful consideration should be given to the planning and rollout of such tests.

5.12 Validation Reporting

One or more validation reports should be produced summarizing the activities performed, any deviations from the validation plan, any outstanding and corrective actions, and providing a statement of fitness for intended use of the system.

Validation planning together with the scope and design of the global information system will determine where reports are generated, and how they are communicated and made available for reference. A single core validation report should be produced with local Validation Reports produced where locally installed hardware and/or variations to functionality exist. These can either refer to the core Validation Report or all reports can be summarized within a global report.

For further guidance on validation reporting, see *ISPE GAMP® 5* [4].

5.12.1 Core Validation Report

The core Validation Report should be written in the corporate language. Items to be considered include:

- **Author:** ideally the author of the Validation Plan, who has been involved throughout the project and has global compliance and validation knowledge, will produce the report.

- **Approver:** core team members, who include the Business Process Owner, QA, and a technical representative, with the report having a detailed review by project team members.

- **Distribution:** controlled versioned copies should be made available for each local site or end user group.

5.12.2 Local Validation Report

The core Validation Report should be referenced in any local Validation Report. This will demonstrate appropriate testing coverage of system functionality globally and locally.

Local Validation Reports may be written in local language, with an executive summary in the corporate standard language to be considered, which briefly summarizes the purpose, scope, and conclusions of the report. Due to global regulatory needs, it is likely that an executive summary will be written in English.

6 Appendix 2 – Operation Phase System Management Processes

Providing support for, and maintaining, a validated global information system can be as challenging as the initial validation effort. Although the desired deliverables are, for practical purposes, identical to purely local systems, the challenges are not. Maintaining a global information system is more complex a task. The following are key processes for successful management of a global information system throughout its operational life.

6.1 Operational Change Management

Change control is necessary during the project and system validation (see Section 4.2 of this Guide) and during the operational life time of a system. The main variable is the degree of formality of the change process.

The basic process for operational change control should be defined and managed. It should be as simple as possible, e.g., the number of operational handovers, especially between different sites, should be minimized.

A software tool that tracks change status, permits updates as the change progresses, and allows electronic approvals can be a help to deal with the complexity. Write access to the change management tool should be given to personnel who monitor, control, and execute changes. Read access can be widely available. Further role-based restrictions are also advisable. For example, someone whose role is limited to approvals should not be able to edit a change record. In a global information system, the impact of a missing or inappropriately modified record is potential greater because of scale.

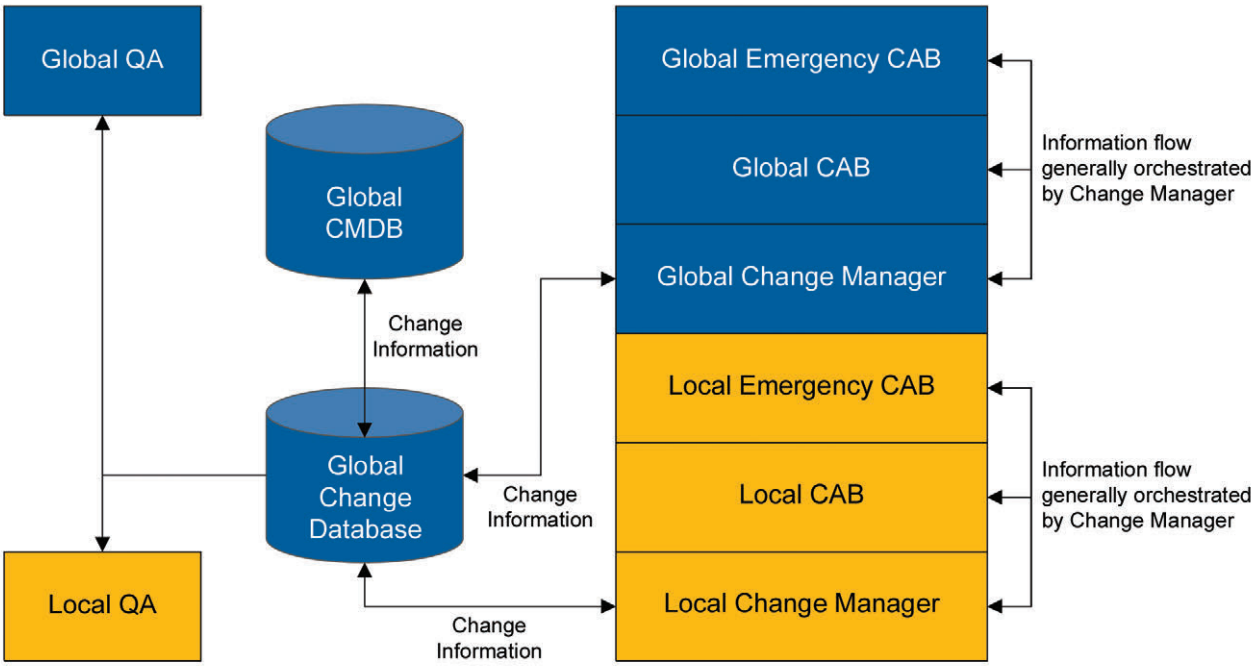
Change control presents several challenges that are magnified when considered in respect to a global information system:

- Notification:
  - Not all changes require wide notification, but there needs to be a process to determine at what level the change is communicated in advance
- Evaluation of the change:
  - Accountability for evaluating impact
  - Global and local assessment
  - Cross evaluations of both business and IT changes to minimize unintended consequences; this may require links between several independent change management processes
  - Verify that local interfaces will still work
- Priority of the change:
  - Accountability for prioritization
  - Criteria for implementation, e.g., immediate, service window, or upgrades
  - Clear criteria for when a change can or should be designated as an emergency

- Approval of the change:
  - Accountability for approval, dependent upon type of change, e.g., Operating System (OS) patch installation versus application upgrade
  - Accountability for emergency change approval
- Documentation of the change:
  - Accountability for creation, storage and inspection readiness of documentation and records
- Handover of the change:
  - Ensure that language issues have been addressed
  - Ensure that rollouts are coordinated globally, if necessary
  - Ensure that all necessary documentation is available to all sites (this is important to support regulatory inspections)
  - See also Release Management (Appendix 2, Section 6.1.1)

One mechanism for handling change is through application of the ITIL® model [10] using both a "Change Manager" and a CAB. These should be structured to cover both global and local needs.[8] Figure 6.1 shows a graphical representation of how such an organization could be structured. While this is not the only possible approach, it has the advantage of scalability, which is considered critical. In addition, the communication channels discussed are critical in any global change management system.

Figure 6.1: Possible Change Advisory Board Structure



[8] ITIL® also recommends a "Management Board" above the CAB. This board approves changes that are of especially high business impact. For the sake of simplicity, this Guide does not address the "Management Board", since the regulatory decisions would most typically be handled at the lower levels.

A Change Manager is usually empowered to authorize low-impact changes in order avoid burdening the CAB with trivialities. The Change Manager usually chairs the CAB. The CAB usually authorizes major changes. QA should be involved in the CAB for changes to validated functionality. A benefit of such an approach is that it facilitates changes that do not require QA approval, but provides QA with an overview of the changes that are considered by the CAB. The minimum qualifications for the local Change Managers should be established, as these individuals make the initial decision of what goes to the CAB and, therefore, QA review. Change Managers should maintain a list of classes of change that are considered executable based solely on their approval, and this list should be ratified by the full CAB (including QA). The integrity of this process should be maintained. The process should not be circumvented. Risk management approaches (see Appendix 6 and *ISPE GAMP® 5* [4]) should be applied in the assessment of change impact.

Regulated companies may find it necessary or preferable to have multiple CABs. For example, a local CAB may exist that is geared toward the site's infrastructure and dedicated local applications, but this group is unlikely to know enough about other sites running a global application to be able to assess impact effectively, or even to know who to notify of a change. Conversely, a global CAB may not have sufficient information about local circumstances to understand the change request in the local context, and might, therefore, be inclined not to approve legitimately necessary local changes. Change Managers at all levels should learn to recognize and address such potential disconnects. A periodic (e.g., weekly) Change Managers meeting is a strong recommendation to facilitate communication and early recognition of issues. Such meetings may be brief, but the communication should be frequent in order to facilitate business priorities and minimize the temptation to act in isolation.

The QA participant at the global level should be empowered to make decisions with global impact. The QA participant should either understand or, at least, be aware that there may be differences in local regulations. For example, rules around patient privacy rights for clinical data can differ dramatically, and may be an significant consideration for data migration.

The QA authority approving changes should understand differences in patient privacy rights for clinical data, or recognize when they need to consult with local experts. This can significantly slow the change process, so a mechanism and expectations for response time should be defined. Change planning, where feasible, needs to allow time for some non-IT processes.

In a two level CAB model, a global CAB might cover one or more global applications and even the global infrastructure. Alternatively, there could be multiple global CABs that are concerned only with specific applications; the disadvantage of this approach is regarding changes in the infrastructure, which could trigger several or all of the CABs. All approaches have their advantages and disadvantages, but the CAB should have sufficient understanding either to assess the wider effects of a change, or to know where to find the information needed. Communication channels between the global and local teams need to be open and free in both directions.

Global CABs need a formalized process that ensures that all changes approved globally are adequately communicated to local owners. Conversely, local changes need to be communicated to the global owner so that any extended effects of the change can be assessed and notifications given. This two-way communication can also facilitate keeping an accurate configuration.

Supplier driven changes generally should be managed with the help of the supplier. They may provide some of the test evidence or simply reference release notes to support the assessment of risk for the change. This involvement should help to ensure the smooth global rollout of such changes.

Communication lines need to be open with infrastructure support groups, as application changes are not the only type of change that can affect a validated global system. For example, a planned upgrade of a layered software product like a database manager needs to be announced far enough in advance to allow the team supporting the validated global application to assess local and global consequences of the upgrade, and to schedule any remedial activities needed to accommodate the new software.

Infrastructure groups need to be aware that large global information systems may need significant time to react to such a move, and it is possible that a legacy environment may have to be maintained while preparations are made.

Emergency changes can be especially difficult to handle for a global application. The ITIL® [10] approach of defining an Emergency CAB ((ECAB), typically a subset of the full CAB) may not always be workable if the global CAB includes members from geographically disparate sites. Regulated companies may have to accept either less efficient emergency change processes, or accept the risk that globally implemented emergency changes may adversely affect some local instances.

The emergency change control process should be thoroughly planned and understood, and should be given high visibility, to minimize risk and confusion. Proactive buy-in for the emergency change process should be obtained from all sites and QA. Should a situation arise requiring a response more rapid than the ECAB can handle, the regulated company may wish to empower the CoE to act, and involve the ECAB as soon as possible afterward.

Standard changes should not be allowed to escalate to emergency status through the accumulation of internal failures or delays. Inefficiency should not be regarded as an excuse for a change becoming an emergency.

6.1.1 Release Management

The process for executing a change should follow to the formal release management practices of the regulated company.[9] Changes may be released to users in several ways:

- **Delta release:** execution of a single change in the production environment. Full documentation accompanies the delta release.
- **Emergency release:** correction to a small number of known problems. Release is often in advance of documentation delivery; otherwise similar to delta release.
- **Full release:** multiple changes are built, tested, and distributed together. Regression testing is part of the process. Version upgrades are an example of a full release.
- **Package release:** at least two releases (delta or full) in combination. Multiple version upgrades are an example.

The choice of a release strategy for a given change is generally based on urgency and timing. Patient risk is a contributor to the urgency calculation, but business priorities are also a factor. Cost should also be a consideration, as full or package releases are more efficient and generally more compliant with regulatory expectations, as documentation and testing are generally better than when changes have been implemented piecemeal. Care should be taken to evaluate any potential increased risks related to postponing a change.

It can be beneficial to have a planned release schedule. Scheduled releases are managed generally as either package or full releases. A structured release process can simplify business planning by ensuring that most changes are executed together at a time that the regulated company can anticipate.

Release management requires specific elements of planning which will have possible global and local ramifications. Where rollout is not be done simultaneously at all sites, the impact on the need, and the ability, to share data between sites should be evaluated. Communication plans need to inform global users of the impact and schedule for major changes. Local sites need to be made aware of requirements for installation of changes.

A major requirement for releasing any change is the ability to reverse the change should unforeseen circumstances arise. Such a plan is called a rollback strategy.

[9] ITIL® provides useful guidance if the regulated company does not have a structured release management process. The description of types of releases is taken from ITIL® [10].

6.1.2 Roll Back Strategy

Any change request should include a roll back strategy in case the change does not work as expected; this is especially true of changes that might be implemented to a global information system. There may be problems at a local site that compromise system functionality, while at other sites the change works flawlessly, because of the difficulty for the global team to fully understand the ramifications of a change to all local instances.

Ideally in such cases the change could be rolled back only at the local site while diagnosis and remediation is performed; however, this may not always be possible.

In these circumstances a risk-based recovery plan should be available which addresses:

- Impact assessment and escalation process:
  - What is the impact across the global landscape?
  - How does the risk of rolling back the change at sites where the change was successful compare to the risk of having some sites with less than satisfactory results?
- Decision making process with clearly defined roles and responsibilities:
  - What is the role of the global groups (CoE, global CAB)?
  - What is the role of the global information system owner, global Change Manager?
  - Can the local site/system owner force a global roll back?
- Questions to be answered when executing the plan include:
  - Can the local site live with the problems whilst they are being investigated?
  - Can the site work off another site's system for the short term?
  - Can the rollback be local/regional rather than global?

On rare occasions a roll back may not be possible. In such cases, a risk assessment should be conducted to identify how the risk of irreversible harm should be managed. In severe cases, it might be desirable to clone the live system and test the change on the clone. If it fails, the clone can be scrapped.

Note: having a roll back strategy does not justify reducing the amount of testing planned for a change. Test planning for a change, like validation test planning, should be based on the risk and impact of the change.

6.1.3 Executing Change

Execution of a change on a global information system can be complex. For centralized systems, it may be difficult to find a time to shut the system down to execute the change that does not negatively impact business users somewhere. For distributed systems, it may be possible to replicate the change (or otherwise execute it) on various instances at less intrusive times. For systems that may replicate back to a centralized database, however, this may cause difficulties if the change included alteration of the database architecture. Planning the change execution process requires that these issues are addressed.

Testing of a proposed change may be more complex, especially if the environments used globally differ substantially. It is possible that the test plan associated with a change may have to be executed entirely or in part at multiple sites. Decisions regarding scope, rigor, and location of testing should be technically justified, based on risk, and documented.

Should the CoE (or other change agent) find it necessary to execute a roll back, it is important that this be approached calmly, and that some testing is done to verify that the roll back did in fact work as expected since a failed roll back can sometimes just exacerbate the functional problems. This applies to full roll back of a global change or to partial roll back (i.e., at a specific site). The verification/test process for the roll back may require user participation.

It may be necessary to engage business continuity processes, if backing out a change is a highly complex process or if the system becomes unavailable during the change process. When deciding whether this is necessary, the time within the business day for affected users should be consider. For example, a change executed in Europe at night may still adversely affect users in North America.

Communication is an important part of change execution, and groups implementing a change should be sure to communicate to parties at all affected sites what was done and how it will affect operation of the computer system. Documentation efforts should accommodate expectations of the sites. Release notes can be a good mechanism for communicating changes. Other aspects of communication that need to be considered include updating on-line help files, if applicable. These may need to be provided multiple languages. Planning of the change should consider the time needed for translation.

6.1.4 Closure Process

A common failing in many change control processes is a failure to close out the change. Teams plan, execute, and test the change, and when it works they neglect to finish the work. Several tasks remain that are important, and many companies have received regulatory observations for this. The vulnerability of global information systems is higher because many local sites are subject to inspection, and these will all point back to global records. A failure at the global level thus increases the liability in many places.

Common regulatory observations around change control that could be exacerbated for global information systems can include:

- Failure to update or amend specification documents (URS, Functional Specification (FS), Software Design Specification (SDS) or system description) affected by the change
- Failure to obtain all required approvals
- Failure to retain change documentation (including test data sets and results)
- Approval of changes after they have been executed. This can be extended to include misuse of emergency change processes to circumvent the standard approval process.
- Failure to close the change request as “implemented” or “not implemented”. The latter is especially common: change requests that are never executed should still be closed in due course, but frequently fall through the cracks. The former may present difficulties if the change implementation requires a long time to complete at multiple sites.
- Failure to close the change record in a timely manner

The change procedure should define clearly that all parts of the process should be completed, and internal controls such as periodic review and/or audits should be used to confirm it. If an automated change tool is used, the company should consider automated alert notices for changes past their scheduled implementation dates that have yet to be closed. Automated tools should also have built-in checks that prohibit further processing if prerequisites are not satisfied.

6.1.5 Change Records

An automated comprehensive enterprise solution to managing all change records (logs and supporting documentation) is clearly the best answer, as local and global application and infrastructure teams can then use the same tools and search the same data. Records management is substantially easier in this case.

The accessibility of change records is more important than their location. They should be readily available to IT staff who are troubleshooting a problem and to Application Support Managers, Business Owners, and QA in case of regulatory audit. As a minimum, the records of changes executed at the global level should be available in one location that is accessible to local change managers. It is advised not to attempt global change management without a computerized centralized change management tool, as there are so many ways in which a manual process can fail.

The minimum content of change records should include as appropriate:

- Identity of the requester
- Details of the impact assessment:
  - Impact (minor/significant/major), including a brief justification of this assessment
  - Planned steps for implementation
  - Test strategy (based on risk and impact)
- Priority (low/medium/high/urgent)
- Risk-based roll back plan (not always necessary for minor changes)
- Approval to execute change
- Closure:
  - Status: Proposed, scheduled, executed, cancelled, completed
  - Follow up tasks completed, e.g., documentation, post-execution monitoring if warranted

Responsibility and accountability for change records should be assigned. While responsibility is often delegated, the ultimate accountability for global records would lie with the global business owner and local records with the local owner. This does not mean that the owners should manage or even own the records themselves; that task may lie with the owner of a change control tool, for example. However, owners are ultimately accountable for their system being under adequate change control, and if change is managed outside their direct control they need to be comfortable with the process and to know that regulators will hold them accountable for the records.

Auditing of change control records is something that regulators can be expected to do, and consequently should be something that internal QA groups do as well. This means that local system owners need to understand the communication channels that will enable prompt access to global change records. QA auditing of change records is typically part of the periodic validation review, but it may be supplemented by directed audit of the change control process, if desired.

The length of time for which records should be retained can be a function of a combination of regulatory and business considerations. Retention of global change records should accommodate all local requirements. Differences in local requirements often lead to the policy of retaining records according to the most stringent of the local requirements. Where this becomes impracticable companies may want to consider a risk management approach to record retention.

6.2 Configuration Management

Configuration management is intended to help ensure that a regulated company knows exactly what software and hardware components they have installed at any point in time (including which versions), and what parameters are set that affect the way an application functions. This helps to facilitate incident and problem management and contributes to protecting data integrity.

Note: documentation is considered as a configuration item for a system. In general, managing it this way can make the maintenance of a good global documentation package easier because of the formality of the control processes associated with configuration management.

Part of the work of the global development team should be to define all the CIs for the 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 are both configurable parameters and include hardware components, common infrastructure components like servers and network[10] software components, and documents. Further information see the *ISPE GAMP® Good Practice Guide: IT Infrastructure Control and Compliance (Second Edition)* [12].

At some point, a handover needs to occur from the project team to the group responsible for configuration management (a CoE is a good candidate). The process for this transferal needs to be agreed and understood by all parties. This configuration will establish a baseline and it should be possible to restore the system to this point if required to do so.

Note: re-baselining should occur periodically, with the local instances coordinating and demonstrating compliance to the current norm (or at least cataloging the differences in the local configuration from the global baseline). Validation periodic review is a candidate as a trigger for this activity.

There should be a centralized list of configuration items; however, it is not necessary, and may not be advisable, to manage all CIs centrally. For example, an application CMDB might not be the best place to manage workstation configuration. Workstation configuration could be managed in the infrastructure group's CMDB, if they are using a different tool, as this is probably an infrastructure support responsibility.

There needs to be clear ownership of every CI, however, whether local or global. If ownership is local, there needs to be an established mechanism for ensuring that the centralized list is updated if a CI is changed and for notification of global internal authorities if a change to a CI has potential global impact.[11]

Changes to infrastructure, such as to some hardware components, the operating system, or other layered software, can have a significant effect on the ability of the application to run, and on the ability for sites to share data. Even if these infrastructure elements are not under the direct control of the Application Support Manager or the Business Process Owner, they should be listed as configuration items.

Mechanisms should be constructed to prevent, as appropriate, change of these items without notification of, and in some cases perhaps even permission from, the Application Support Manager or the Business Process Owner and QA. Such notification needs to be sufficiently in advance so that those supporting the application can evaluate, and if necessary mitigate, the proposed change. Many infrastructure elements, however, are either dynamic (e.g., virus definitions) or have little discernable effect on particular applications (e.g., network switches).

[10] **Note:** the ideal situation would have common infrastructure components already listed in a CMDB, and that the global application would just have to 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.

[11] This mechanism should be defined in conjunction with the change control process.

Possible outcomes from this evaluation include:

- Execution of the change as proposed
- Execution of the change with mitigation of undesired aspects
- Execution of the change around the application (e.g., not upgrading or patching the server on which a GxP application is running), retaining a legacy environment without the change for operation of the validated application (this is usually not considered a good solution because proliferation of legacy environments is highly undesirable from a configuration management standpoint)
- Non-execution of the change

6.2.1 Configuration Management for Centralized Systems

A centralized global model can be significantly easier to manage in terms of configuration than a distributed model like client-server. This is one of the reasons that modern applications tend to be web based rather than the older client-server model popular in the 1990s and early 2000s.

The centralization of change management results in centralization, and hence simplification, of configuration management, because configuration management processes are so closely interwoven with change management processes.

Configuration management of a global information system is a task that is challenging. In a SaaS model the job of configuration management becomes a supplier responsibility, although the effectiveness and control of configuration management should be evaluated as part of the supplier assessment, given that ultimate accountability lies with the regulated company.

One of the main goals of configuration management of a centralized global information system is to ensure that changes made to the system do not exclude any users around the world, assuming that the challenge of documentation has been mastered. For example, if a regulated company wishes to do a system upgrade that will only allow users to access the system through a newer browser, the CoE should verify that all users have access to the new browser. This information should be available in the CMDB.

If all users do not have the proper software, then this should delay the scheduling of the upgrade until all sites have the required infrastructure in place.

6.2.2 Configuration Management for Distributed Systems

While client-server architecture is far less common than it once was, it can serve as a worst case scenario for complexity. The need to coordinate globally and locally managed configuration changes is key to distributed systems, and the major source of complexity.

It can be difficult to monitor multiple sites without a strong process rigorously applied through a good tool. A single configuration management solution should be applied universally throughout a global information system. One solution is the model proposed by ITIL® [10].

Staff with local responsibility should maintain awareness of how their CIs differ from the global standard, and should keep the CoE aware of this. This information can be essential to successful planning and management by the CoE of global changes.

6.3 Incident Management

Local incidents that are directly attributed to the global information system should be communicated and managed at a global level. If it is unclear where the problem is, the CoE should be engaged, as they may have seen a similar case elsewhere or may be able to help troubleshoot.

Local incidents that are limited but could have similar impact at another locality should be communicated through an established network or process. Local incidents that clearly have no global implications can be handled at an exclusively local level.

Risk should also be considered; if the incident carries significant risk, it should be reported to the CoE even if it appears to be of purely local origin and solution. This can aid the CoE in identifying and addressing similar incidents elsewhere.

6.4 Service Desk

Well-structured and resourced service desks can be valuable in assisting end users and they also can provide a degree of on-going training. Considerations in setting up service desks for a global information system include:

- Needs within a CoE approach (see Section 4.3.2)
- Multilingual requirements, if any
- Times of operation to support multiple the relevant time zones
- Acceptable wait times for the end user, for both confirming/acknowledging a problem and providing a problem resolution
- If multiple sites provide service as the service desk:
    - Combination of the knowledge base and coordination of answers needs to be considered
    - A common approach to incident management with multiple service desks is to transfer responsibility for follow ups to the next site if the incident requires attention for several hours. This transfer process should be smooth and effective.
- Coordination of a centralized service desk with local technical support; if a desk visit is necessary this transfer process should also be smooth and effective.
- Procedures and tools to escalate incidents for quick resolution, including prioritization. Prioritization should be considered. The service desk should understand if different regions need to apply different business rules for assigning priority. (For example, one region may have process requirements that carry substantial legal or financial consequences if a system is down for a long time, but other regions do not have same concerns.)
- Service agreements between the service desk, user groups, and other support organizations to establish expectations

In addition to answering questions from end users, the service desk can also serve as a central repository for reporting of performance incidents and requesting feedback from end users on necessary upgrades. Obtaining this information in a central location can help in identifying diverse issues such as inadequate training or functional deficiencies of the system. Monitoring system performance as apparently random events in several locations may show a trend when viewed as a whole. Collated information from a service desk can provide performance metrics that can be an input into a periodic review.

6.5 System Security

IT security needs to be planned from the outset of the project. There should be an established framework that the regulated company follows for all systems. This could be a global standard, e.g., ISO 27001 [13] or NIST [15], or an approach developed internally.

System administrators should know when existing privileges should be granted, amended, or revoked, e.g., when an employee starts, moves to another position within the regulated company, or leaves. Procedures should be established involving the Human Resources department, so that account administrators are notified in a timely manner in accordance with predefined and approved procedures. Periodic verification should be performed by a central authority (e.g., a CoE) to verify that account and access management processes are working adequately and reflect current role related needs. QA should monitor access control practices to ensure that data integrity is not compromised.

The unique aspect of managing risks and threats to which global information systems may be vulnerable is the potential need to have local authorities with limited administrative privileges, e.g., for the creation of accounts. Use of such accounts should be as limited as possible, e.g., password resetting should be managed through the global help desk or CoE. Elevated privileges should not be given to active users of the application. Persons with a potential motive to make unauthorized changes to data should **not** have the ability to do so. A local administrator, who uses the privilege only occasionally, who is trying to delete a user named, e.g., David, should not be able to delete all users named David globally; the potential for damage is significantly greater.

The unique challenge with global information systems is to enforce a single standard for data control that is aligned with the strictest legal and regulatory demands. What may be culturally acceptable background access or manipulation of information at one site may be viewed as illegal access or fraud in a different location. Security configuration and management processes should ensure that a regulated company can avoid having to defend itself against allegations of misconduct.

Other issues that could impact security include:

- For SaaS, IaaS, or PaaS systems the supplier's security controls need to be specifically addressed in supplier assessment. The SLA and/or contract should define timely notification requirements of any security breaches that may affect the regulated company.
- Access by suppliers to systems and data if they become involved in troubleshooting or repair processes should be managed
- Management of patching processes in a distributed environment is more complex than for centralized systems
- Monitoring and management of vulnerability
- Intrusion detection and prevention
- How is data in the system handled at rest and in transit? Is encryption needed, and to what extent?

6.6 Performance and Capacity Planning

Performance requirements should establish average time limits for the global information system to respond to user requests in a meaningful manner.

A global information system can grow in unforeseen ways and those growth elements that can affect system performance need to be defined. If the global information system only occasionally uses a central server, but peer-to-peer communication is heavily utilized, then server growth is most likely not a major issue, but the ability to expand network bandwidth may be important. Any centralized service needs to be evaluated and growth requirements defined, e.g., for database growth, database administration, security, network diagnostics. Planned redundancy should be considered to alleviate common mode failures that can affect the system extensively.

Licensing agreements may become a limiting factor if not managed properly. Failure to manage licenses could incur significant expense, for users who no longer access the system. Usage and demand should be monitored globally so that it does not become necessary to limit the number of simultaneous users in order to assure performance or meet licensing requirements.

6.7 Performance Monitoring

Users, support staff, and owners at local operational areas should be surveyed by the CoE periodically to ensure that they are receiving satisfactory service. There may be regional issues that are unnoticed by global management. Standards and metrics should be developed, against which monitoring results can be compared. Action limits also should be established, at which time action should be taken if performance slips. These standards and expectations should be documented in an OLA or SLA.

Incidents should be tracked and categorized. Problems should be analyzed globally (including understanding possible local impact), to ensure that the application works as expected and remains validated. Incidents resolved locally should be included in this analysis, as they may provide insights into possible service improvements.

Interfaces should be monitored and evaluated for possible data integrity vulnerability. This could be the jurisdiction of either the CoE or IT. Where appropriate, users should be notified of an interface failure.

CoE personnel can take ownership of second and third level problem management, and should keep their management and system owners aware of the status of major problems. Where problems are significant and moderate to long term, periodic updates for users also should be part of a communication strategy that will help minimize any worsening of the problem.

Automated tools should be considered for performance monitoring, wherever possible including those owned by the supplier that might be advantageous.

6.8 Backup and Recovery of Software and Data

The management of backup and recovery will be particularly dependent upon the architecture of the application. Generally, responsibility for this lies with the data center where the data actually resides (which could be at a supplier for SaaS, IaaS, or PaaS solutions), so if there is one central database managed at a CoE, it should handle this task. If the data is distributed, the regional data centers should perform the task.[12] Procedures should be established which define what is included in the backup, how often the backup is performed, and who performs the backup.

[12] While it is possible to manage backup of regional servers centrally, if that path is chosen Wide Area Network (WAN) bandwidth becomes an important factor.

There should be a common global understanding of what is included in the backup, and how often the backup is performed. The basic requirements for this should be defined in a documented backup plan, although there should be additional documentation defining directory structures for the backup, etc.

Retention of backups is an issue that may be dependent to an extent on local regulations and laws. For example, privacy laws or legal discovery rules could have an effect on how long backups of clinical studies should be kept.

The policy for retention of backups should not be confused with the policy for retention of archived data. In general, the use of backup copies as archives is not considered a good practice. For global information systems, the additional concern relates to privacy law. For example, there may be specific requirements to delete records related to employees who have left the company, and while this is reasonably simple in a true archive, it may be very difficult to remove such records from a backup tape.

Procedures should be in place for system data recovery. Who may request a recovery should be controlled in a global information system, as the possible effects of this could be further ranging than those making the request may realize. For example, such a recovery may overwrite data collected at another site. The business community should also be notified when a data recovery has been initiated.

The restoration process should be tested periodically and may be conducted in conjunction with disaster recovery testing.

Note: for distributed systems timely replication of a database may adequately meet the need for data backup for some sites. At least one site should execute standard backups, however, so that a clean copy is available in case a propagating corruption, virus, etc., were to compromise all on-line copies of the data.

6.9 Record Retention, Archive, and Retrieval

While archiving has elements in common with backup, it does not serve the same purpose and the two should not be confused or used interchangeably. Backup is intended to support recovery from a problem, and includes both data and software, whereas archiving is the intentional removal of data from on-line status in order to free disk space, maintain adequate system performance and/or meet other business requirements for data security and preservation. Software may be archived as well, but this is typically only to support restoration of a legacy environment, if necessary.

The following are related to managing archives and should be considered in the context of global data control and compliance policies:

- The rate of the creation of business and GxP critical data on a global scale, which most companies find to be increasing, may require fluidity in the frequency of archiving events. Automation of archive processes can alleviate this.
- The control and storage of data at local, regional, and global information system levels should be defined.
- Compliance with various national GxP or other regulations on electronic records management, including legal requirements to destroy certain records.

Archival may be managed regionally, as might backup, but it may be beneficial to give the CoE more control over the archival process to ensure that the data is managed appropriately. Archives should have a predefined finite life time, after which the records should be evaluated and a decision made as to whether they should be destroyed or retained for a further defined period. Retention of archives needs to meet the regulatory requirements of all relevant health authorities as well as conform to local law and this should be considered when establishing retention policy.

It is possible, albeit unlikely, that the interpretation of different legal record retention requirements will differ or even conflict (e.g., if privacy law were to require record destruction after a set period); therefore, the retention of archives needs to meet the regulatory requirements of all relevant health authorities. This should be considered when establishing retention policy. One possible example of such a conflict is personnel records, which include relevant training records. These must be destroyed in some countries when an individual leaves a regulated company.

Note: this could conflict with US FDA expectations where the GLPs specifically require the retention of training records. If conflicts are found, both QA and Legal departments will need to be consulted and involved in the final decision.

6.10 Business Continuity and Disaster Recovery

Planning should include consideration of containing the effects to the local source, to minimize the impact of any disaster on a global system. Such plans should be tested, to assure that business continuity requirements are met. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) should take into account possibly different levels of risk at different sites. For example, one site may have requirements based on the ability to produce a lifesaving medicine that cannot tolerate a system outage of more than a few hours, while other sites could be down for days without severe deleterious effects. The effects evaluated should include the loss of global and local resources, both simultaneously and independently.

In some ways, disaster recovery may be easier for a global system, while in others it is more complex. The ability to use another of the regulated company's own data centers as a hot site for recovery can simplify matters. For a distributed system, it may be possible to get up and running again simply by recovering the affected site's data from another site's database server. The effect of the added data volume and business community to the recovery site's infrastructure, however, needs to be understood. Incapacitating a second site by adding an unacceptable load to the system in order to supply the disaster site with what is probably an intolerable level of service, is unlikely to be acceptable.

A combination of planning and testing should help to ensure that disaster recovery under such circumstances is acceptable. For example, when defining user requirements, the two largest sites could be designated as disaster recovery hot sites, in which case it should be ensured that infrastructure with adequate capacity is specified in the hardware design phase. During testing, loads that can be handled acceptably should be verified.

Periodic disaster recovery drills also should be performed to test the solution and preparedness for a disaster. Reasons for this include:

- Verification that the right people are identified and properly prepared to recover the system
- Verification that staff know how to restore the system
- Verification that changes to the system have not affected the ability to recover
- Verification that system growth has not rendered the disaster recovery solution inadequate

A major factor in the success of disaster recovery is the ability to get the right people involved as quickly as necessary, which may be a particular challenge if the disaster is in a time zone which is significantly removed from that of the recovery site, e.g., North America and Japan.

If the internal hot site strategy cannot be implemented, any alternative needs to be analyzed in fulfilling the requirements of all affected sites.

It may be a valid business decision that only the needs of the largest sites will be given precedence, and that work arounds will be defined in the Business Continuity Plan for smaller sites.

Regardless of which strategy is selected, it needs to be communicated to, and understood by, all affected parties, and the resulting procedures need to be periodically exercised.

In addition, training programs should be established for the personnel who are involved in implementing such plans, including the possible involvement of global resources in a local recovery effort, and vice versa.

For SaaS systems, most business continuity controls are managed by the supplier; however, verification of these processes should be part of the supplier evaluation. If any global or local compensating controls are necessary to supplement the supplier processes these should be addressed as part of the implementation processes, and depending on their nature, tested in validation.

6.11 Periodic Review

The principles of periodic review for a global information system are the same as for a purely local system. The complexity level is greater. Aspects of periodic review for which global information systems have an added level of complexity include:

- **Configuration:** the recorded or documented configuration should match the actual current configuration. Configuration management processes managed locally should be demonstrated to be effective. Local difference from the defined standard should either be remediated to conform or justified and documented. If conflicts exist, then an updated baseline configuration should be agreed at a central or core level and a more effective configuration management process implemented.

- **Change Management:** for distributed systems review should verify that centrally driven change has been properly implemented locally, especially patches or updates to application, database, or operating system. Further, the review process should include looking for “creeping change”: a significant number of minor changes to the system may collectively start to impact on the initial system that underwent full validation, implementation, and test. Regression testing should be conducted in conjunction with changes to verify that nothing outside of planned scope was changed. Such regression testing might have both global and local components. If the regression testing was not done, a degree of additional testing, both locally and globally, may be warranted. In addition, there may be some changes that were not tested or documented. Any suggested additional testing should be based on risk management principles.

- **Specifications:** current versions of specification documentation should reflect the as-built system, updated when driven by the change process. Local sites should have access to current global specifications. Any local changes should be known at the global level and reflected in either core or local documentation. Any discrepancies should be remediated.

- **Traceability:** changes to the system should be reflected in appropriate specification documentation, e.g., URS, FS, or Design Specification (DS). Traceability between these documents should be transparent and available at both core and local levels. In areas where traceability has been lost it should be reestablished, at least between test cases and user requirements.

- **Regulatory expectations:** the understanding of current regulatory expectations should be consistent with supporting documentation. Discrepancies should be addressed, either through a documented justification or through remediation.

- **Performance history:** problem and incident logs related to the system should be reviewed to determine whether there have been recurring problems that should be fixed, or impacts upon data quality. All local areas should be satisfied with the overall performance of the system and where concerns are raised, documented action should be taken.

- **Security practices:** access to the system should be controlled and access lists should reflect current users. This is especially difficult if access privileges are managed centrally. Access lists should be reviewed periodically for the effectiveness of the management process. If the periodic review is conducted at the global level it is probable that it will have to be coordinated with local review of access privileges.

- **Business Continuity:** backup processes and periodic restore testing should be checked. Disaster recovery testing should occur with a predefined frequency; this could consist of a combination of tabletop and physical testing. Contact information for key global personnel who need to be engaged in business recovery should be verified as current.

For global systems, the Periodic Review needs to account for the current status at all sites and the CoE.

For distributed systems, it may be most effective to coordinate several local review efforts with that done by the CoE, and then issue a composite report from the CoE. For centralized systems, more work can be performed by the CoE.

7 Appendix 3 – Architecture Design Considerations

A global information system can have a data architecture that is centralized or distributed; however, there are several different aspects of centralization to consider.

7.1 Centralized System

The term "centralized" may be described as:

- **Centralized systems:** one or more large systems (servers) located in the same facility and controlled from there.
- **Centralized processing:** all applications are run on the central system, regardless whether they are organization-wide in nature or specific to, for example, a division.
- **Centralized information:** all information, whether needed by the entire organization or not, is stored at the central facility, regardless of where the application is hosted. For example, the application could reside on servers in a corporate data center but all data could be stored at a cloud provider. Alternatively, albeit less commonly, a SaaS application could store data in the client firm's data center. This might be considered desirable, if the data is considered extremely sensitive, but it is not a very common or efficient approach to SaaS. In general, it is considered better to enhance the data integrity controls at the supplier's data center.
- **Centralized control and support:** a manager and technical support will control and maintain the equipment and applications. SaaS is the ultimate incarnation of this approach.

7.1.1 Advantages

- Ease of application of change control and standards enforcement
- Ease of configuration management
- Ease of system information analysis
- Ease of implementing security controls
- Promotes the global use of substantially identical business processes
- Centralized approach to business continuity and disaster recovery will probably get the global business community back in business faster

7.1.2 Disadvantages

- Vulnerability to outages where a single point of failure exists. Disasters are more impactful.
- Wide potential impact of changes
- Difficulty managing some of the security controls (central sites often have difficulty dealing with issues like local staff turnover due to isolation from business users)
- Mandating the global use of substantially identical business processes may add complications

7.2 Distributed System

The term “distributed” may be described as:

- **Distributed systems:** one or more large systems located at several facilities
- **Distributed processing:** applications run on multiple discrete platforms
- **Distributed information:** information is stored locally or on multiple discrete systems that may or may not be accessed collectively. A hybrid use of this redundancy could take advantage of centralized backup and disaster recovery planning. If some sites were unaffected by a disaster or recovered quickly, a temporary business continuity solution could be to allow other sites to work off one of the local implementations that is on line.
- **Distributed control and support:** a manager and technical support will control and maintain the platform and applications locally

7.2.1 Advantages

- Incremental updates and flexibility, e.g., new additions to the distributed system, can be implemented gradually without major interruptions provided there are no core dependencies on remote system components
- Availability and resource sharing: if any one system fails the impact can be designed to be minimal since all the other interconnected systems can provide an alternative role (provided system versions are kept aligned)
- Higher data availability if data is replicated at multiple sites
- Easier to comply with local laws, e.g., for personally identifiable information, which may have local requirements as to what can or should be retained and for how long due to data protection laws

7.2.2 Disadvantages

- Can be difficult to test and determine failure – the more complex and the more integrated the system, the harder it is to test and to determine the cause of failure or performance degradation. (In small systems, this can be easier and would, therefore, be an advantage.)
- Coordination and control: the physical distance between different groups can make it difficult to manage and impose standards for the network, security and management of data collection, and analysis along with application change control. There is, therefore, a higher risk that a system may evolve in an uncontrolled fashion. This may be mitigated by consistent use of modern tools.
- Incremental update processes can result in temporary loss of synchronization
- More complex security requirements
- Requires local management for break/fix scenarios
- There is no one individual responsible for maintenance

7.3 Software as a Service

SaaS is really the centralized approach carried to its logical conclusion; however, specific unique aspects of SaaS architecture affect approaches to the global information system. While there is no inherent reason that a SaaS solution cannot be validated and compliant, there are complications, and these are amplified for systems that are global in nature.

Business continuity and disaster recovery capabilities are often a major driver in the decision by a regulated company to move to a SaaS solution. SaaS suppliers typically work via multiple data centers and flexible cloud-based data management schemes. This usually provides better continuity and recovery scenarios than a life sciences company can manage, and at lower cost.

When contracting with a SaaS supplier both parties should thoroughly understand the very basic question of what defines a disaster. For a regulated company a disaster might need to be declared 30 minutes after a system that supports manufacturing goes down, with the risk being the loss of product worth millions of dollars. This could be a direct clash with a supplier whose internal processes call for a fourhour assessment of the extent of the problem. This should be clarified before a problem occurs.

7.3.1 Advantages

- System management is contracted to a company whose core business is management of that system.
- Ideally, validation is a shared responsibility with the supplier, who validates core functionality.
- Upgrade processes follow a predictable schedule, and the client will typically be updated to the latest release.
- Change control and incident management will be a supplier responsibility.
- User support processes are typically very robust, accessible to multiple time zones, and react rapidly.
- Business continuity and disaster recovery processes are generally well designed, well tested, and effective.

7.3.2 Disadvantages

- Business process flexibility will be limited in that it should conform to software capability.
- Dependent on supplier to agree to implement desired enhancements.
- Supplier mandated maintenance windows may not be convenient.
- Reliant on supplier to manage data integrity; because of scale, the supplier may be a more attractive target for cybercrime.
- System failure can have significant implications.
- If the supplier is unwilling to own the validation activities, it can be difficult for a regulated company to manage it when they do not control the change processes for the system. Customers may not even know when the supplier applies minor patches; and periodic update processes can be problematic because changes can be made not only to the platform, but also to the application itself. This may have several effects:
    - Lack of the option to stay with a stable, validated version of the software
    - Possible insufficient time for the customer to validate a change

- Very little recourse if there is a validation problem

- No option to introduce changes in a staged manner

It is advisable that the SaaS supplier owns the validation of a SaaS application. Regulated companies should be aware that that they cannot effectively maintain a validated state for an application that they do not control. If a supplier is unwilling to accept this stipulation, serious consideration should be given to not using the application.

Note: the regulated company is accountable for the adequacy of the control, management, and integrity of the data stored, processed, or managed in the computer systems that it uses. It is considered essential to ensure that continual communications and proper lead time for changes is given to accept the change at both global and local levels.

7.4 Risk Management Considerations Driven by Architecture Choices

Architecture choices lead to different risks. Selecting the appropriate architecture should be based on a balance of the following:

- Return on investment
- Risk tolerance of the company
- Probability of risk realization
- Impact if the risk is realized

Table 7.1 presents a summary of the key risks associated with architecture.

Table 7.1: Risks and Hazards Associated with Architecture

Architecture Hazard	Risk
Centralized versus distributed versus web-based versus SaaS decision is not based on a full understanding of user needs or supplier capabilities	Failure to understand what are the most critical business needs, e.g.: • Minimized latency • Centralized backup • Instant mirroring of data Business continuity requirements, e.g., the ability to log on to another instance if the local one is down Disaster recovery requirements The ability to see or use data from another location These could compromise the utility of the application
Failure to understand the nature of the data coming from all locations could lead to Placement of data in a locality where data protection laws are inadequate Unwillingness of some parts of the organization to use the application	Inadequate information security and/or compromised data integrity
Minimum platform standards are not met universally	Some users may not be able to use the system effectively
Management of system administration is not properly allocated (e.g., to a CoE)	Possible data integrity issues if data management processes are not effectively handled Possible user complaints, either universally or regionally Possible drift, e.g., different sites apply patches inconsistently or are at different antivirus levels
Inadequate service desk coverage	Exclusion or inadequate support of regional users due to inconvenient hours, language issues, or failure to understand regional problems
Inadequate business continuity or disaster recovery provisions	Failure to understand business processes in all regions could unnecessarily expose the organization to risks associated with unplanned down time or loss of information
Capacity of the application is inadequate	Regional growth expectations that are not well understood could lead to architecture and design decisions that cannot adequately support such growth
Latency	Latency, both network and potentially with peripheral data sources, may be an issue that compromises data integrity. Testing may be very difficult and the effect of very large data sets needs to be considered. Performance monitoring for latency may be critical.

8 Appendix 4 – Application Architecture Effects on Validation Strategy

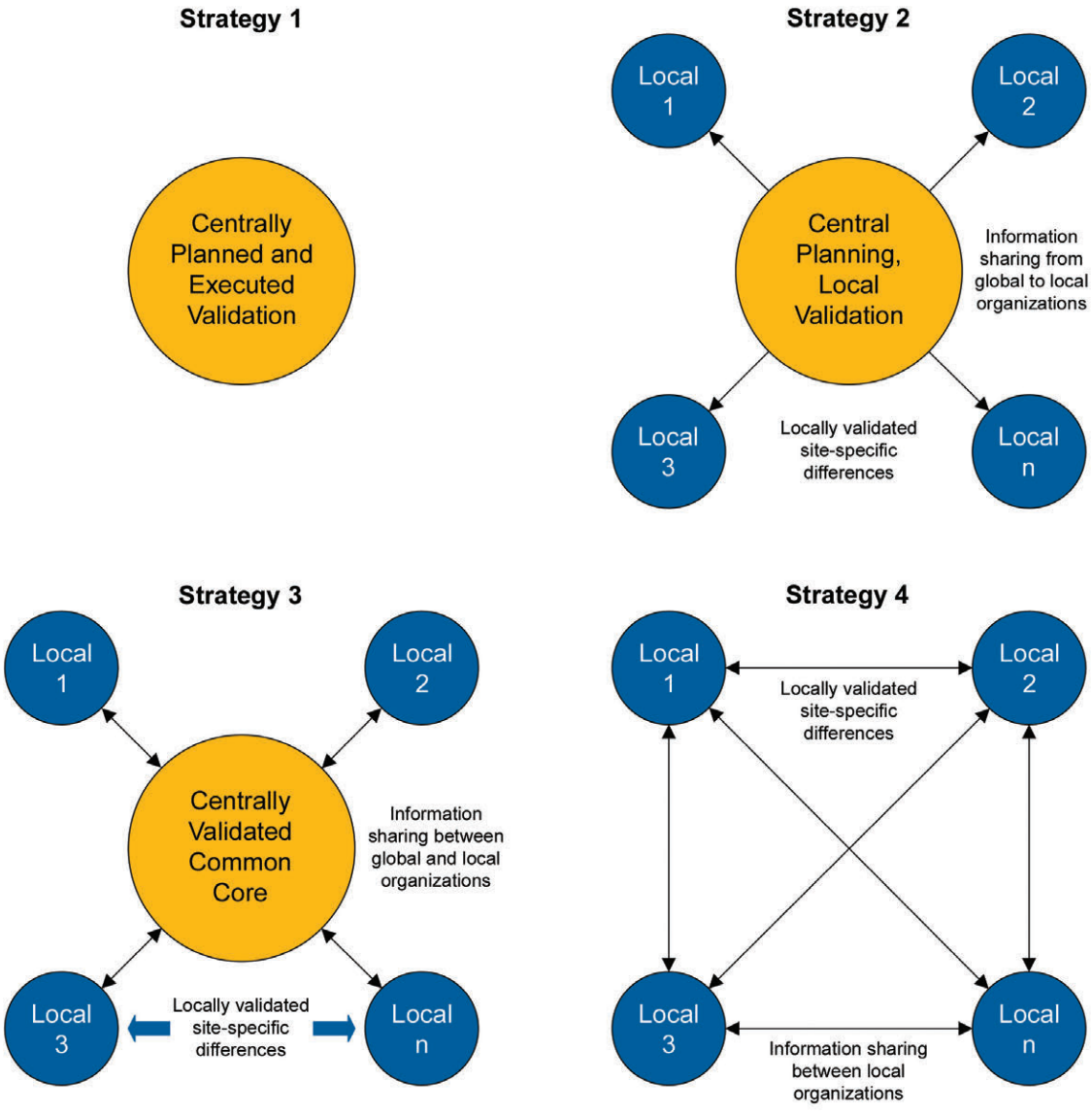
This appendix describes the application architecture and associated responsibilities, along with testing and documentation synergies.

A team leader responsible for validation should be appointed as a member of the core project team as early as possible, preferably in the Concept phase. The team leader responsible for validation should be aware of and have input to decisions relating to the application architecture that will be made as a part of project initiation and planning.

The selection of a high level validation strategy can be impacted by the architecture of the application being implemented.

Figure 8.1 shows a graphical representation of the four major strategies derived from application architecture.

Figure 8.1: Validation Strategies Based on Application Architecture



8.1 Potential Validation Strategies

8.1.1 Strategy 1

Simplest of the strategies, this is a single global, centralized validation effort done on behalf of the entire business community. This works only for applications managed from a single point. Note that SaaS systems can fit into this strategy, although it is more common that they will require a hybrid of Strategies 1 and 3, depending on the nature of the system. This is because interfaces into other systems are likely to have some uniquely local aspects. However, if the local differences are very small in number, it may be most efficient to include these in scope of the global validation, making it a pure Strategy 1 exercise.

Note: For a SaaS system the central validation should belong to the supplier (even though accountability for the validation remains with the user company). It is not considered feasible for a regulated company to try to own validation activities for a system that they do not control. If a supplier refuses to accept ownership of the validation, the regulated company should consider looking elsewhere for a solution. If the regulated company does not accept the adequacy of the supplier validation, there are two basic choices:

1. To try to supplement the supplier's validation work, which is likely to prove difficult

2. To find another supplier

8.1.2 Strategy 2

Completely centralized planning with local execution of validation is an unusual strategy, and not generally recommended, as it will not be economical in terms of resource requirements. This approach could be applied to any architecture, although it may be best suited to multiple implementations of the same core system where local validation of hardware and configuration is necessary.

8.1.3 Strategy 3

This strategy was possibly the most common one at the end of the twentieth century, when client-server architecture was in its ascendancy, with a core validation accompanied by local validation efforts addressing local differences for each deployed instance of the application. As bandwidth became less of an issue and web-based applications became more sophisticated, a more centralized approach became more common again. However, as systems have become increasingly interlinked, this has meant that while it is less common to have local differences in the system itself, there are likely to be interfaces to local systems that need to be validated.

The most efficient use of this scheme is considered to minimize actual functionality differences so that local validation efforts can be concentrated on local application infrastructure and business process.

Note: for web-based systems this may be simplified in that there may be no local application infrastructure; this will be true for most SaaS applications.

Under this scenario, there will be a locally prepared and managed Validation Plan, local testing activities, and a local Validation Report. Many document templates, including the Validation Plan and Validation Report, may, generally, be leveraged from the global efforts.

A local site may require some modifications or additions to the core functionality. This may involve a local supplement to some of the global documentation. It may include a local supplement to the Validation Plan, which is managed similarly to the global Validation Plan, but with local approvals. Regulated companies may wish to add a global approval to such plans to ensure that the local differences are allowable under the global standards and planning. This can also help to ensure that the internal company global authorities (e.g., the CoE) understand what is being done at each site.

Other global documentation also may have locally prepared and approved supplements, such as the user requirements, functional specifications, design specifications, etc. There may be additional locally approved and executed testing in this scenario as well, since functional testing executed at the global level will inadequately challenge the local differences.

A thorough analysis of traceability of the modified specifications can reveal which functional tests need to be modified so that redundancy can be avoided.

There should be a local Validation Report summarizing all local activities.

8.1.4 Strategy 4

A completely local validation approach may be warranted if local instances of the application are configured and managed in substantially different ways.

8.2 Application Architecture and Test Strategy

Validation test phases allow leveraging of test resources for a global system:

- **Installation verification:** Hardware verification involves installation with a distinct geographic connection and therefore is generally local. Software verification needs to be carried out where the software is installed, and is thus global or regional, depending on how distributed the system is.
- **Functional testing:** Tests internal application function, which can be generally independent of hardware platform and therefore global.
- **Requirements testing:** Tests application functions in the context of the business process, which can be local or global, and the operating environment, which is often local.

Note: if local operating environments are effectively identical, this can eliminate the need for any local testing designed to challenge the environment. For example, such challenges are not typically necessary for web-based applications. Similarly, if business processes are globally standard, there is no need for local testing against business processes.

It should be possible, therefore, to do a single global test phase for internal application functions (calculations, database functions, data entry, etc.), subjects that are normally covered in functional testing. If there are no local differences in application configuration that would invalidate such testing, this strategy is suited to all architectures.

While remote sites may depend on installation verification done elsewhere, the site at which the application infrastructure is installed should always be the owner of the infrastructure upon which the application resides; therefore, that site should take responsibility for installation verification of the application on its equipment. A CoE or the global team may dispatch help to the local site for installation and testing.

The ability to achieve testing synergy in requirements testing is dependent upon both the architecture and the uniformity of business processes. Requirements testing specifically related to application performance on local infrastructure (e.g., response time) will always be local, but if sites use the same business processes some architectures can support at least some centralized approaches to requirements testing.

Validation reporting under these strategies is often fragmented with global and local portions. Local sites should ensure that they have access to all applicable validation documentation available for regulatory inspection, regardless of whether it was generated locally or at a centralized site. Similarly, the CoE or global team should be able to obtain local documents in a reasonable time frame. Where possible, access to documentation should be covered in an OLA or SLA.

Table 8.1 summarizes considerations for test strategy in relation to application architecture. Note: this is a high level summary, and business processes, application configuration, and infrastructure architecture can all affect strategy choices beyond the recommendations of this table.

The rationale for choices regarding local centralized or global testing should be justified in the Validation Plan.

Table 8.1: Application Architecture Strategies

System Types	Example	Description	Validation Planning	Test Planning	Installation Verification	Functional Testing	Requirements Testing	Validation Reporting
Remote Web Access Single Central Server	Global Drug Safety System	Centralized system resides at one facility, accessed globally via web browser	Global	Global	Global	Global	Global*	Global
Remote Web Access Distributed Servers	ERP, EDMS	Web access distributed to multiple servers to enhance performance	Global and Local	Global and Local	Local	Global	Local	Global and Local
Software as a Service	ERP, Customer Relationship Management (CRM), Clinical Monitoring	Software and hardware owned and operated by the supplier	Global with significant supplier input	Supplier, possibly supplemented	N/A	Supplier††	Global**	Global, with supplier input
Client Server, Single Central Server	LIMS, ERP, Clinical Monitoring	Centralized system resides at one facility, accessed by workstation clients. Application leverages desktop processing power.	Global	Global	Global (Local Client)	Global	Global*/Local	Global†
Client Server, Distributed Servers	LIMS, ERP, Clinical Monitoring	Clients accessing different application and/or database servers. Application leverages desktop processing power.	Global and Local	Global and Local	Local	Global**	Local	Global and Local

Table 8.1: Application Architecture Strategies (continued)

System Types	Example	Description	Validation Planning	Test Planning	Installation Verification	Functional Testing	Requirements Testing	Validation Reporting
Distributed Servers, Access only to Local Server	Standard-ized ERP systems for "independ-ent" sites	System installed in multiple locations according to global standards. Some local variation possible. May be web access, client server, or terminal emulation. Users external to that site do not typically access data.	Global and Local	Global and Local	Local	Global**	Local	Global and Local

* Assumes that local business processes are identical

† Verification of local workstation installation generally independent of validation report

** Specific local requirements would require functional testing at a local level

†† Interfaces to local systems require validation; could be global or local

9 Appendix 5 – Example Case Studies

The following six case studies are intended to show how the principles of this guide can be applied to a variety of common business systems. **Note:** that these do not reflect the only way to approach these systems, but rather one possible approach. There will always be small differences in the way in which companies implement such systems, often based on architectural choices such as internal management versus SaaS.

9.1 Global MES Implementation

Description: Global information system providing standardized approach to controlling and reporting on manufacturing, managing deviations, and reporting results. Standardized format allows easy recipe management and result roll up for statistical analysis. Locally managed interfaces with a wide variety of equipment, including some that is unique to one site.

Issue	Consideration
Architecture Assumption	Distributed system for control. Database could be central or local, but is assumed central for this example. Many locally interfaced automation systems.
High Level Approach	Initial pilot at one manufacturing site. Phased roll outs to other sites.
Business Processes	Global manufacturing management need to evaluate business processes worldwide, and in order to maximize efficiency of the new solution they may have to mandate conformance to certain standardized business practices. Failure to do so may end up requiring local modifications to the software that reduce the efficiency of adopting a global approach.
System Ownership	Global owner for the overall MES solution, main supplier relationship, responsibility for core validation, responsibility for CoE. The global owner needs to be identified as early in the project as possible and needs to participate actively (probably on the Steering Committee). Local owner responsible for local validation and ensuring all local and global information system management processes meet the local business needs of the system
Steering Committee	The global Steering Committee should have the global Business Process Owner, the global application Support Manager, a global QA representative, the local owners from the pilot site, the CoE head and maybe an SME from IT or engineering. Local committees should be structured similarly, but also include a CoE member. Steering Committees should have the authority to make and enforce decisions, e.g., mandating process changes for reluctant users.
Project Team	Initial global team involves process, engineering, and IT SMEs from pilot site, global IT, global QA, and possible external system implementers. After pilot is complete and CoE is established, global project team consists of SME(s) from pilot site and CoE staff. Local project teams for subsequent implementations consist of local SMEs and IT plus close and frequent participation from global team members, especially the CoE.
User Requirements	Global user requirements should focus on commonalities desired for all sites, including technologies and compatibilities, basic functions, data management, etc. Local requirements can be more detailed in technical requirements, e.g., down to specific models of equipment that must be compatible. Requirements gathering should pay special attention to interfaces and associated data integrity implications.

Issue	Consideration
Legal and Regulatory	An approach should be defined that will provide compliance for all affected laws and regulations. This may entail committing to limit certain sites to only supplying a subset of markets. A thorough analysis of national laws and regulations is necessary in order to recognize possible conflicts. While it is extremely unlikely that different nations GxP expectations differ, there may be other laws, e.g., related to employee privacy, which may conflict for example with record retention expectations related to training records. QA and Legal departments need to agree and document an approach to such conflicts.
Implementation Approach	A pilot approach is highly recommended for any distributed system. The pilot project team should comprise both local and global members, with all of the latter and some of the former prepared to support the next implementation in the roll out. For an application as complex as MES, it may even be beneficial to do the pilot project in phases, with the first phase limited to a single production line in order to reduce the number of initial variables.
Validation Approach	Global validation of core functionality, probably in conjunction with implementation at a pilot site. Core validation documentation is managed by the CoE, and updated as necessary when additional sites implement functionality that will be used elsewhere as well. The local team manages purely local functionality, interfaces to purely local systems, and all verification work on local devices or infrastructure. Requirements and user acceptance testing are also performed locally. **Note:** that some of the local documentation could be useful globally if there are other sites making the same products or using the same equipment. The initial pilot will be a combination of core functionality validation that can be applied globally and purely local validation based on business process and local equipment. Pilot documentation should be prepared in such a way as to make separation of global and local elements for future reference simplistic. **Note:** for an in depth analysis of implementing a compliant global MES see the *ISPE GAMP® Good Practice Guide: Manufacturing Execution Systems – A Strategic and Program Management Approach* [23].
CoE Responsibilities	The CoE will be responsible for all system management tasks where centralization of responsibility and accountability makes sense. Where a “follow the sun” approach is required (i.e., tasks are passed around daily between work sites that are many times zones apart), this will be coordinated by the CoE. General responsibilities include: • Manage overall revision level of system, probably including pushes of patches and updates to distributed servers • Own validation of core functionality • Coordinate with local support staff for integration of new equipment • Manage centralized database • Coordinate backup of centralized resources, maximizing availability as required by local users • Incident and problem management (second level) • Change management (shared) • Vendor management • Archiving and record retention • Support roll out at future sites • Maintain a list of equipment and configurations that have been qualified to work within the MES framework • Support future site implementations and validations

Issue	Consideration
Local Responsibilities	• Own validation of locally unique components and interfaces into the MES • Management of local infrastructure (servers, Local Area Network (LAN), devices, equipment) and interfaces • Recipe management • Deviation management • Incident and problem management (first level) • Change management (shared) • Backup of locally stored records (if any)
System Management	• **Change control:** local and global elements • **Incident management:** level 1 local, level 2 global, interface to level 3 (supplier) owned by global CoE • **Problem management:** global • **Security management:** security groups defined globally, users managed locally • **Configuration management:** core elements managed globally by CoE, interfaces and any other unique local elements managed locally • **Training:** core curriculum developed globally, delivered locally (or via on-line tools) • **Document management:** core project documentation, validation, specifications owned globally. CoE should have access to local documentation.
Supplier Management	Expectations for supplier support for the system need to be agreed for all involved venues, and documented in a SLA with the CoE, backed by an Underpinning Contract (UC) between the CoE and the supplier. This should clearly define parameters for issues like off-hours support and potential support through supplier subsidiaries or partners. If the supplier will ever have access to business data (e.g., for support or testing) the UC should also include protection of intellectual property and privacy.
Availability Management	Due to the nature of an MES, down time (especially if unplanned) can be exceedingly expensive, possibly putting millions of dollars' worth of product at risk. An attractive approach for a global information system might seem to be automated failover to servers at another manufacturing site. If this is the intent, it should be assured that the failover site's infrastructure is capable. Planned down time can be critical as well if a manufacturing site needs to access information stored at another location. Mirroring of information might be a solution to this issue.
Data Management	Similar to the availability of the control aspects of the application noted above, data availability may be critical to the integrity of the supply chain. Data from the MES application needs to be available in a timely manner to facilitate product release and shipping, and it is possible that this data may need to be available at other sites besides the site of manufacture. MES systems record real time data and the cost of losing such information can be extremely high, for example making a batch of product unreleasable. Backup strategy needs to account for the criticality of this information, e.g., via real time or near real time backup. Data integrity concerns require MES systems to have strictly controlled role-based access, a task that will demand diligence and close cooperation between local and global authorities.

Issue	Consideration
Records Management	Records retention requirements for all countries where product was distributed should be satisfied. When the system is retired there is an expectation that the data is readable throughout its retention period. For proprietary formats it may be necessary to make special arrangements to retain this ability, e.g., via migration to a new format or arrangements with the supplier to recover data to a readable format on demand. When records are due for destruction this could either be managed by the CoE or a records management group. For a global information system, the responsible business authority needs to verify that none of the records scheduled for destruction are in a hold status to support litigation. Once the go ahead for destruction is received, all copies of the record should be purged. For a distributed system this may mean verifying destruction at multiple locations.

9.2 Global ERP Implementation

Description: Global information system providing unified control over a variety of aspects of finance and supply chain management. It may also manage functions in such varied areas as Human Resources and facility management. For most companies with an ERP system it represents the single largest IT investment.

Issue	Consideration
Architecture Assumption	Approach can either be centralized or distributed. A common approach (which will be the scenario described below) is a hybrid with two or three hubs serving the global population.
High Level Approach	Pilots of major modules at different sites, possibly overlapping or even simultaneous, depending on the availability of central resources. Teams from the pilots become the SMEs for future implementation of the various modules. Overlapping phased roll outs of the different modules at subsequent sites.
Business Processes	With the broad scope of ERP, it is wise to establish a strict policy of not customizing the core software. This will in turn drive the need for globally standardized business processes, which may be unpopular with local elements. However, allowing variations could place at risk the ability to share data and report status globally. Standardization will ultimately be far more efficient than trying to implement for slightly different processes every time. It is extremely important that the pilot sites do not establish processes that cannot comply with regulations at a future deployment. Accordingly, global Legal and QA authorities should be consulted before committing to a new global business process.
System Ownership	Global owner for the overall ERP solution typically resides with the Chief Financial Officer (CFO). This is a reasonable assignment for management of the global contract and similar issues. It is also sensible to designate global owners for other modules of the system; for example, manufacturing modules to the global head of manufacturing, etc. This places ownership with an individual who is better acquainted with the relevant business processes. Since most companies do not validate their entire ERP solution, validation responsibility for the relevant GxP modules resides with the owners of the modules in question. Local ownership should model the global approach, i.e., the overall local ownership residing with the local CFO or finance head, but the modules owned within the relevant business areas. Local owners are responsible for local validation and ensuring all local and global information system management processes meet the local business needs of the system.

Issue	Consideration
Steering Committee	The global Steering Committee should have the global Business Process Owner (CFO), the global process (module) owners, a global QA representative, the CoE head, and given the scale of the project, the Chief Information Officer (CIO) or a designee. It is probably not practical to include local owners from pilot sites, although they should be considered ad hoc members. Local committees should be structured similarly, including a CoE member. Steering Committees should have the authority to make and enforce decisions, e.g., mandating process changes for reluctant users.
Project Team	A multi-tiered approach to setting up project teams is generally advisable for projects of this magnitude. A top level global project team will focus on planning and coordination, with a healthy emphasis on clearing or avoiding international obstacles. Sometimes this top level team might manage resources that are available to all other teams, for example a software testing team. It may well be ideal to have global project teams for each of the major business operations that are being brought under the umbrella of the ERP system as well, e.g., finance, supply chain, Human Resources, etc. These teams will coordinate with the operation level team and focus on issues like business process standardization and supporting local implementations within their areas. They will also coordinate local implementations, helping with things like managing validation of core functionality in order to maximize efficiency of the approach. Local teams may be organized by business process, and will interact heavily with the corresponding global teams. Local teams will leverage as much work from the pilots and subsequent roll outs as possible, but will still have some testing and validation work that must be managed locally. In all cases, project teams need to include business process SMEs, IT, at least one CoE member, and for GxP modules, QA representatives. For such large projects, it is also common to bring in external SMEs with experience in implementing this particular ERP tool.
User Requirements	Global user requirements should focus on commonalities desired for all sites, including technologies and compatibilities, basic functions, data management, etc. Requirements gathering should pay special attention to interfaces and associated data integrity implications. While in an ERP system, it is desirable to keep specific local requirements to a minimum. Differences in local laws and regulations may require the business process, and hence the software, to accommodate unique needs. In some cases, this can be addressed globally. For example, it is better to define a requirement such that a difference can be addressed by configuration rather than hard coding. User groups need to recognize that sometimes it is better to change the business process than it is to have an incompatible user requirement.
Legal and Regulatory	An approach should be defined that will provide compliance for all affected laws and regulations. A thorough analysis of national and state laws and regulations is necessary in order to recognize possible conflicts. While it is extremely unlikely that different nations GxP expectations differ, there may be other laws, e.g., related to employee privacy, which may conflict, for example, with record retention expectations related to training records. QA and Legal departments need to agree and document an approach to such conflicts. A conclusion may entail committing to limit certain sites to certain activities. For example, if a country has weak privacy protections perhaps no sensitive personal data should be stored there.

Issue	Consideration
Implementation Approach	Multiple pilots based on business function, centrally coordinated. Pilots of different modules may run concurrently, or at least overlapping, timing largely dependent on the ability of central authorities to support remote work. Commonly an external implementation partner will be engaged because of the huge increase in demand for IT, business, and validation resources. Subsequent implementations leverage knowledge and documentation from the pilot and later experience with each module.
Validation Approach	The entire application will not be validated. Only modules with GxP impact will undergo formal validation, although many of the system management operations will have to adhere to GxP standards in order to maintain the validated state of the GxP modules. Global validation of core functionality, probably in conjunction with implementation of a GxP module at a pilot site. Core validation documentation is managed by the CoE, and updated as necessary when additional sites implement functionality that will be used elsewhere as well. Purely local functionality and interfaces to purely local systems (if any), and all verification work on local infrastructure are managed by the local team. Requirements and user acceptance testing are also performed locally in order to accommodate local processes and to challenge local infrastructure. **Note:** that some of the local documentation will be globally useful for subsequent implementations.
CoE Responsibilities	For an ERP CoE, multiple CoE locations often make sense, not only to ensure "follow the sun" capability (i.e., tasks are passed around daily between work sites that are many times zones apart), but also to accommodate a large user group who may speak several languages. The CoE will be responsible for all system management tasks where centralization of responsibility and accountability makes sense. Where a "follow the sun" approach is required (i.e., tasks are passed around daily between work sites that are many times zones apart), this will be coordinated by the CoE, with formalized hand-off processes for problems and incidents that merit continual attention. General responsibilities include: • Manage overall revision level of system, probably including pushes of patches and updates to distributed servers • Own validation of core functionality • Coordinate with local support staff for integration of new equipment • Manage centralized database • Coordinate backup of centralized resources, maximizing availability as required by local users • Incident and problem management (second level) • Change management (shared) • Vendor management • Archiving and record retention • Support roll out at future sites • Support future site implementations and validations
Local Responsibilities	• Own validation of locally unique components and interfaces into the ERP • Management of local infrastructure (servers, LAN, devices, equipment) and interfaces • Incident and problem management (first level) • Change management (shared)

Issue	Consideration
System Management	• **Change control:** local and global elements • **Incident management:** level 1 local, level 2 global, interface to level 3 (supplier) owned by global CoE • **Problem management:** global • **Security management:** security groups defined globally, users managed locally • **Configuration management:** core elements managed globally by CoE, interfaces and any other unique local elements managed locally • **Training:** core curriculum developed globally, delivered locally (or via on-line tools) • **Document management:** core project documentation, validation, specifications owned globally. CoE should have access to local documentation.
Supplier Management	Expectations for supplier support for the system need to be agreed for all involved venues, and documented in a SLA with the CoE, backed by an UC between the CoE and the supplier. This should clearly define parameters for issues like off-hours support. If the supplier will ever have access to business data (e.g., for support or testing) the UC should also include protection of intellectual property and privacy.
Availability Management	ERP availability needs can vary based on module and circumstance, but in general high availability will probably be determined to be necessary. Strategies such as data mirroring and automated failover may be desired. Some of the GxP functionality such as manufacturing support may fall into this high availability category. In such cases the measures to ensure availability need to be part of the validation scope.
Data Management	Similar to the availability of the control aspects of the application noted above, data availability may be critical to both the integrity of the supply chain and to certain financial processes. Data from the ERP application needs to be available in a timely manner to facilitate product release and shipping, and it is possible that this data may need to be available at other sites besides the site of manufacture. The ERP system is will also involved in possible recall scenarios. Backup strategy needs to account for the criticality of this information, e.g., via real time or near real time backup. Data integrity concerns require ERP systems to have strictly controlled role-based access, a task which will demand diligence and close cooperation between local and global authorities.
Records Management	Records retention requirements for all countries where product was distributed should be satisfied. When the system is retired there is an expectation that the data is readable throughout its retention period. For proprietary formats it may be necessary to make special arrangements to retain this ability, e.g., via migration to a new format or arrangements with the supplier to recover data to a readable format on demand. When records are due for destruction this could either be managed by the CoE or a records management group. For a global information system, the responsible business authority needs to verify that none of the records scheduled for destruction are in a hold status to support litigation. Once the go ahead for destruction is received, all copies of the record should be purged. For a distributed system this may mean verifying destruction at multiple locations.

9.3 Global Chromatography Data and Control System

Description: Global information system providing standardized approach to controlling chromatography instruments, centralizing raw data management, and enabling the sharing of method and result files.

Issue	Consideration
Architecture Assumption	Centralized database with method and result files. Instrument control via local PC. Interface box with battery backup transfers results to PC in real time but can accumulate and store up to eight hours of data if communication is lost. PC sends raw and processed data to central database upon completion of run. Data reprocessing can be done by downloading raw data from central database to PC. Reprocessed data is versioned and automatically sent to central database.
High Level Approach	Initial pilot at one manufacturing site. Phased roll outs to other sites. Migrate retained raw data to new database for each site. Within individual sites roll out of control systems may be further phased as dictated by the replacement of PCs and instruments. This may require a work around to get control parameters from old equipment to the new database.
Business Processes	Global manufacturing needs QC (Quality Control) data available through a common platform so that results can be shared between sites, eliminating the need to repeat analyses. A business decision has been made to migrate existing raw data files to the new format because the new integration algorithm is more precise. Because of the large expense of replacing otherwise functional control systems, the replacement of equipment will proceed at a slower pace, necessitating a work around (software or manual) so that the control parameters are retained with the raw data.
System Ownership	Global head of QC or a designee will own the overall Chromatography Data System (CDS) solution, main supplier relationship, responsibility for core validation, and responsibility for CoE. The global owner needs to be identified as early in the project as possible and needs to participate actively (probably on the Steering Committee). Local head of QC or a designee will assume owner responsibility for local validation and ensuring all local and global information system management processes meet the local business needs of the system.
Steering Committee	The global Steering Committee should have the global Business Process Owner (head of QC), the global information system owner (possibly the same person), a global QA representative, the local owners from the pilot site, the CoE head, and maybe an SME from IT. Local committees should be structured similarly, but also include the global perspective of a CoE member. Steering Committees should have the authority to make and enforce decisions, e.g., mandating process changes for reluctant users.
Project Team	Initial global team involves process SMEs, and IT SMEs from pilot site, global IT, and possible external system implementers. After Pilot is complete and CoE is established, global project team consists of SME(s) from pilot site and CoE staff. Local project teams for subsequent implementations consist of local SME's, QA, and IT plus close and frequent participation from global team members, especially the CoE.

Issue	Consideration
User Requirements	Global user requirements should focus on commonalities desired for all sites, including technologies and equipment compatibilities, basic functions, data management, etc. User requirements need to account for major instrument clusters; it is possible that the system will have to accommodate several different brands of chromatograph because the expense of replacing a sizable portion of the estate is intolerable. Requirements should also account for different types of instruments to be included, e.g., Liquid Chromatography (LC), Gas Chromatography (GC), Gel Permeation Chromatography (GPC). Requirements gathering should pay special attention to interfaces and associated data integrity implications. Local requirements can be more detailed in technical requirements, e.g., down to specific models of equipment that must be compatible.
Legal and Regulatory	With the exception of diagnostic laboratories that might use this kind of system, data privacy is unlikely to be a concern. The primary focus will be on record integrity and preservation throughout the retention period. The global team should understand regional requirements for data retention, as well as the scope of required regulations. For example, in the US lab records supporting the release of blood products need to be retained longer than those for the release of drug product, and the European record retention requirement for blood product analysis is even longer. The relevant company authorities need to come to agreement on how to handle all differing or conflicting laws and regulations.
Implementation Approach	A pilot approach is highly recommended for any distributed system. The pilot project team should comprise both local and global members, with all of the latter and some of the former prepared to support the next implementation in the roll out. It may make sense to have the initial pilot cover only a small fraction of the intended supported equipment, enabling concentration on the centralized functionality and minimizing emphasis on local differences. Subsequent roll outs can expand the equipment scope at an appropriate rate.
Validation Approach	Global validation of core functionality, probably in conjunction with implementation at a pilot site. Core validation documentation is managed by the CoE, and updated as necessary when additional sites implement functionality that will be used elsewhere as well. Purely local functionality, interfaces to purely local systems, and all verification work on local devices or infrastructure are managed by the local team. Local testing will concentrate on verifying that the local setup is functioning according to global norms, and may include testing of an extended range of supported instruments. The latter should be captured in documentation managed by the CoE, enabling facile qualification of those instruments at future sites.

Issue	Consideration
CoE Responsibilities	The CoE will be responsible for all system management tasks where centralization of responsibility and accountability makes sense. Where a "follow the sun" approach is required (i.e., tasks are passed around daily between work sites that are many times zones apart), this will be coordinated by the CoE. General responsibilities include: • Manage overall revision level of system, probably including pushes of patches and updates to distributed servers • Own validation of core functionality • Coordinate with local support staff for integration of new equipment • Manage centralized database • Coordinate backup of centralized resources, maximizing availability as required by local users • Incident and problem management (second level) • Change management (shared) • Vendor management • Archiving and record retention • Manage a list of instruments that have been qualified with the CDS • Provide consulting support, and possibly document templates, for sites wishing to qualify new brands or models of instruments • Support implementation and validation of the CDS at future locations
Local Responsibilities	• Own validation of locally unique instruments and interfaces into the CDS • Management of local infrastructure (servers, LAN, interfaces, equipment) • Deviation management • Incident and problem management (first level, usually through the service desk) • Change management (shared)
System Management	• **Change control:** local and global elements • **Incident management:** level 1 local, level 2 global, interface to level 3 (supplier) owned by global CoE • **Problem management:** global • **Security management:** security groups defined globally, users managed locally • **Configuration management:** core elements managed globally by CoE, interfaces and instruments managed locally • **Training:** core curriculum developed globally, delivered locally (or via on-line tools) • **Document management:** core project documentation, validation, specifications owned globally. CoE should have access to local documentation.
Supplier Management	Expectations for supplier support for the system need to be agreed for all involved venues, and documented in a SLA with the CoE, backed by an UC between the CoE and the supplier. This should clearly define parameters for issues like off-hours support. Instrument support should be managed locally, with the same service level management expectations. If the supplier will ever have access to business data (e.g., for support or testing) the UC should also include protection of intellectual property and privacy.

Issue	Consideration
Availability Management	Depending on the nature of the products supported, availability could be a critical issue; if the product has an extremely short shelf life then concepts like immediate mirroring of data and failover to a hot site might be warranted. Planned down time can be critical as well if users need to access information stored at another location. Mirroring of information might be a solution to this issue as well. For less critical analyses, less expensive availability management strategies that reflect risk are appropriate.
Data Management	As above, data availability may be critical to the integrity of the supply chain for short shelf life products. Data from the CDS application needs to be available in a timely manner to facilitate product release, and it is possible that this data may need to be available at other sites besides the site of manufacture. CDS systems record real time data, and depending on the nature of the instrument and the analysis, the density of the accumulated data can be quite high. The cost of losing such information can be extremely high, for example making a batch of product unreleasable or forcing a recall. Backup strategy needs to account for the criticality of this information, as well as the time required for backup. This can affect such decisions as whether the process should occur real time or near real time. Data integrity concerns require CDS systems to have strictly controlled role-based access, a task that will demand diligence and close cooperation between local and global authorities.
Records Management	Records retention requirements for all countries where product was distributed should be satisfied for all types of products analyzed using the software. When the system is retired there is an expectation that the data is readable throughout its retention period. For proprietary formats it may be necessary to make special arrangements to retain this ability, e.g., via migration to a new format or arrangements with the supplier to recover data to a readable format on demand. When records are due for destruction this could either be managed by the CoE or a records management group. For a global information system, the responsible business authority needs to verify that none of the records scheduled for destruction are in a hold status to support litigation. Once the go ahead for destruction is received, all copies of the record should be purged. For a distributed system this may mean verifying destruction at multiple sites.

9.4 Global Drug Safety System Implementation

Description: Global information system that tracks reported adverse events and manages the processing of all cases from initial triage through reporting and case closure. Allows:

- Accurate recording of events and products (suspect, company, prior, and concomitant), coding terms against industry standard thesauri,
- Conducting seriousness, causality, and listedness/expectedness assessments, reporting of adverse events to appropriate health authorities.

Provides standard drug safety reports for paper and electronic reporting to meet expedited and periodic reporting requirements supporting the varying requirements of global regulatory authorities.

Issue	Consideration
Architecture Assumption	Centralized system with mirrored local servers where necessary to address performance issues.
Business Processes	The Business Process Owner uses the application to support the collection, detection, assessment, monitoring and reporting to regulatory authorities of adverse effects associated with the company's pharmaceutical products.
System Ownership	Global owner for the overall drug safety solution, main supplier relationship, responsibility for core validation, responsibility for CoE. Local owner responsible for validation of local regulatory reporting in cooperation with the CoE and ensuring all local and global information system management processes meet the local business needs of the system.
Steering Committee	The global Steering Committee should have the global Business Process Owner, a global QA representative, IT, the CoE head, and user representation. The latter should include someone local and possibly one or more local owners from other sites.
Project Team	Project teams need to include business process SMEs, IT, at least one CoE member, and QA. It would be very wise to include users as well, representing both those who manage records, those who create them and those responsible for generating the reports to the regulatory authorities.
User Requirements	Global user requirements should focus on commonalities desired for all sites, including technologies and compatibilities, basic functions, record management, reporting, etc.
Legal and Regulatory	An approach must be defined that will provide compliance for all affected laws and regulations. A thorough analysis of national and state laws and regulations is necessary in order to recognize possible conflicts. While it is extremely unlikely that different nations GxP and Good Pharmacovigilance Practices (GPV) expectations differ, there may be other laws, e.g., related to employee privacy, which may conflict for example with record retention expectations related to training records. QA and Legal departments need to agree and document an approach to such conflicts.

Issue	Consideration
Implementation Approach	Under the assumption that a number of regional drug safety applications are already being used in the company, the following steps are recommended. A series of workshops should be conducted with the global Business Process Owners to design a "TO BE" global business process and workflow. The system will be configured to support the new "TO BE" business process and then an additional series of workshops should take place using the configured system to confirm both the "TO BE" business process and the supporting configuration. Concurrently a team of business and technical personnel have to create a normalized data file from the different regional drug safety databases. Data mapping and final data normalization rules will then be defined at workshops with the Business Process Owners from which a data migration specification can be developed. Code will be written and tested, dry runs conducted, and then a migration qualification will be performed using a series of automated and manual tests.
Validation Approach	Global validation of system functionality in support of the global business process. The CoE manages global validation documentation and local reporting documentation.
CoE Responsibilities	The CoE will be responsible for all system management tasks. Where a "follow the sun" approach is required, the CoE will coordinate this, with formalized hand-off processes for problems and incidents that merit continual attention. General responsibilities include: • Manage overall revision level of system • Own validation • Manage centralized database • Coordinate backup of centralized resources, maximizing availability as required by local users • Incident and problem management (second level) • Change management (shared) • Vendor management • Archiving and record retention • Support roll out at future sites • Support future implementations and validations
System Management	• **Change control:** local and global elements • **Incident management:** level 1 local, level 2 global, interface to level 3 (supplier) owned by global CoE • **Problem management:** global • **Security management:** security groups defined globally, users managed locally • **Configuration management:** managed globally by CoE • **Training:** core curriculum developed globally, delivered locally (or via on-line tools) • **Document management:** project documentation, validation, specifications owned globally
Supplier Management	Expectations for supplier support for the system need to be agreed for all involved venues, and documented in a SLA with the CoE, backed by an UC between the CoE and the supplier. This should clearly define parameters for issues like off-hours support. If the supplier will ever have access to business data (e.g., for support or testing) the UC should also include protection of intellectual property and privacy.
Availability Management	Drug safety data is critical to patient and product safety. High availability is a necessary requirement. Strategies such as data mirroring and automated failover may be desired. The measures to ensure availability need to be part of the validation scope.

Issue	Consideration
Data Management	Backup strategy needs to account for the criticality of this information, e.g., via real time or near real time backup. Data integrity concerns require drug safety systems to have strictly controlled role-based access, a task that will demand diligence and close cooperation between local and global authorities.
Records Management	Records retention requirements for all countries where documents are applicable must be met. When the system is retired there is an expectation that documents are readable throughout their retention periods.

9.5 Global Electronic Document Management System

Description: Global information system providing unified control over documentation, including management of approvals, versioning, and retention. This is a large investment with critical regulatory and business impact.

Issue	Consideration
Architecture Assumption	Approach can either be centralized or distributed. Distributed approaches will have to deal with synchronization issues that could be problematic with such a system. While a centralized system avoids that, there will need to be local configurations to satisfy local laws for privacy and retention.
High Level Approach	Pilot at a major site, followed by phased roll outs to allow for local elements to be properly designed and configured. Team from the pilots becomes the SMEs for future implementation of the various modules.
Business Processes	Depending on configuration, the user may create a document from within the system or save it to the system after external creation. Some solutions may build in workflow, for example a check in/check out process to manage versions edited by a group. It may also include routing for approvals. Ergo the system will have to comply with electronic record rules and may have to comply with electronic signature rules as well. The system should be able to support different business rules based on geography in order to meet local legal requirements for document retention. For documents used in multiple nations it should be possible to adjust the retention period as necessary. It may also be necessary to limit the visibility of certain documents (e.g., SOPs) only to the sites where they are applicable.
System Ownership	Global owner for the overall solution may not have an obvious home. If there is a global information or records management function, the head of this may be a logical choice. QA is another possibility, although this would require dealing with both GxP and non-GxP users. Local ownership should be placed in a records management department. Local owners are responsible for local validation (probably limited to validation of the locally configured parameters related to retention) and ensuring all local and global information system management processes meet the local business needs of the system.

Issue	Consideration
Steering Committee	The global Steering Committee should have the global Business Process Owner, a global QA representative, IT, the CoE head, and user representation. The latter should include someone local and possibly one or more local owners from other sites. Depending on the architecture choice, a local committee may not be necessary. This will probably be the case for a centralized system. If a distributed architecture is selected it may pay to set up a local committee along lines similar to the global one.
Project Team	In all cases, project teams need to include business process SMEs, IT, at least one CoE member, and QA. It would be very wise to include users as well, representing both those who manage records and those who create them.
User Requirements	Global user requirements should focus on commonalities desired for all sites, including technologies and compatibilities, basic functions, record management, etc. Requirements gathering should pay special attention to interfaces and associated data integrity implications. Local requirements will generally concentrate on configuration issues, such as setting up retention policy within the application, security groups, etc.
Legal and Regulatory	An approach should be defined that will provide compliance for all affected laws and regulations. A thorough analysis of national and state or provincial laws and regulations is necessary in order to recognize possible conflicts. While it is extremely unlikely that different nations GxP expectations differ, there may be other laws, e.g., related to employee privacy, which may conflict for example with record retention expectations related to training records. QA and Legal departments need to agree and document an approach to such conflicts.
Validation Approach	Global validation of core functionality. Core validation documentation is managed by the CoE, and updated as necessary when additional sites implement functionality that will be used elsewhere as well. Purely local functionality and interfaces to purely local systems (if any), and all verification work on local infrastructure are managed by the local team. Requirements and user acceptance testing are also performed locally in order to accommodate local processes and to challenge local infrastructure. **Note:** that some of the local documentation may be globally useful for subsequent implementations.
CoE Responsibilities	The CoE will be responsible for all system management tasks where centralization of responsibility and accountability makes sense. Where a “follow the sun” approach is required (i.e., tasks are passed around daily between work sites that are many times zones apart), this will be coordinated by the CoE, with formalized hand-off processes for problems and incidents that merit continual attention. General responsibilities include: • Manage overall revision level of system, probably including pushes of patches and updates to distributed servers • Own validation of core functionality • Coordinate with local support staff for integration of new equipment • Manage centralized database • Coordinate backup of centralized resources, maximizing availability as required by local users • Incident and problem management (second level) • Change management (shared) • Vendor management • Archiving and record retention • Support roll out at future sites • Support future site implementations and validations

<table>
<tr><th>Issue</th><th>Consideration</th></tr>
<tr><td>Local Responsibilities</td><td>Management of local infrastructure (servers, LAN, devices, equipment) and interfaces, if any
Incident and problem management (first level)
Change management (shared)</td></tr>
<tr><td>System Management</td><td>Change control: local and global elements
Incident management: level 1 local, level 2 global, interface to level 3 (supplier) owned by global CoE
Problem management: global
Security management: security groups defined globally, users managed locally
Configuration management: core elements managed globally by CoE, interfaces and any other unique local elements managed locally
Training: core curriculum developed globally, delivered locally (or via on-line tools)
Document management: core project documentation, validation, specifications owned globally. CoE should have access to local documentation.</td></tr>
<tr><td>Supplier Management</td><td>Expectations for supplier support for the system need to be agreed for all involved venues, and documented in a SLA with the CoE, backed by an UC between the CoE and the supplier. This should clearly define parameters for issues like off-hours support.

If the supplier will ever have access to business data (e.g., for support or testing) the UC should also include protection of intellectual property and privacy.</td></tr>
<tr><td>Availability Management</td><td>Availability needs can vary based on document type, but the need for high availability for some kinds of documents (e.g., SOPs) will probably drive the application of a high availability requirement for the application.

The architecture choice will have some impact on the availability strategy. If a distributed solution is selected, mirroring of data on both the local and a remote server could be a viable solution. Storage in the cloud might be another.</td></tr>
<tr><td>Data Management</td><td>Backup strategy needs to account for the criticality of this information, e.g. via real time or near real time backup.

Data integrity concerns require EDMS systems to have strictly controlled role-based access, a task that will demand diligence and close cooperation between local and global authorities.</td></tr>
<tr><td>Records Management</td><td>Records retention requirements for all countries where documents are applicable should be met.

When the system is retired there is an expectation that documents are readable throughout their retention periods.

When records are due for destruction this should be managed through a records management group. For a global information system, the responsible business authority needs to verify that none of the records scheduled for destruction are in a hold status to support litigation. Once the go-ahead for destruction is received, all copies of the record should be purged. For a distributed system this may mean verifying destruction at multiple locations.</td></tr>
</table>

9.6 Global Clinical Data System

Description: Global information system used to collect, manage and review clinical data. This is a large investment with critical regulatory and business impact.

Issue	Consideration
Architecture Assumption	Web-based workflow driven centralized database system. SaaS solutions are often very well suited to clinical data management because of the capacity flexibility.
Business Processes	The Business Process Owner designs a clinical database to model their clinical protocol and meet their needs for storing and retrieving data. They also create on-line representations of their case report forms for data entry, verification, and editing. Data is validated, discrepancies are resolved and data is merged. Data can then be accessed, retrieved and analyzed.
System Ownership	Global owner for the overall clinical trial management solution, main supplier relationship, responsibility for core validation, responsibility for CoE.
Steering Committee	The global Steering Committee should have the global Business Process Owner, a global QA representative, IT, the CoE head, and user representation. The latter should include someone local and possibly one or more local owners from other sites.
Project Team	Project teams need to include business process SMEs, IT, at least one CoE member, and QA. It would be very wise to include users as well, representing both those who manage records and those who create them.
User Requirements	Global user requirements should focus on commonalities desired for all sites, including technologies and compatibilities, basic functions, record management, etc. Requirements gathering should pay special attention to interfaces and associated data integrity implications.
Legal and Regulatory	An approach must be defined that will provide compliance for all affected laws and regulations. A thorough analysis of national and state laws and regulations is necessary in order to recognize possible conflicts. While it is extremely unlikely that different nations GxP expectations differ, there may be other laws, e.g., related to employee privacy, which may conflict for example with record retention expectations related to training records. QA and Legal departments need to agree and document an approach to such conflicts.
Implementation Approach	Pilot of the application via a large clinical trial is recommended. This reflects the complexity of configuration required for workflows, creating and managing metadata standards, etc. In addition to developing the application itself, new business processes supporting it will be required. Subsequent implementations leverage knowledge and documentation from the pilot.
Validation Approach	Global validation of system functionality in support of the global business process. The CoE manages global validation documentation and local reporting documentation.

Issue	Consideration
CoE Responsibilities	The CoE will be responsible for all system management tasks. Where a "follow the sun" approach is required (i.e., tasks are passed around daily between work sites that are many times zones apart), this will be coordinated by the CoE, with formalized hand-off processes for problems and incidents that merit continual attention. General responsibilities include: • Manage overall revision level of system • Own validation • Manage centralized database • Coordinate backup of centralized resources, maximizing availability as required by local users • Incident and problem management (second level) • Change management (shared) • Vendor management • Archiving and record retention • Support roll out at future sites • Support future implementations and validations
System Management	• **Change control:** local and global elements • **Incident management:** level 1 local, level 2 global, interface to level 3 (supplier) owned by global CoE • **Problem management:** global • **Security management:** security groups defined globally, users managed locally • **Configuration management:** managed globally by CoE • **Training:** core curriculum developed globally, delivered locally (or via on-line tools) • **Document management:** project documentation, validation, specifications owned globally
Supplier Management	Expectations for supplier support for the system need to be agreed for all involved venues, and documented in a SLA with the CoE, backed by an UC between the CoE and the supplier. This should clearly define parameters for issues like off-hours support. If the supplier will ever have access to business data (e.g., for support or testing) the UC should also include protection of intellectual property and privacy.
Availability Management	There is a high availability requirement for this application. Mirroring of data on a local and a remote server could be a viable solution. Storage in the cloud might be another.
Data Management	Backup strategy needs to account for the criticality of this information, e.g., via real time or near real time backup. Data integrity concerns require clinical systems to have strictly controlled role-based access, a task that will demand diligence and close cooperation between local and global authorities. If a SaaS application was used during a clinical trial, the end of the project should include the removal of the data from the cloud and appropriate archival. This process is often called "de-clouding".
Records Management	Records retention requirements for all countries where documents are applicable must be met. When the system is retired there is an expectation that documents are readable throughout their retention periods. When records are due for destruction this should be managed through a records management group. For a global information system the responsible business authority needs to verify that none of the records scheduled for destruction are in a hold status to support litigation. Once the go ahead for destruction is received, all copies of the record should be purged. For a distributed system this may mean verifying destruction at multiple locations.

10 Appendix 6 – Quality Risk Management Approach

Risk management principles should be a primary consideration in all aspects of planning and operational activities.

The following QRM approach is based on that described in *ISPE GAMP® 5* [4], and is aligned with the ISO 14971 [24] and ICH Q9 [25] frameworks. It is an iterative approach used throughout the life cycle from concept to retirement.

This Appendix uses the following key terms taken from *ISPE GAMP® 5* [4]:

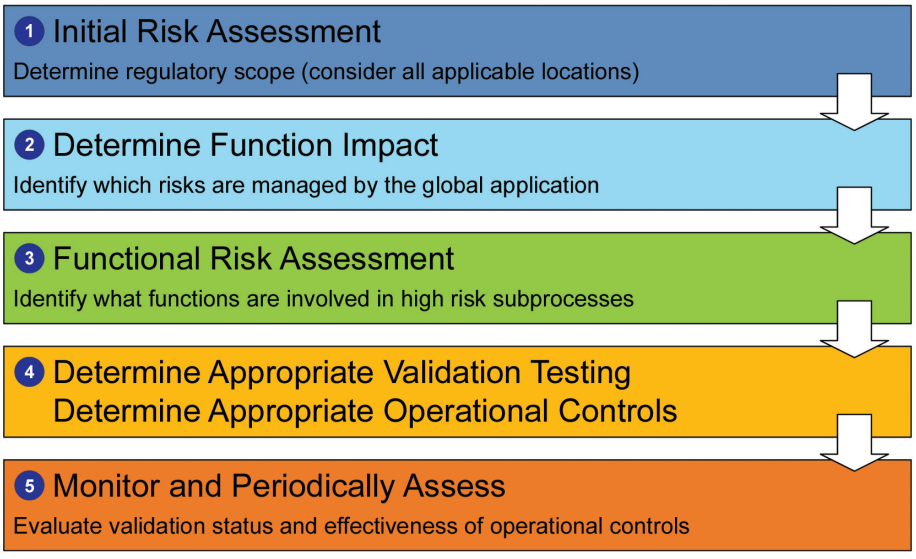
- **Harm:** Damage to health, including the damage that can occur from loss of product quality or availability.
- **Hazard:** The potential source of harm (ISO/IEC Guide 51 [26]).
- **Risk:** The combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51 [26]).
- **Severity:** A measure of the possible consequences of a hazard.

A five step process is suggested:

1. Perform initial risk assessment and determine impact
2. Identify functions with impact on patient safety, product quality, and data integrity
3. Perform functional risk assessments and identify controls
4. Implement and verify appropriate controls
5. Review risks and monitor controls

These steps are described in Figure 10.1.

Figure 10.1: Quality Risk Management Process



Step 1 – Perform Initial Risk Assessment and Determine Impact

An initial risk assessment should be performed based on the defined and documented intended use. The initial risk assessment should be based on process risk information and product requirements.

The results of this initial risk assessment should include a decision on whether the system is GxP regulated. This assessment should also include an overall assessment of the level of impact on patient safety or public health, and may also consider other risk areas such as data privacy and security.

The level of effort, formality, and documentation of any subsequent steps should be determined based on level of risk and product impact.

If the detailed nature of data to be collected by the system is known at this point, a similar assessment of any potentially applicable data privacy rules is also essential. National data privacy laws vary greatly, and knowing these can be critical for requirements planning.

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

System functions and features that have an impact on patient safety, product quality, and data integrity should be identified by building on information gathered during Step 1, referring to relevant specifications, and taking into account the product development approach, product architecture, and the nature of the hardware and software components involved.

This should be performed based on substantially complete specifications and should account for the all global business process risks as well as any risks derived from local variation.

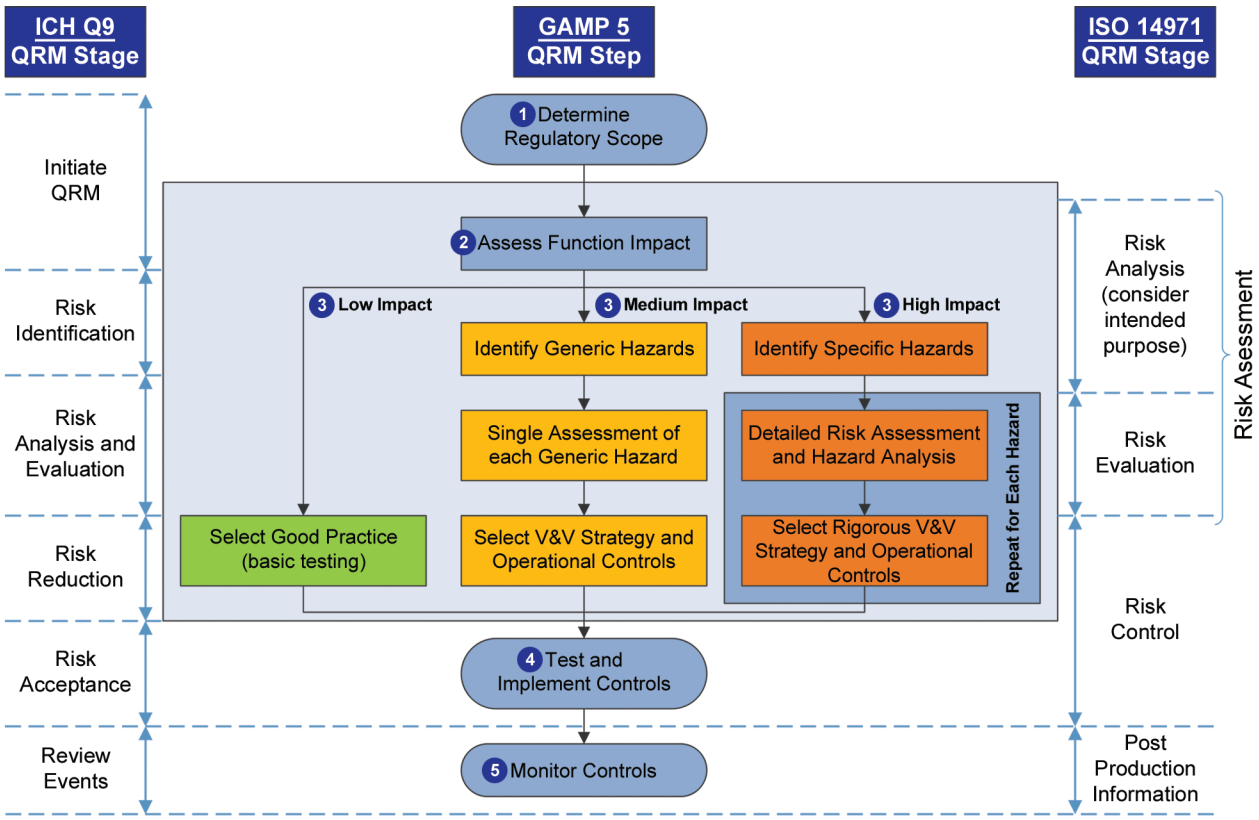
Any regulated electronic records and signatures should be identified.

Step 3 – Perform Functional Risk Assessments and Identify Controls

Functions identified during Step 2 should be assessed by considering possible hazards, and how the potential harm arising from these hazards may be controlled. Any differences in risk levels based on local variation (e.g., because of local legal requirements or the way the system is used locally) should be noted.

It may be necessary to perform a more detailed assessment that analyzes further the severity of harm, likelihood of occurrence, and probability of detection (*ISPE GAMP® 5, Appendix M3* [4] provides one example of such an approach).

Figure 10.2: Relationship between *ISPE GAMP® 5* [4], ISO 14971 [24], and ICH Q9 [25] approaches



The decision as to whether to perform detailed assessment for specific functions should be dealt with on a case-by-case basis and documented.

System architecture may affect this decision. For example, consider a global application managed from a single site with user access through a web browser versus an application based on client-server architecture, with hourly global replication of changes to local data. Data configuration management in the first case is straightforward, but in the second instance the possibility exists that if data configuration is not managed effectively, synchronization of data across sites or regions may be lost, threatening the ability to share or exchange data. For further information, see Appendix 3.

In this example, data management of the centralized web-based system would follow the low impact path through the process, focusing on good IT practice. The client-server example, however, would follow either the medium or high impact path, depending on the criticality of the system and data, and could lead to additional controls being established.

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

- Restriction of intended use
- Restriction to specific users
- Enhanced training

- Modification of application functionality and features
- Selection or rejection of specific platforms
- Modification of system design or architecture
- Limiting or controlling availability of the application
- Modification or enhancement of user instructions
- Increased rigor of testing

Step 4 – Implement and Verify Appropriate Controls

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

The verification activity, typically design review and design verification as well as testing, should demonstrate that the controls are effective in performing the required risk reduction.

Controls that are implemented locally may be verified locally or centrally, although assessment of their effectiveness needs to include local feedback.

Step 5 – Review Risks and Monitor Controls

Following testing and implementation of required controls, residual risk should be evaluated. If residual risk is not acceptable, additional controls may be required.

A process should be established to collect and review information about the system during operation. Previously unanticipated hazards, or examples of risk control failure should be reviewed, and appropriate new or modified risk control measures identified, if necessary.

Controls that are implemented locally may be monitored locally or centrally, although assessment of their effectiveness needs to include local review.

11 Appendix 7 – Global Project Management Considerations

The successful implementation of a compliant and validated global information system is dependent upon on how well the basic concepts and process of project organization and project management has been performed. Failure is usually caused by the lack of sound, basic organizational processes or effective project management.

A single person needs to be assigned as the overall Project Manager, regardless of whether a hierarchical or matrix organizational structure is chosen for a project. It is helpful if the Project Manager has experience with regulated systems, although this may be mitigated by an experienced validation team leader.

The validation team leader should have an active and continuous role in the project for several years, and should have strong leadership, administrative, and technical abilities. Leadership skills should include the ability to recognize and understand the importance of regulatory requirements. The validation team leader should also be aware of various cultural customs, and to react to them appropriately.

The elements of the project that will be managed globally and those elements that will be managed locally, should be decided and clarified from the outset, along with applicable quality standards to be applied. This decision should consider the local availability of appropriately skilled resources and the capacity to provide support from global resources, if needed.

For further information on issues that need to be addressed in taking a locally developed and documented system and making it a global information system, see Appendix 10.

The need for conflict resolution can be magnified in global projects, so this is considered an important skill for project management. Cultural differences are considered a critical element, even for small geographical areas with cultural diversity, as this has the potential to seriously disrupt a project if not understood and respected. Conflicts should be dealt with and resolved within the project's organizational structure, with all cultural differences respected.

For a global project, the managerial emphasis may be focused on timely and on-budget delivery of the project. Care should be taken to align this emphasis with global and local regulatory needs. In addition, the Project Manager should recognize cultural issues that affect project execution. For example, not all cultures will react the same way to a request to work more than the customary work week to keep to schedule.

The Project Manager is usually responsible for delivering the project against the validation plan (see Appendix 1). Aspects of global projects that should be given specific attention by project management include:

- Regulatory
- System ownership
- Technical approach
- System architecture
- Data management
- Procedural
- Cultural
- Funding

- Handover from project team to operational team (this is more complex because a global support organization may have to increase scope of support to accommodate new local implementations with some level of uniqueness)

Principal considerations for the Project Manager include:

- Overall project
- Budget
- Cost allocations
- The need for commitment of key team members

For further information on the regulatory, system ownership, technical approach, system architecture, data and procedural aspects, see Appendix 1.

11.1 Cultural

Cultural differences within organizations should be considered at the Concept phase. Language related aspects should be taken into consideration.

11.1.1 Language

All communication and documentation should be clear and transparent to the entire global business community, as well as the regulatory authorities. Use of jargon, e.g., technical slang or ambiguous expressions should be avoided, unless specifically defined in a project glossary or definitions section.

11.1.1.1 Legal Requirements

Legal requirements for a business activity can differ substantially from region to region. The legal interpretation of language can differ from region to region and from legal jurisdiction to legal jurisdiction.

Legal advice should be obtained from key sites involved at the very start of the project and throughout the project life cycle.

Legal requirements can also impact technical aspects of system design and architecture. For example, the expectations for protection of personal privacy or intellectual property vary greatly based on the location of users and/or people whose personal data may be recorded in a database. This can affect several aspects of planning, design, and operation:

- Whether data should be encrypted and to what extent
- Whether data should be stored on equipment in nations with weak privacy protection
- Whether data should be stored on equipment in nations with weak intellectual property protection
- Management of non-production environments that may have production data with private information
- Requirements relating to who can have access and to what level for system support
- Training requirements for users and/or system support staff

The regulated company should identify the relevant legislation in each country of installation and perform a suitable risk assessment to identify the impact and risks to the project.

11.1.1.2 Corporate Standards

Companies should define a corporate language and standards of communication, which should be communicated across the organization:

- Project management and the local team leaders should be proficient in this language
- Native speakers should review documentation for compliance with corporate standards and for accuracy and clarity
- Non-native speakers should review documentation for ease of comprehension

11.1.1.3 Local Standards

Local language specific standards should be established early in the project. Operating procedures or training may be legally required to be in the local language. These requirements should be recognized at the start of the project, since it may require significant resources to provide translation, especially if subject matter expertise is necessary to accurately translate.

There may be legal requirements in some countries for displayed screens to be shown in the local language and for any local customizing to be documented in the local language.

11.1.1.4 Documentation Standards

Consideration should be given to use of compatible documentation sets, based on legal and corporate language requirements using standard application software and templates, e.g.:

- Templates for deliverables
- Document management
- Project plans and reports
- Specifications
- Test plans and test scripts
- SOPs

11.1.1.5 Communication Standards

Communication planning and adequate communication is considered critical to a system implementation that is global. Use of local languages to discuss and communicate complex issues is recommended, with the corporate language used to confirm conclusions and appropriate actions. For international meetings, discussions, including technical discussions, need to be held in a language common to all participants, but leaders need to be sensitive to language issues and make an effort to verify understanding and consensus.

Special consideration should be given to sensitivity and use of specific words, e.g., “Yes” may be taken to mean “understood” but not imply agreement and “No” may be interpreted as rude and aggressive in some regions. Project managers should be particularly sensitive in this area, and should ensure that understanding is mutual.

Some words that are translated literally may not mean the same thing to native speakers. For example, a German speaker who is fluent in English might say “Execute testing until June 1”, whereas a native English speaker would say “Execute testing by June 1.” Taken literally, it is possible to interpret the former as an instruction to test continually until the calendar reaches June 1, while the actual intent of both statements was simply that testing should be completed no later than June 1.

11.1.1.6 Executive Summaries

In cases where documentation in local languages may have some exposure outside of that region, consideration should be given to providing an executive summary in English, or in the official corporate language, in order to promote maximum global understanding of the scope and purpose of such documents.

11.1.2 Geographical

Projects with widely dispersed geographical locations may create problems of communication, coordination, and support.

11.1.2.1 Communication

Improvements in communication and virtual presence tools have made some aspects of global communication easier, e.g., video conferencing. Communication with remote teams, however, remains a challenge and can become problematic.

Consideration should be given to the difficulties of communication and coordinating team activities over multiple time zones. For example, the scheduling of teleconferences that intrude on one or more groups’ personal time can be interpreted as a sign that they are of less importance or priority, which can significantly impact both morale and productivity. If this is unavoidable, the inconvenience should be spread equally; this can send a message to the remote team that they are valued.

Teams should also avoid making decisions without input from remote sites based on the inability to get a local conference room at a time when the members in remote locations are accessible. Such actions can send a negative message to remote users or members of the team and communication activities should be planned accordingly.

General communications regarding the project should reach all parties as close to simultaneously as possible. For example, North American associates should not be asked to participate in a teleconference at 2:00 AM Eastern Standard Time (EST) and 11:00 Pacific Standard Time (PST) that is taking place in Europe at 8:00 AM Central European Time (CET), but nor should they get the news several days later, or worse, second hand from European colleagues. Holding a second call at 8:00 AM PST/11:00 AM EST will keep everyone feeling valued.

Occasionally, global project managers may have to deal with passive-aggressive behaviors that can manifest in such ways as failure to attend conference calls, lateness of deliverables, etc. The Project Manager needs to be able to distinguish between such problematic behavior and actual justifiable reasons. A face to face kickoff meeting can build relationships that can head off such problems, but if they do occur a very strong communication effort between the parties is needed.

11.1.2.2 People and Travel

Distributed locations still create the need for travel, which should be planned and budgeted. Local project managers can find it much easier to respect and trust a global Project Manager who sees value in coming to their site, meeting and briefing the local team, and listening to their ideas. It is inadvisable to schedule all face to face meetings at the headquarters site.

Consolidating the global project development activities at one location provides a basis for effective communication and working, but has two impacts with negative connotation:

- It creates potential problems of temporary relocation of people and services
- Local sites may still feel left out of the process even if they are represented by temporarily relocated staff from their location

Consolidating the global project development activities at one location can be an effective solution if appropriately managed, and if frequent and detailed communications are treated as critical project deliverables.

Local holidays and seasonal traditions should be taken into account, especially national holidays.

11.1.2.3 Documentation

Location and availability of documentation is considered vital for both company and regulatory needs. Generally, documentation is held centrally with a process for recording, storing, and retrieving documentation (including controlled copying) that will meet local requirements for document accessibility (e.g., to support an audit).

A globally accessible EDMS for project documentation approval is usually considered the best solution, but can be expensive to implement. Regulated companies may consider that a centrally approved rationalized approach for a paper based circulation is a viable and more pragmatic option.

Where an EDMS is in place, managing test documentation may be problematic if a purpose built electronic testing application is not established. EDMSs can continue to be used after the global information system project. This may substantially decrease the cost of supporting changes. Offshore testing may be preferred for cost reasons, but can present several challenges. If testing is to be approved at a site other than the test site, either paper is shipped or a solution should be agreed with QA for scanning and approval of other than original records. While regulators may accept true copies, sometimes QA units are more conservative. In addition, the disposition of the original records needs to be agreed upon. It is unlikely that a contracted supplier of testing services will be willing to maintain original records throughout the required retention period.

For SaaS solutions, much of the documentation may not be routinely accessible to the regulated company. This documentation should be verified during supplier audit, and as part of contract negotiations, an agreement should be reached to provide regulator access during inspections, if required. If the SaaS supplier finds this unacceptable the regulated company has to accept that risk or find another supplier.

Turnaround time for documentation in support of audits should be considered, including regulator access to SaaS supplier documentation. The OLA or SLA should define these requirements and commitments.

11.1.2.4 Supplier Availability and Support

Supplier availability to support multiple sites on a global basis should be established early in the project to ensure that sufficient coverage is available, and to establish alternative support mechanisms for locations where suppliers can provide only lower levels of support.

Commonly, local resources may be contacted in cooperation with the supplier to ensure successful implementation of new technology.

11.1.3 Legal

A review of the legal requirements covering all aspects of implementing and using the business process/system should be performed. Legal advice should be obtained from the key sites involved at the very start of the project and throughout its life cycle.

11.1.3.1 Work, Health, and Safety Rules

Project management should work with the Legal and Human Resource departments of geographical areas involved in the project to determine local work, health, and safety rules. They should take these rules into account when building their teams, developing timelines, and assigning work throughout the project life cycle, e.g., audit trail and use of confidential personal information, or local health and safety rules.

11.1.3.2 Certification

Geographical locations may require certification of:

- Systems
- Equipment
- Infrastructure
- Suppliers
- Personnel

For each element, there may be a need to have certification to an external standard or by an external organization. Documentation of certification may also have a legally defined standard.

11.1.3.3 Contractual Issues/Procurement

Systems, equipment, and services may be used in many different geographical regions from that in which they are obtained.

Purchase contracts should be reviewed in regard of any local regulatory implications. For example, the terms of a warranty may not allow local service outside the country of purchase.

Consideration needs to be given to contractual issues when portions of systems are located at another organization (such as a partner, supplier, or application service provider). Ownership of and responsibilities for project activities should be identified.

When negotiating with suppliers for global support, it should be ensured that the support organization can handle all of the sites requiring support, both in terms of time zone coverage and language.

It may be advisable to consider strategically located support centers to be a primary factor in supplier selection and contract negotiation. It is considered better to have one supplier support all locations. Although engaging two different support organizations may seem like a viable (and possibly less expensive) option, it can be complicated to ensure that they are aligned, and misalignment can cause significant difficulty.

11.2 Funding

Validation of global projects should be adequately funded and managed throughout. This should be identified, decisions should be made and documented, and then properly communicated to everyone involved within a timeframe that allows for the corporate budgeting schedule.

How this is handled will have serious impact (either positive or negative) on the resources made available to the validation of a global project and its timeline, e.g., is the project itself going to have a global budget that covers all expenses including:

- Costs for all parties that travel to attend meetings, training sessions, etc.
- Additional resource and capacity costs
- Hardware and software costs
- Global and local customization costs
- Outsourcing costs (both project and operational)
- Enhancement costs
- Maintenance and support

Each location involved may be expected to absorb all of the expenses listed above within their departmental budgets for their personnel involved in the global project and/or any associated hardware and software (including licenses).

All identified costs may be divided between the global budget and local departmental budgets, but should be managed. Consistency of the budget with a hierarchical or matrix organization is helpful.

12 Appendix 8 – Supplier Management and Good Practice

This Appendix is intended to provide guidance on good practice for suppliers of products and services in support of a global information system. It may also be used as the basis for assessment of such suppliers. It is applicable to any supplier of products, or provider of services associated with system development, maintenance, or support.

The term supplier may refer to any company, function or project within a regulated company, or to any third party supplier, contracted to provide products or services associated with global systems, including comprehensive solutions like SaaS.

General supplier good practice as described in *ISPE GAMP® 5* [4] is appropriate to the development of global information systems. Guidance is given in this Appendix for suppliers providing software development and support (e.g., product suppliers, integrators), and suppliers providing managed services, cloud operations, or SaaS.

12.1 Supplier Good Practice – Development and Support

Table 12.1 summarizes supplier good practice activities that apply to product development and support. In this Appendix "product" covers products used as components of a global system, a specific global information system being developed for a regulated company, applications that the supplier manages (SaaS), or other cloud services, such as IaaS or PaaS.

Table 12.1: Supplier Good Practices

Practice	Description
Establish QMS	The supplier QMS should: • Provide a documented set of procedures and standards • Ensure activities are performed by suitably competent and trained staff • Provide evidence of compliance with the documented procedures and standards • Enable and promote continuous improvement While a comprehensive QMS is considered important for any supplier, it is considered critical where the scope of the QMS is expanded to include management of parts of the production operating environment (SaaS, IaaS, or PaaS). Suppliers new to supporting a regulated company may wish to leverage a customer's QMS when developing their own. However, a regulated company that demands a supplier follows their QMS instead of the supplier's own is discouraged.
Establish Requirements	The supplier should ensure that clear requirements are defined and provided or made available for review by the regulated company. Suppliers wishing to support the life sciences industries should be aware of EU GMP Annex 11 [1] supplier expectations.
Quality Planning	The supplier should define how their QMS should be implemented for a specific product, system, or service.
Assessments of Sub-Suppliers	Suppliers should formally assess their sub-suppliers as part of the process of selection and quality planning.
Produce Specifications	The supplier should specify the system to meet the defined requirements.

Table 12.1: Supplier Good Practices (continued)

Practice	Description
Perform Design Review	The design of the system should be formally reviewed against requirements, standards, and identified risks to ensure that the system will meet its intended use.
Change Management	The supplier should have defined processes for change management. Changes to the support model should be communicated to the customer as soon as they are decided. This is especially true for termination of support of older software versions, so that the customer can plan accordingly. Timelines need to be long enough for the customer to replace or upgrade the system before the old version goes out of support. SaaS suppliers should, in general, have a predictable update schedule. They should also make changes available in a test environment before they are committed to production so that customers can evaluate them in their business environment and make any necessary local changes to interfaces, etc. This is considered important because SaaS suppliers generally do not allow the customer to stay on an older version beyond the scheduled update. As much time as the supplier can accommodate should be used, since the regulated company may have to deal with several different interfaced systems around the globe.
Software Production/ Configuration	Software should be developed and deployed in accordance with defined standards, including appropriate code review processes. Appropriate tools should be used to support software production activities.
Perform Testing	The supplier should test the system in accordance with predefined test plans and test specifications.
Commercial Release of the Product	System release to customers should be performed in accordance with a formal process.
Provide User Documentation	The supplier should provide adequate system documentation. As applicable, this includes technical release notes, user manuals, on-line help files, etc.
Support and Maintain the Product in Operation	The supplier should support and maintain the product in accordance with established processes. The process for managing and documenting product changes should be fully described. There should be a documented and monitored SLA for any services provided. This is considered important for a software product, but it is considered critical for solutions that include providing an operating environment (e.g., SaaS, IaaS, or PaaS) or storage services (such as cloud storage). The SLA needs to address the requirements of all locations using the global information system.
Product Replacement and Retirement	The supplier should manage the replacement or withdrawal of products in accordance with a documented process and plan. The retirement process should define how long the supplier will support the product once it is withdrawn from the market, and the terms of such support.

12.2 Supplier Quality Management System

Suppliers should follow an established quality approach, e.g., the quality approach outlined in ISPE GAMP® 5 [4]. It should define:

- The process being followed to deliver and support the product, application or service
- The quality organization and its responsibilities, recognizing that suppliers of IT products and services are not structured the same way as life sciences companies, there should still be some level of segregation of duties. For example, the head of the quality organization should not also be responsible for product development, product support, finance or marketing.
- Deliverables
- Definition of service levels
- Documentation
- Planned reviews of the quality approach and internal audits
- Approach to continuous improvement of the quality approach and its use

Regulated companies may need to accept some level of risk related to the quality management process, including taking on some of the quality management activities, because suppliers of cloud-based services (SaaS, IaaS, PaaS) generally do not cater specifically to life science industries. However, some flexibility in relation to quality processes is generally advisable; the focus should be on how well a process is controlled, not on whether the controls are specifically designed for GxP. Risks that are accepted for this reason should be clearly documented in a risk register or similar document.

The quality approach should be based on a life cycle concept for the development and subsequent support of the product. This Guide does not recommend any particular life cycle or development methodology, but rather highlights those activities expected of suppliers.

The quality approach should include formal procedures covering the activities supporting system development, including:

- Requirements, specification, and testing
- Software management, control, and release, including all versions currently supported for all platforms and operating systems
- Distribution of the software
- Development change control
- Configuration management
- Traceability
- Training of supplier staff
- Document management

- Backup and restore
- Disaster recovery and business continuity (especially for SaaS), and emphasizing the global nature of the application

If a product is part of a larger validated system, the supplier quality processes should be compatible with the quality processes of the regulated company responsible for the overall system. If the supplier processes do not align well enough, the decision about the suitability of the supplier should be risk based. For example, if it is deemed critical to have immediate automated failover, but a SaaS supplier refuses to initiate failover until an eight-hour problem analysis phase is completed, the supplier may not be suitable. Similarly, if a failover process can only be initiated during normal business hours at the supplier's headquarters site, this may not be compatible with the needs of a global company, and the supplier may not be suitable.

For additional information related to IaaS and PaaS please see the *ISPE GAMP® Good Practice Guide: IT Infrastructure Control and Compliance (Second Edition)* [12].

12.3 Supplier Quality Planning

Quality planning should define the activities, procedures, deliverables, and responsibilities for establishing delivery and monitoring of the product or service.

The required information may be satisfactorily covered by other contractual documents such as a SLA, in which case a separate plan would not be required. SLAs should be established with all supporting organizations, as appropriate.

The supplier should define how the QMS would be implemented for a specific product or service. This should include defining:

- The life cycle model being followed and the project organization, activities, procedures, deliverables, and responsibilities for establishing the fitness for intended use.
- The approach to software development should define software development techniques and tools.
- Quality management responsibilities (supplier versus regulated company).
- If the supplier has a large customer base in the life science industries there may be a special support model (this is unusual unless the product is specifically geared to a GxP environment, e.g., a clinical trial management tool). **Note:** that such models may not be used in some countries serviced by the global system, or they might have slight differ scope based on differing regulation.

For further details on Quality and Project planning, see *ISPE GAMP® 5* [4].

12.4 Sub-Supplier Assessments

Suppliers should formally assess their sub-suppliers/sub-contractors as part of quality planning. Sub-suppliers/sub-contractors also should be periodically reassessed in accordance with the QMS. Regulated companies should not take on assessment of these sub-suppliers/sub-contractors; this is a supplier responsibility. However, the regulated company should ensure that suitable sub-suppliers/sub-contractors processes and quality standards exist and are followed.

The decision how to assess sub-suppliers/sub-contractors should be based on a documented risk assessment. If the regulated company wants any influence over the criteria for selection of sub-suppliers/sub-contractors this should be stated clearly in the contract or signed quality agreement with the principal supplier.

A common practice is to outsource testing. The contract with the principal supplier should be clear regarding expectations for testing. This includes who is responsible for developing test strategy, writing test scripts, executing testing, reviewing and evaluating and results, and approving them.

For further details on supplier assessments, see *ISPE GAMP® 5* [4].

12.5 SaaS Supplier Evaluation Considerations

Many SaaS suppliers provide applications that while not directed at regulated areas touch on them and as a result are subject to GxP controls. For example, a SaaS solution for CRM may include sales call support. This in turn often involves the ordering of drug samples, which is regulated. Such suppliers will not often have the corporate structures in place that are familiar to regulated company auditors.

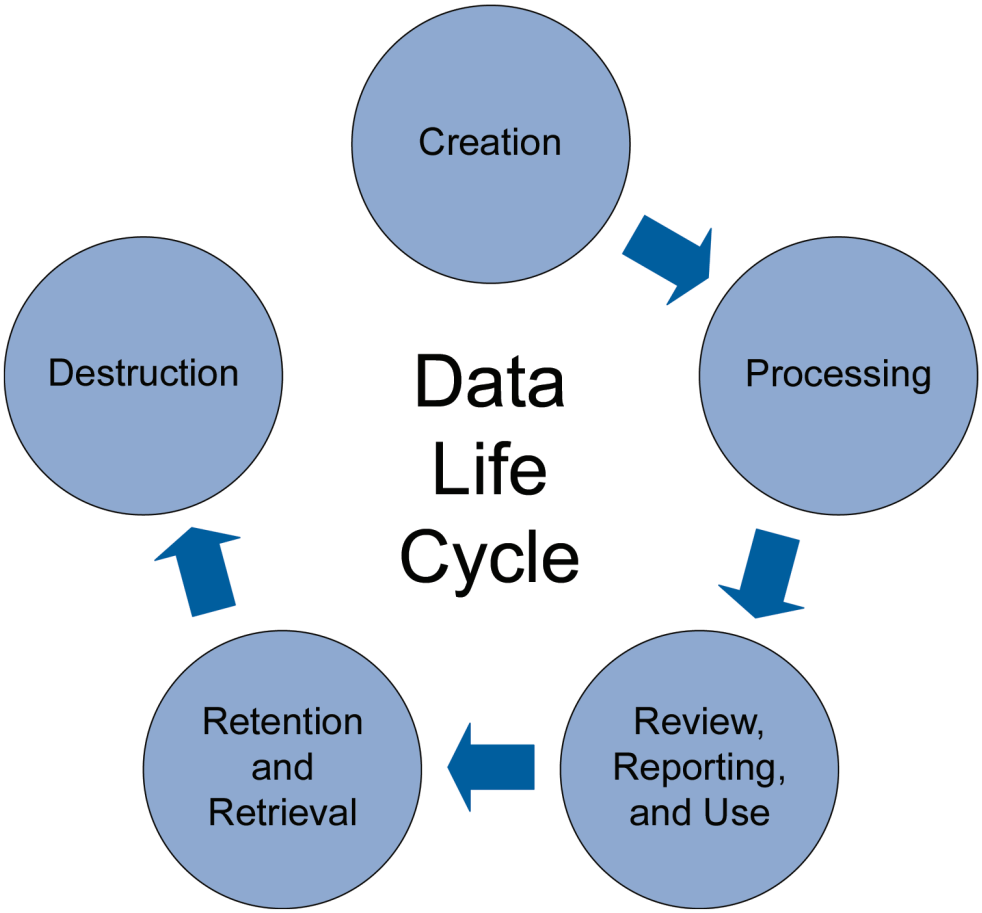
However, this does not mean that the supplier does not have good controls around the processes that regulated companies look at. For example, perhaps instead of an approval of a specification from the quality organization the firm may have an SME do a review. If the net outcome is the same (a clear and technically correct specification), that can be acceptable. The emphasis should not be proving that the supplier has GxP processes (most will not), but rather that their processes are GxP compatible, i.e., they have controls that ensure that they can achieve a level of quality that is at least commensurate with the risk of the business process.

For further information on IaaS and PaaS considerations, see the three companion ISPE GAMP® Cloud Special Interest Group (SIG) Concept Papers [27] and *ISPE GAMP® Good Practice Guide: IT Infrastructure Control and Compliance (Second Edition)* [12].

13 Appendix 9 – Data and Record Management Life Cycle

Regulatory compliance in a global context requires companies to collect, store, protect, and make available increasing volumes of data, records, and information. Companies should set, establish, practice, and maintain business acceptable standards and processes for data and record management throughout the system life cycle recognizing that data and records age over many years as shown in Figure 13.1. For further information, see the *ISPE GAMP® Guide: Records and Data Integrity* [28].

Figure 13.1: Data Life Cycle



To ensure effective control, regulated companies should follow a well-defined data life cycle. While data management planning is not generally considered part of the life cycle, it is necessary to define how compliance with the stages in Figure 13.1 will be achieved. This is considered critical for global information systems where many of the life cycle activities may be under the control, or the influence of, a widely diverse group of individuals.

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. Getting key stakeholders involved early in the planning process is considered critical. In addition, the data management strategy should identify those individuals appointed to take on the policy setting and administration roles and who are adequately trained in global regulatory requirements as they relate to managing data and information. The data management strategy and life cycle will play a key role in the records management process.

13.1 Data Management Planning

Policies and procedures to support the life cycles should be established to ensure a proper level of control.

Data management within the global enterprise is an activity involving the creation, processing, review, use, storage (including both short-term and archival), retirement, and eventual destruction of data held on computerized systems.[13] It is needed for the benefit and, in the case of regulatory or legal requirements, the protection of the business and patients. As such, planning for data management should take account of global requirements for:

- Business processes defined and owned by the business and used to ensure new and existing computerized systems support the business globally
- Underlying databases and data models, to ensure the compatibility of data across geographic boundaries for example:
    - Policies, standards, and guidelines for data ownership that will ensure proper (compliant) creation and use of data throughout the organization
    - Clearly defined responsibilities and accountability for ownership, management, administration, and use at the organizational, regional, local, and individual level
    - Establishing a balance between accessibility and security

Regulated companies need to establish data management standards and processes that include planning, implementation, administration, and control of data that are universal within the company. Without this, complications can arise for global information systems because of the dispersed nature of the data users, and sometimes of the data itself.

13.2 Business Process Requirements

In planning for data management, identifying a means of leveraging industry best practices and experiences throughout the data life cycle is considered beneficial. Requirements derived should be documented in URSs, and may relate to:

- Data creation or migration
- Defining metadata that is required to maintain the meaning and integrity of the data
- Data validation or verification
- Policy for addition, deletion, or modification of data
- Retrieval and use of data
- Data authority
    - **Data:** officially recognized information that can be verified and provided by a data owner.

[13] These stages are derived from the WHO Guidance on Good Data and Record Management Practices [29].

  - **Data Source:** 1) The location where data that is being used come from. In a database management system, the primary data source is the database, which can be located in a disk or a remote.[14] 2) A specific data set, metadata set, database or metadata repository from where data or metadata are available.[15]

  - **Data Owner:** This is an individual(s) authorized by the business organization to develop or manage data for a specific business purpose

- Data access (for systems and individuals)
- Copy management
- Data version control
- Data storage and archival and retrieval
- Data retention
- Data migration, if applicable
- Database architecture, centralized or distributed
- Definition of critical data:
  - For regulatory compliance (i.e., required by predicate rules)
  - For business success
- Defining and communicating all data definitions and links between data elements
- Data auditing

Although best practices are typically based upon clearly defined and applicable standards, procedures, and guidelines, it is important to ensure their applicability. Applicability should be assessed relevant to use:

- Within and across organization boundaries
- Between locales and regions
- How data quality can be assessed in relation to corporate and regulatory data standards

Note: some national or regional legislation, notably privacy protections, may make it illegal for specific data to be kept on servers in non-compliant countries. In some cases, compliance with an approved program may be a way for sites in these countries to be compliant, though that may not be an option. Local and global privacy officers should be brought into the conversation very early in such cases.

Similar to the above consideration, some regions have intellectual property laws that may not be in line with the needs of a regulated company. A full understanding of the nature and sensitivity of the data is necessary before making a decision where data can be available or stored.

When planning for a global information system, data management requirements, comparable to those discussed, should be established prior to the selection of the system architecture. Some architectures are more beneficial to

[14] From Techopedia™ Technology Dictionary [30].
[15] From the OECD Glossary of Statistical Terms [31].

specific data management considerations than others. For example, if wide access and high availability are critical, a SaaS application may be a good choice. However, if data at the highest level of confidentiality will be managed in the system, a solution where the supplier has access, even to encrypted data, may not be the ideal choice.

13.3 Life Cycle Considerations

For global information systems, most of the data life cycle issues are the same as for purely local systems; however, there are some issues that need to be considered.

13.3.1 Creation

When data is coming into a system from disparate sources there should be a standard for uniformity that includes:

- Precision
- Format
- Language (including characters that may not be used in all languages, e.g. ñ, ß, ç, or the entire Cyrillic or Greek alphabet)
- Time stamps (12 or 24 hour clock, Universal Time Coordinated (UTC), local, or other time zone, unambiguous data format)

Data coming into a global information system via migration may have to undergo extensive cleanup in advance.

Note: where data is created in an external system, including mobile devices, there may be a need for protections like encryption (at rest and/or in transit) even before the data is processed. This is a consideration for many electronic data capture systems supporting clinical studies.

13.3.2 Processing

In general, issues related to processing should not be substantially different for global information systems, assuming that the data comes out of the creation step clean and conforming to standards. Under unusual circumstances latency might have an effect on processing.

13.3.3 Review

Similar to the standards for data creation, there should be a common set of expectations against which review is executed. Reviewers should receive the same training globally.

13.3.4 Analysis and Reporting

As long as global standards are followed there should be no uniquely global risks.

13.3.5 Retention and Retrieval

Many records will have different requirements related to the jurisdiction to which they apply. For example, in the United States (US) records related to blood product handling are required to be retained for ten years, while the EU and Japan require that they be held for thirty years. The opposite may be the case for records that impact employee data privacy; some of those may need to be destroyed shortly after an employee leaves the company in some European nations, while there may be no such requirement in the US. Consider however, that privacy law in the US is managed at the state level, not national, so some privacy requirements are likely to exist in states like Massachusetts (one of those with strongest protection) and not in others.

In addition to retention times, there may well be requirements for encryption to protect personal data, especially medical records.

13.3.6 Destruction

Once data is no longer needed it should be destroyed. Companies may manage archived data ineffectively because it is easy to ignore data sitting in the archive. However, while data storage is relatively inexpensive, when terabytes of information are involved significant cost becomes a more important factor. Another major risk relates to the fact that if a regulated company has the information, it is discoverable for litigation purposes. The cost of legal discovery services can be substantial, so it is far better not to have expired records that would need to be included in such searches. The global aspect of this issue is the exposure to litigation in multiple countries.

Another global challenge related to data destruction is ensuring that all of the copies of the data are destroyed. This can be a greater problem for distributed systems, including SaaS systems where the provider may have information belonging to a company at multiple locations. In addition to purging databases and archives, backups to other media need to be included, which may exist at multiple sites for a global information system.

13.4 Data Quality

Once established, the quality of the data should be maintained and supported throughout a global information system, to meet user requirements both locally and globally. Principles governing data quality, both operationally and procedurally, include:

- Data should be owned. A business 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.

- Data should be accurate (within defined parameters), appropriately precise, and complete.

- Data should be available. Data availability requires a data management environment within which users can find the data they need, when they need it. The business should not be put at risk of making bad decisions because incomplete or stale data.

- Data should be accessible. Access to relevant and accurate data is critical to making good business decisions. Data management should ensure that the right people have access to the right data.

- Data should be secure and its integrity should be maintained:

    - Globally distributed information environments create an increased need for managing the security of the data effectively so that there is reduced risk of accidental or intentional changes to data, accidental or intentional misuse of data, or loss of data.

- Data should be assessed for value, cost, business benefits, or regulatory needs.

- Data should be consistent, relevant, and conform to agreed standards:

    - Data consistency is frequently an under emphasized issue and can be a major factor complicating the management of global systems. Even when using the same language there are problems: color versus colour, computerized versus computerised, organizational versus organizational, etc. It may be difficult to maintain data consistency when data is received from different sources. This can be further complicated when data types acquired from different sources are not acquired in the same way, such as where one site compiles clinical data directly from case report forms, whereas another uses a contracted intermediary for data entry. In these circumstances, there should be a clear and shared understanding of the data standards.

- Technical issues also may adversely affect data consistency, especially if external systems process the data. Issues like data format (e.g., for dates), the number of significant figures, rounding, and truncation algorithms should be understood and addressed.

- Time stamps can be problematic. Aside from the date format issue noted above, if it is critical to know exactly when a specific datum was created or modified and if the system is used across time zones, that system should probably be required to either stamp all actions with the time for a single time zone (e.g., UTC) or it should display a time zone notation.

- These issues may be addressed by ensuring that a well defined and documented data definition exists, agreed to by the data creators, managers, and users (i.e., meaning of the data, quality of the data, use of the data, etc.).

- Technical solutions, such as designing global dropdown menus into the application, building data dictionaries that recognize synonyms and simple glossaries also may be of assistance. Maintaining a master copy of data also may help maintain consistency. In some situations, multiple copies or versions of the data need to be maintained and controlled. In such cases synchronization of the data will need to be planned and implemented, or the result will be diversion of the data.

- Having well managed and consistent data will make it more useful for global uses, for example global trending, as well as placing the company in a better position to meet regulatory expectations for data integrity and quality.

13.5 Data Migration

Data migration, the physical moving of data from one system (database) to another, spans a variety of activities within the life cycle of quality management of data. These activities are designed to ensure that both the requirements of the business continue to be met, including those directly or indirectly associated with meeting regulatory requirements for historical data preservation, and protecting mission critical data.

There are three key elements to a data migration that should be addressed in order to ensure that data quality is retained:

- Conversion program (validated, qualified, verified, or otherwise assured to work properly).

  Data migration needs to account for format differences, some of which may be major issues, in the various source systems. For example, if the incoming data is in another language or even another alphabet, this needs to be addressed.

- Transcription verification (including for metadata)

- Data cleansing where errors occurred

Failure to plan the migration effectively and to seek input from stakeholders across the enterprise can seriously compromise one of the business's most valuable assets by putting data quality at risk of:

- Not meeting regulatory expectations for demonstrable technical and procedural controls for management of electronic records

- Poor or flawed decision making, incurring associated costs to the business (increased product time to market, reduced competitiveness, increased costs) as a result of incorrect, incomplete, inaccessible, or unavailable data

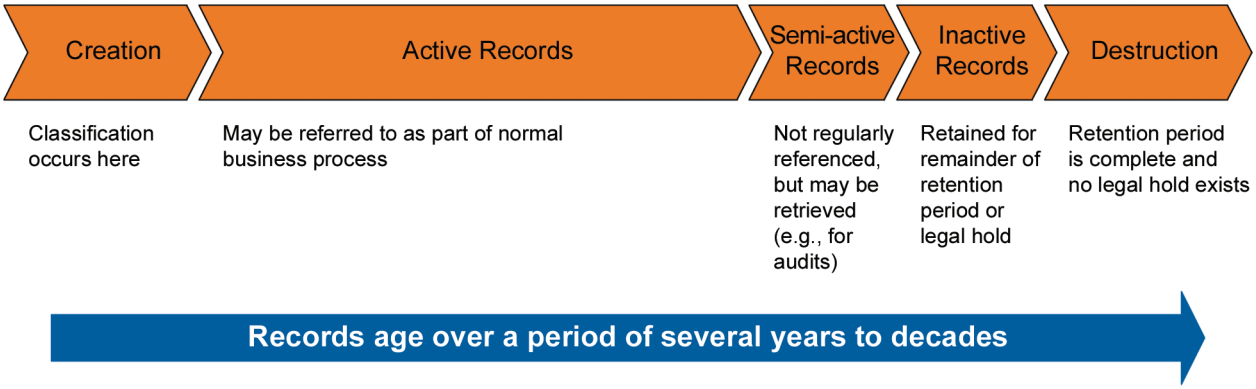
- The necessity to put a freeze on data collection in the predecessor system when deploying new systems. This would be defined in the data migration plan, including scope, i.e., whether the freeze is global or local. For changes to existing systems this will more likely be a brief shutdown of the system while the change is implemented.

For further information, see the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition)* [21].

13.6 Record Management

Record managers follow most of the same principles outlined above for data management, but they tend to think in different terms based on a record life cycle that readily translates to paper, as well. Figure 13.2 shows what is considered to be a record life cycle by most records management professionals.

Figure 13.2: Record Life Cycle



13.6.1 Record Creation

From a record management standpoint, this generally includes a combination of the WHO Creation and Processing steps, and possibly Analysis and Reporting [29]. Records need to be classified (e.g., as GxP, data privacy sensitivity) in order to understand which laws and regulations apply to their management. The global concerns are the same as those discussed in the data life cycle.

13.6.2 Active Records

Active records may be in the analysis and reporting stage of the data life cycle, or may be in the storage and retrieval phase. Active records are routinely subject to retrieval for business purposes. Electronically, they will reside in the active database. Paper records will be readily retrievable in a short time. For global systems, this might involve replication to local sources in distributed systems.

13.6.3 Semi-active Records

These records can continue to be referenced for business purposes, although rarely. For example, they may be needed to support a regulatory inspection. Electronically, they may reside in a near-line archive with limited access. Expectations for the retrieval of semi-active records needs to be clearly defined. For global information systems, near-line archives can be local, although it is probably better to do this globally in order to minimize the number of copies of the record being managed.

Regulated companies may prefer to limit themselves to active and inactive, rather than use a semi-active stage in their life cycle.

13.6.4 Inactive Records

Most archived records fall into this category. These records are very unlikely to be retrieved, but are being held to conform to retention policy. For global information systems, it is recommended that one archive should be managed globally, which will make the eventual destruction of the record simpler.

13.6.5 Destruction

This stage of the record life cycle is effectively the same as for the data life cycle.

13.6.6 Record Aging and Risk

For some records the risk associated with them is not constant throughout the record life cycle. This can impact the measures and controls required to safely, effectively, and economically manage the records. The risk related to a set of records should be evaluated when a data migration is contemplated. Data migration for records with a long retention period may be required multiple times. If the risk related to the records is low, it might be reasonable to migrate the records to a medium with a longer lifespan, e.g., paper, PDF, flat file, etc.

For global information systems, this risk assessment is more difficult, as it needs to consider the risks related to all sites and jurisdictions with an interest in the data.

Whenever a decision is made to convert records to a less processable format a well-documented risk assessment should be performed. It should consider all applicable risks for all jurisdictions and for potential uses of the information. For example, clinical data relating to a mature product that is being phased out of production might be a candidate for conversion to another format. However, if the product is planned for introduction to a new country, or is being considered for a new therapeutic indication, it may be more beneficial to migrate the records and keep them processable.

13.7 Data Destruction

Data destruction needs to account for all local laws. In addition, the trigger data that starts the retention countdown may not be the same in all sites for the same records. For example, records relating to process validation may no longer be required at a primary manufacturing site, but if a smaller site is still making that product the validation records are still active and the retention countdown should not start yet.

In addition, approval processes for record destruction should build in the verification that no other sites still need the record. This process includes checking to make sure there are no litigation holds in other countries.

When a record is designated for destruction, all copies should be destroyed. Otherwise replication processes might regenerate the record elsewhere.

In unusual circumstances, there may be conflicting requirements. For example, some national privacy protections may mandate that employee records are destroyed upon termination of employment, but the US GLP regulation [19] requires retention of training records for anyone involved in a preclinical study. Policy for handling this kind of conflict should be established by the corporate Legal department in consultation with QA.

14 Appendix 10 – Converting a Local System into a Global System

Occasionally a regulated company will find that a local business solution provides the best solution to globally standardizing the business process, and will decide that the computer system used at that location is the most sensible tool available. However, there are likely to be several cultural, business, and technical hurdles involved in such a transition.

14.1 History

The local system will have been developed, supported, and used locally for a period of time. Personnel involved in the development, implementation, and use of this system usually have a team and cultural dynamic. They are comfortable with, or at least used to, this dynamic. They have established ownership of the system design, documentation, and the way the system is currently used. A decision to move a local system to a global profile will change the team and cultural dynamic by introducing new members, new requirements, and sometimes, new management.

The global project team should be prepared for resistance to change from the local team members. The new global team should include some local team members, as they will likely know the most about the existing system. Additionally, their participation can be of help in overcoming any resistance within the local business community.

14.2 Business Process

The team charged with changing a local system to a global information system should consider that this evolutionary process may also have to be applied to the business processes that the global information system will support.

The project team should be constantly aware of the possibility of losing synchronization; therefore, they should compare this design to the established business processes and perform an impact assessment when:

- the existing system is assessed
- new requirements are collected
- the global information system design starts to emerge

Unless business processes within the global organization are standardized, the impact may be severe; this should be taken into account when developing project scope and timelines.

14.3 Supporting Documentation

Existing documentation supporting the local system, if any, should be assessed for further usage by the global project, including language, format, and content.

The following topics should be part of the assessment, to determine whether the existing documentation can be used and the next steps to be taken:

- What was the language used for the supporting documentation of the local system?
- Did local documentation follow a standard?

- If there is a corporate language, was it used for this system?
- If there is no corporate language, what language will be used for the global project?
- If the local documentation is not in the language that will be used for the global project, should the existing documentation be translated, or should the global project start from the beginning?
- If translation is necessary, the team should be wary of well-intentioned bilingual team members who don't really have a talent for writing in the target language. It may be worthwhile to engage a professional technical translator, although there should always be a technical review by SMEs of all work done by outside translators.
- Which tools or applications were used to develop the local documentation?
- Are the tools/applications that were used the global standard within the company?
- Can the data be exported for reuse in the global tools/applications?
- Are there global standards governing the contents and layout of supporting documentation such as:
    - Business process models
    - User requirements
    - Functional specifications
    - Design specifications
    - Risk assessment
    - Traceability
    - Test scripts
    - Training materials
    - Operating procedures

14.4 System Design and Technical Architecture

Moving a system from a local to a global profile has a major impact on the actual system design and the technical infrastructure required to support the new design. This, in turn, may lead to changes in the geographic location(s) of the technical infrastructure, support organization, and ultimate system ownership.

Such changes should be thoroughly planned, and where possible, executed with minimum impact to the existing local process. If the planned architecture will be distributed, consideration should be given to whether the existing site could become one of the nodes in the global architecture. If not, it is prudent not to decommission the local infrastructure until the global site is stable, perhaps after the system has been rolled out to one or more new sites.

14.5 System Support

If a CoE is planned, the CoE should be established and staffed prior to altering the existing architecture. This will have the benefit of both ensuring that there is someone in place to help with any problems, as well as providing a learning opportunity for the CoE staff. Current local support staff may have valuable relationships with suppliers that support the system. It is advisable to bring one or two local staff already familiar with the system into the CoE into order to “jump-start” the CoE.

The regulated company may decide to appoint a global business owner other than the current owner. This may be appropriate, based on overall responsibility and accountability. The local owner, whether they remain a local owner or not, should do everything possible to facilitate the transition of responsibility.

15 Appendix 11 – References

1. EudraLex Volume 4 – Guidelines for Good Manufacturing Practices for Medicinal Products for Human and Veterinary Use, Annex 11: Computerized Systems, June 2011, http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

2. EudraLex Volume 4 – Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use, Chapter 4: Documentation, January 2011, http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

3. Pharmaceutical Inspection Co-operation Scheme (PIC/S), https://www.picscheme.org/.

4. *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems,* International Society for Pharmaceutical Engineering (ISPE), Fifth Edition, February 2008, www.ispe.org.

5. ISPE GAMP® guidance documents, International Society for Pharmaceutical Engineering (ISPE), http://www.ispe.org/publications-guidance-documents/series.

6. US Federal Food and Drug Administration (FDA), www.fda.gov.

7. EudraLex Volume 4 – Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use, http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

8. Health Canada – Good Manufacturing Practices, http://www.hc-sc.gc.ca/dhp-mps/compli-conform/gmp-bpf/index-eng.php.

9. International Council for Harmonisation (ICH), www.ich.org.

10. Information Technology Infrastructure Library (ITIL®), https://www.axelos.com/best-practice-solutions/itil.

11. ISO/IEC 20000 Information Technology -- Service Management series, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

12. *ISPE GAMP® Good Practice Guide: IT Infrastructure Control and Compliance, International Society for Pharmaceutical Engineering (ISPE),* Second Edition, 2017, www.ispe.org.

13. ISO/IEC 27001:2013 Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements, ISO/IEC JTC1, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

14. ISO/IEC 27002:2013 Information Technology -- Security Techniques -- Code of Practice for Information Security Controls, ISO/IEC JTC1, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

15. National Institute of Standards and Technology (NIST), www.nist.gov.

16. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems,* International Society for Pharmaceutical Engineering (ISPE), First Edition, January 2010, www.ispe.org.

17. ISO/IEC 27000 Information Technology – Security Techniques series, ISO/IEC JTC1, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

18. *ISPE GAMP® Good Practice Guide: Electronic Data Archiving,* International Society for Pharmaceutical Engineering (ISPE), First Edition, July 2007, www.ispe.org.

19. 21 CFR Part 58 – Good Laboratory Practice (GLP) for Nonclinical Laboratory Studies, Code of Federal Regulations, US Food and Drug Administration (FDA), www.fda.gov.

20. Sarbanes-Oxley Act of 2002, US Securities and Exchange Commission (SEC), http://www.sec.gov/about/laws/soa2002.pdf

21. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems,* International Society for Pharmaceutical Engineering (ISPE), Second Edition, December 2012, www.ispe.org.

22. ISO 9000 Quality Management series, International Organization for Standardization (ISO), www.iso.org.

23. *ISPE GAMP® Good Practice Guide: Manufacturing Execution Systems – A Strategic and Program Management Approach,* International Society for Pharmaceutical Engineering (ISPE), First Edition, February 2010, www.ispe.org.

24. ISO 14971:2007 Medical Devices -- Application of Risk Management to Medical Devices, International Organization for Standardization (ISO), www.iso.org.

25. International Council for Harmonisation (ICH), ICH Harmonised Tripartite Guideline, Quality Risk Management – Q9, Step 4, 9 November 2005, www.ich.org.

26. ISO/IEC Guide 51:2014 Safety Aspects -- Guidelines for their Inclusion in Standards, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

27. ISPE GAMP® Cloud Special Interest Group (SIG) Concept Papers, International Society for Pharmaceutical Engineering (ISPE), July 2016, www.ispe.org.

28. *ISPE GAMP® Guide: Records and Data Integrity,* International Society for Pharmaceutical Engineering (ISPE), Second Edition, 2017, www.ispe.org.

29. WHO Technical Report Series, No. 996, Annex 5: Guidance on Good Data and Record Management Practices, World Health Organization (WHO), 2016, http://apps.who.int/medicinedocs/en/d/Js22402en/.

30. Techopedia™, https://www.techopedia.com/definition/30323/data-source.

31. OECD Glossary of Statistical Terms, Organisation for Economic Co-operation and Development (OECD), http://stats.oecd.org/glossary/index.htm

32. NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, National Institute of Standards and Technology (NIST), US Department of Commerce, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

16 Appendix 12 – Glossary

16.1 Acronyms and Abbreviations

CAB	Change Advisory Board
CAPA	Corrective and Preventive Action
CDS	Chromatography Data System
CFR	Code of Federal Regulations
CI	Configuration Item
CMDB	Configuration Management Data Base
CoE	Center of Excellence
CRM	Customer Relationship Management
DS	Design Specification
ECAB	Emergency Change Advisory Board
EDMS	Electronic Document Management System
ER/ES	Electronic Records/Electronic Signatures
ERP	Enterprise Resource Planning
FDA	Food & Drug Administration (US)
FS	Functional Specification
GAMP®	Good Automated Manufacturing Practice
GC	Gas Chromatography
GPC	Gel Permeation Chromatography
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GEP	Good Engineering Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GPV	Good Pharmacovigilance Practice
IaaS	Infrastructure as a Service
ICH	International Council for Harmonisation
IT	Information Technology
ITIL®	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LC	Liquid Chromatography
LDAP	Lightweight Directory Access Protocol
LIMS	Laboratory Information Management System

MES	Manufacturing Execution System
MHRA	Medicines and Healthcare Products Regulatory Agency (UK)
OLA	Operational Level Agreement
PaaS	Platform as a Service
PIC/S	Pharmaceutical Inspection Convention and Pharmaceutical Inspection Cooperation Scheme
PII	Personally Identifiable Information
PM	Project Manager
QA	Quality Assurance
QC	Quality Control
QMS	Quality Management System
QRM	Quality Risk Management
RFP	Request for Proposal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SDS	Software Design Specification
SLA	Service Level Agreement
SME	Subject Matter Expert
SOP	Standard Operating Procedure
UAT	User Acceptance Test
UC	Underpinning Contract
URS	User Requirements Specification
WAN	Wide Area Network
WHO	World Health Organization

16.2 Definitions

Application Support Manager

This is the IT role responsible for system management, i.e. configuration management, change management, backup and archive management, etc. This is not to be confused with the business process ownership role.

Business Process Owner *(global)*

The individual within the business community who is responsible for the overall business use of the system. Care must be exercised in naming this person, since 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 HQ; it could be assigned to a local owner (see below) at one of the largest user sites.

Business Process Owner *(local)*

This is a site-level 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 highly 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.

Change Advisory Board (CAB)

A group that oversees the change control process.

Centralized System

A system architecture wherein data is stored in a centralized database and processing occurs on a single centralized server.

Center of Excellence (CoE)

A group of subject matter experts that provide IT and business support to the business community. They generally provide second level support working with the help desk and are typically the primary interface with the supplier of the computer system.

Core

When used in the context of global information systems, the processes, functionality, tasks or other elements that are identical across all implementations. These are generally managed centrally.

Core Functionality

Functionality of the computer system that is identical across local implementations.

Core Processes

Processes that should be carried out the same way across all implementations of the global system.

Core Validation Activities

Validation activities that can be performed once and shared with teams working on local implementations. These activities need not be repeated locally.

Core Validation Team

A team with responsibility for core validation activities. This team may have other global responsibilities, such as coordinating local efforts.

Emergency Change Advisory Board (ECAB) (ITIL®)

A group empowered to endorse emergency changes to a computer system when it is not feasible to convene the full CAB.

"Follow the Sun" Support Model

An approach to that ensures 24 hour active support to all users around the world. This generally involves the hand-off of incident management at the end of the business day to support staff at another site to work on the issue, and so on until it is resolved. The same effect can be achieved through round-the-clock staffing at a central location.

GxP Regulated Computerized System

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

GxP Regulation

The underlying international pharmaceutical requirements, such as those set forth in the US FD&C Act, US PHS Act, FDA regulations, EU Directives and guidelines, Japanese regulations, or other applicable national legislation or regulations under which a company operates. These include but are not limited to:

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

Harm (ICH Q9 [25])

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

Hazard (ISO/IEC Guide 51 [26])

The potential source of harm.

Help Desk

An organization that acts as a single point of contact between users and IT. They help users solve simple problem and facilitate solution of more complex issues by experts.

Infrastructure as a Service (IaaS) (NIST Special Publication 800-145 [32])

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls).

Information Technology Infrastructure Library (ITIL®)

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

Lightweight Directory Access Protocol (LDAP)

A method for centrally managing single sign-on access.

Likelihood of Occurrence

The probability of a hazard occurring and causing harm.

Operational Level Agreement (OLA)

Defines the responsibilities of an internal support group, including the process and timeframe for delivery of their services. The objective of the OLA is to present a clear, concise and measurable description of the service provider's internal support. The OLA is not a substitute for an SLA with the supplier. Its purpose is to define the underpinning internal responsibility of the IT Support group.

Platform as a Service (PaaS) (NIST Special Publication 800-145 [32])

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Probability of Detection

The probability that a fault will be detected before harm occurs.

Process Owner (*ISPE GAMP® 5* [4])

The person ultimately responsible for the business process or processes being managed

Quality Risk Management (QRM)

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.

Regression Testing

Testing geared toward demonstrating that a change has not affected a system or part of a system that it was not intended to affect.

Replication

The process of creating and managing duplicate versions of a database. Replication not only copies a database, but also synchronizes a set of replicas so that changes made to one replica are reflected in all the others. For database applications where users are geographically widely distributed, replication is often the most efficient method of database access.

Risk (ISO/IEC Guide 51 [26])

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

Recovery Point Objective (RPO)

This is effectively the definition of how much data can be lost in a disaster recovery effort. For example, an RPO of 4 hours means that no more than the immediate 4 hours' worth of data collected prior to the disaster is unrecoverable.

Recovery Time Objective (RTO)

This is the speed at which full use of the system must be restored. For example, an RTO of 24 hours gives the disaster recovery team one day to restore business function of the system. RTO is an important determinant for architecture choices; e.g. a 1 hour RTO virtually mandates mirroring of the application and data.

Software as a Service (SaaS) (NIST Special Publication 800-145 [32])

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user- specific application configuration settings.

Service Level Agreement (SLA)

An SLA is an agreement between an IT service provider and a customer. The SLA describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple services or multiple customers.

Single Sign-on (SSO)

A technique for carrying identity of the user from an earlier login to log into another system without further action on the part of the user.

Severity (ICH Q9 [25])

A measure of the possible consequences of a hazard.

System Owner (*ISPE GAMP® 5* [4])

The person ultimately responsible for the availability, and support and maintenance, of a system and for the security of the data residing on that system.

Underpinning Contract (UC)

The ITIL® term for the contract between the regulated company and a supplier. The UC must have provisions to ensure that SLA requirements will be met.

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

www.ISPE.org