GAMP Good Practice Guide:

Global Information Systems Control and Compliance

ENGINEERING
PHARMACEUTICAL
INNOVATION

Preface to the GAMP Good Practice Guide: Global Information Systems Control and Compliance

This document, the GAMP® Good Practice Guide: Global Information Systems Control and Compliance, is intended as a supplement to Guide for Validation of Automated Systems (GAMP® 4). It considers major issues that confront companies validating a multi-site computerized system and is intended to provide some insight into addressing issues of control and regulatory compliance efficiently and effectively throughout the lifecycle of a globally deployed IT system.

This document has been designed so that it may be used in conjunction with guidance provided in *GAMP® 4* and other ISPE publications, such as the ISPE Baseline® Guides.

Disclaimer:
This Guide is meant to assist pharmaceutical companies in managing the validation of Global Information Systems. The GAMP Forum Global Information Systems Special Interest Group (SIG) cannot ensure and does not warrant that a system managed in accordance with this Good Practice Guide (GPG) 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 (including the GAMP Forum), or the officers, directors, employees, members, or agents of each of them, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

All trademarks used are acknowledged.

ISBN 1-931879-86-9

Acknowledgements

The production of the GAMP® Good Practice Guide: Global Information Systems Control and Compliance was initiated by the GAMP Council and Steering Committees, sponsored by ISPE and industry, and governed by a Special Interest Group (SIG) chaired by Arthur (Randy) Perez, Novartis and vice-chaired by Kate Townsend, BusinessEdge.

The following SIG members provided the bulk of material, comments, and reviews:

Winnie Cappucci	Berlex
Marie Carpenter	Pfizer
Barry Feldman	Lachman Consultant Services Inc.
Klaus Krause	Amgen
Kiet Luong	GlaxoSmithKline
Bill McDonald	GlaxoSmithKline
Doina Morusca	Invensys
Arthur (Randy) Perez	Novartis
Iain Robertson	Clarkston Canada
Peter Robertson	AstraZeneca
Paul Seelig	Merck (retired)
Carl Turner	PL Consultancy
Joe Tyska	GlaxoSmithKline
Frank Vivino	Mi Services Group
Eilen Young	Novartis

The SIG Chairs wish to thank everyone for their commitment and contributions throughout the production phase; it has been instructive and pleasant to work with such a devoted group of professionals in a truly international environment.

Special thanks to those individuals and organizations who hosted face-to face meetings and workshops:

The production was overseen by the GAMP Americas Steering Committee, who provided invaluable directions, and reviewed material.

The GAMP® Editorial Review Board on behalf of ISPE was Gail Evans, Colin Jones, Tony Margetts, Arthur (Randy) Perez, and Sion Wyn.

The local editorial team, on behalf of the SIG was: Carl Turner, Peter Robertson, and Arthur (Randy) Perez. The GAMP® Council would like to give special thanks to Peter Robertson and Carl Turner for countless hours of work during the development and editing of this Guide.

Members of the GAMP® Forum Council and Steering Committees, along with the ISPE Technical Documents Committees are thanked for their participation in the review of this Guide.

The GAMP® Council would like to thank Karl-Heinz Menges (RPDA, Germany) for regulatory review.

The GAMP® Council would like to thank all those involved in the worldwide review of this Guide during 2004. To view this list, please go to www.ispe.org/gamp/.

Table of Contents

Table of Appendices

1 Introduction

1.1 Overview

The past two decades have seen a distinct trend toward globalization in the life science industries.

As companies find themselves operating from multiple sites worldwide, or with groups and departments split between multiple locations in a country, or even using "third-party distributors," the problems of information sharing become more complex. There are many competitive advantages to efficient and effective information sharing. Research and development activities often span international boundaries. Integrated activities can be achieved only with excellent communication between everyone involved, and in the 21st Century this means that the ability to share electronic information effectively is paramount.

With drug development costs that may exceed one billion US dollars, time to market is a key 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 is certainly a major requirement for disparate 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 these multi-site computer systems can be very difficult. For regulated systems, such as a clinical database or an ERP system, validation issues add an extra layer of complication. The GAMP® Good Practice Guide: Global Information Systems Control and Compliance considers major issues that confront companies validating a multi-site computerized system.

1.2 Purpose

This Guide is intended to provide an understanding of the issues faced by teams that are tasked with completing a global deployment of an IT system, in particular, to provide some insight into addressing issues of control and regulatory compliance efficiently and effectively.

The intended audience for this guidance is both central and local in an organization and includes the following:

- Project Management
- Business Process Owners
- System Integrators
- Validation Team
- Quality Assurance
- Technical Support (IT)

This Guide is intended as a supplement to *GAMP® 4.* An understanding and knowledge of the *GAMP® 4* is considered a prerequisite to the use of this Guide.

1.3 Scope

The *GAMP® Good Practice Guide: Global Information Systems Control and Compliance* addresses compliance with international pharmaceutical regulations and guidelines for computerized systems. It covers the following:

- new systems and extensions to existing ones
- existing validated systems to be maintained

A wide range of healthcare 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)

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

- US Food and Drug Administration (FDA) regulations and Compliance Policy Guides
- Relevant sections of EU GMPs, e.g., Annexes 11 and 18.
- Pharmaceutical Inspection Cooperation Scheme (PIC/S) Guidance
- Health Canada GMP regulations
- ICH Guidelines
- Japanese MHLW GMPs

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

A checklist for considerations covering details contained within this document is referenced in Appendix 5 of this Guide.

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

1.4 Benefits

This Guide aims to assist in the efficient, effective, and compliant development, implementation, and maintenance of widely used systems.

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

- achieving maximum synergy 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

1.5 Objectives

Methods by which global system implementation is conducted should be practical and efficient in addition to meeting regulatory compliance expectations.

To this end, the following objectives applied to the development of this Guide:

- Provide a consistent document that, in conjunction with *GAMP® 4* and other Good Practice Guides, encourages stakeholders to take advantage of current good practices in the field to achieve compliance with applicable regulations.
- Define *global systems* and other key terms and concepts referenced or introduced.
- Provide guidance on good practice for unique aspects of computerized systems implemented on a global basis.

References are provided to supporting information available in other GAMP® guidance. Where additional information is not available in *GAMP® 4*, this Guide provides more specific detail.

The GAMP® Council believes that the guidance developed has met these criteria.

1.6 Key Concepts

The key concepts and principles of a global implementation include the following:

- definition of core and local needs for hardware, software, and infrastructure
- harmonization and agreement of global standards and processes
- effective ownership of accountability and allocation of responsibilities and resources
- relevant, consistent, and effective communication and documentation, and application of standards
- management of expectations arising from cultural diversity

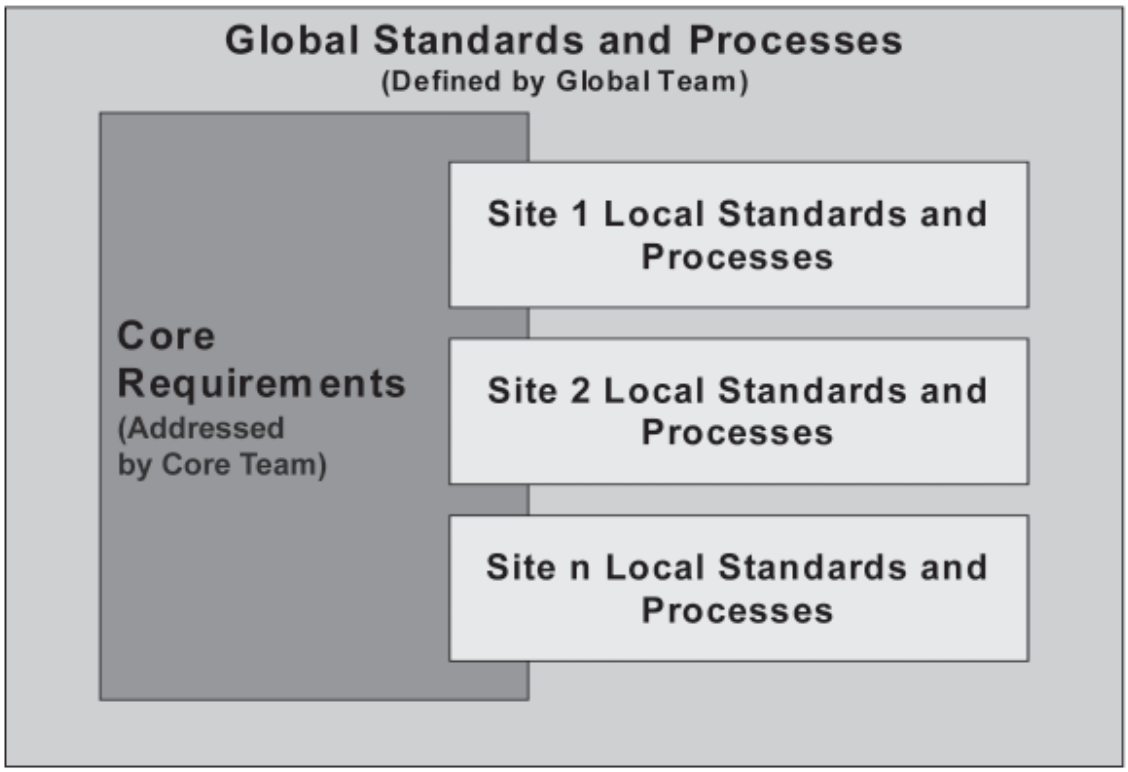
A global implementation can be defined as a centralized system in that one or more large systems are located in the same facility, or a distributed system in that one or more large systems can be located at several facilities or sites.

In the context of this document, ‘global’ will refer to the concept of a whole system and ‘core’ refers to elements that are common to each site.

Within a global team, a ‘core’ team will exist to address common elements.

Figure 1.1 shows how global standards and processes encompass global requirements, which interlink in with localized standards and processes. Note: in certain circumstances, local standards and processes may fall outside global standards and processes.

Figure 1.1: Global Standards and Processes



1.7 Structure of this Guide

The main body of the GAMP® Good Practice Guide: Global Information Systems Control and Compliance is divided into four main sections:

- Project Management
- Validation and Implementation
- Global Systems Management
- Data Management

The appendices provide additional material and guidance to assist in the identification of regulations, issues, and topics that should be considered.

Figure 1.2 shows the position of the guidance in relation to other GAMP® guidance.

Figure 1.2: Positioning of the GAMP® Good Practice Guide: Global Information Systems Control and Compliance

This Guide discusses particular issues, which relate to systems that apply to more than one site or function. Discussion of general issues covered in GAMP® is minimized where possible with some contextual references.

2 Project Management Considerations

The successful implementation of a compliant and validated global system is dependant upon how well the basic concepts and process of project organization and project management has been performed. Failure is rarely caused by esoteric factors, but rather by the lack of sound, basic organizational processes, and effective project management.

Whether a hierarchical or matrix organizational structure for a project is chosen, it is the assigning of a single person as the overall Project Manager that is most critical. That individual, who will have an active and continuous role in the project, should have strong leadership, administrative, and technical abilities.

It should be made clear from the outset which elements of the project will be managed globally and which elements locally, along with applicable quality standards to be applied.

Taking a locally developed and documented system and making it a global system also can be a challenging task. It is almost never a simple matter of taking the existing system, adding new users, and going live. There are a number of issues that need to be addressed covering this specific area, which is covered in Appendix 3 of this Guide.

Conflict resolution is a critical role for project management. Culture in particular is a critical element, even for small geographical areas with cultural diversity, as this can seriously disrupt a project. 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 is often focused on timely and on-budget delivery of the project. Care should be taken to align this emphasis with global and local regulatory needs.

Key aspects of project management that should be taken into consideration and addressed for global projects include the following:

- Cultural
- Regulatory
- Data Management Planning
- System Architecture
- Procedural
- Funding

2.1 Cultural

Cultural differences within organizations should be considered at the conceptual phase. The following subsections discuss language related aspects that should be taken into consideration.

2.1.1 Language

All communication and documentation should be clear and transparent to the entire global 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.

Legal Standards

Legal standards for a business activity can differ substantially from country to country. The legal interpretation of language can differ from country to country and even from legal jurisdiction to legal jurisdiction.

It is important to have legal advice from key sites involved at the very start of the project and throughout the project life cycle.

The organization 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.

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.
- Non-native speakers should review documentation for ease of comprehension.

Local Standards

Local language specific standards, which apply at local levels, should be established early in the project. Operating procedures or training may have to be in the local language and these requirements should be recognized at the start of the project.

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

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 including:

- Word Processing
- Document Management
- Spreadsheets
- Project Plans and Reports
- Specifications
- Test Plans and Test Scripts

Communication Standards

Communication planning and adequate communication is 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.

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 construed to be rude and aggressive in certain countries. Project managers should be particularly sensitive in this area.

Consideration should be given to establish a common glossary of terms.

Executive Summaries

In cases where documentation in local languages may have some exposure outside of that country, 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.

2.1.2 Organization

Understanding of the organization is a critical factor for the successful validation of any project, especially a global project. The following subsections discuss aspects that need to be specifically emphasized:

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.

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

Steering Committee

On global projects, the Steering Committee has the critical role of ensuring for the company the timely and cost effective completion of the project. This will include building effective regulatory compliance mechanisms and processes.

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

- Project Sponsor
- Project Manager
- Business Process Owner
- Key Technical Areas, e.g., Information Technology or Engineering
- Quality Assurance
- Representation of User Stakeholders

The Steering Committee should plan to meet on a periodic basis, timed regularly, and related to the duration and milestones of the project, which helps to ensure that the desired outcome is driven to the required timeframe. There should always be a Global Steering Committee, which should be considerate and understanding of local needs. Depending upon the nature of the project, local steering committees also may be appropriate.

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
- Resolution of conflicts between local/global or local/local priorities
- Resolution of other issues

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

Project Structure

A choice exists between **hierarchical** and **matrix** project structures.

Hierarchical structures provide clear communication and line management control, but have serious 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 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.

To operate effectively, the matrix structure often needs local project management representatives.

Project Manager

The role of the Project Manager depends to a significant extent on how the project is organized, but will always require leadership, technical, and administrative abilities. These key attributes need to be demonstrated on a continual basis with consideration being given to deputies to support language or local needs. Strength and depth of management is important, rather than dependence on a specific individual.

The Project Manager would take the role of mentor and trouble-shooter with conflict resolution being a critical element or task. The Project Manager should always recognize and be equipped to deal with cultural issues that may arise during the life cycle of the project.

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

Consideration should be given to the various disciplines and complexities of the subject matter. The ability to work as a team will be critical.

System Ownership

It is essential that system ownership be established at the beginning of the project. During the project, delegation to an operational role may take place, but it is critical that system ownership is defined throughout the project.

While ownership should be internal to the business, third-party involvement in support services or operations is becoming more common. In such cases, careful consideration should be given any agreements regarding documentation, availability of service, and maintenance.

2.1.3 Geographical

Projects with widely dispersed geographical locations may create problems of communication, coordination, and support. The following subsections describe key points for which careful planning should be considered:

Communication

Consideration should be given to the difficulties of communication and coordinating team activities especially 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 morale.

Teams also have to be wary of making decisions without input from remote sites for reasons as mundane as the inability to get a local conference room at a time when the members in remote locations are accessible. Such activities can send a very negative message to remote users or members of the team and communication activities should be planned accordingly.

People and Travel

Distributed locations create the need for potentially extensive travel, which should be planned and budgeted. For reasons similar to those for communication, it may not be advisable to schedule all face-to-face meetings at the headquarters site. Technological tools exist that make remote meetings more productive.

Consolidating global project development activities at one location provides a basis for effective communication and working, but creates potential problems of temporary re-location of people and services.

Overall project, budget, and cost allocations, along with the need for commitment of key team members are principal considerations for the project manager. Local holidays and seasonal traditions also need to be taken into account.

Documentation

Location and availability of documentation is vital for both company and regulatory needs. Normally, documentation will be 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 electronic document management system for project documentation approval is probably the best option, but can be expensive to implement. Many companies will find a centrally approved rationalized approach for a paper-based circulation a viable and more pragmatic option.

Turnaround time for documentation in support of audits should be considered.

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.

2.1.4 Legal

A review of the legal requirements covering all aspects of implementing and using the business process/system should be performed. It is important to have legal advice from the key sites involved at the very start of the project and throughout its life cycle. The following subsections discuss areas which should be considered:

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.

Certification

Geographical locations may require certification of the following:

- Systems
- Equipment
- Infrastructure
- Suppliers
- Personnel

For each element, there may be a need to have a certification to an external standard or by an external organization. Documentation of certification also may have a legally defined standard. For example, in Poland only certified engineers can approve documents, although to do this, they have an official stamp (rubber and ink) to confirm their certification.

Contractual Issues/Procurement

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

It is important that purchase contracts are reviewed in regard to any local regulatory implications. For example, the terms of a warrantee 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). In particular, it is important to identify ownership of and responsibilities for project activities.

2.2 Regulatory

While global regulations are reasonably consistent, they are not completely consistent. Differences exist between GxP communities and between the regulations of some geographical areas and countries. A global review of applicable regulations and *de facto* standards should be performed and agreed early in a project life cycle, as problems here will have impact on the global 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 Tables 2.1 and 2.2.

Table 2.1: Regulatory Topics for Consideration

Topics
Audit Trail
Backup and Recovery
Change Management
Configuration Management
Data Privacy
Deviations/Corrective Actions
Disaster Recovery
Document Management
Electronic Signatures
Facilities
Incident Reporting
Management Responsibilities
Performance Monitoring
Personal Qualification/Training/ Availability
Quality Management
Raw Data/Source Data
Record Retention and Archiving
Regulatory Audit
Risk Based Compliance
Security Management
Signatures
Supplier Audit
System Retirement
Validation Life Cycle

Table 2.2 identifies examples of US and EU regulations and guidance in which topics specified in Table 2.1 should be considered.

Table 2.2: Global Regulatory Considerations

Regulations
US 21 CFR Part 11
US 21 CFR Part 50, 54, 56, 312, 314 (US GCP)
21 CFR Part 58 (US GLP)
FDA Compliance References: Bioresearch Monitoring - Computerized Systems (CPGM 7348.808)
21 CFR Part 203 (US PDMA)
21 CFR 210, 211(US GMP)
Computerized Drug Processing; CGMP Applicability to Hardware and Software (FDA CPG 7132a.11)
21 CFR Part 600, 601, 610 (US Biologics)
21 CFR Part 820 (US QSR)
21 CFR Part 812, 814 (US Devices)
ICH E6 (ICH GCP)
ICH Q7A (ICH Bulk API)
ICH E10 Choice of Control Groups and Related Issues in Clinical Trails
EU/EC GMP - Annex 11 'Computerised Systems' to Council Directive 2003/94/EC
EU/EC GMP - Annex 13 'Manufacture of Investigational Medicinal Products' to Council Directive 2003/94/EC
EU/EC GMP - Annex 15 'Qualification and Validation' to Council Directive 2003/94/EC
EU/EC GMP - Annex 18 'GMP for API' to Council Directive 2003/94/EC
EU/EC GDP Council Directive 92/25/EEC amplified by Guideline 94/C/63/03
EU/EC Esig Framework Council Directive 1999/93/EC - Annex 1,2,3, and 4
Guidance
FDA Guidance. Computerized Systems Used in Clinical Trials.
FDA Guide to Inspections of Pharmaceutical Quality Control Laboratories
FDA Guidance on the General Principles of Process Validation
FDA Guide to Inspection of Computerized Systems in Drug Processing
General Principles of Software Validation; Final Guidance for Industry and FDA Staff – CDRH
EU/EC GMP Volume 1 and Volume 4 PIC/S Guidance Documents

Other regulations and guidance exist, such as the GMP Guidelines: Health Canada Guidance and PIC/S, as well as Japanese and Australian regulations. A risk management approach should be taken based on the global requirements.

Conflicting requirements that arise from the wide variety of perspectives in a global review process should be addressed with agreed requirements and documented in, e.g., the User Requirements Specification. In order to facilitate this, an association of regulations against topic areas covered in the above tables has been conducted (see Appendix 1 of this Guide).

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

2.3 Data Management Planning

Companies face increasing pressures to improve their use of computerized systems to achieve business goals, to streamline business processes, and to meet business related compliance requirements of regulatory bodies. As a result, regulatory compliance in a global context requires companies to collect, store, protect, and make available increasing volumes of data, records, and information. In addition, they should set, establish, practice, and maintain business acceptable standards and processes for data management throughout the project.

Data management within the global enterprise is an activity involving the identification, implementation, administration, and control of data held on information systems. It is required for the benefit, and in the case of regulatory requirements, the protection of the business and patients. As such, planning for data management should take account of global requirements for the following:

- Business models defined and owned by the business and used to ensure new and existing systems (including applications) 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 custodianship 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

Companies need to establish data management standards and processes that include planning, implementation, administration, and control of data. Complications will arise for global systems because of the dispersed nature of the data users, and sometimes of the data itself.

Key roles and areas of responsibility that should be established are shown in Table 2.3.

Table 2.3: Data Management Roles and Responsibilities

Role	Responsibility
Data Manager	Responsible for *global policy setting* including standards and guidelines covering training in and compliance to business relevant standards and guidelines.
Data Owner	Responsible for the *accuracy and availability* of the data either global or local.
Data Administrator	Responsible for *administration and control* of data either global or local.

2.3.1 Data Management Objectives

It is vital that a firm has adequate, well-established, and well-communicated data management principles. In arriving at a suitable data management strategy/methodology, data management principles should take into account global and local business and regulatory requirements that may be complex in nature.

Through proper design and execution of the plan, data users, regardless of locale, will experience access as required within and across organizational and geographical boundaries to securely stored data. The data will be delivered according to business need such that it can be read, manipulated, transformed, and eventually deleted *with integrity* in order to achieve a competitive business advantage and ensure regulatory compliance. Key to such a plan achieving success should be the establishment of an environment with controls that assure avoidance of potential compliance related problems such as data integrity issues, inconsistency, inaccuracy, uncontrolled replication, misuse, and in the extreme, unrecoverable loss.

The requirement for data management spans almost all areas of a global business, and should be centrally established. This means that when a new global system is being developed, there should be pre-defined and understood governing principles, supplemented with a life cycle model for data management. This should facilitate the definition of business requirements and the establishment of processes for data management that will meet expectations across the global business environment with minimal conflict with local regulations.

Objectives need to take into account that regulatory and legislative jurisdictions will probably be crossed in addressing the strategy, and as a consequence, it is important to involve regulatory compliance and legal specialists in defining the data management policy requirements by site, GxP area, regulatory regime, etc.

One of the most problematic issues facing data management planners is likely to be legal requirements related to privacy of personal data. At date of publication, such requirements are generally stricter in several European countries than in the United States although laws such as the Health Insurance Portability and Accountability Act (HIPAA) introduce such considerations into the management of clinical data in the US.

2.3.2 Business Models

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 User Requirements Specifications, and may relate to some or all of the following:

- Data Creation or Migration
- Defining Metadata
- Data Validation or Verification
- Policy for Addition, Deletion, or Modification of Data
- Retrieval and Use of Data
- Data Authority
- Data Ownership
- Data Access Techniques
- Copy Management

- Data Version Control
- Data Archive or Migration
- Database Architecture: Centralized or Distributed
- Define Critical Data:
  - to 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

From the perspective of development and execution of a data management plan, the data life cycle and the application life cycle should be viewed in parallel, at least as far as maintaining quality through both life cycles is concerned. Getting stakeholders involved early in the planning process is critical. In addition, the data management plan should identify those individuals appointed to take on the policy setting and execution roles and who are adequately trained in global regulatory requirements as they relate to managing data and information.

2.3.3 Policies, Standards, and Guidelines

The policy setting role (e.g., data and quality assurance managers) should operate in a global context to:

- ensure provision of data management policy, strategies, standards and guidelines across regulatory jurisdictions
- promote quality based data management as an across the enterprise activity
- identify appropriate training to ensure adequate compliance and controls can be met and are demonstrable

2.3.4 Underlying Databases and Data Models

The execution role (data and database administrators with global responsibilities) should ensure that:

- Data is administered in a consistent fashion across locales and region, e.g., that there is a consistent global application of quality control of data models.
- There are adequate and consistent provisioning and maintenance standards and guidelines.
- There are tools for data modeling and data administration.

- There are coherent, consistent, secure, and stable databases environments and architectures.
- Data copy management meets business requirements.
- There is an effective, compliant, and well controlled infrastructure.

Additional guidance and information covering aspects of data management is covered in Section 4.8 and Appendix 2 of this Guide.

2.4 System Architecture

The technological factors are primarily hardware and software technologies and related standards. The key factors to consider are Design, Administration, Environments, and Performance.

2.4.1 Design

A global system can be centralized or distributed.

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, e.g., a division.
- Centralized information: all information, needed by the entire organization or not, is stored at the central facility.
- Centralized control and support: a manager and technical support will control and maintain the equipment and applications.

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.
- Distributed control and support: a manager and technical support will control and maintain the platform and applications locally.

Centralized System

Advantages:

- ease of application of change control and standards enforcement
- ease of configuration management
- ease of system information analysis

- ease of implementing security

Disadvantages:

- vulnerability to outages where a single point of failure exists
- potential impact of changes

Distributed System

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 due to data replication at multiple sites
- easier to comply with local data protection laws

Disadvantages:

- Can be difficult to test and determine failure – the more complex and the more integrated the system the harder 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 makes it difficult to manage and impose standard for the network, security, and management of data collection and analysis along with application change control. Therefore, there is a higher risk that a system may evolve in an uncontrolled fashion.
- 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, etc.

Regardless of choice, the points below should be considered, many of which should be negotiated with the responsible infrastructure support groups. Depending upon the organization of the IT function in the company, this may mean that several local infrastructure groups need to be involved.

- 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[1]
- security, access controls, availability, integrity, confidentiality, and authentication
- network availability and stability
- testing of contingencies involving cross-site communications

Finally, architecture can play a pivotal role in determining the most appropriate strategy in validation testing. Further details covering this aspect are covered in Appendix 4 of this Guide.

2.4.2 Administration

It is quite common for some or all of the system administrative functions discussed in this section to be the responsibility of infrastructure support. If infrastructure support is largely a local responsibility, a negotiated agreement should ensure that adequate service is provided to the global user community. For example, a Help Desk open only during US business hours is not going to serve users in Japan adequately.

The following sections describe important areas for which plans or procedures should be implemented early in a global project.

Help Desk

Well-structured and resourced Help Desks are valuable in assisting end users and they also can provide a degree of on-going training. Important considerations in setting up Help Desks for a global system include:

- multilingual requirements, if any
- times of operation to adequately serve multiple 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 Help Desk, combination of the knowledge base and coordination of answers needs to be considered.
- coordination of a centralized Help Desk with local technical support
- procedures and tools to escalate issues for quick resolution, including prioritization
- service agreements between the Help Desk and the user groups to establish the expectations for these features

[1] This can be critical for time stamps on electronic records. Since system clocks are generally controlled by infrastructure support, a master clock server will need to be designated.

In addition to answering questions from end users, the Help Desk also can serve as a central repository for reporting of performance incidents and soliciting feedback from end users on necessary upgrades. Obtaining this information in a central location can help in identifying training issues, functional deficiencies of the system, and monitoring system performance as apparently random events in a number of locations may show a trend when viewed as a whole. Collated information from a Help Desk can provide performance metrics that can be an important input into a Periodic Review.

Disaster Planning/Business Continuity

To minimize the impact of any disaster on a global system, planning should include consideration of containing the effects to the local source. It is very important that such plans are tested to assure that business continuity requirements are met. The effects evaluated should include the loss of global and local resources, both simultaneously and independently.

In addition, training programs need to 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. As the global system evolves and changes are made, a methodology needs to be established that assures a periodic or event driven review of the disaster recovery plans and training programs.

These features should be built into service agreements between the relevant parties.

2.4.3 Environments

The 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.

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, due to the complexity of the system, the test environment may not be an exact copy of the actual production system.

- 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 pre-production environment with databases refreshed from production. One useful technique can be to test during shutdown periods with subsequently refreshed databases.

- Deployment of software from a global testing location to local sites should be addressed. Effective planning and establishment of controlled procedures will help to resolve potential communication and timing issues along with any additional re-testing that may be required as a result. This is especially true if any parallel testing is performed.

- Once deployed and operational, clearly defined procedures covering development and testing at both centralized and local levels is essential, and it may be necessary to maintain a dedicated team of developers and testers to continually support the system for a long time.

2.4.4 Performance and Capacity Planning

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

A global system can grow in unforeseen ways and those growth elements that can affect system performance need to be defined. If the global 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 the 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. It will be useful to consider planned redundancy to alleviate common mode failures that can affect the system extensively. Licensing agreements may become a limiting factor if not managed well. It is important to monitor usage and demand globally so that it does not become necessary to limit the number of simultaneous users to assure performance or meet licensing requirements.

2.5 Procedural

When conducting a global validation project, more planning is generally 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 all act to pull otherwise straightforward procedures in opposing directions.

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

- Change Control
- Configuration Management Planning
- Security Planning
- Validation Methodologies
- Training
- Periodic Review

2.5.1 Change Control

There are two levels of change control that should be planned for: project change control and operational change control. Managing change globally is one of the most challenging aspects facing a global project team and a global system owner. Failure to do this well can lead to project delays, software bugs, and regulatory compliance problems.

Project Change Control

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. Coordination of groups working across multiple sites with a common objective is key. For example, if a developer changes a variable name in a module he is working on, 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 subject is discussed further in *GAMP® 4*, Appendix M8 (see Appendix 7, reference 1).

Operational Change Control

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.

All of the concerns discussed relating to project change control are still valid issues, but more formality may be required around approvals and documentation. Many operational changes will require approval from a delegated quality assurance representative in addition to the system owner (or designee). Ideally, a global change control process should be in place to help with this and with notification of the appropriate people. Notification may have to extend to the global user community if the change affects how they use the application.

This subject is discussed further in Section 4.1 of this Guide and in *GAMP® 4*, Appendix O4 (see Appendix 7, reference 1).

2.5.2 Configuration Management Planning

Configuration Management is intimately entwined 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) and that designates someone 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 global system owner to manage the overall configuration listing with noted deviations. This can be important if the system becomes the target of regulatory inspection. Of particular concern and attention should be situations where coding is taking place at multiple locations, when rigorous configuration management becomes truly critical.

2.5.3 Security Planning

Global systems should adhere to a global minimum security standard, and planning should be geared in that direction. If enterprise standards do not already exist, standards should be established in the context of the global system. Similarly, if it is determined that the minimum existing standards are not adequate, appropriate standards should be defined.

Issues that should be managed to such standards include:

- password format
- password expiry
- minimal granting of administrative rights
- requesting, granting, modifying user accounts
- role-based security, as appropriate
- measures to ensure that access rights are revoked for people who no longer require access to the system
- electronic or digital signature standards, if applicable
- history of access rights
- security policy

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

2.5.4 Validation Methodologies

An important factor in recommending the adoption of a single standard for a System Development Life Cycle (SDLC) and validation for a global system lies in the need for the global system owner to be able to manage both the system and validation documentation. Uniform templates or document structures can simplify the process and transferability of the documentation can simplify the regulatory audit process as well. *GAMP® 4* provides an approach to this (see Appendix 7, reference 1). The issues for the stages of validation are discussed in Section 3 of this Guide.

2.5.5 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 will have to be careful to take into account local cultural issues and needs.

- 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.

- 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 using video/DVD or computer-based training, especially if Web-based, can be very efficient and useful if properly supported by appropriate additional local, or accessible central, expertise.

A consistent and thorough process for training new users after the system has gone live and the project team has been disbanded should include a comprehensive set of user manuals and procedures, which are maintained and available.

2.5.6 Periodic Review

Because of the larger scale, complexity, and number of changes typically applicable to global systems, the need for a periodic review of a global system, particularly for distributed systems, is greater than for single-sited systems and is mentioned here to encourage the planning of such exercises at the implementation stage. The process is discussed in more detail in Section 4.7 of this Guide.

Periodic Review should be conducted as often as warranted, typically on an annual basis. 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 revalidate the global system either in part or in its entirety. The Periodic Review process is described in *GAMP® 4*, Appendix O1 (see Appendix 7, reference 1).

2.6 Funding

It is important that validation of global projects is adequately funded and managed and that this is identified, decisions made, 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
- 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.

3 Validation and Implementation

Key aspects of validation and project implementation that should be taken into consideration and addressed for global projects include the following areas:

- System Ownership
- Validation Planning
- User Requirements Specification
- Risk Management
- System Specification, Design Review, and Traceability Management
- Testing
- Validation Reporting

In addition, while supplier evaluation is a routine element in the procurement\validation of any system, care should be taken to ensure that any supplier audit results are acceptable globally in order to avoid multiple audits.

For discussion of full life cycle activities refer to *GAMP® 4* (see Appendix 7, reference 1).

3.1 System Ownership

Every system should have an officially designated system owner, whose responsibilities reflect regulatory requirements. The system owner also may be the business process owner. The system owner is ultimately responsible for ensuring that the system is maintained in a validated state of control and is responsible for all the activities listed in *GAMP® 4*, Table 7.1 (see Appendix 7, reference 1). For global systems, there is often a system ownership team, lead by the global system owner.

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, are focused on the local system access, implementation, maintenance, and user training. Regardless of membership, the ability to act should be aligned with pre-defined responsibility.

Where global systems are developed to serve multiple and diverse business processes, ownership may be assigned to parties other than the business process owner, such as Quality Assurance (QA) or a senior IT manager. When this occurs it is critical that there is a formalized relationship established to ensure the system develops and evolves in concert with the business processes. In addition, any potential conflicts of interest involving QA as the global system or business process owner should be clarified.

Formalized relationships, roles, and responsibilities need to be documented, e.g., in an organization chart, and referenced from the Validation Plan to maintain accountability. This is particularly important when complex structures are developed and should be updated in a timely manner when system ownership changes due to organizational or personnel changes.

The concept of a Centre of Excellence (COE) should be considered as part of establishing system ownership and this is covered further in section 4 of this Guide.

3.2 Validation Planning

Validation planning is discussed in *GAMP® 4*, Appendix M1 (see Appendix 7, reference 1).

Validation planning should commence as soon as practical after project inception. Validation activities that have long durations may be extended further when multi-site considerations are taken into account. Basic computer system project planning guidelines are provided in *GAMP® 4*, Appendix M6 (see Appendix 7, reference 1).

A suggested checklist of key roles and responsibilities for validation of a global system with local variations is provided in Appendix 4 of this Guide.

The first step in validation planning is a review of critical global project success factors (cultural, regulatory, architectural, and procedural) as they relate to validation. Unresolved issues from the over-all project-planning phase need to be quickly addressed during the validation-planning phase to assure the project does not lose momentum. Ideally validation planning will start with the involvement of a validation representative at the initial project-planning phase.

In the initial phase a determination should be made as to whether the global system will be centrally or locally managed. Often there will 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 one of the local validation teams, in which case their site is known as the host or sponsor site. Important considerations to consider 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 re-do the core validation in addition to their site qualification 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.

The Validation Plan needs to 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.

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 may be considered. In addition, effort should be made early in the project to plan the qualification strategy both for efficiency, and if using the development system for qualification purposes, effectiveness.

3.3 User Requirements Specification

User Requirement Specifications (URS) preparation is discussed in *GAMP® 4* Sections 6.1 and 7.3, and Appendix D1 (see Appendix 7, reference 1).

The first step in the specification of global user requirements is to define the scope of the business processes and the presentation of this in a flow diagram format is particularly useful in cross cultural, multi-lingual projects. 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.

When defining business processes, data requirements are often neglected or gathered separately. However, when defining global business processes, particular attention needs to be given to setting standards for data that is shared.

Integrated multi-site, multi-discipline business processes are often 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.

The business process owner can take the responsibility for all the regional business process definitions or establish a guideline format for the 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 begin. In certain situations, it may be obvious; however, it is recommended to formalize this decision to avoid any 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 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.

Companies also may 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 the approvals process without making this unduly bureaucratic.

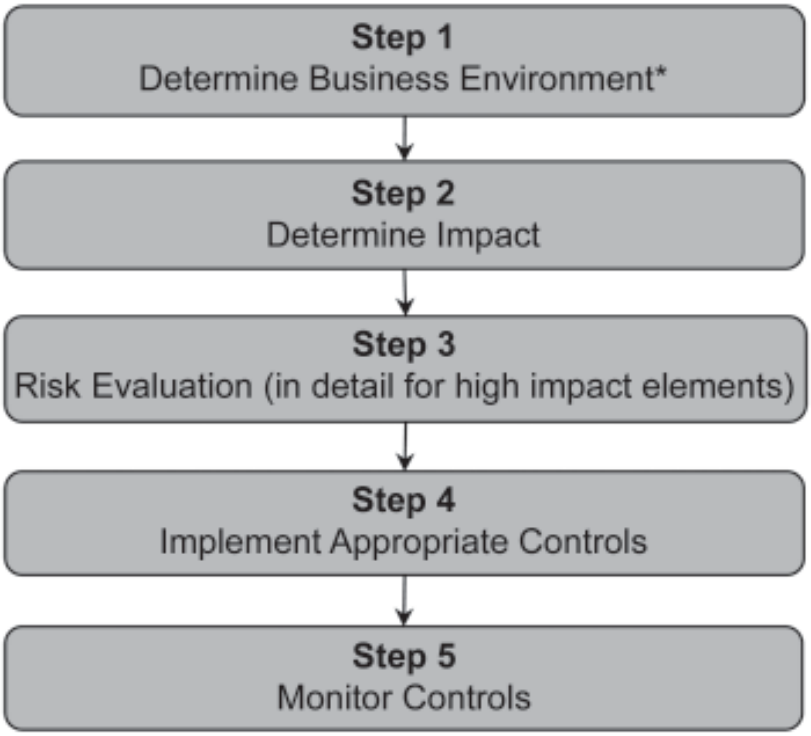
3.4 Risk Management

Basic risk assessment is discussed in *GAMP® 4*, Appendix M3 (see Appendix 7, reference 1).

The application of risk management principles in developing a validation strategy for global systems will be the same as it would for a purely local system. There will be some specific risks associated with the global nature that need to be understood and managed.

The approach adopted in GAMP® Good Practice Guides (see Appendix 7, references 11 and 12) employs a modification of the methodology used in ISO 14971 (see Appendix 7, reference 3). As modified for assessing global information systems, this is a five-step process as shown in Figure 3.1. Appendix 4 of this Guide discusses the role the application architecture can play in the approach to certain validation tasks. Similarly, the risks associated with the manner in which these tasks are approached can vary significantly depending on factors such as architecture, the way the system is used, and the nature of the process the system is controlling, etc.

Figure 3.1: Risk Management Steps



For example, consider configuration management in two scenarios.

In the first case, a global application is managed from a single site with user access through a Web browser.

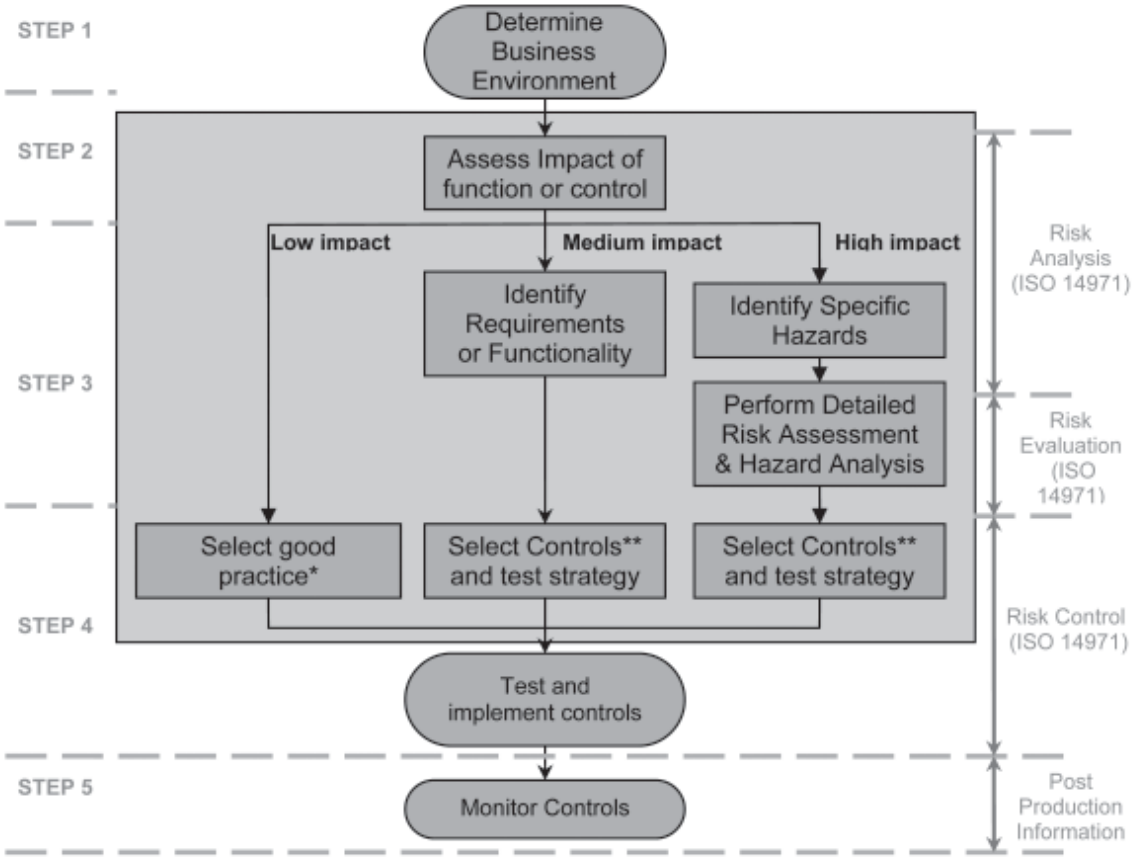
In the second case, the application is client-server architecture with hourly global replication of changes to local data. The impact of configuration management in the first case is probably minimal, but in the second instance, the possibility exists that if configuration management is not conducted effectively, sites may lose synchronization of configuration, which could in turn threaten the ability to share or exchange data.

This example illustrates how the manner in which a global system is built can have a major effect on the way the system should be managed. Similar analyses may be appropriate for functionality that may have global ramifications. For example, if it is imperative that users should have immediate access to recently entered data; a search on remote data could be a higher impact function. Further evaluation of architecture and procedures would then be warranted as a basis for establishing appropriate controls.

Figure 3.2 shows an approach to risk assessment based upon the concept of differing levels of impact. In the configuration management example above, the centralized Web-based system would employ the low-impact path through the diagram below, which implies that good IT management practices should be adequate. However, the client-server example would follow either the medium or high impact path,[2] which would lead to the conclusion that additional controls are appropriate.

[2] The selection of medium vs. high could be strongly influenced by the criticality of the system itself. A Quality Control LIMS would be high impact, while a plant capacity planning tool would be medium.

Figure 3.2: Modified ISO 14971 Scheme



* Good practice covers good IT practices and good engineering practices, and includes such processes as backup, security management, etc.
** In addition to good practice

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

3.5 System Specification and Design Review

Functional specification preparation is provided in *GAMP® 4* Sections 6.1 and 7.6, and Appendix D2 (see Appendix 7, reference 1).

System design specifications preparation is provided in *GAMP® 4*, Appendices D3 and D4 (see Appendix 7, reference 1).

Details of review and traceability are provided in *GAMP® 4* Appendices D5 and M5 (see Appendix 7, reference 1).

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, which will assist in ensuring that all key elements are reviewed and tested.

3.6 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 GIS is considered in this section.

A primary issue with a global system is maintaining consistency between local and global modifications, and maintaining a Traceability Matrix (TM) and other related documentation over an extended period of time.

Personnel turnover, and changes to a system, drives the need for comprehensive system documentation to control a system. The TM is an integral component of this system documentation and when combined with procedures and training from the start of the project can help to ensure the integrity of the system.

The topology of the global system needs to be considered with developing the TM and designing the business processes to maintain that system. For a global system shared across a network that is maintained in one location, the TM 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 a clear owner of the TM and to ensure for the transfer of responsibility when the owner is changed.

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

A global system is used in many different cultures and extends beyond single individual tenure. This requires a naming and numbering convention for the documentation that is simple to administer, well documented so others can easily learn and apply the convention, and which lends itself to creating a meaningful TM.

Table 3.1 gives an example matrix that includes a column that permits identifying which area is responsible for the requirement. Simplicity is essential to these conventions to ensure ongoing compliance across multiple languages and personnel change that may occur over an extended time period.

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

The documentation numbering conventions need to 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 might consider developing a global documentation traceability matrix that clearly indicates governance at global or local levels and how the documentation cascades down.

Table 3.1: Example Format for a Traceability Matrix for a Global System

1. URS Reference Number	2. Description	3. Scope of Requirement	4. GxP or Regulatory Impact	5. Other Impact	6. Functional Specification Reference	7. Design Specification Reference	8. Test or Verification Reference	9. Comments
URS1.0	Descriptive Text	Global	Y	N	FS02 3.1.4(a)	DS 4.5.1	OQ 4.5.3	Clarifying text
URS1.0.1	Descriptive Text	Local	N	Y	FS03 4.31	DS 6.8.2	IQ 3.2.6	Clarifying text
Etc.								

(Extended, based on tracking table example in *GAMP® 4*, Appendix M5 (see Appendix 7, reference 1).)

Key to the table:

1. **URS Reference Number**
   All user requirements need to be listed.
2. **Description**
   This can be optional; however, including the full URS section or a brief reference can be very helpful to anybody using the TM. Consider including key words that identify specific types of critical functionality, e.g., security, audit trails, calculations, etc.
3. **Scope of Requirement (local, core, or global)**
   The scope that this URS section effects should be listed, such as global, core, or local. This scope will also identify what area has responsibility for maintaining this section of the TM. When there are multiple local areas, it is necessary to include the specific local area this URS section effects.
4. **GxP or Regulatory Impact (Y/N)**
   If there is a GxP, 21CFR Part11, or other regulatory impact, then there should be a test reference number in column 8, or a reference showing how this requirement was verified.
5. **Other Impact**
   The system may require some formal verification or testing for reasons other then GxP (e.g., Safety, Health, Environment, Financial) and for which it would be a good practice to trace from requirement to testing. Indicating a Y in this column could be used to assure column 8 is filled in with a test reference or other form of verification.
6. **Functional Specification Reference**
   Enter the FS that defines the URS section. If the URS section will not be satisfied by this system, then this should be made clear by an appropriate notation, such as "Not Met" or an SOP reference that is used to satisfy the URS. Some requirements may be met by means other than software, and verified by means other than testing.
7. **Design Specification Reference**
   Enter the Design Specification, or Configuration that satisfies the FS.
8. **Test or Verification Reference (e.g., IQ, OQ, PQ)**
   A reference to a specific test should be included where there is GxP impact. Even when there is no GxP impact, good development practices encourages completion of this column in order to trace testing to requirements.
9. **Comments**
   Include any comments that add information particularly where reference needs to be made to additional testing or requirements that have arisen as part of this exercise.

It should be noted that for high complexity systems, especially where there are numerous one to many or many to one relationship, the use of a spreadsheet could become inefficient and/or confusing. An automated tool can be the most effective way of managing requirements and traceability for large systems; the utility of such a tool is enhanced for global systems.

3.7 Testing

Test details are provided in *GAMP® 4*, Appendix D6 (see Appendix 7, reference 1).

Application architecture effects on validation strategy are covered in Appendix 4 of this Guide.

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

It is important when planning the validation testing that a careful analysis is done 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 have 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.

Particular areas for consideration during test planning cover:

- 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 systems will tend to have a greater number of interfaces to consider although the issues are no different to any system interface.

3.7.1 Standardization of Documentation

There are advantages to defining test templates on a global basis. Doing so helps to ensure that local testing is conducted in a consistent manner, which complies with global practices. It helps also to give a more seamless appearance to the local validation package, which should be a combination of global and local documents. Finally, it presents a uniform appearance to regulators who may evaluate the system at one or more local sites.

3.7.2 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.

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

There are many automated test management tools that can be useful in managing distributed test effort and making the output and status visible to all concerned.

3.7.3 Deviation Handling

Deviations from the planned test process that have purely local effect should be handled locally according to the established deviation management process. Some deviations may have more significant effect; so 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.

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

3.7.4 Test Script Error Handling

Errors found in test scripts need to be communicated expeditiously 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.

3.7.5 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. Specific guidance on handling of test incidents and progress is given in *GAMP® 4*, Appendix D6 (see Appendix 7, reference 1).

3.7.6 Review of Test Results

A responsible core system technical reviewer, system owner, and quality assurance for GxP impact areas should approve validation test results as a minimum for core testing with local testing being reviewed and approved by a similar local team.

3.7.7 Change Management

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

3.7.8 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 also may be required locally. Careful consideration should be given to the planning and rollout of such tests.

3.8 Validation Reporting

Details on validation reporting are provided in *GAMP® 4*, Sections in 7.10 and 9.16, and Appendix M7 (see Appendix 7, reference 1).

Validation planning together with the scope and design of the global 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. Either these can refer to the core validation report or all reports can be summarized by a global report.

3.8.1 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 system owner, quality assurance, 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 in either hardcopy or electronic copy format.

3.8.2 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.*

4 Global System Management

Providing support for and maintaining a validated global system effectively is as challenging as the initial validation effort.

Many issues face companies trying to manage global systems, including:

- **Accountability:** most companies make someone responsible for system management, but assigning accountability is also important. A local data center may be responsible for backup and archiving, but there needs to be accountability to ensure that changes thought to be purely local do not compromise other sites.
- **Communication:** many aspects of system management require communication between sites and to global users.
- **Configuration management and version control:** an overall guiding hand is helpful, if not imperative, to keeping sites synchronized.
- **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.
- **Security management:** central management of security reduces the number of security administrators needed, but communication with local sites is imperative to ensure that access control reflects current needs.
- **Common resources for problem resolution:** significant synergy can be achieved if many of the problems with the system can be addressed centrally.
- **Service Level Agreements (SLAs):** SLAs should be established that define expectations for the system for both internal and outsourced services.
- **Management of future global validation issues:** validation is an issue whenever changes are executed.
- **Documentation management:** global validation documents need a home and a responsible caretaker.

While several models for global system management can be envisioned, this Guide will discuss one particular strategy that can help: establishment of a global “Competency Center” or “Center of Excellence” (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.

The CoE should have the responsibility for:

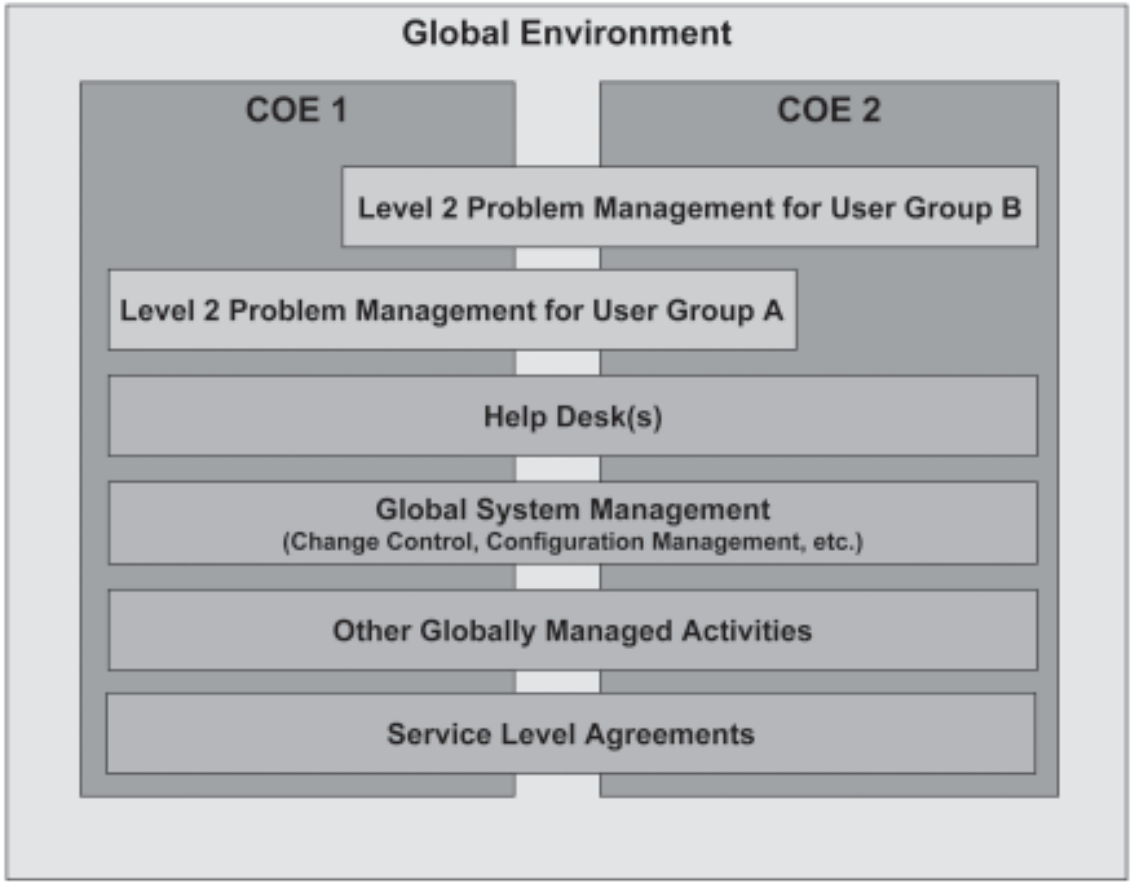
- managing the global application core, including:
- managing configuration
- managing global change controls process
- possible involvement in local change control processes
- managing application level security

- possible center for referrals for solution of 'level 2' or higher problems (those not soluble by the front line Help Desk)

In cases where there are multiple CoEs, problem management may be shared in order to support off-hours work. The CoE(s) also may be given responsibility in relation to backup, archival, disaster recovery, and training.

Figure 4.1 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 Help Desk[3] interacts fully with both CoEs. Usually problem management will be handled by the CoE most local to the problem although high priority issues could be worked on by the second CoE in cooperation with the first, e.g., during the first's off-hours. Both CoEs would assume full responsibility (and accountability) for system management issues like change control and configuration management. Ideally, a single SLA would tie user expectations together, although it might be that business practices at different sites might make multiple SLAs desirable.

Figure 4.1: Center of Excellence Concept



[3] It does not matter if the help desk is a centralized function or distributed in this model.

Critical to keeping any system validated is the rigorous application of the elements of system management. This is vastly more complex if a system is managed differently (or worse, to different standards) at various sites. To this end, a globally standardized service management methodology like ITIL[4] can greatly facilitate consistent system management, and should be embraced by CoEs.

Companies should consider adopting such a standard approach to ensure that all 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.

The CoE is an ideal vehicle for negotiating an SLA with the system owner defining what expectations users should have for performance and availability. The CoE also can manage Operating Level Agreements (OLAs) with internal suppliers (e.g., for network support) and Underpinning Contracts (UC) with external suppliers (e.g., the application supplier's help desk).

4.1 Operational Change Control and Management

Operational Change Control is covered in *GAMP® 4*, Appendix 04, and Change Management is covered in *GAMP® 4*, Appendix M9 (see Appendix 7, reference 1).

Change control is intimately intertwined with configuration management since most of the changes that need to be managed in conjunction with a computer system are changes to the configuration. Managing change is a complicated and exacting process under any circumstances, and it is vastly more difficult when applied globally, due to the need for a much wider evaluation of potential effect. This emphasizes the need for a well-defined process that stresses thorough and effective planning, management, and communication of changes.

Not all changes should be evaluated globally. The challenge is developing a process that routes the change requests appropriately.

4.1.1 Change Control

Change control is necessary during the project and system validation (see Section 2.5 of this Guide) and during the operational lifetime 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, i.e., the number of physical handovers, especially between different sites, should be minimized. A software tool that allows electronic approvals can be a great help in overcoming these complications.

4.1.2 Change Management

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

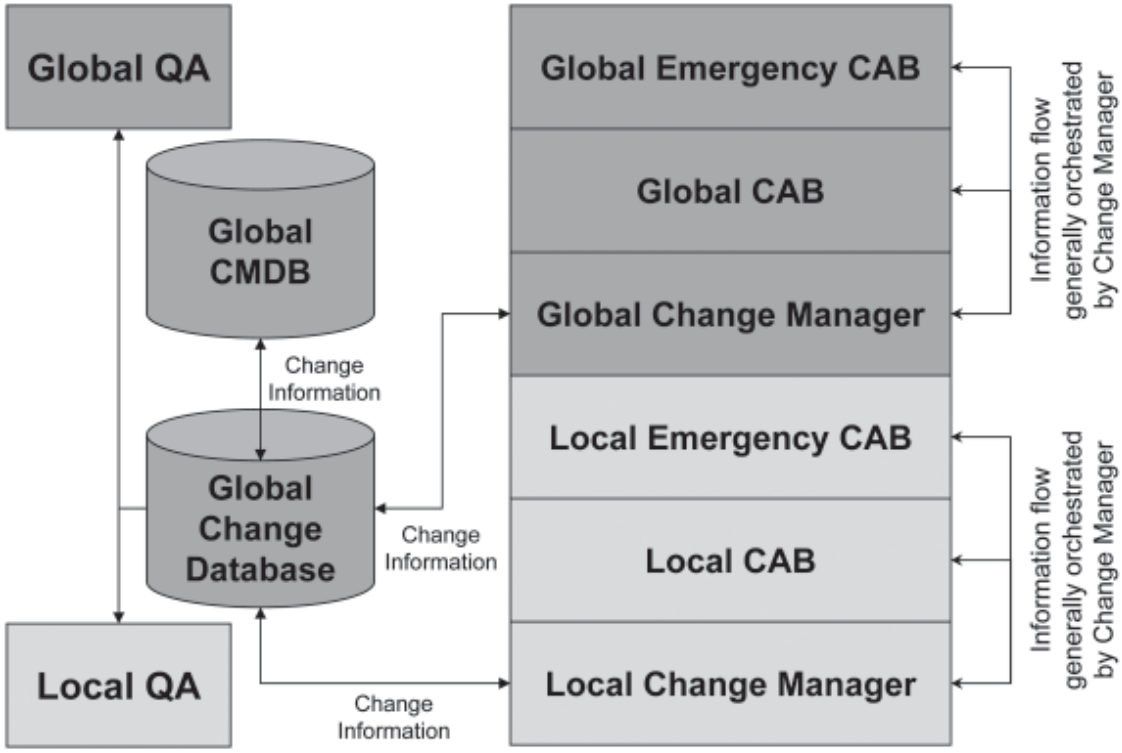
- evaluation of the change:
  - accountability for evaluating impact
  - global and local assessment

[4] Information Technology Infrastructure Library (ITIL) is a methodology developed in the UK that has become the de facto global standard for IT service management. Many of the processes described in ITIL are key to good system management.

- priority of the change:
  - accountability for prioritization
  - criteria for implementation, e.g., service window or upgrades
- approval of the change:
  - accountability for approval, dependant upon type of change, e.g., OS patch installation versus application upgrade
  - accountability for emergency approval
- documentation of the change:
  - accountability for creation, storage and inspection readiness of documentation and records

One of the best mechanisms for handling change is through application of the ITIL model using both a 'Change Manager' and a 'Change Advisory Board' (CAB). These should be structured to cover both global and local needs.[5] Figure 4.2 shows a graphical representation of how such an organization could be structured.

Figure 4.2: Possible Change Advisory Board Structure



[5] 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 document does not address the 'Management Board' since the regulatory decisions would most typically be handled at the lower levels.

A Change Manager is empowered to authorize low-impact changes in order avoid burdening the CAB with trivialities, and usually chairs the CAB, which authorizes major changes. QA should be involved in the CAB for validated applications. One of the benefits of such an approach is that it facilitates changes that do not require QA approval, but provides QA with an overview of what those changes are. Of paramount importance is establishing minimum qualifications for the local Change Managers. This is a critical issue because these individuals make the initial decision of what goes to the CAB, and hence QA review. Change Managers should maintain a list of classes of change that are considered executable based solely on their approval. It is important to maintain the integrity of this process, and not to circumvent the process simply because it is expedient to do so. Risk Management tools such as those described in Section 3.4 of this Guide and Appendix M3 of *GAMP® 4* (see Appendix 7, reference 1) should figure prominently in the assessment of change impact.

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 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 enough 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 Change Managers meeting or teleconference is a strong recommendation to facilitate communication and early recognition of issues.

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

The QA authority approving changes should understand such differences, or at least recognize when they need to consult with local experts. This can have the unwanted effect of drastically slowing the change process, so defining a mechanism and expectations for response time is important.

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 particular applications. The disadvantage to 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 salient point is that the CAB should have enough understanding to either 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 should have 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 also will facilitate keeping an accurate configuration (see Section 4.1.6 of this Guide).

Since application changes are not the only type of change that can affect a validated global system, communication lines need to be open with infrastructure support groups. 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 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 approach of defining a CAB Emergency Committee (CAB-EC), typically a subset of the full CAB, may not always be workable if the global CAB includes members from geographically disparate sites. Companies may have to accept either less efficient emergency change processes, which may not be palatable, or accept the risk that globally implemented emergency changes may adversely affect some local instances.

To minimize risk and confusion, it is imperative that the emergency change control process is thoroughly planned and understood, is given high visibility, and proactive buy-in for the emergency change process is obtained from all sites and quality assurance. Should a situation arise requiring a response more rapid than the CAB-EC can handle, the company may wish to empower the CoE to act, involving the CAB-EC as soon as possible afterward.

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

4.1.3 Release Management

The process for executing a change should adhere to the formal release management practices of the company.[6] Changes may be released to users in a variety of 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.
- **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. Cost also should be a consideration, as full or package releases are more efficient, and generally more compliant with regulatory expectations since documentation and testing are generally better than when changes have been implemented piecemeal.

Release management requires certain elements of planning which will have possible global and local ramifications. Sometimes rollout will not be done simultaneously at all sites. In such cases, 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.

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

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 system. Because of the difficulty for the global team to fully understand the ramifications of a change to all of the local instances, there may be problems at a local site that compromise system functionality, while at other sites the change works flawlessly.

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?
- 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 system owner, global Change Manager?
  - Can the local site/system owner force a global rollback?

Questions to be answered when executing the plan include:

- Can the local site live with the problems while 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 rollback 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.

It should be stressed that having a rollback 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

Executing Change

Execution of a change on a global 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 weighed and 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 rollback, it is important that this be approached calmly, and that some testing is done to verify that the rollback did in fact work as expected. This applies to full rollback of a global change or to partial rollback (i.e., at a particular site). The verification/test process for the rollback may require user participation.

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.

4.1.4 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 felt regulatory wrath for this. The vulnerability of global 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.

Steps often left incomplete include:

- updating or amending specification documents (URS, FS, SDS or System Description) affected by the change.
- obtaining required approvals
- ensuring retention of change documentation (including test results)
- Closure of 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.

The change procedure should define clearly that all parts of the process should be completed, and internal controls such as 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.

4.1.5 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. Unfortunately, not all companies have such tools, and may, therefore, have fragmented change records.

The accessibility of change records is more important than their location. They should be available to IT staff who are troubleshooting a problem and to system owners and QA in case of regulatory audit. At the very least, the records of changes executed at the global level should be available in one location that is accessible to local change managers. In this respect, the least desirable answer to maintaining change records is a paper-based system.

The minimum content of change records should include as appropriate:

- identity of the requester
- details of the impact assessment:
  - impact (minor/significant/major)

  - test strategy (based on risk and impact)

- priority (low/medium/high/urgent)
- roll back plan (not always necessary for minor changes, based on risk)
- 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 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.

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.

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.

4.1.6 Configuration Management

The configuration management challenge is particularly great for a global system. Complexity can vary greatly based on system architecture. For example, a centralized global model will be significantly easier to manage in terms of configuration than a distributed client-server model. This Guide focuses on the latter, which is a reasonably common architecture and which can serve as a "worst case scenario" for complexity.

It can be difficult to monitor multiple sites without a strong process rigorously applied through a good tool. It is imperative for a global system that a single configuration management solution is universally applied throughout. One good solution is the model proposed by ITIL.

Part of the work of the global development team should be to define all of the Configuration Items (CIs) for the system, including the attributes and relationships for these CIs. (Note that 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 not only configurable parameters, but also include hardware components, common infrastructure components like servers and network,[7,8] software components, and documents.

[7] 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 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.

[8] Further information on this topic may be found in the *GAMP® Good Practice Guide: IT Infrastructure Control and Compliance* (see Appendix 7, reference 13).

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

Of particular note is that 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.

While there ought to be a centralized list of configuration items, it is not necessary, and often not advisable to manage all CIs centrally.

However, there needs to be clear ownership 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 authorities if a change to a CI has potential global impact.[9]

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

Changes to infrastructure, such as to some hardware components, the operating system, or other layered software, can have a profound effect on the ability of the application to run, and on the ability for sites to share data. If these infrastructure elements are not under the direct control of the application 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 owner and quality assurance. Such notification needs to be sufficiently in advance so that those supporting the application can evaluate, and if necessary mitigate, the proposed change. However, many infrastructure elements are either very dynamic (e.g., virus definitions) or have little discernable effect on particular applications (e.g., network switches).

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, retaining a legacy environment without the change for operation of the validated application (this is not usually a good solution because proliferation of legacy environments is highly undesirable from a configuration management standpoint)
- non-execution of the change

4.1.7 Issue Management

The approach to issue management will depend upon the structure of the system. Whether a centralized or distributed system, a documented procedure should be considered which defines suitable global communications and takes into account local implications.

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

Local issues which are directly attributed to the global system should be communicated and managed at a global level.

Local issues which are limited, but could have similar impact at another locality, should be communicated through an established network or process.

4.2 System Security

System security is covered in *GAMP® 4*, Appendix O3 (see Appendix 7, reference 1). Consideration should be given to accepted international security standards for a global system, e.g., ISO 17799 or the NIST standards (see Appendix 7, reference 5).

A challenge for any system administrator is to know when existing privileges should be granted, amended, or revoked, e.g., when an employee moves to another position within the company or leaves. This is exacerbated if accounts are managed globally so procedures should be established involving the Human Resources Department and Quality Assurance to notify account administrators in a timely manner in accordance with predefined and approved procedures. Periodic verification should be done by a central authority (e.g., a CoE or QA) to verify that account and access management processes are working adequately.

Physical security for global systems will, generally, be the responsibility of local IT and/or security staff.

4.3 Performance Monitoring

Performance monitoring is covered in *GAMP® 4*, Appendix O5 (see Appendix 7, reference 1).

Users, support staff, and owners at local operational areas should be polled periodically to ensure that they are receiving satisfactory service. This is important because 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 SLA.

It is important to track and categorize incidents and analyze problems globally (including understanding possible local impact) to ensure that the application works as expected and remains validated.

The CoE approach is a good structure to support this activity.

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 long term, periodic updates for users also are an important part of a communication strategy that will help minimize exacerbation of the problem.

Automated tools should be considered for performance monitoring, wherever possible.

4.4 Backup and Recovery of Software and Data

Backup and recovery of software and data are considered in *GAMP® 4*, Appendix O7 (see Appendix 7, reference 1).

Impact on the business associated with backing up databases should be weighed against the cost, including 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. The requirements for each site should be assessed when deciding whether a local copy of the backup is required.

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; 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. Procedures should be established which define what is included in the backup, how often the backup is performed, and who performs the backup.

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 the URS 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 a good tactic.

Procedures should be in place for system data recovery. It is essential in a global system to control that may request a recovery since the possible effects of this could be further ranging than those making the request may realize, e.g., such a recovery may overwrite data collected at another site. It is equally important that the user community be notified when a data recovery has been executed.

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

It is worth noting that timely replication of a database (see Section 4.8.2 of this Guide) may adequately meet the need for data backup for some sites. However, at least one site should execute standard backups so that a clean copy is available in case a propagating corruption, virus, etc., were to compromise all on-line copies of the data.

4.5 Record Retention, Archive, and Retrieval

Record retention, archive, and retrieval are considered in *GAMP® 4*, Appendix O6 (see Appendix 7, reference 1).

While archiving has much in common with backup, it does not serve the same purpose and the two should not be used interchangeably or confused. 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 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 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.[10] Archives should have a predefined finite lifetime, after which the records should be destroyed. Retention of archives needs to meet the regulatory requirements of all relevant health authorities 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 have to be destroyed in Germany when an individual leaves a company. Unfortunately, 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 have to be party to the final decision.

Some GxP systems also may have overlap with financial regulations, e.g., the US Sarbanes-Oxley Act.

Record retention policies should attempt to satisfy all applicable regulations.

4.6 Business Continuity and Disaster Recovery

Business continuity and disaster recovery is considered in *GAMP® 4*, Appendix O8 (see Appendix 7, reference 1).

Companies should have enterprise disaster recovery plans, within which recovery of a specific global system will be included. Such a plan will identify recovery sites and priorities. Owners of global systems need to ensure that their business needs are considered within the enterprise plan. While such details as identifying 'hot sites' would be premature, considering business continuity and disaster recovery during requirement planning will help to ensure business needs can be met. The discussion below should be read as being in the context of this overall plan.

In some ways, disaster recovery may be simplified for a global system, while in others it is more complex. The ability to use another of the company's own data centers as a hot site for recovery can simplify matters; it may be possible to get up and running again simply by recovering the affected site's data to another site's database server. However, the effect of the added data volume and user community to the recovery site's infrastructure needs to be well 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 ensure that disaster recovery under such circumstances is acceptable. For example, when defining user requirements, the two largest sites should be designated as disaster recovery hot sites, and it should be ensured that computers with adequate capacity are specified in the hardware design phase. During testing, it should be verified that the loads can be handled acceptably. Periodic disaster recovery drills also should be carried out to test the solution and preparedness for a disaster.

[10] If backup is to be managed centrally, WAN bandwidth becomes an important factor.

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 workarounds 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.

4.7 Periodic Review

Periodic review is covered in *GAMP® 4*, Appendix O1 (see Appendix 7, reference 1).

The purpose of periodic reevaluation of validated, global systems is to assess the continued overall effectiveness of the GxP related systems and to maintain their validated and compliant status. Aspects of periodic review for which global systems have an added level of complexity include:

- **Configuration:** the recorded or documented configuration should match the actual current configuration. Local owners should agree on what the actual configuration is, and adequate configuration management for local components should be effective. 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:** ensure that centrally driven change been properly implemented locally, especially patches or updates to application, database, or operating system.

- **"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. A degree of additional testing, both locally and globally, may be warranted beyond that performed in conjunction with the 'minor 'change. In addition, there may be some changes that were not tested or documented. Additional testing should be based on risk management principles.

- **Traceability:** changes to the system should be reflected in appropriate design documentation, e.g., URS, FS, or SDS. 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.

- **Specifications:** current versions of specification documentation should reflect the 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.

- **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 has 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. Backup processes and the regularity of testing restoration also should be checked.

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

QA should be involved in the re-evaluation 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.

4.8 Global Systems Data Management

4.8.1 Data Quality

Principles governing data quality, both operationally and procedurally, include the following:

- 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), clear, and complete.

- Data should be available and accessible.

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

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

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

Three key areas, which are often overlooked in global systems, are data availability, accessibility, and consistency.

Availability

Data availability requires a data management environment within which users can find the data they need, when they need it, from among all data that is not required. Operational procedures need to ensure that users are not placed at risk for making business decisions based on incomplete or stale data.

Accessibility

Access to relevant and accurate data and information is critical to making good business decisions. Quality data management includes responsibility and accountability for corporate data management policy, standards, and guidelines that specify what can be provided to users and how and when that access should be provided.

These policies and procedures may be enforced through the management and maintenance of user permissions (entitlement) within the system itself.

Effective global policies and procedures provide a basis for facilitating continuous improvement in data quality, including accessibility, the ability to share the data, and reduced risk of regulatory non-compliance.

Consistency

Data consistency is frequently an underemphasized 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, trunk versus boot, 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, it is important that there is 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 particular datum was created or modified and 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., GMT) 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 certain 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.

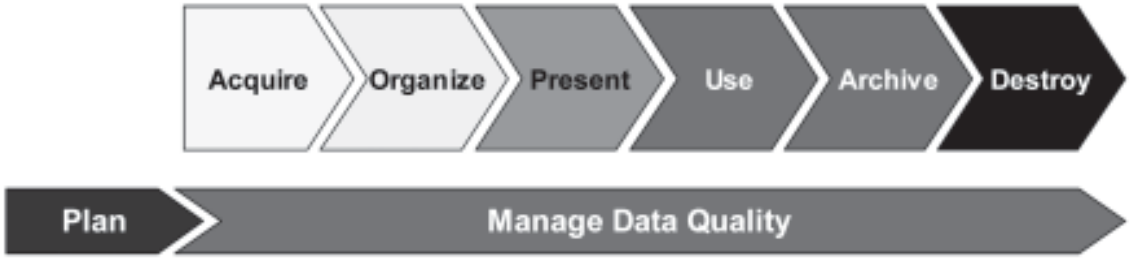
Having well managed and consistent data will make it more useful for global uses, e.g., global trending, as well as placing the company in a better position to meet regulatory expectations for data integrity and quality.

4.8.2 Data Management Life Cycle

Data management should follow a well defined life cycle, which covers planning, acquisition, implementation, data use, and data retirement. This is exceptionally critical for global systems where many of the steps in the life cycle model in Figure 4.3 may be under the control, or at least the influence of a widely diverse group of individuals.

The life cycle is dependent for its successful implementation on ‘fit for purpose’ computer-based information management systems; or in the case of paper records, document management repositories, or libraries. Planning of data management is discussed in Section 2.3 of this Guide and a guidance checklist is provided in Appendix 2 of this Guide.

Figure 4.3: Data Management Roadmap



The roadmap shown in Figure 4.3 should be considered in the context of a global system and each area should have supporting processes, models, tools, and procedures.

Once established, it is critical that the quality of the data be maintained and supported throughout a global system so as to meet user requirements both locally and globally.

Equally important is the ability to demonstrate that the requirement for data quality is being met on an ongoing basis from business and regulatory perspectives. The maintenance and assurance of data quality may be accomplished through the application of agreed standards via the use of validated processes, controls, and procedures.

Within each organization, it is imperative to demonstrate how data is critical to business processes and users, what can be achieved by improvements in data quality, and at what cost (the return on investment including the return in meeting regulatory compliance).

Part of this process is to develop a data management strategy that includes:

- data migration (when applicable: it is not necessary to have a migration strategy until such time as a migration is foreseen)
- data (base) replication
- backup/recovery
- data archiving and retrieval
- data access management
- record destruction management

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)

- transcription verification
- 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
- leading to 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

Database Replication

Organizations rarely store all of their data in a single (physical) database. Most companies also have more than one type of DBMS.

A single globally accessible database has several advantages from both a regulatory and operational standpoint:

- consistency: everyone looks at the same data
- unambiguous time stamps associated with data creation, manipulation, or deletion
- security management can be easier

While in practice, a single globally accessible database has many advantages; however, there are potential disadvantages as well:

- Care should be taken to ensure that the aggregate size of the database does not become unwieldy, or even unmanageable, and result in compromised data quality.
- A single point of failure is established. Applications dependent on access to that database will be negatively impacted by its failure.
- A single database may not be capable of being performance tuned to suit all applications. This creates potential for data loss or unavailability.

Having an online replicated database where different sites access their own database instances can mitigate these risks, but care should be taken not to compromise integrity as represented in the first set of bullets above. A logically consistent approach to data sharing between applications and users, and database copy management requires the establishment of corporate data models and a data management strategy that covers:

- location of data, e.g., stored or held centrally, distributed, held locally
- ownership of data
- Frequency of database replication, which when considered with business practices at affected sites, should be often enough to ensure that decisions are not based on stale or incorrect data.

- The approach to security and preferred platforms, i.e., the development and enforcement of global standards that will support business/user requirements.

- The infrastructure (including the support organization)[11] should be capable of supporting database replication. This means that:

  - Operations like backup need to be coordinated with replication.

  - Network bandwidth should be available when needed.

Database Backup and Recovery

See Section 4.4 of this Guide.

Data Archiving and Retrieval

See Section 4.5 of this Guide.

4.8.3 Data Access Management

See also Section 4.2 of this Guide and *GAMP® 4*, Appendix O3 (see Appendix 7, reference 1).

Access management is a key element of risk to data. It is generally dependent on 'role-based' permissions within the application, and is thus, more complex than general system access. This can be especially difficult if the intent is to manage access from a global resource, e.g., a CoE, although such an approach can reduce risk to data if handled well.

As with access to infrastructure, globally distributed information processing 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.

A global system increases the complexity of managing data access entitlement and permissions and requires that the security of data management systems be integrated into the overall security fabric of the enterprise. Security policies, procedures, and tools such as Enterprise Lightweight Directory Access Protocol (LDAP) services and public key infrastructure certificate based services, can be helpful in this regard. An added benefit is that this may make the administration of a given system easier for IT departments.

[11] In large organizations, the infrastructure is frequently supported by a different organization that supports the application. Infrastructure support is often the responsibility of a purely local organization although global infrastructure support groups are becoming more common.

Appendices

Appendix 1
Regulatory Matrix

As part of the preparation of this Good Practice Guide an analysis was done of major regulations and guidance documents from the United States, Europe, Japan, and Canada (listed below in Table A1.1). The purpose of this effort was to assess global approaches to 24 aspects of computer systems compliance as identified by the SIG. These appear in Table A1.2. The resulting matrix was too large to publish in the format of this Good Practice Guide, but it is available as a spreadsheet through the ISPE Web site at www.ispe.org/GIS_Appendix1. The matrix provides specific references to points within the regulatory documents that touch on the issues from Table A1.2, and can be used to assess potential similarities or differences in the regulations.

This matrix represents a snapshot of global regulations as of this publication, and will not be updated. However, the spreadsheet format allows the reader to download it and update it as is seen fit.

Table A1.1: Global Regulations and Guidance Assessed

21 CFR Part 11 (US ERES)
21 CFR 210, 211(US GMP)
21 CFR Part 203 (US PDMA)
21 CFR Part 50, 54, 56, 312, 314 (US GCP)
21 CFR Part 58 (US GLP)
21 CFR Part 600, 601, 610 (US Biologics)
21 CFR Part 812, 814 (US Devices)
21 CFR Part 820 (US QSR)
Computerized Drug Processing; CGMP Applicability To Hardware and Software (FDA CPG 7132a.11)
EU/EC E-Commerce Council Directive 2000/31/EC
EU/EC Esig Framework Council Directive 1999/93/EC - Annex 1
EU/EC Esig Framework Council Directive 1999/93/EC - Annex 2
EU/EC Esig Framework Council Directive 1999/93/EC - Annex 3
EU/EC Esig Framework Council Directive 1999/93/EC - Annex 4
EU/EC GDP Council Directive 92/25/EEC amplified by Guideline 94/C/63/03
EU/EC GMP - Annex 11 ‘Computerised Systems’ to Council Directive 91/356 and 91/412
EU/EC GMP - Annex 13 ‘Manufacture of Investigational Medicinal Products’ to Council Directive 91/356 and 91/412
EU/EC GMP - Annex 15 ‘Qualification and Validation’ to Council Directive 91/356 and 91/412
EU/EC GMP - Annex 18 ‘GMP for API’ to Council Directive 91/356 and 91/412
FDA Compliance References: Bioresearch Monitoring - Computerized Systems (CPGM 7348.808)
FDA Guidance for Industry, Part 11, Electronic Records; Electronic Signatures - Scope and Application
FDA Guidance on the General Principles of Process Validation
FDA Guidance. Computerized Systems Used in Clinical Trials.
FDA Guide to Inspection of Computerized Systems in Drug Processing
FDA Guide to Inspections of Pharmaceutical Quality Control Laboratories

Table A1.1: Global Regulations and Guidance Assessed (continued)

GAMP® 4
General Principles of Software Validation; Final Guidance for Industry and FDA Staff - CDRH
GMP Guidelines - Health Canada Guidance
ICH E10 Choice of Control Groups and Related Issues in Clinical Trails
ICH E6 (ICH GCP)
ICH Q7A (ICH Bulk API)
OECD The Application of the Principles of GLP to Computerised Systems ref: ENV.MC/CHEM(98)17 as revised in 1997 and issued 26/01/1998
PIC/S Guidance. Good Practices for Computerized Systems in Regulated "GXP" Environments (Aug 2003)

Table A1.2: Validation and Compliance Activities Examined in Global Regulations and Guidance

Audit Trail	Performance Monitoring
Backup and Recovery	Personnel Quals/Train/Availability
Change Management	Quality Management
Configuration Management	Raw Data/Source Data
Data Privacy	Record Retention/Archiving
Deviations/Corrective Actions	Regulatory Audit
Disaster Recovery	Risked Based Compliance
Document Management	Security Management
Electronic Signatures	Signatures
Facilities	Supplier/Vendor Auditing
Incident Reporting	System Retirement
Management Responsibilities	Validation Lifecycle

Appendix 2
Data Management Considerations Checklist

Included in this Appendix are two tables that group basic principles for data quality and life cycle elements, considered in Sections 5.2 and 5.3 of this Guide. The tables should be used to identify the measures taken to meet the requirements:

Table A2.1: Data Quality

Principle	Requirement	Considered
Affordability	Minimize duplication of effort	
	Coordinate data management effort	
	Adhere to common standards	
	Manage risk and cost	
Accuracy	Data values represent the properties they describe	
	Assign and track data accuracy	
Accessibility and Security	Access and control on a local and global level	
	Data security and control, covering audit trial	
	Legal	
	Confidentiality	
Time Stamps	Corporate Policy	
	Business requirements	
	Regulatory requirements	
	Maintain chronologically accurate relationships between components	
Ownership and Intellectual Property	Secure management of third-party contract source code	
	Joint or shared ownership	
	Third party components (licensed products)	
Risk Mitigation	Policy defining data storage and replication	
	Data retention policy and procedure	
	Management of source data	
	Change management	
Availability	Policy and procedure defining availability and usage	
	Centralized database	
	Definition of data elements	
	Consistency of data	
Technical Compatibility	Defined Architecture	
	Transmission method	
	Media format defined, (Digital, Analogue, Paper, other)	

Table A2.2: Data Life Cycle

Principle	Requirement	Considered
Plan	Local policy considerations	
	Global and local resources	
	Standards	
Acquire	Integrity and maintenance	
	Synchronization management	
	Metadata standards, language and purpose	
	Compatibility of data sources and formats	
	Authenticity	
	Confidentiality	
	Transport interface	
Organize	Access to data	
	Manage version dependencies	
	Acceptable access times	
	Data replication strategy	
Present	Error detection capability	
	User acceptability	
	Usage consistency	
Use	Performance	
	Issue management	
	Access logs and security implications	
	Service level agreements	
Archive	Business	
	Technical	
	Compliance with regulations	
	Indexed and searchable	
	Paper or e-copies available	
	Maintenance and control of data	
	Secure data sharing	
Destroy	Retirement	
	Change management record retention	
	Data disposition	
	Removal of expired records	
	Deletion synchronization	

Appendix 3
Local System into a Global System

History

The local system has been developed, supported, and used locally for a period of time. All of the people involved in the development, implementation, and use of this system 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. When you decide to move a local system to a global profile, you 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. However, it is very important that the new global team include some local team members. They know more about the existing system than anyone else in the company. Additionally, their participation can be of enormous help in overcoming any resistance within the local business community.

Business Process

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

As the existing system is assessed, new requirements are collected, and the global system design starts to emerge, the project team should constantly compare this design to the established business processes and perform an impact assessment. 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.

Supporting Documentation

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

The subjects listed in Table A3.1 should be part of the assessment and determine whether the existing documentation can be used, and the next steps to be taken:

Table A3.1: Documentation Supporting Conversion of a Local System to a Global System

Subject	Response\Details
What was the language used for the supporting documentation of the local system?	
If there is a "corporate language," was it used for this project?	
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?	
What tools or applications were used to develop the local documentation?	
Are the tools/applications used global standards?	
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 Matrix • Test Scripts • Training Materials • Operating Procedures	
Did local documentation follow a standard?	

System Design and Technical Architecture

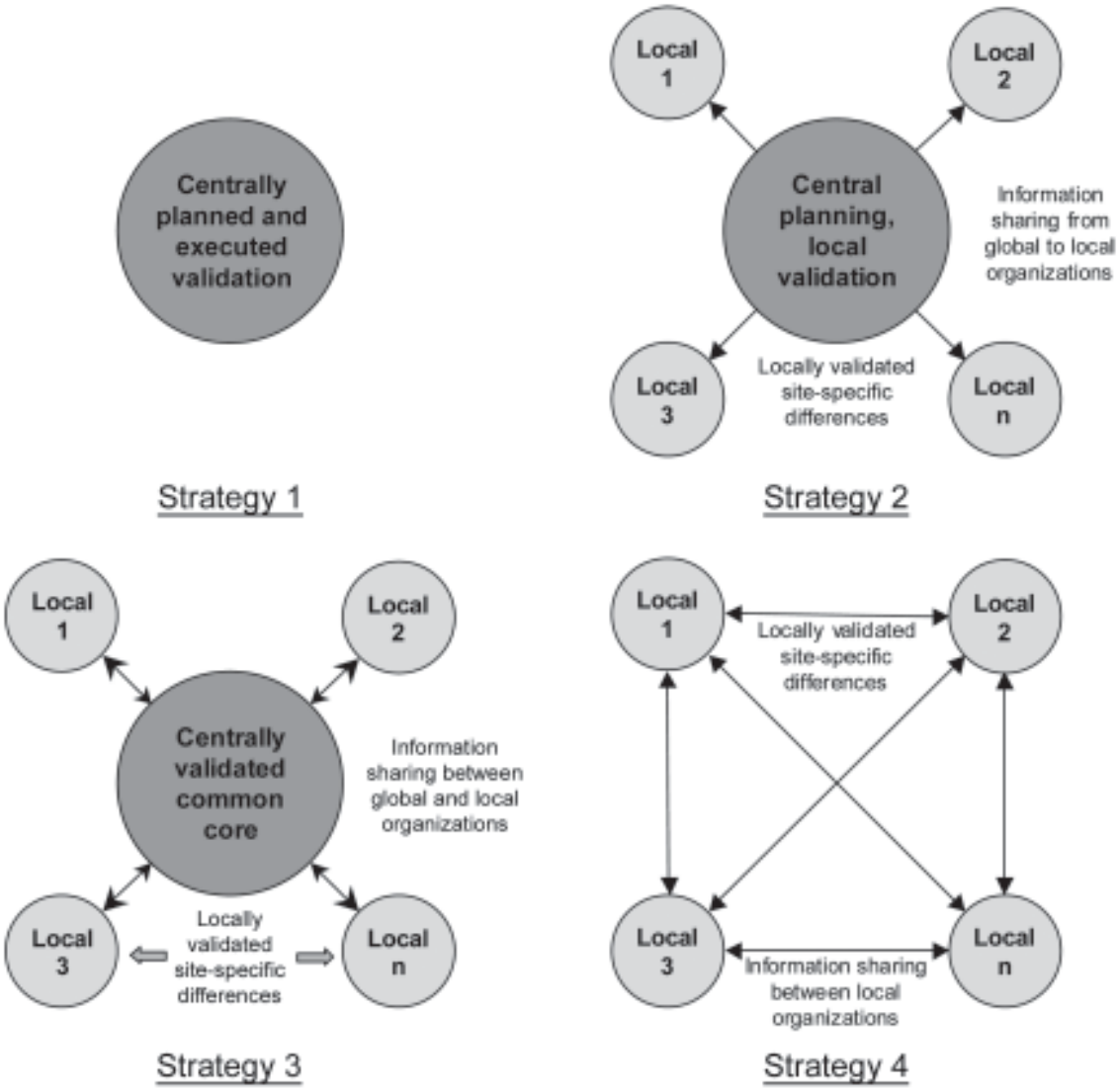
Moving a system from a local to a global profile has a major impact on the actual system design and the technical infrastructure required to support the new design. This, in turn, may lead to changes in the geographic location(s) of the technical infrastructure, support organization, and ultimate system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

Appendix 4
Application Architecture Effects on Validation Strategy

It is vital that a team leader responsible for validation be appointed as a member of the core project team when a project is initiated. The team leader responsible for validation should be aware of and have input to many decisions that will be made as a part of the project initiation and planning phase.

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

Figure A4.1: Application Architecture Strategies



Testing and documentation synergies are especially important, and are discussed in this Appendix. However, before this can be addressed, a fundamental decision regarding the organization of the validation project should be made. Figure A4.1 shows a graphical representation of the four major strategies derived from application architecture.

Strategy 1: Simplest of the strategies, this is a single global, centralized validation effort done on behalf of the entire user community. This works only for applications managed from a single point.

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.

Strategy 3: Perhaps the most common strategy is a common global core element of the application validated centrally with local validation efforts addressing local differences for each deployed instance of the application.

Clearly the most efficient use of this scheme will be to minimize actual functionality differences so that local validation efforts can be concentrated on local application infrastructure (IQ) and business process (PQ). 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.

Occasionally, however, a local site will require some modifications or additions to the core functionality. This will entail a local supplement to some of the other global documentation. It will include a local supplement to the Validation Plan, which is managed similarly to the global Validation Plan, but with local approvals. Some organizations 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 also helps ensure that the 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. Clearly, there will be additional locally approved and executed testing in this scenario as well since OQ testing executed at the global level will inadequately challenge the local differences.

A thorough analysis of traceability of the modified specifications will reveal what OQ tests need to be modified so that redundancy can be avoided.

Finally, there should be a local Validation Report summarizing all local activities.

Table A4.1 provides a checklist for documentation under this strategy.

Strategy 4: A completely local validation approach may be warranted if local instances of the application are configured and managed in substantially different ways.

Table A4.1: Documentation Responsibilities Checklist for Global Systems with Centrally Validated Core Functionality

Activity/ Document	Site	Date	Prepared by	Reviewed by	Approved by	Status
Business Process Model	Global					
User Requirements Documents	Global*					
Functional Specifications	Global*					
Design Specifications	Global*					
Global Validation Plan (core functionality)	Global					
Local Validation Plan (local features)	Local					
Design Qualification (Inc. Gap Analysis)	Global					
Traceability Matrix	Global*					
IQ Protocol templates	Global					
IQ Protocol(s)	Local					
IQ Report(s)	Local					
OQ Protocol Template	Global					
OQ Protocol(s)	Global*					
OQ Report	Global*					
PQ Protocol(s)	Local					
PQ Report	Local					
Validation Report (Locally unique features)	Local					
Validation Report (Global Release)	Global					
Training Materials	Global					
Training Execution	Local					
*May have local addendum if there are unique local differences in functionality						

Application Architecture and Test Strategy

V-model based validation test phases conveniently allow maximum leveraging of test resources for a global system. This is inherent in the nature of the test phases:

- IQ: deals with installation of hardware with a distinct geographic connection, and therefore, generally local.
- OQ: tests internal application function, which can be generally independent of hardware platform, and therefore, global.
- PQ: tests application function in the context of the business process, which can be local or global, and the operating environment, which is local.

Therefore, it should be possible to do a single global test phase for internal application functions (calculations, database functions, data entry, etc.), subjects that are normally covered in OQ. Assuming that there are no local differences in application configuration that would invalidate such testing[1], this strategy is well suited for all architectures.

While remote sites may depend on IQ 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 IQ of the application on its equipment. A CoE or the global team may dispatch help to the local site for installation and IQ.

The ability to achieve testing synergy in PQ is dependent upon both the architecture and the uniformity of business processes. Some PQ, 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 PQ 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 SLA.

Table A4.2 summarizes considerations for test strategy in relation to application architecture. Note that 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 as to local centralized or global testing should be justified in the Validation Plan.

[1] For example, verification of output from a calculation is typically an OQ activity, but if Site A required the output to two significant figures, and Site B requires three, the verification activity should be moved to PQ for the non-standard site.

Table A4.2: Application Architecture Strategies

System Types	Example	Description	Validation Planning	Test Planning	IQ	OQ	PQ	Validation Reporting
Single Central Server Remote Terminal Emulation	Global Drug Safety System	Centralized system resides at one facility, accessed via terminal emulation	Global	Global	Global	Global	Global*	Global
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 is distributed to multiple servers to enhance performance	Global and Local	Global and Local	Local	Global	Local	Global and Local
Client Server *Single Central Server*	LIMS, ERP, Clinical Monitoring System	Centralized system resides at one facility, accessed by workstation clients. Application leverages desktop processing power.	Global	Global	Global (Local Client IQ)	Global	Global*/ Local	Global†
Client Server *Distributed Servers*	LIMS, ERP, Clinical Monitoring System	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
Distributed Servers Access only to Local Server	Standardized MRPII Systems for "Independent" Manufacturing 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
†Local workstation IQ generally independent of validation report
**Local customization would require a local OQ component

Appendix 5
Checklist of Considerations for Global Systems

Checklist of Considerations for Global Systems

Topic	Guidance Reference	GAMP 4 Reference	Considered ✓ (Initial and Date)
PROJECT PLANNING AND MANAGEMENT			
Language			
Legal Standards	2.1.1		
Corporate Standards	2.1.1		
Local Standards	2.1.1		
Documentation Standards	2.1.1		
Communication Standards	2.1.1		
Organization			
Stakeholders	**2.1.2**		
Steering Committee	**2.1.2**		
Project Structure	**2.1.2**		
Project Manager	**2.1.2**		
Project Team	**2.1.2**		
System Ownership	**2.1.2**		
Geographical			
Communication	**2.1.3**		
People and Travel	**2.1.3**		
Documentation	**2.1.3**		
Supplier Availability and Support	**2.1.3**		
Legal			
Work, Health, and Safety Rules	**2.1.4**		
Certification	**2.1.4**		
Contractual Issues/Procurement	**2.1.4**		
Regulatory			
Regulatory Requirement Topics	**2.2**		
Regulatory Commonalities and Conflicts	**2.2**		
Data Management Planning			
Data Management Objectives	**2.3.2**		
Business Models	**2.3.3**		
Policies, Standards, and Guidelines	**2.3.4**		
Underlying Databases and Data Models	**2.3.5**		

Checklist of Considerations for Global Systems (continued)

Topic	Guidance Reference	GAMP 4 Reference	Considered ✓ (Initial and Date)
Responsibilities and Accountabilities	**2.3.4 & 2.3.5**		
System Architecture			
System Design (Centralized versus Distributed)	**2.4.1**		
Helpdesk Design	**2.4.2**		
Disaster Planning/Business Continuity	**2.4.2**		
Environments	**2.4.3**		
Performance and Capacity Planning	**2.4.4**		
Procedural			
Project Change Control	**2.5.1**		
Operational Change Control	**2.5.1**		
Configuration Management Planning	**2.5.2**		
Security Planning	**2.5.3**		
Validation Methodologies	**2.5.4**		
Training	**2.5.5**		
Periodic Review	**2.5.6**		
Funding	**2.6**		
VALIDATION AND IMPLEMENTATION			
System Ownership	**3.1**		
Validation Planning	**3.2**		
User Requirements Specification	**3.3**		
Risk Management	**3.4**		
System Specification and Design Review	**3.5**		
Traceability Management	**3.6**		
Testing			
• Standardization of Documentation	**3.7.1**		
• Automated Test Tools	**3.7.2**		
• Deviation Handling	**3.7.3**		
• Test Script Error Handling	**3.7.4**		
• Handling of Test Failures	**3.7.5**		
• Review of Test Results	**3.7.6**		
• Change Management	**3.7.7**		

Checklist of Considerations for Global Systems (continued)

Topic	Guidance Reference	GAMP 4 Reference	Considered ✓ (Initial and Date)
• Regression Testing	**3.7.8**		
Validation Reporting			
• Core Validation Report	**3.8.1**		
• Local Validation Report	**3.8.2**		
GLOBAL SYSTEM MANAGEMENT			
Change Control	**4.1.1**		
Change Management	**4.1.2**		
Release Management	**4.1.3**		
Closure Process	**4.1.4**		
Change Records	**4.1.5**		
Configuration Management	**4.1.6**		
Issue Management	**4.1.7**		
System Security	**4.2**		
Performance Monitoring	**4.3**		
Backup and Recovery of Software and Data	**4.4**		
Record Retention, Archive, and Retrieval	**4.5**		
Business Continuity and Disaster Recovery	**4.6**		
Periodic Review	**4.7**		
Data Quality	**4.8.1**		
Data Availability	**4.8.1**		
Data Accessibility	**4.8.1**		
Data Consistency	**4.8.1**		
Data Management Life Cycle	**4.8.2**		
Data Migration	**4.8.2**		
Database Replication	**4.8.2**		
Data Access Management	**4.8.3**		

Appendix 6
Glossary

Glossary

1 Definitions

Archive

The process by which electronic data and document stores are regularly copied and retained for long-term retention of the data. Archived data is generally removed from the on-line database.

Back-up

The process by which electronic data and document stores are regularly copied and retained for the purpose of restoration following a problem. Back-up copies are generally retained for a short term.

Bespoke System (GAMP® 4)

A system produced for a customer, specifically to order, to meet a defined set of user requirements. Also called Custom Built System.

Centre of Excellence (CoE)

An organization with specific expertise in a computer system that acts as a resource for evaluating technical issues associated with problems, changes, upgrades, etc. in support of the global community. The CoE may play a strong role in supporting validation.

Centralized System

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

Change Advisory Board (CAB) (ITIL)

A group of people who can give expert advice to change management on the implementation of changes. This board is likely to be made up of representatives from all areas within IT and representatives from business units.

Change Advisory Board Emergency Committee (CAB-EC) (ITIL)

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

Change Manager

Change manager is an ITIL role. This person is responsible for the change control process. The change manager may be empowered to authorize minor changes without CAB approval. The change manager often chairs the CAB.

Client Server

An application architecture that takes advantage of local processing power of client PCs. Data storage is centralized or distributed among one or more server, while some or all processing occurs on the user's PC.

Configuration Item (CI) (ITIL)

A component of a system – or a document, such as a request for change, associated with an infrastructure – which is (or is to be) under the control of configuration management. CIs may vary widely in complexity, size, and type – from an entire system (including all hardware, software, and documentation) to a single module or a minor hardware component.

Configuration Management (ITIL)

The process of identifying and defining the configuration items in a system, recording and reporting the status of configuration items and requests for change, and verifying the completeness and correctness of configuration items.

Configuration Management Database (CMDB) (ITIL)

A database, which contains all relevant details of each *CI* and details of the important relationships between *CIs*.

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.

Critical

The use of 'critical' within this Guide means that the items have the identified potential to impact public health in a significant way, e.g., affecting product quality or drug safety data. There may be other items, not associated with public safety, that have a significant impact on, for example, economy, environment, or operations, and these may need to be identified as 'business critical' items.

Data (IEEE)

1. Representations of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means.

2. Sometimes used as a synonym for documentation.

Data Element (ISO)

1. A named unit of data that, in some contexts, is considered indivisible and in other contexts may consist of data items.

2. A named identifier of each of the entities and their attributes that are represented in a database.

Distributed System

A system architecture wherein database and/or processing occur on multiple servers. This is usually based on geographic considerations, but also may be load-driven.

Global Information System

A computerized system deployed at more than one location that is managed centrally. The degree of centralized control can vary to a great extent.

Global System Owner

The individual with final accountability for the performance and compliance of the overall global system. Responsibility for executing the associated activities is normally delegated.

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.

Information Technology Infrastructure Library (ITIL®)

A globally recognized methodology for IT service management. ITIL processes include solutions for several important system management processes.

Lightweight Directory Access Protocol (LDAP)

The LDAP protocol (directory service) is a TCP/IP-based directory access protocol. It is considered the standard solution for directory services in Internet-based networks. LDAP has a universal format, which supports display of all names.

Local System Owner

The individual with accountability for the performance and compliance of the local implementation of the system. Responsibility for executing the associated activities is often delegated.

Metadata

Metadata is simply data used to describe other data. It can be used to describe information such as file type, format, author, user rights, etc. and is usually attached to files, but invisible to the user.

Pharmaceutical Inspection Convention/Cooperation Scheme (PIC/S)

The Pharmaceutical Inspection Convention and Pharmaceutical Inspection Cooperation Scheme (jointly referred to as PIC/S) are two international instruments between countries and pharmaceutical inspection authorities, which provide together an active and constructive cooperation in the field of GMP.

Record (IEEE)

A set of related data items treated as a unit, e.g., in stock control, the data for each invoice could constitute one record.

Recovery

Loading of backed-up data onto a computer system to recover from a problem.

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.

Retrieval

Loading of archived data onto a computer system for business purposes requiring access to the old data.

Traceability

The ability to link a user requirement specification through functional specifications and design specifications to test cases. It should be possible to look at a specification and determine how it was tested, or to look at a test and determine what specifications it challenges.

2 Acronyms and Abbreviations

CAB Change Advisory Board

CAB-EC Change Advisory Board Emergency Committee

CI Configuration Item

CoE	Centre of Excellence
CMDB	Configuration Management Database
CSV	Computer System Validation
Dev	Development
DS	Design Specification
DBMS	Database Management System
ERP	Enterprise Resource Planning
FS	Functional Specification
GAMP	Good Automated Manufacturing Practice
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GxP	*Covers* GCP, GDP, GLP, and GMP
GIS	Global Information System(s)
GPG	Good Practice Guidance
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
ITIL®	Information Technology Infrastructure Library
IQ	Installation Qualification
ISPE	International Society for Pharmaceutical Engineering
LDAP	Lightweight Directory Access Protocol
Mgt	Management
OQ	Operational Qualification
Op	Operations

PIC/S	Pharmaceutical Inspection Convention/Cooperation Scheme
PQ	Performance Qualification
QA	Quality Assurance
R&D	Research and Development
SDLC	System Development Life-Cycle
SDS	Software Design Specification
SOP	Standard Operating Procedure
TM	Traceability Matrix
URS	User Requirement Specification

Appendix 7
References

References

1. *GAMP® 4, GAMP Guide for Validation of Automated Systems*, ISPE (Publishers), 2001.

2. PIC/S Guidance on Good Practices for Computerised Systems in Regulated "GxP" Environments (PI011-2) (available at www.picscheme.org).

3. ISO 14971:2000 Medical Devices – Application of Risk Management to Medical Devices. The Official Web site for the ISO may be visited at http://www.iso.org.

4. ISO 10007:2003 Quality Management Systems – Guideline for Configuration Management. The Official Web site for the ISO may be visited at http://www.iso.org.

5. ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management. The Official Web site for the ISO may be visited at http://www.iso.org.

6. ISO 9000:2000 Quality Management Systems – Fundamentals and Vocabulary. The Official Web site for the ISO may be visited at http://www.iso.org.

7. IEEE Std. 610.12-1990 Standard Glossary of Software Engineering Terminology

8. OGC (ITIL) Information Technology Infrastructure Library (ITIL), Service Support Service Support (CCTA) (IT Infrastructure Library) The Stationery Office Books.

9. FDA Glossary of Computerized System and Software Development Terminology.

10. ISPE Baseline® Pharmaceutical Engineering Guides for New and Renovated Facilities, Volume 5, Commissioning and Qualification, March 2001.

11. *GAMP® Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures*, ISPE (Publishers), 2005.

12. *GAMP® Good Practice Guide: Validation of Laboratory Computerized Systems*, ISPE (Publishers), 2005.

13. *GAMP® Good Practice Guide: IT Infrastructure Control and Compliance*, ISPE (Publishers), 2005.

ENGINEERING
PHARMACEUTICAL
INNOVATION

ISPE Headquarters
3109 W. Dr. Martin Luther King Jr. Blvd., Suite 250
Tampa, Florida 33607 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

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

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

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

www.ISPE.org