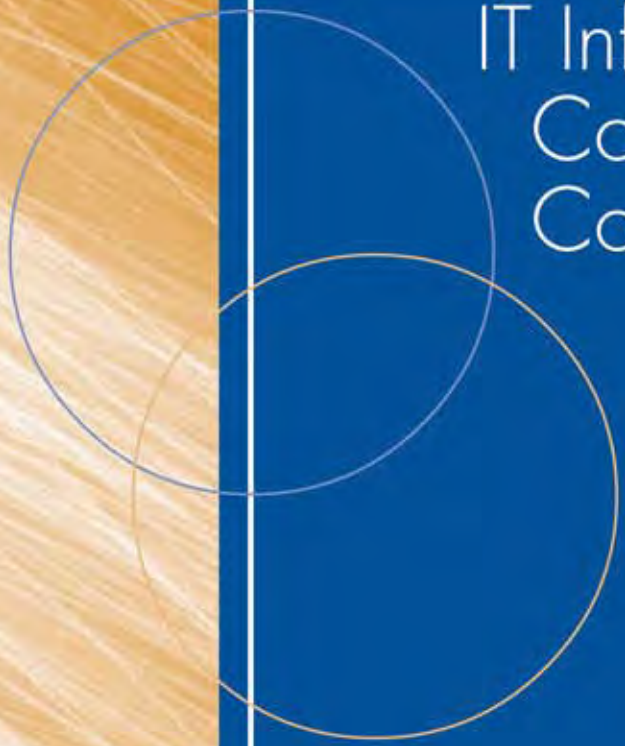
GAMP Good Practice Guide:

IT Infrastructure Control and Compliance



ISPE

ENGINEERING
PHARMACEUTICAL
INNOVATION

Preface to the GAMP Good Practice Guide: IT Infrastructure Control and Compliance

This document, the GAMP® Good Practice Guide: IT Infrastructure Control and Compliance, is intended as a supplement to the Guide for Validation of Automated Systems (GAMP® 4). It provides an approach to meeting current regulatory expectations for compliant IT Infrastructure platforms, including the need to identify, qualify, and control those aspects impacted by GxP.

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 IT Infrastructure platforms. The GAMP Forum cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability:
In no event shall ISPE or any of its affiliates (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 1-931879-85-0

Acknowledgements

The production of the GAMP® Good Practice Guide: IT Infrastructure Control and Compliance was initiated by the GAMP® Europe Steering Committee and governed by a Special Interest Group chaired by Niels Holger Hansen and Hasse Greiner of Novo Nordisk. The IT Infrastructure Special Interest Group was sponsored by Chris Clark of NAPP Pharmaceuticals Ltd.

The following Special Interest Group members provided the bulk of material, comments, and reviews:

Finn Andersen	NNIT A/S
Nandakishore Banerjee	Isardata
Wayne Barraclough	Parexel
Heinrich Berlejung	Propack Data GmbH
Martin Bigum	NNIT A/S
Mark Cadman	Parexel
Mark Cherry	AstraZeneca
Tony de Claire	Mi Services Group
Chris Clark	NAPP Pharmaceuticals Ltd
Evjatar Cohen	Rusco Services
Christine Cooke	Pfizer
Margaret Gold	AstraZeneca
Hasse Greiner	Novo Nordisk
Jerry Hare	GlaxoSmithKline
Lars Herhold	Parexel
Michael von Jessen	NNIT A/S
Hani Kamel	Novo Nordisk
Jeroen Knaepen	CTG
Arne Kristensen	NNIT A/S
Orlando Lopez	Cordis (a Johnson & Johnson company)
Bob McDowall	McDowall Consulting
Ole Hald Møller	Novo Nordisk
Claude Muller	Novartis Pharma AG
Morten Palm	NNIT A/S
Steve Papworth	Eli Lilly Company Limited
Arthur (Randy) Perez	Novartis
Yves Samson	Kereon AG
Juergen Schmitz	Novartis
Jens Seest	Novo Nordisk
Poul Skallerup	Novo Nordisk
Allan Søberg	Novo Nordisk
David Stephenson	ABB
David Stokes	Mi Services Group
Rocco Timpano	Pfizer
Anders Vidstrup	Novo Nordisk
Michael Wyrick	Washington Group International

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

Special thanks are given to those individuals and organizations who hosted face-to-face meetings and workshops.

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

The GAMP® Council would like to give special thanks to Hasse Greiner for countless hours of work during the development this Guide.

The GAMP® Council would like to thank the following regulator for his review:

Robert D. Tollefsen, FDA (US)

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

GxP regulated companies have an ever increasing dependency on computerized systems when conducting their day-to-day businesses.

The validated status of GxP applications that are dependent upon an underlying IT Infrastructure[1] is compromised if that IT Infrastructure is not maintained in a demonstrable state of control and regulatory compliance.

The consequences of the IT Infrastructure being out of effective control can be significant. Depending on the nature of a failure, an entire site or geographic region of operations could be brought to a standstill while the problem is resolved.

The infrastructure should be brought into initial conformance with the company's established standards through a planned qualification process building upon acknowledged good IT practices. Once in conformance, this state should be maintained by documented standard processes and quality assurance activities, the effectiveness of which should be periodically verified.

Key aspects to consider include:

- installation and operational qualification of infrastructure components
- configuration management and change control of infrastructure components and settings in a highly dynamic environment
- management of risks to IT Infrastructure
- involvement of service providers in critical infrastructure processes
- security management in relation to access controls, availability of services and data integrity
- backup, restore, and disaster recovery
- archiving

This document has been developed by GAMP® Forum, a technical subcommittee of ISPE. It supplements the existing *GAMP® 4*, GAMP® Guide for Validation of Automated Systems.

GAMP® guidance aims to achieve validated and compliant automated systems meeting all current GxP regulatory expectations, by building upon existing industry good practice in an efficient and effective manner.

[1] Throughout the document 'IT Infrastructure' and 'infrastructure' are used synonymously to indicate an aggregation of platforms and services including their associated processes, procedures, and personnel.

1.2 Purpose

This Guide provides comprehensive guidance on meeting current regulatory expectations for compliant IT Infrastructure platforms, including the need to identify, qualify, and control those aspects impacted by GxP.

This Guide intends to satisfy the growing need for guidance on key IT Infrastructure subjects in relation to current international GxP regulations, and to align terminology and language with other GAMP® Good Practice Guides.

The Guide is intended primarily for regulated life science industries, including pharmaceutical, biological, and medical devices, but also provides valuable information for suppliers of systems, products, or services.

This Guide includes the description of a scaleable qualification framework which has been derived from key principles and practices. It describes how this framework can be applied to different platform types in order to determine the extent and scope of qualification efforts.

In addition, this Guide provides an overview of current best practices for the design, qualification, and operation of an IT Infrastructure with emphasis on the qualification requirements of the major components.

1.3 Scope

This Guide addresses compliance with international GxP regulations and considers:

- the establishment of new platforms and extensions to existing ones
- existing platforms already in support of GxP applications

Current GxP requirements related to IT Infrastructure platforms 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 specifically have been considered in producing this document:

- US Federal Food and Drug Administration (FDA) regulations and Compliance Policy Guides
- relevant parts of EU GMPs, e.g., Annexes 11, 15, and 18
- PIC/S Guidance

This Guide covers a range of IT Infrastructures, from those found in companies operating globally to isolated or semi-isolated GxP regulated infrastructures.

This Guide also may prove useful to managers of IT Infrastructures which are not regulated by GxP.

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.

Business Continuity Planning should be led by the business users and application (system/data) owners. It is outside the scope of this Guide. This Guide considers IT Infrastructure disaster recovery and contingency planning, but not the need for alternative operating procedures pertaining to the business processes in case of failure. When performing Business Continuity Planning, companies should ensure that the impact of the IT Infrastructure is assessed and that any resulting requirements are met by those responsible for the infrastructure.

1.4 Benefits

This Guide applies a structured approach, including Risk Management, to the qualification, management, and control of IT Infrastructure platforms supporting GxP applications.

A vertical, or system based, approach to qualification and audit of IT Infrastructure would be inefficient and impractical, as overlapping and often identical platform elements would be dealt with repeatedly. To avoid unnecessary effort, this Guide describes a horizontal, or platform based, approach.

Benefits of a horizontal approach include:

- higher level of standardization throughout the entire life cycle
- minimal overlap in documentation
- minimal overlap in qualification
- minimal overlap in audits, inspections, and assessments

The approach described in this Guide also seeks to build upon:

- The relatively low residual risk to GxP applications and records attributable to the IT Infrastructure platforms. This is in contrast to application software which is usually designed to create and manipulate data, whereas platforms are usually designed to ensure a high degree of integrity of the data supported.
- Industry standard components are widely used which typically include error detection and self-correction features, leading to relatively high probability of detection and low likelihood of failure (see Appendix 13, reference 15).
- the current good IT practices and international standards typically applied to ensure reliable network performance
- the availability of efficient, automatic, and standardized IT Infrastructure monitoring and management software tools
- the many similar platform components used in similar configurations across a company

1.5 Objectives

IT Infrastructure Control and Compliance should target those IT related aspects that could potentially affect product quality and public health. In order to be effective, however, applicable methods also must be practical and efficient. To this end, the GAMP® Council set out the following guiding principles for the development of this Guide:

- Provide a consistent, standalone document that would guide stakeholders to take advantage of current best practices in the field to achieve compliance with applicable regulations.

- Define *infrastructure* and other key terms and concepts referenced or introduced.
- Provide guidance on best practice for network, client, and server qualification and management.
- Provide guidance on security issues in the light of BS7799/ISO17799 (see Appendix 13, reference 6).
- Address change control in light of virus signature updates and security patches.

The IT Infrastructure SIG believes the targets have been addressed by this Guide.

1.6 Structure of this Guide

This Guide consists of a main body and a set of supporting appendices.

The main body contains a framework for achieving IT Infrastructure Control and Compliance. Following the introductory and background material, the main body covers:

- IT Infrastructure elements
- using a Quality Management System
- applying Risk Management
- qualification of new platforms
- maintaining the qualified state during operation
- retirement of platforms
- qualification of legacy platforms

The supporting appendices contain guidance and examples of current good practices to implement the framework, including:

- Roles and Responsibilities
- Risk Assessment
- Qualification Deliverables
- Standard Operating Procedures (SOPs)
- Periodic Reviews
- Infrastructure Security
- Upgrade and Patch Management
- Outsourcing
- Server Management

- Client Management
- Network Management

1.7 Key Concepts

1.7.1 Horizontal Platform Based Approach to IT Infrastructure

The IT Infrastructure exists to support the primary business, by providing:

- platforms to run the business applications[2] (e.g., CDMS, IVRS, LIMS, or ERP)
- IT Infrastructure processes that facilitate a capable and controlled IT environment
- general IT services (e.g., email system, office tools, intranet facilities, file storage)

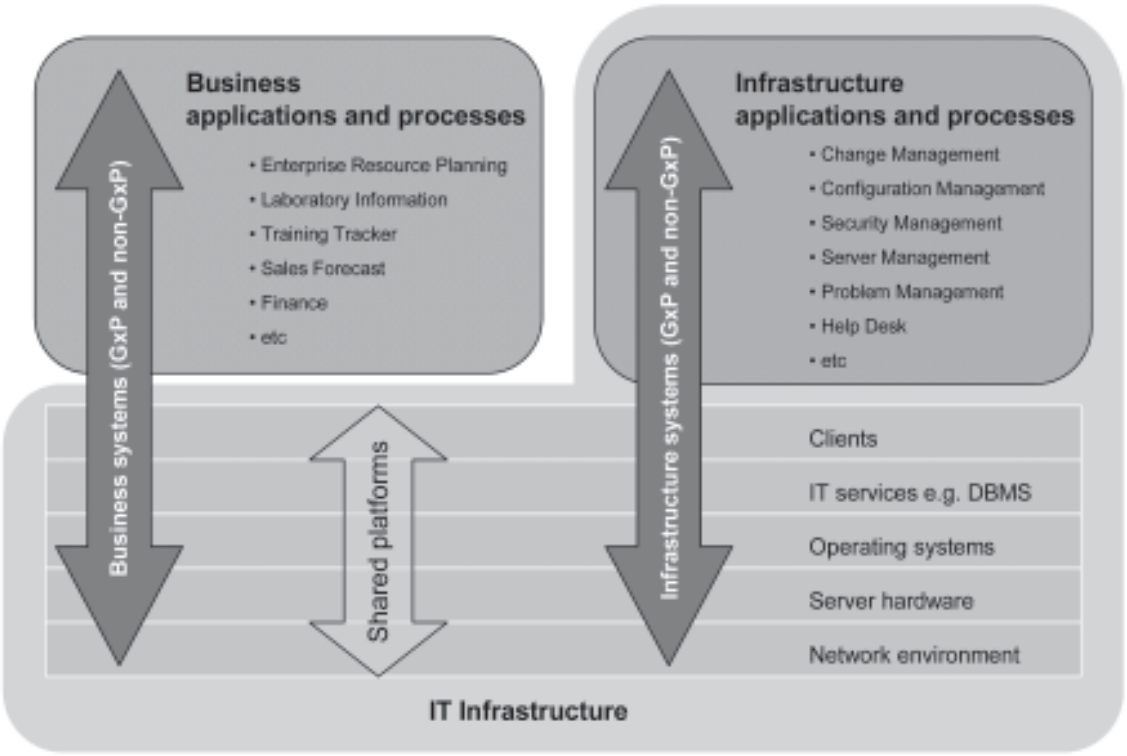
IT Infrastructure applications may share services and platforms with business applications, e.g., user accounting, Configuration Management, centralized data backup. IT Infrastructure applications that support IT Infrastructure processes could be considered part of the IT Infrastructure, and are usually owned and administered by the same group that is responsible for other IT Infrastructure elements. This is in contrast to business applications that would be the responsibility of the relevant business unit.

Figure 1.1 shows how the IT Infrastructure elements link together to form an integrated environment for running and supporting applications and services. Figure 1.1 illustrates that computerized systems[3] consist of the applications in question and all the parts of the platforms required making the systems function as required. Parts of the platforms, e.g., the network and clients, could be shared by multiple systems.

[2] 'Business application' is used in this context to distinguish between infrastructure applications and business applications employed to support the company's primary businesses.

[3] 'Computerized systems' and 'systems' are terms used interchangeably in this Guide.

Figure 1.1: Applications, Infrastructure Processes, and Platforms



Where platform components support multiple applications, these components should be qualified separately from the applications to avoid unnecessary duplication of activities and effort. Separate qualification of the IT Infrastructure means that adding or changing a business application would require only the validation of the application. Similarly, changing components in the IT Infrastructure may not require further validation of the business application; however, the risk to GxP applications of each controlled change should be assessed.

This is referred to as the horizontal, platform based approach.

If standard platform components, such as standard server and client configurations, are adequately managed, the initial qualification of the platform component becomes a standard qualification package which permits efficient and cost-effective duplication of the platform component. The standard, re-usable, qualified platform components are referred to as *building blocks* throughout this Guide.

1.7.2 Key Terminology

The following key terms are used in this document:

Requirements

Requirements for infrastructure platforms and services are often specified in documents such as Service Level Agreements (SLAs) and described in broad terms that allow the platform management groups to keep up with the pace at which platform technology and requests for transmission bandwidth and computing power develops. This is especially the case for larger infrastructures mainly supporting administrative type applications, where platforms are qualified and made available at or before the time when new or updated applications need them. For infrastructures primarily supporting real-time applications, such as process control, the requirement specifications may be more specific.

Commissioning

Commissioning is a term used for a well planned, documented, and managed engineering approach to the start-up and handover of facilities, systems, and equipment to the end-user, that results in a safe and functional environment that meets established design requirements and stakeholder expectations.

In the context of IT Infrastructures, this concept may be useful for aspects of IT Infrastructure which do not support GxP activities directly.

Qualification

Qualification is a process of demonstrating the ability of an entity to fulfill specified requirements. In the context of an IT Infrastructure, this means demonstrating the ability of components such as servers, clients, and peripherals to fulfill the specified requirements for the various platforms regardless of whether they are specific or of a generic nature.

The qualification strategy should follow the Quality Management System (QMS) as described in Section 3 of this Guide. The qualification scope and depth should be determined by a Risk Assessment as described in Section 4 of this Guide and planned as described in Section 5 of this Guide.

Formalization of prior commissioning activities may assist the process of qualification by producing some of the required documentation and avoiding repeat testing.

Basic requirements of qualification include:

- QA involvement at the appropriate level
- formally verified and approved design solutions that meet specified requirements
- test results compliant with GxP requirements for documentation
- tests and verifications aimed at establishing conformance to specifications
- provisions to ensure that the qualified status of the entity is maintained
- traceability of actions and activities

Validation

In the context of an IT Infrastructure, validation applies to those GxP applications that run on the IT Infrastructure rather than the IT Infrastructure platforms themselves, where the focus should be on qualification of components.

Some companies may decide to use the term ‘validation’ to emphasize the critical importance of some infrastructure applications that are pivotal to successful application validation (e.g., password management and authentication of electronic signatures). Where this occurs, the substantive compliance activities should be the same as those presented in this guidance.

2 IT Infrastructure Elements

On-going quality management of the IT Infrastructure includes assurance that all processes and procedures are in place to control the life cycle activities of the IT Infrastructure platforms, and that qualified personnel are available to complete assigned tasks.

Aside from infrastructure services, the IT Infrastructure may be looked upon as consisting of three major elements of fundamentally different nature, namely:

- Platforms
- Processes
- Personnel

The three listed elements support applications directly and are covered in the following sections.

2.1 Platforms

Platforms provide a well defined foundation for other well defined hardware or software components.

Table 2.1 provides guidance on how to assign GAMP® categories to individual platform components that require qualification, which enables an appropriate qualification strategy to be developed. *GAMP® 4*, Appendix M4 (see Appendix 13, reference 1), defines the GAMP® categories and provides an appropriate approach to follow for each category.

Table 2.1: Platform Components and GAMP® Categories

Platform Components	Generic Qualification Strategy
Networks	Networks consist of passive and active components. Passive type network components include cables, connectors, outlets, and conduits. Active network components include switches, hubs, repeaters, bridges, routers, domain servers, wireless hotspots, and firewalls. Except for customized cables which would be GAMP® HW category 2, most network building blocks are GAMP® HW category 1, and SW categories 1 or 2. Note 1: while such standardized components are not considered to be computerized systems, critical configuration information should be recorded and managed. Note 2: A network that is not controlled by the company, such as the Internet, inherently provides a system which adds to the challenge of meeting regulatory and company requirements for security, availability, integrity, confidentiality, etc.

Table 2.1: Platform Components and GAMP® Categories (continued)

Platform Components	**Generic Qualification Strategy**
Hardware and Peripherals	Includes all computer equipment, including power supplies, boards, network interface cards, disk storage arrays, printers and other peripherals, etc., needed to execute programs in direct support of applications, and for providing basic IT Infrastructure services. Hardware and peripherals used in the IT Infrastructure are typically GAMP® HW category 1.
Firmware	Firmware is often considered an indivisible part of the hardware component. However, in those instances where firmware is updated independently, it should be managed as software in its own right, and typically, would be GAMP® SW category 2.
Operating Systems	Includes operating systems and communication protocol implementations. Device drivers are usually designed and maintained by hardware suppliers to allow operating variants to effectively interact with their hardware products. Most operating systems and drivers are GAMP® SW category 1. Note 1: Configuration of operating systems should be documented. Note 2: Specific operating system features which are important to a GxP application may be validated as part of the application, e.g., the use of operating system user access and privilege functionality where the application software has no such built-in functionality.
Data Management Software	Includes file storage software, database management systems, web-services, interface, and communications software, etc. Elements of Data Management Software often support more than one application. Most Data Management Software is GAMP® SW category 1, because they are part of the operating system environment, and typically, are standardized. Some may be other GAMP® SW categories depending on complexity and configurability.
Servers	Server building blocks or individually configured servers are usually built of standardized components and configured in accordance with specifications. The actual set-up should dictate the chosen qualification strategy. Therefore, most server building blocks are a combination of GAMP® HW category 1, and SW categories 1 or 2.
Clients	Client building blocks or individually configured clients, range from 'thin' to 'thick' clients which may process and store data locally. The actual set-up should dictate the chosen qualification life cycle model. Therefore, most client building blocks are a combination of GAMP® HW category 1, and SW categories 1 or 2.
Applications	Applications implement processes and may consist of everything from an 'off-the-shelf,' standardized software package configured with user defined parameters to a set of programs and parameters designed to meet unique user requirements. Applications are GAMP® SW categories 3, 4, or 5. The validation of applications is outside the scope of this Guide.

Companies should determine which categories apply to platform components. Approaches to making such determinations are described in *GAMP® 4*, Appendix M4 (see Appendix 13, reference 1).

2.2 Processes

The number of IT Infrastructure processes a company decides to implement and the method of implementation depend mainly on the criticality of the business processes being supported and on the size of the company.

The processes listed cover typical aspects that are required for good business practice, as well as compliance. This list, which takes into account ITIL (see Appendix 13, reference 13) is indicative only, and organizations may view different processes as being sub-processes to other processes.

- Change Management
- Configuration Management
- Security Management
- Server Management
- Client Management
- Network Management
- Problem Management
- Help Desk (also known as Service Desk in ITIL)
- Backup, Restore, and Archiving
- Disaster Recovery
- Performance Monitoring
- Supplier Management

Key processes are considered further in Section 6 of this Guide.

2.3 Personnel

Management should define roles and responsibilities (job descriptions) in terms of tasks to be undertaken, and the qualifications and experience needed. Individual job descriptions should be assigned to named individuals fulfilling those roles, permanently or on an ad-hoc basis.

Key roles that may be identified include:

- Executive Management (Project Sponsorship)
- Project Manager

- application (system/data) owner[4]/administrator/application oriented SMEs
- data owners if not coinciding with application (system) owner
- IT Infrastructure process owner/administrators/SMEs, e.g., IT support engineers
- platform owner/administrator/SMEs, e.g., network engineers
- independent QA in relation to information technology
- IT Quality and Compliance

Technical and managerial staff with appropriate educational background and experience should be available. Provision of training should be planned to ensure the required skills are developed and maintained. Staff should be made aware of any regulatory requirements that apply to their duties, trained in those procedures that are applicable to them, and re-trained as changes occur. Records of training should be maintained.

Appendix 1 of this Guide provides more detailed guidance on the various roles.

3 Quality Management System

This section describes how a Quality Management System (QMS) may assist in providing evidence that the IT Infrastructure is in a controlled state, and the key requirements for the QMS to attain this goal.

3.1 Quality Manual

A Quality Manual should set quality objectives in line with corporate Quality Policy. A top level document relating to IT Infrastructure should cover:

- identification of key IT Infrastructure processes (especially those that pertain to IT Infrastructure qualification and operational management), and how they interact
- procedures, detailed work instructions, templates, and other standards that apply
- required records and documentation to be maintained

This information can either be included in the Quality Manual or as a separate document. Quality Manuals and top level documents should be approved by QA. For further information, see ISO 9000:2000 Quality Management Systems – Fundamentals and Vocabulary (see Appendix 13, reference 7).

[4] Sometimes referred to as ‘application owner’

3.2 Roles and Responsibilities

Roles and responsibilities should be defined for all important functions. Job descriptions or other documents should reflect the assignment of roles and responsibilities.

3.3 Record Management

Appropriate controls need to be in place to ensure the retrievability, storage, and protection of records. The controls should provide evidence of quality levels of the IT platform, and compliance with regulations.

For further information on document management see *GAMP® 4*, Appendix M10 (see Appendix 13, reference 1).

3.4 Documentation

Documentation for platforms, processes, test results, etc., should be maintained in order to meet requirements for inspections by regulatory authorities.

IT staff should ensure that documentation is readily available and this should be challenged during internal assessments and QA audits. Tools and utility systems should be available during regulatory inspections to provide displays and printouts, as required.

There should be a consistent approach to documentation across an organization. Systems and processes for the creation, review, and approval of documents should be established and maintained (e.g., by use of standard templates and forms, electronic document management systems).

3.5 Testing

Test documentation generated as a result of the execution of test specifications during qualification should meet the following general requirements:

- traceable to the specification that required the documentation
- reviewed and approved by required units or individuals, usually including QA
- clear and objectively verifiable acceptance criteria
- each test step or test case traceable to the pertinent section in the applicable requirement or design specifications
- accurate records of observations made by identifiable and trained personnel
- Entries should reflect the actual observation and not just pass or fail, except when the criteria for pass and fail are made absolutely clear by the specification.
- Hardcopies of screen dumps, or the collation of such information by a computerized tool, should be added to support test results, where appropriate.
- Entries should be made in legible, permanent handwriting, or using a suitable computerized tool.

- Corrections should be made without obscuring the original entry. The date, reason, and identity of the person making the correction should be clear, or by using a computerized tool that supports adequate automatic audit trailing.

The rigor with which the above requirements are met will depend upon the impact and risks associated with the component being tested.

Computerized reporting tools may used for reporting system configuration and installation.

It may be appropriate to use standard checklists or test specifications during testing, e.g., when checking the installation of platform building blocks.

3.6 Standard Operating Procedures

Standard Operating Procedures (SOPs) should be prepared and should describe critical processes and services. SOPs should be reviewed to ensure that they comply with any user specified requirements, established company IT policies, practices and regulations, and supplier specifications.

Procedures should specify the records that need to be generated to provide information for maintenance and troubleshooting, as well as auditable evidence that adequate controls are in place and followed.

Appendix 4 of this Guide suggests a list of SOPs that may be considered as part of an IT Quality Management System.

3.7 Training

Training should be planned and documented, as described in Section 2.3 of this Guide. Formal structured training programs, either in-house or external, should be considered. Technical and regulatory training requirements for external service providers and contractors also should be determined.

3.8 Periodic Review and Evaluation

Subject matter experts, or members of IT Quality and Compliance, should review processes, systems, or platforms to ensure that they meet specified requirements. In addition, the review provides an opportunity to monitor the effectiveness of the QMS and to consider improvements.

The scope, depth, and frequency of assessments should be based on impact and risk. Operational history and known problems should be taken into account. A sampling technique typically is used when planning the assessments.

Periodic Reviews are an important element of maintaining the qualification status of the IT Infrastructure throughout its operational life, and may be undertaken as a scheduled or event driven exercise, e.g., following a major upgrade to hardware or platform software.

Specific areas that could be included in Periodic Reviews of IT Infrastructure are described in Appendix 5 of this Guide.

Documented Periodic Reviews of IT Infrastructure components may be referenced from Periodic Reviews of GxP applications.

For further information on Periodic Reviews, see *GAMP® 4*, Appendix O1 (see Appendix 13, reference 1).

3.9 Audit by QA

Audits should be conducted by QA staff that are independent of the group being audited. Such audits help to assure that processes and procedures meet the specified quality and compliance requirements.

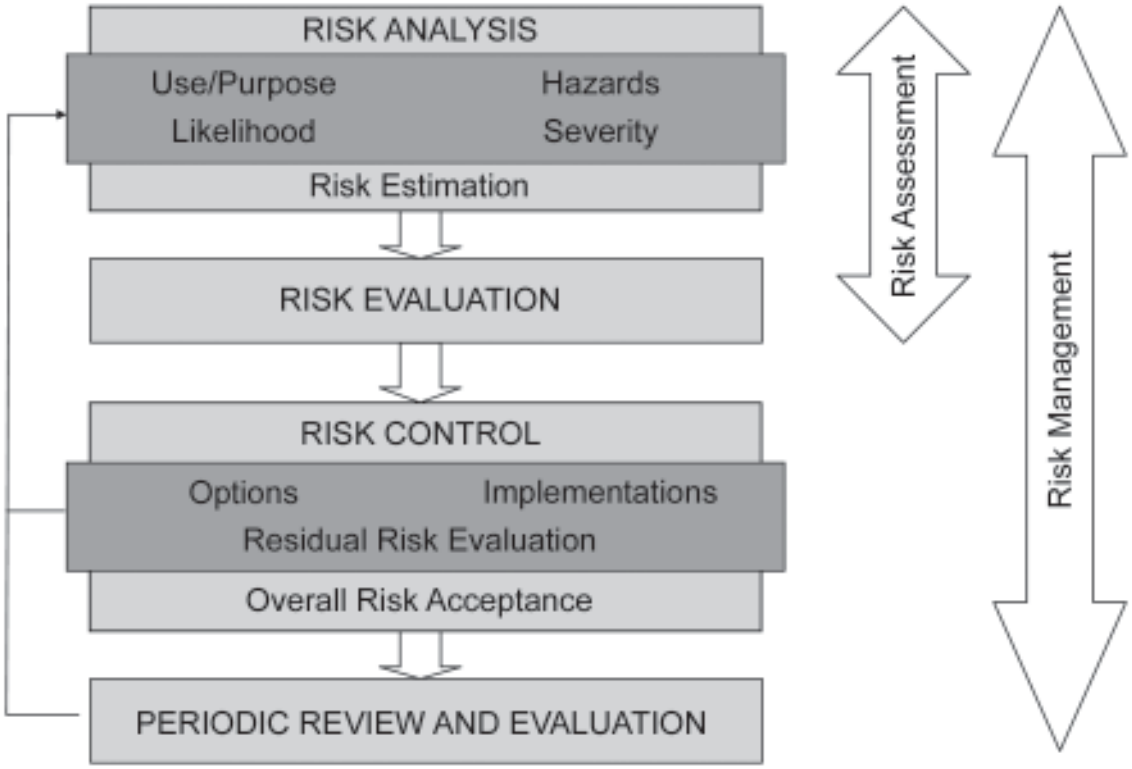
A company may contract external consultants or draw on internal, independent experts to assist the audit.

The scope, frequency, and objective of audits should be determined by QA.

4 Applying Risk Management

Risk Management is defined by ISO as the systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, and controlling risk. Figure 4.1 shows the major phases of the Risk Management Process.

Figure 4.1: Risk Management Process Overview (ISO)[5]



[5] Figure 4.1 is based on a figure that appears in ISO 14971 and appears here with the kind permission of the Danish Standardization Organization.

Risk Assessments should be performed for each major life cycle phase of an object or groups of objects (e.g., platforms, data) identified as important to a company's business. For example, companies need to determine which aspects of the IT Infrastructure to qualify and the required extent of that qualification. Risk Management provides a method for identifying those aspects in a controlled way. This involves a number of key activities:

1. Identify the IT Infrastructure components that may require qualification, based on an analysis of the applications and processes supported by the IT Infrastructure, and the applicable regulations.

2. Assess these IT Infrastructure components based upon the identified hazards and vulnerabilities and assessed impact on critical aspects, recognizing that in many cases the risk will be relatively low (see Section 4.4 of this Guide). This step involves analyzing and evaluating risks to decide if controls are required to manage those risks.

3. Implement controls commensurate with the risks identified for the IT Infrastructure components. These controls should be documented and justified with reference to the identified risks.

4. Assess proposed changes to qualified components.

5. Monitor effectiveness of controls by Periodic Review.

Companies also may decide to apply this Risk Management approach to IT Infrastructure components which do not support GxP applications, but which are business critical.

Where external companies are employed, e.g., Contract Research Organizations, it is important that the regulated company communicates Risk Management requirements.

For further information on Risk Management, see Appendix 2 of this Guide and:

- *GAMP® 4*, Appendix M3 (see Appendix 13, reference 1)

- FDA, Pharmaceutical cGMPs for the 21st Century: A Risk-Based Approach

- ISO 14971:2000 Medical Devices – Application of Risk Management to Medical Devices (see Appendix 13, reference 10)

- NIST Special Publication 800-30 – Risk Management for Information Technology Systems (see Appendix 13, reference 12)

4.1 Identification and Assessment of Components

Application/data owners and QA should define which platform components (or types of component) and tools require qualification. For IT Infrastructure components, the criticality of the GxP applications they support, along with impact on integrity and availability of data should be considered (for further information on security requirements, see Appendix 6 of this Guide).

Platform management groups may assign the same level of criticality to all components and data unless system/data owners specify different levels of criticality. Infrastructure staff should not be expected to assess GxP compliance independently.

Non-GxP applications operating on the IT Infrastructure may affect GxP applications; these should be identified within the Risk Assessment process, and suitable controls included.

Additionally, results of Risk Assessments carried out in other areas of the business may influence IT Infrastructure assessments. Key areas include safety and environment, financial record keeping, business drivers, or considerations of corporate image.

The risk analysis process should identify potential hazards and vulnerabilities. In the context of platform qualification, such hazards may result in risks to:

- records related to product quality or patient safety:
  - integrity – short term or long term
  - confidentiality – if required by the company
  - availability – at the right place and time
- availability of services – affects the business and compliance if persistent
- validity of IT Infrastructure processes, e.g., User Access Accounting
- availability and training of key staff

Once identified, the impact and likelihood of these hazards should be assessed and documented.

If the combination of impact and likelihood of occurrence, together with the probability of detection, is acceptable, or if the hazard can easily be removed, there is no need for further remedial action. For typical platform building blocks, the Risk Assessment process may reveal unacceptable risks. In such cases, the company needs to consider elimination by redesign, or mitigation by applying manual, semi-, or fully automated controls. Identified controls should then be implemented as part of on going operation (see Section 5 and Section 6 of this Guide).

Risk Assessment is typically an iterative process, performed progressively during planning and specification as more information becomes available.

Appendix 2 of this Guide provides an example of a Risk Assessment of IT Infrastructure components and suggested controls.

4.2 Implementation of Controls

A range of controls may be appropriate to mitigate the identified risks, including:

- testing
- redesign, including incorporation of redundancy
- the deployment of various automatic performance, diagnostic, alarm, and security monitoring tools, which greatly reduces the likelihood of undetected harm
- updated or new policies, guidelines, and instructions
- extra education or training
- supplier assessments and management

- identification of new or updated roles and responsibilities
- provision of extra staff, facilities, tools, and office space

Successful implementation of the required controls should be verified during qualification, and Periodic Review (see Section 4.4 of this Guide).

4.3 Assessment of Changes to Qualified Components

The impact and risk associated with proposed changes to IT Infrastructure components should be assessed as part of the change management process, and appropriate controls implemented.

4.4 Periodic Review and Evaluation

During Periodic Review of IT Infrastructure, the company should reconsider the risks and verify that controls, established during IT Infrastructure development and qualification, are still effective. The review also should consider:

- if previously unrecognized hazards are present
- if the estimated risks arising from a hazard are no longer acceptable
- if the original assessment is otherwise invalidated

If necessary, the results of the evaluation should be fed back as an input to the Risk Management process. If there is potential for the residual risks or their acceptability has changed, the impact on previously implemented risk control measures should be considered, and results of the evaluation documented.

5 Qualification of Platforms

This section describes how a platform, or a major addition to an existing platform, may be brought into compliance with the company's established standards using a planned qualification process. (Minor additions are usually managed via change control).

5.1 Overview of Process

A Platform Project and Qualification Plan, describing the life cycle activities to be undertaken to qualify each platform type, should be created. Unique platforms normally will be qualified as part of the application validation. The plan should cover the approved and effective SOPs required and the deliverables that will be the output of the qualification process, as well as responsibilities and approvals required. It is recognized that this information may be contained in other documents in accordance with company procedures.

The qualification strategy typically is based on one of two scenarios:

1. Platform specifications are independent of any specific applications. They are developed from generic requirements and bound by company policies. Development of system (application) specifications will therefore take these existing, available, standardized platform capabilities into account.

2. Platform requirements are mainly derived from system (application) specifications on a case by case basis.

In case (1), the building block concept applies, and the qualification plan is usually described in the SOPs. Qualification commences with little interaction with application (system) owners, as qualified platforms are considered commodities.

In case (2), the building block concept is not likely to be usable to its fullest extent, and significant interaction with application (system) owners is required as the platform qualification is largely a one-off.

In both cases, the associated risks should be formally assessed to determine how design choices may impact critical aspects. The output of the detailed Risk Assessment also will determine the scope and intensity of the qualification process. For example, qualification scope may be greater if no segregation technology is used to provide effective barriers between components which support GxP and non-GxP activities.

Infrastructure requirements provided should include regulatory requirements, ensuring that the primary responsibility for understanding and interpreting GxP regulations does not rest with infrastructure staff.

The assessed risks will help determine which components and configurations are required, and the rigor of supplier assessment, where applicable (e.g., questionnaire or full audit).

Following procurement, the next activity is to create an Installation Qualification (IQ) plan. IQ will provide evidence that all components have been installed and configured as specified. Where appropriate, certification evidence may be used to support IQ.

Following successful IQ, an Operational Qualification (OQ) plan should be applied, where appropriate, to provide evidence that critical features of the platform perform as specified.

The final stage in the process of qualifying an IT platform is the creation of a report that summarizes the results of the required qualification activities, and formally concludes the qualification process.

The activities outlined above are described in more detail in the following sections.

The use of re-usable building blocks (see Section 1.7.1 of this Guide) is recommended, where possible, to minimize the need for the introduction of new platform components (e.g., the use of standard, qualified, server, and client platforms).

The preferred qualification strategy is, therefore, based on qualifying *types* of building blocks and subsequently running abbreviated qualifications of individual *instances* of those building blocks.

Typical deliverables required when qualifying *types* and *instances* of building blocks are shown in Appendix 3 of this Guide.

5.2 IT Infrastructure Life Cycle Model

The following life cycle model outlines one way to manage complex IT Infrastructure projects; smaller additions to existing IT Infrastructures may use a model that combines the phases mentioned in Table 5.1. While indicating a general flow of life cycle phases, Table 5.1 is not intended to imply that all phases are strictly sequential, typically, overlap and iterations will occur during the project.

Table 5.1: Typical Life Cycle Phases

	Life Cycle Phases	Typical Deliverables
Achieving Qualification	Planning Phase (planning continues across all phases)	• Project Plans and Project Qualification Plans These would typically cover: • Project scope • Responsibilities • Deliverables and approvals • Project related risks • Quality and regulatory considerations • Processes (to be developed through the phases) • SOPs (to be developed through the phases) • Timelines • Training • Funding
	Specification and Design Phase	• Identification of all pertinent sources of requirements • Platform specifications • Design specifications • Degree of customization required • Drawings and diagrams • Parameter settings • Grouping of standard configurations into building blocks
	Risk Assessment and Qualification Test Planning	• Impact assessment • Identification of hazards • Design considerations • Likelihood of detection • Assessment of IT Infrastructure process effectiveness • Scoping of qualification • Defined test and inspection specifications • Acceptance criteria • Reviews and approvals
	Procurement, Installation and IQ Phase	• Supplier evaluation • Requests for tender • Installation qualification tests (completed IQ) • Supplier release and installation documentation • Temporary storage • Labeling and issuance • Construction, integration, assembly • Tests (e.g., of network assemblies) • Verified configuration item list • Verification of SLAs, contracts, or licenses • Introduction of Configuration Management and change control

Table 5.1: Typical Life Cycle Phases (continued)

	Life Cycle Phases	Typical Deliverables
	OQ and Acceptance Phase	• Operational tests and verification of specifications and agreed deliverables (completed OQ)
	Reporting and Handover Phase	• Summary reports • Approval of acceptance criteria • Transition Plans • Transfer of source documents and access rights • Service contract inauguration
Maintaining Qualification	Operation and Maintenance Phase (See Section 6 of this Guide)	• Change Management • Configuration Management (should be established prior to qualification) • Security Management • Management of servers, clients and networks • Problem Management • Help Desk • Backup and Restore and Archiving • Disaster Recovery • Performance monitoring of critical IT Infrastructure processes • Supplier Management • Periodic Reviews
Retirement	Retirement (Decommissioning/ Withdrawal) Phase (See Section 7 of this Guide)	• Decommissioning plans • Data/information archiving • Transfer of processes and data

Each life cycle phase required to achieve qualification is discussed further in the following sub-sections.

5.3 Planning

This Guide does not describe general project management strategies, methods, and tools in detail, but focuses on achieving compliant IT Infrastructure platforms.

5.3.1 Platform Qualification Plan

Separating the qualification of platforms from the validation of GxP applications means that adding or changing an application will not affect the qualified status of the platform (unless the change involved modifications to the platform). The validation of GxP applications should be managed by Validation Plans, as described in *GAMP® 4* (see Appendix 13, reference 1). The qualification of platforms should be managed by Platform Qualification Plans.

The Platform Qualification Plan should reference:

- applicable company policies and requirements
- any specific requirements derived from the applications or services that the platform is intended to support, see Section 5.1 of this Guide

- any existing pre-qualified building blocks in terms of standard platform building block qualification packages, e.g., for certain server types
- required new or referenced processes
- any new or modified SOPs

GAMP® categorization of the platform (see Section 2.1 of this Guide) assists with the development of an appropriate qualification strategy. During preparation of the plan, an initial high level Risk Assessment should be performed based on the platform's potential to cause harm to those records and functions that the system/data owner has identified as critical. Unless otherwise specified, platform managers should apply equally high standards to all records.

Appendix 2 of this Guide provides an example of a Risk Assessment of IT Infrastructure components.

New projects may require the introduction of new building blocks to meet requirements. With appropriate planning, these new building blocks can be added to the set of pre-qualified building blocks and will be available already qualified for future projects or changes.

Other constraints such as project Risk Management[6] and resource and time management are outside the scope of this Guide.

The Platform Qualification Plan should include or refer to:

- responsibilities for qualification
- life cycle activities
- deliverables in the form of specifications, test plans, test data, and reports, preferably organized to generate building blocks
- Timelines and interdependencies, e.g., in the case of a new IT Infrastructure, completion of network qualification before commencing hardware, server, client, and utility qualification. In another example, separate teams could perform work in parallel on a given network qualification, utilizing pre-qualified client building blocks.
- required reviews and approvals
- constraints and prerequisites
- overview of IT Infrastructure platforms, components, and boundaries
- critical records managed by the platform
- training requirements
- initial Risk Assessments

[6] Project Risk Management is concerned with risks pertaining to the project itself, e.g., lack of management commitment, availability of key staff, equipment, or other resources.

- need for verification of operational procedures

Consideration should be given to challenge testing of key operating system and utility software functions (e.g., those impacting data integrity and security) and critical hardware operation (e.g., loss/recovery of power).

Timely coordination with affected application (system/data) owners is required so that they can plan to update their application validation packages accordingly. Furthermore, application (system/data) owners should be encouraged to reference platform qualification packages from each application validation package to exploit the concept of horizontal, platform based, qualification.

QA should oversee the qualification processes being used. Therefore, QA should approve the Platform Qualification Plan and corresponding report to ensure it addresses all the expected regulatory and security-related expectations. Different organizations may have dissimilar requirements for review and approval of specifications, design documents, test plans and completed test sheets, and corresponding reports.

The Platform Qualification Plan may need to be updated once detailed information is available during later project phases.

Appendix 3 of this Guide lists typical deliverables from a platform qualification project and suggested responsibilities for production, review, and approvals.

5.3.2 Considerations for Legacy Platforms

A legacy platform, in the context of this Guide, is a platform that has been in use for some time without any formal qualification.

Key questions for such a platform include:

- What are the functional, performance, and security requirements for the platform?
- What is the status of existing processes?
- Is there an established QMS or a list of SOPs?
- Is there an updated inventory, high level network diagram, or configuration item list?

For a legacy platform that is running in a substantiated satisfactory manner, any intensive testing of the system may affect the continued operation. Therefore, consideration should be given to the production of an 'Experience Report' that summarizes the inventory and operational status and history of the platform, as basis for further planning.

Given the often extensive nature of IT Infrastructures, qualification of legacy platforms is likely to be a significant exercise that should be carefully planned, budgeted, and resourced. This is further complicated by the fact that the IT Infrastructure is subject to a high degree of change.

5.3.2.1 Determining Extent of Qualification

The legacy IT Infrastructure should be audited against company procedures and current regulatory expectations. Gaps should be identified and documented; Risk Assessments should be used to justify which legacy platforms require qualification to remediate identified gaps. In establishing priorities for the work, and to focus effort, key regulatory and business drivers for qualifying the IT Infrastructure should be considered, including:

The possible impact of the Platform on GxP Applications	• impact of platform failure • impact of platform changes
Maintaining a Secure Environment	• external connections • access control to business critical or GxP applications • access control to the platform(s) • securing business critical and GxP records
Facilitating Platform Disaster Recovery	• network diagrams • inventory of components • configuration management and change control • document management

5.3.2.2 Existing Documentation

Maximum use of existing documentation should be made to minimize timelines and rework effort. Focus should be on the required document content being present and accurate, rather than document formatting.

It is probable that relevant information and documentation for the support of platform qualification will already exist within application validation documentation and records.

5.3.2.3 Testing

Priority should be given to critical platform components identified by the Risk Assessment, as follows:

Basic Installation Verifications (IQ)	To verify that hardware and software items match the documented specifications. Note: re-installing working components for the sole purpose of gathering IQ documentation may not be an appropriate approach. This should be highlighted by the Risk Assessment.
Confirming Verifications	Confirmation that the key configuration settings match the documented specifications.
Operational Tests (OQ)	Should be considered for identifying potential gaps or issues relating to reliable operation of the platform(s), and also may form the basis for the development of (or assessment of existing) performance, support, and monitoring procedures. The following areas should be considered: • Storage Capacity • Response Times • Concurrent Sessions/Users • Availability • Backup/Recovery Testing • Access Security Processes/Procedures

For existing IT Infrastructures which are performing satisfactorily, stress and load testing is not a priority unless there are specific, reported performance issues.

5.4 Specification and Design Phase

A company should specify requirements for the various platform components in the form of controlled documents, such as reusable, generic requirement specifications, for each type of platform component (building block), or they should be embedded in contracts or Service Level Agreements (SLAs).

Inputs to the requirements include company policies and requirements derived from the applications that will ultimately run on the platform, such as functionality, compatibility, capacity, and security.

Company policies may dictate requirements in relation to suppliers, products, topology, and settings.

Specified platform requirements should be maintained, and be traceable to subsequent verification and qualification records. The use of a template is recommended for capturing platform requirements, including GxP related operational settings originating from individual application specifications.

Design specifications should be produced based on approved requirements and verified during qualification.

5.4.1 Networks

Network design specifications should be established to:

- define the topology and diagrams of the network to address segmentation, network performance, and security considerations
- serve as basis for procurement of network parts
- act as an overview of topology for maintenance and inspections/audits

5.4.1.1 Network Layers and Terminology

The standard model for networking protocols and distributed applications in multi-vendor environments is the ISO Open Systems Interconnection Reference Model (OSI Model) (see Appendix 13, reference 17).

The four-layer model described is based on an abbreviated OSI Model, and establishes some common terminology relating to qualification activities:

Layer 1 This layer defines the physical network in terms of hardware (copper or optical cables, outlets, patch cables, repeaters, hubs, network interface cards, and device drivers).

Layer 2 This layer is used for basic communication, addressing, and routing. Switches usually work on this layer.

Layer 3 This layer handles communication among programs. Routers and firewalls usually work on this layer.

Layer 4 End-user applications reside on this layer and communicate via software ports.

Test and qualification activities are directed toward assuring connectivity, functionality, and general conformance to design specifications on each separate layer, individually.

5.4.1.2 Topology

The network topology design is often presented as a drawing. The criticality of various network segments may vary, and this has to be taken into account when agreeing the topology. Issues to consider in the topology design include:

- segregation of GxP regulated networks from administrative networks
- protection and control of different GxP regulated networks
- the need for built-in redundant networks
- the serviceability of the network (e.g., via SNMP)
- the possible interfaces between segregated networks
- protocols supported in the different networks

The design should produce a drawing that outlines the topology and defines the primary network components, trunk cables, and dedicated network servers (e.g., Domain Name Servers).

If leased communication lines are part of the wide area network, the company should assess the capabilities of the carrier in terms of performance and security (see Appendix 8 of this Guide).

Topology diagrams should provide a high level representation of the infrastructure. Due to the dynamic nature of IT Infrastructures, documentation of the detailed configuration would likely be kept in dedicated databases rather than diagrams. Diagrams should focus on the key components of the infrastructure, identified during qualification planning.

5.4.2 Servers and Peripherals

5.4.2.1 Hardware

When server hardware is installed, it should be based on supplier recommendations, including environmental considerations. Configuration information should be included in the platform specifications and checked for compliance during Installation Qualification.

Redundancy in server building blocks, power supplies, and storage building blocks should be considered based on the results of the Risk Assessment.

Peripheral equipment is usually standardized off-the-shelf equipment with embedded firmware (e.g., sheet-printers, label-printers, bar code scanners, electronic signature capturers, and cameras).

Peripherals may be attached to servers, clients, or directly to the network, allowing centralized administration via management protocols.

Many types of peripherals are shared by systems in a general purpose operational mode. IT Infrastructure administrators often apply default factory settings, or settings conforming to corporate or site specific standards. Application specifications should not deviate from these settings unless it is specifically required, justified, and documented.

5.4.2.2 Operating Systems

Most operating systems allow a large number of parameter settings that can affect the way the server (or client) works. In general, these fall into three categories:

1. manufacturer supplied default values that remain unchanged

2. Manufacturer supplied default values that will be altered to produce specific behavior by the server. These parameters also may be changed to optimize performance.

3. parameters that are supplied blank, and should be completed by the customer, and without which the server may not work

It is not necessary to record default parameters that will remain unchanged. All other parameters, especially the blank parameter values that need to be entered, should be included in specifications, and verified as needed during IQ.

5.4.2.3 System Time Management

In a global IT Infrastructure, it is important to include provision for effective time synchronization which is traceable to an international standard, or as a minimum, a company time standard. Considerations when deciding on the time synchronization management layout include:

- traceability to an international standard (absolute time synchronization), e.g., Coordinated Universal Time (UTC), or International Atomic Time (TAI)
- availability to a reliable time source and the preferred way to disseminate system time
- management of summer/winter time offsets
- management of local time offsets

Specifications for time management should be verified during IQ and OQ.

Responsibilities for and access to setting and resetting of system time should be documented.

5.4.2.4 Storage Systems

Special consideration should be given to certain types of storage systems, such as Storage Area Network (SAN) and Network Attached Storage (NAS).

SAN storage systems are characterized by having their own high-speed network, consisting of dedicated network components for the SAN such as routers, hubs, switches, and gateways.

NAS storage systems are not attached to a separate network and consist of a dedicated server with a disk array storage system.

The chosen design of storage systems depends on the estimated load on the storage and the topology of the network.

Specifications for storage systems should be verified during IQ and OQ; however, the only practical way of performing OQ on a storage system is via a connected server.

5.4.3 Clients

Clients provide users access to shared services and resources (e.g., file servers, printers) and data processing capabilities through the installed client software (e.g., application servers, web browsers, work productivity tools, and email services). In some cases, clients also host local GxP applications, and use of the client may thus range widely in terms of scope, criticality, and need for qualification, validation, and management.

For management reasons, the clients may be grouped into categories with different capability and management profiles, e.g., a client hosting a GxP application should be more strictly managed than one which primarily provides the user with email services. A typical classification of clients and their associated management policies might be:

- 'un-restricted', i.e., open to user modifications provided that the modifications conform to company security and general software policies, and accepting centrally controlled updates
- 'restricted', i.e., closed to user modifications while still accepting centrally controlled updates

- 'controlled', i.e., closed for all modifications except via formal change management and qualification of changes with the possible exception of high priority security patches.

When deciding a classification, special consideration should be given to:

- security based on identified risks, and where available, the use of technical controls, such as automatically activated and password protected screensavers
- control of local clocks, particularly where used to timestamp electronic records or control time-sensitive processes
- preserving data integrity, wherever regulated electronic records are stored and can be changed within the desktop environment

As part of the client preparation process, companies may choose to install a standard set of software or use an image-generating tool, which mirrors an image onto clients of a released software configuration in the form of a building block.

Centralized management of updates via dedicated management protocols is advisable (see Appendix 10 of this Guide).

When a client hosts a 'thick' client or an entire GxP application, the application should be validated. For further information ,see *GAMP® 4* (see Appendix 13, reference 1).

5.4.4 Support and Diagnostic Tools

Tools should be carefully selected and risks to continuing operation of platforms should be assessed.

Tools should be introduced and used, as a minimum, in accordance with good IT and engineering practices, including consideration of:

- ensuring that the tool satisfies company standards and policies, e.g., security requirements
- verifying that the tool delivers the required functionality and does not modify critical records or affect platform performance
- maintaining an inventory of tools used

Examples of tools include vulnerability scanners, intrusion detectors, network loading, network diagnostics, and centralized distributing software.

Platform managers may employ tools to fulfill SLA requirements or implied requirements.

5.4.5 Data Centers/ Server Rooms

Companies may have a variety of demands for their data centers/server rooms commensurate with practicalities, costs, and risks in terms of security and quality factors. Common considerations include:

- Geographical location in relation to ease of access for staff and the ability to connect to backbone data links, the ability to monitor and control, and potential harm or disturbances from nearby installations or activities. Some companies may choose to double or triple their main data centers/server rooms to achieve the required assurance of availability.

- Provision of adequate space and environment for the intended purpose, and protection from undesirable outside factors of any relevant shape and form, e.g., contaminants, lightning, flooding, earthquakes, and other natural phenomena, intrusion, theft, attacks, accidents.

- Security considerations such as 'camouflage,' trap rooms, fences, guards, gates, access controls, logs, surveillance cameras, lighting, alarms. It may be desirable to build data center/server rooms inside other buildings on the company campus thus reducing the overall exposure to the outside.

- The use of raised floors and adequate conduits for internal cabling. Uninterruptible power supplies should be used to provide the required, filtered Volt-Amps (VA) for specified durations, in case of black or brown outs.

- Grounding and shielding, which are best achieved if planned well ahead of actual construction, and establishment of ground planes utilizing interlaced, conducting building parts that comply with national or international standards and codes may be considered.

- Cooling and the desired rate of air volume changes should be established

- Fire protection utilizing adequate technologies based on a reliable detection and trigger system.

5.5 Risk Assessment and Qualification Test Planning

Risk assessment is typically an iterative process, performed during planning and specification as more information becomes available. As the specification and design is completed, it becomes possible to perform more detailed assessments to establish the appropriate level of qualification testing required. GAMP® software and hardware categories should be taken into account during these assessments (see Section 2.1 of this Guide).

For individual or groups of components, the extent of qualification should be determined using the approach described in Appendix 2 of this Guide, which provides an example of a Risk Assessment process.

Appropriately qualified staff should review the design to determine the extent to which the proposed components, topology, and considerations for robustness may impact critical aspects of operation. The review should provide:

- assurance that a chosen design will deliver the required results with an acceptable level of risk, or provide useful input to changes in the IT Infrastructure design to reduce the likelihood of harm, or increase the probability of detecting any occurrence of harm

- knowledge of critical components or parameters that would need special attention in the maintenance procedures, e.g., provisions for robustness and security

- guidance on the appropriate level of supplier assessment required, where applicable

- identification of critical aspects that should be covered by the qualification process and which should consequently be managed by the configuration and change management processes or other processes

- an assessment of IT Infrastructure processes and their effectiveness to reduce the likelihood of undetected harm caused by the platform malfunctions, e.g., use of automatic performance, diagnostic and security monitoring tools

- scope of required qualification testing:

  - what to test, including identified controls

  - how much to test
  - test result documentation
  - acceptance criteria
- level of QA involvement required
- indication of training required
- a list of any new SOPs or changes to existing SOPs required to help mitigate identified risks

A benefit of using pre-qualified building blocks with standard qualification packages is that following the initial qualification only subsequent changes need be assessed for impact and risk.

For further information on Risk Assessment, see *GAMP® 4*, Appendix M3 (see Appendix 13, reference 1).

5.6 Procurement, Installation, and IQ

Components and services should only be procured from suppliers who can demonstrate an acceptable quality level and effective support, commensurate with the expected lifetime of the item and the risk associated with the failure of the item.

Upon receipt, goods should be checked for compliance with order specifications, labeled as needed, and stored in a safe place to facilitate subsequent safe installation.

It may be useful to run brief power-on tests to verify basic operations before taking the platform onto the target site, or stage entire assemblies at the supplier's premises and run a formal factory acceptance test before transport to the target site.

5.6.1 Supplier Evaluation

Companies may use a supplier evaluation program to ensure that critical components or services are only procured from approved suppliers. In some cases, a board of designated experts will evaluate relevant information gathered of a potential or existing supplier, and classify accordingly, e.g.:

Approved	If delivery history or gathered information is satisfactory – note this classification is not always given following the first audit since there are often issues to rectify. Depending on the issues, such a scenario should not necessarily be seen as a problem.
Conditionally approved	If delivery history or gathered information is not fully satisfactory, mitigation may include a closer follow up, and more intensive tests and witnessing than otherwise justified.
Not approved	When information or delivery history is inadequate or unsatisfactory.

On site supplier assessments performed or overseen by QA should be considered when the deliveries are in support of GxP regulated activities.

For further information, see *GAMP® 4*, Appendix M2 (see Appendix 13, reference 1).

5.6.2 Installation and IQ

Installation and integration methods should comply with company standards, and be based on supplier recommendations and the concepts of Good Engineering Practice (GEP) and good workmanship. Installation should conform to approved platform specifications.

GEP should include commissioning tests to verify conformance to specified engineering standards.

IQ verifies that the required physical hardware and software components have been installed and configured correctly in accordance with the platform and design specifications. Test specifications should specify how certification results and other tests and verifications together satisfy the required level of IQ.

It is recommended that the concept of building blocks for each platform component be used where possible to maximize the efficiency of the qualification process (see Section 1.7.1 of this Guide). Once building blocks have been qualified, duplicates of these building blocks may be configured with the main focus of qualification being to verify that a duplicate has been produced. This can be achieved by preparing installations scripts in advance for the production of a duplicate, based on images or similar, and by verifying the operation of the installation script during qualification of the building block.

5.6.2.1 Verification of Documentation

During this stage, the adequacy of the following documentation should be verified (where applicable):

- design specification
- hardware and software descriptions
- system operation manuals
- technical manuals
- system use SOPs (may be in draft, to be verified at OQ)
- network topology diagram (physical layout)
- network logical diagram (explaining switching capability and resilience)
- landscape overview (a depiction of the environments set up to facilitate operation and maintenance of a system)
- system labeling convention (wiring closets, cables, and equipment)
- cable lists as appropriate
- logical address lists
- supplier documentation, including system configuration details and installation guides

All critical items should be managed by the Configuration Management process including change management.

5.6.2.2 Environmental Conditions

There should be verification that the power supply and environmental conditions comply with requirements and standards, e.g.:

- temperature and humidity (e.g., in server rooms)
- electrical power and circuit protection documentation verification
- wiring, cabling, termination/connection documentation verification
- normal power up/power down verifications

5.6.2.3 Servers

Documented verification is required that the installation of the server hardware and software has been completed using the parameters and values established in the design stages. As a minimum, this should consist of a set of instructions for accessing the parameters on the new server, and for comparing these with those specified in the design documents.

Companies should consider preparing and maintaining verified server configurations, and use these to efficiently duplicate new servers. In order to achieve this, a Configuration Items List (CIL) is required.

For hardware, the list should contain key configuration items such as:

- make and model of the server
- type and amount of memory
- number of CPUs and disks
- disk controller
- additional information needed to rebuild the server

For software, the CIL should contain the components that are installed so that the server can be safely rebuilt or duplicated to the same configuration.

Examples of configuration items include:

- operating system
- service programs for communicating with the server hardware and application software
- service packs, hot fixes, and security patches to the operating system and service programs
- access control settings
- network settings

The configuration items should be identified by means of version numbering or similar. Appropriate documentation should be available during IQ for verification of the configuration items.

Server management groups would be concerned with meeting stated and implied requirements for manageability, availability, connectivity, and security.

Documentation of hardware components could be a report from the server management software, and documentation of software components could be in the form of screenshots, showing the correct version numbers of the components.

5.6.2.4 Clients

As described for servers, companies should consider preparing and maintaining an image or installation script containing the results of one verified client installation and use it to duplicate new clients for maximum control and efficiency.

Individual system specifications may require non-generic client software to be added to clients as part of the roll out. Wherever practicable, system specific installation scripts should be prepared and tested on a single standard client instance and distributed using a centralized distribution service. Some distribution services automatically log whether or not the installation is successful, otherwise the result should be verified and recorded manually.

5.6.2.5 Networks

Physical Network Layer

In new facilities, customized cabling (cobber or fiber optic) is prevalent and cables should be prepared, installed, inspected, and tested to verify compliance with applicable recognized standards, e.g., ISO/IEC 11801 or ANSI/TIA/EIA 568B. Subject specific standards are provided by all the major standardization organizations.

Outlets, patch panels, patch cords, hubs, and other prefabricated assemblies working on the physical layer level should be procured and installed as specified and included in the tests to provide conclusive evidence of satisfactory performance. Test/inspection considerations should include:

- environmental factors, e.g., heat, dust, moisture, Electromagnetic Compatibility (EMC)
- physical strength of, e.g., fibred cables
- connectors
- transmission performance, e.g., attenuation, refraction

The identity and installation of critical components should be recorded.

The test results should be annotated, reflecting actual values recorded, and signed and dated in accordance with company procedures.

Logical Network Layers

Devices working on the logical layers usually support some management protocols, e.g., Simple Network Management Protocol (SNMP) for the TCP/IP environment enabling a so-called 'managed network.' There should be verification that the network component is compliant with its specification, with the network topology, and with the network management system in use.

The network management system should enable computer aided tracking of network device characteristics, installation, and configuration.

Test of Application Connectivity

This is outside the scope of this Guide and is usually verified as an integral part of the system validation effort. Application testing should not commence until the formal handover of the infrastructure has been completed. This may be by the use of a formal handover certificate or by acceptance and sign-off of the agreed qualification activities by the application team.

5.7 OQ and Acceptance

The final stage of Qualification is to confirm that the IT Infrastructure component operates in an expected manner as defined in appropriate specifications.

Provided the platforms are all commercially available standard products, the focus of OQ should be to test connectivity and where applicable capacity using integrated or add computerized tools, rather than core functionality.

At a minimum, OQ should consist of a set of instructions to be followed, which describe the necessary test steps, expected results, and evidence to be collected. OQ should be based on the outcome of the Risk Assessments already carried out (see Section 5.5 of this Guide) to verify that the sum of requirements derived from serviced applications, if applicable, are met.

Typical tests to consider would include:

- verification of key Data Management Software, e.g., by checking database connectivity
- verification of all permanent IP-addresses, and response times under conditions specified by the Qualification Plan by use of commands that allow the user to verify network connectivity
- verification of the routing pattern under conditions required by the Qualification Plan by use of, e.g., commands that allow the user to trace a network packet to its destination
- verification of security settings across all platform components and checking that default passwords have been altered
- verification of critical firewall features, positive as well as negative testing (it allows traffic that should pass and blocks traffic that should be blocked)
- verification of key Operating System (OS) functionality, e.g., by checking accessibility to defined disk volumes
- verification of time synchronization

Tools available for the OQ tests and maintenance in general will depend on the chosen technology.

Tests should be traceable to requirements where appropriate.

In simple cases, IQ and OQ may be combined in one activity; however, the sequence of installation followed by operational testing should be maintained unless pre-qualified building blocks are used.

5.8 Reporting and Handover

Following the successful execution of Installation and Operational Qualification specifications and closure of any issues, a report should be written which confirms that all of the specified activities have been successfully completed, as well as confirming that all the critical processes are described and implemented. The report should be reviewed and approved by QA.

Depending on the project characteristics, this could be a single report, one per building block, one per platform, or a combination thereof.

The approved report enables platform owners to demonstrate compliance to auditors and inspectors, and provides assurance to application owner(s) that the platforms are in a state of control.

Once all these activities have been confirmed and approved, the platform is ready to load the application and any migrated data and platform qualification documentation produced should support the validation of the application(s).

6 Maintaining the Qualified State During Operation

The IT Infrastructure typically changes frequently, sometimes on a daily or hourly basis, depending on the size of the infrastructure. The IT Infrastructure should be maintained in a documented state of control by ensuring appropriate:

- Change Management
- Configuration Management
- Security Management
- Server Management
- Client Management
- Network Management
- Problem Management
- Help Desk Provision
- Backup, Restore, and Archiving
- Disaster Recovery
- Performance Monitoring
- Supplier Management
- Periodic Review

In order to be efficient and cost-effective, the required documented state of control should be achieved and maintained in an appropriate manner, e.g., automatic tools available should be exploited wherever possible.

The use of a documented QMS, (see Section 3 of this Guide), should address all the listed requirements. The following sub-sections give further guidance on key topics of interest.

6.1 Change Management

The change control process cannot be separated from Configuration Management. When changes are proposed, both change control and Configuration Management activities need to be considered in parallel, particularly when evaluating impact of changes. However, it should be noted that due to the simplicity, the frequency and occasionally the urgency of some changes (e.g., network port patching or security patching), change control procedures need to accommodate timely and effective, yet documented, updating methods.

Change management processes should define how changes to configuration items should be managed, and should include an assessment of the impact on supported GxP applications and the extent of re-qualification required, where applicable.

Further guidance on managing upgrades and patches is given in Appendix 7 of this Guide.

GAMP® 4, Appendix O4, also provides further guidance on change management (see Appendix 13, reference 1).

6.2 Configuration Management

Configuration Management (CM) covers the identification, recording, and reporting of components, including their version, constituent components, and relationships.

As a minimum, all items identified as critical for maintaining the qualified state of the platforms should be kept under CM providing an approved baseline for further evolution and allowing safe restoration of a qualified baseline in case of problems.

Components are typically referred to as Configuration Items (CIs). CIs include hardware items, software items, critical parameter settings, documentation, and any other part of the IT Infrastructure that an organization wishes to control. The level of information held about each CI will depend on the component's attributes. CIs, usually, are defined down to the lowest level at which a component can be independently installed, replaced, or modified.

GAMP® 4, Appendix M9, provides further guidance (see Appendix 13, reference 1).

6.3 Security Management

IT Infrastructure security is required both for business purposes and to satisfy various regulations, such as health, finance, and occupational. Lack of security may compromise availability of applications and services, record integrity and confidentiality, reputation with stakeholders, and may lead to unauthorized use of systems that ultimately would impact on product quality.

Information security is often characterized as the preservation of:

Confidentiality	• ensuring that information is accessible only to those authorized to have access
Integrity	• safeguarding the accuracy and completeness of information and processing methods
Availability	• ensuring that authorized users have access to information and associated assets when required

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures, and computerized functions, such as:

- security incident management
- intrusion detection
- server hardening (e.g., remove superfluous applications, tools, and blocking unused ports)
- virus signature updates
- considerations to origin of software (e.g., from approved suppliers)
- disaster recovery planning
- user access administration

More detailed information on security controls is given in Appendix 6 of this Guide.

6.4 Server Management

The objective of the server management process is to ensure that specified requirements for operational availability, performance, and security are consistently fulfilled by the server. An important part of the process is to manage the server configuration and changes needed to meet the objectives.

The handling and qualification of changes depend on the potential impact that a given change may have on the served platforms and applications. If the change affects GxP applications, the extent of re-qualification required should be considered.

Server management is further described in Appendix 9 of this Guide.

6.5 Client Management

The objective for the Client Management process is to ensure that specified requirements for operational availability, performance, and security are consistently fulfilled by the client. An important part of the process is to manage preparation, deliveries, adaptations, patching, and security issues for the multitude of stationary and mobile units in use across the organization.

The Client Management Group is advised to use computerized tools where possible to centrally manage updates, patches, and security scans to enforce corporate policies.

Client management is further described in Appendix 10 of this Guide.

6.6 Network Management

The objective of Network Management is to ensure that specified requirements for operational availability, performance, and security are consistently fulfilled by the network. Fulfillment of this objective involves identification and use of effective and reliable computerized tools, applications, and devices to assist network staff in monitoring and maintaining network performance in support of other platforms and services.

Network diagrams should be updated when the topology changes during maintenance and the inventory list of components should be updated to reflect the actual network configuration.

Network Management is further described in Appendix 11 of this Guide.

6.7 Problem Management

Problem Management includes control and active management of both problems and errors. A 'problem' is an unknown underlying cause of one or more incidents, and a known error is a problem that is successfully diagnosed, and for which a workaround has been identified.

An essential part of Problem Management is to provide users with an adequate method of recording perceived or acknowledged problems. The Help Desk is an important point of contact and also may be a valuable source of information

All filed problems should be tracked and resolved via approved channels; those that require changes should be input to the Change Management Group.

Problem Management should trend problem reports and strive to counteract escalation of problems by providing timely reports to the platform administration, e.g., to avoid severe service degradation caused by growing congestion in a given network segment.

Standardized utility applications are available to support the Problem Management process, but smaller organizations may use a manual logbook or similar to record and track problems.

6.8 Help Desk

The Help Desk process has the goal of providing the day-to-day support to users of the IT Infrastructure with problems, questions, and general support needs. Staff employed in the Help Desk must be technically skilled with respect to the actual platforms and technology used in the IT Infrastructure to support the business processes in the company.

The Help Desk is typically contacted via a central point (e.g., telephone or using a web application), where the Help Desk case is either solved immediately, or registered in a Help Desk system that manages the Help Desk process. The Help Desk system may be the same as used in Problem Management (see Section 6.7 of this Guide) and also serves as a historical record to facilitate fast response to contacts.

Where a Help Desk case requires the involvement of subject matter experts, the Help Desk service forms the liaison between the user and those experts.

6.9 Backup, Restore, and Archiving

The backup, restore, and archiving capability of data on any computer platform is essential to preserve the integrity of the information contained on these systems in case of system failures.

Whether a given application (system/data) owner requires full or incremental types of backup, a Risk Assessment process should be applied to achieve an appropriate frequency, commensurate with the acceptable residual risk of losing data for a given period of time, and the resulting impact on business.

Archiving is a process that ensures long term availability of data by provisions of safe storage, indexing, and refresh activities.

When a request to perform a restoration of backed up or archived data is received, consideration should be given to whether the person requesting the restoration is authorized to do so, and whether they are authorized to view the data being restored. Procedures also should ensure that the restore process does not inadvertently overwrite data that must not be lost.

More detailed information on backup, restore, and archiving is given in Appendix 9 of this Guide.

GAMP® 4, Appendix O6 and Appendix O7, provide further guidance (see Appendix 13, reference 1).

6.10 Disaster Recovery

Loss of vital parts of the IT Infrastructure and business applications may have serious impact on the business of a company. With the often complex configuration and interdependence of the infrastructure platforms and business applications, business becomes sensitive to even smaller incidents in the IT Infrastructure and business applications. Therefore, Disaster Recovery is an important part of the company's Business Continuity Planning (outside the scope of this Guide). The primary goal of Disaster Recovery is to reduce downtime of critical business applications to an acceptable level following an incident.

Disaster recovery is closely related to the identified Configuration Items (CIs) within the Configuration Management process as well as the backup, restore, and archiving process.

See *GAMP® 4*, Appendix O8, for further guidance (see Appendix 13, reference 1).

6.11 Performance Monitoring

The objective of performance monitoring of devices and services is to monitor and record satisfactory operation of the IT Infrastructure as evidence in support of its continued qualification status, and secondarily, to ensure fulfillment of the Service Level Agreement (SLA) and any other stated or implied expectations.

The review of results or alarms based on this monitoring activity will trigger maintenance, update, support, or disaster recovery activities, and therefore, will form the basis for a fast and proactive infrastructure support service. This approach also should ensure that the platform will be maintained in a state of control during its operational lifetime.

To assure that platform performance requirements are continuously met, surveillance procedures should be developed and alert and action limits defined.

Actual metrics and values should be defined by each company in the context of all relevant deciding factors. In some instances, there may be less risk to product quality or critical records by allowing a higher known loading on a server than embarking upon a project to replace it.

Monitoring frequency should be defined for all metrics taking risks and tool efficiency into consideration. A baseline should be created at the time of installation (or during the Performance Qualification (PQ) of a supported software application), and actual values should be considered based upon those readings.

When using complex process or system management applications, the monitoring and event reaction should be automated to some extent.

Appendix 9 of this Guide lists some typical performance metrics from real life GxP regulated environments, and suggests appropriate alert/actions limits.

Appendix 11 of this Guide provides further guidance on network management.

GAMP® 4, Appendix O5, provides further guidance (see Appendix 13, reference 1).

6.12 Supplier Management

The management of services and deliveries to the IT Infrastructure typically will follow the general policies of supplier management in the regulated company including evaluation of suppliers, selection of suppliers and the management of the relationships with the suppliers. Agreements between the regulated company and the supplier should be documented in contracts, or SLAs, and reviewed at appropriate intervals.

The regulated company should maintain a list of approved or preferred suppliers to ensure that the suppliers meet the company requirements regarding performance, cost, and quality of the delivered services. Company policies often include evaluation of the supplier's performance to meet the agreed services, and an assessment of the availability of suppliers. To mitigate the risk of suffering from shortage or unacceptable deliveries from a supplier it may be valuable to have more than one supplier of the same service/platform (e.g., various brands of clients and servers from several suppliers), also known as 'second sourcing.'

To support the rollout and service of IT Infrastructure platforms and to exploit the concept of building blocks, it may be advantageous to set up requirements related to the supplier regarding availability, e.g., stock-size, of the qualified IT Infrastructure building blocks (e.g., servers, clients, and SW-licenses).

The management of outsourced services are further described in Appendix 8 of this Guide, where the challenges of outsourcing (e.g., responsibilities, contracts, SLAs, supplier audits) are described.

6.13 Periodic Review

Periodic Reviews should establish that procedures meeting current applicable GxP regulatory requirements are approved and in use. The review should establish that qualification and operational records, and review reports are complete, current, and accurate. Periodic Reviews are considered in further detail in Appendix 5 of this Guide.

7 Retirement of Platforms

Business applications often outlive the underlying platforms, and in such circumstances, data needs to be migrated onto the new platform(s). For example, a validated LIMS application may be operational for many years using modified versions of application software until a desirable version is released which requires a server platform update. Alternatively, the existing platform may no longer comply with company standards and become too cumbersome or even impossible to maintain, as suppliers cease providing support on economically acceptable terms.

When a platform is replaced, special consideration should be given to data migration, especially when conversion is required as part of the process. Documented assurance should be provided that:

- all data elements are migrated
- all critical data attributes are preserved (e.g., security settings)
- all supporting data are correctly transferred
- no extra data elements are inadvertently introduced
- any specified conversions have consistently produced the expected results

In many cases, it may be appropriate to apply statistical methods to obtain the required assurance; in other cases, it may be necessary to devise computerized tools to provide a complete, automated verification; some suppliers provide verification tools with the update package. The verification method should be determined by assessing and documenting the risks involved.

The following documents provide further guidance on retirement of platforms:

- *GAMP® 4*, Section 7.11.14 (see Appendix 13, reference 1)
- *GAMP® 4*, Appendix O6 (see Appendix 13, reference 1)
- GAMP® Good Practice Guide: A Risk Based Approach to Compliant Electronic Records and Signatures, Appendix 3 (see Appendix 13, reference 2)

Appendices

Appendix 1
Roles and Responsibilities

1 Introduction

Companies are organized in a variety of ways that fit each individual company's mode of operation, size, objectives, geographic layout, culture, etc.

Companies typically identify roles and responsibilities in a similar way; this Appendix discusses their interrelationships and a possible way of grouping them together.

The term 'owner' is used in this context both as a suggested title for personnel accepting ownership of a given item or process, and for the high level of accountability associated with assuming that role. Often, true ownership can be achieved only by personnel whose primary business objectives are directly dependent on the item's availability and performance.

The term 'independent QA' is used to denote the role of the Quality Assurance group as required by regulatory authorities.

Executive management is responsible for the successful implementation and qualification of the IT Infrastructure platforms, and commits and empowers resources to ensure adherence to all relevant GxP requirements, and other requirements such as those pertaining to security.

The key roles that a company may find useful to identify and allocate resources may include:

- Executive Management
- Project Manager
- Application (System/Data) Owner/Administrator/SMEs
- Data Owner, if not coincident with the Application (System) Owner
- IT Infrastructure Process Owner/Administrator/SMEs
- Platform Owner/Administrator/SMEs
- Independent QA
- IT Quality and Compliance

(See Section 2 of this Guide.)

Roles should be organized to prevent critical objectives from being overlooked. Job descriptions should be assigned to named individuals. Such decisions should be justified and documented.

Technical and managerial staff with appropriate educational background and experience should be available. Provision of training should be planned to ensure the required skills are developed and maintained. Staff should be made aware of any regulatory requirements that apply to their duties, trained in those procedures that are applicable to them, and re-trained as changes occur. Records of training should be maintained.

2 Executive Management (Project Sponsorship)

Driven by business needs, executive management appoints members of management to assume the roles of 'sponsoring' projects and defining general requirements to the IT Infrastructure. Key initial activities include:

- financing the initial feasibility stages
- determining the acceptable level of risk for the organization
- selecting steering committee members
- developing business cases and other formalities needed to obtain a fully funded and supported project established

Close interaction with QA is recommended in these initial stages.

Whether a regulated company owns its IT Infrastructure or leases services from service providers, it is responsible for the qualification status and should specify, therefore, expectations and monitor the continuous fulfillment of those expectations, e.g., negotiate, agree, fund, and monitor general SLAs with IT Infrastructure service providers. Note that ownership and quality assurance of systems and data should not be outsourced for reasons of Control and Compliance.

3 Project Manager

Controls all project activities, including:

- Liaison with system and data owners on working processes and system requirements
- Monitoring compliance of project deliverables with GxP and company standards for documentation, data control, training, software development (if inside the project scope), and technical support
- Preparing the Infrastructure project and quality plan, or Infrastructure Qualification Plan
- Review, approval, and reporting on key project deliverables under the qualification life cycle
- Review and reporting on all change requirements
- Assessing and managing project related risks
- Ensuring timely resolution and escalation of issues

A critical aspect in the initial project phases is the involvement of end-users, QA, and other long term stakeholders. A smooth transfer to the platform owner is a key objective at the end of the project.

4 Application (System/Data) Owner/ Administrator/SMEs

A system consists of the application plus whatever platforms and parts of the infrastructure are required to enable the application run. Therefore, depending on the applicable approach for a given project (see Section 5 of this Guide), the application (system/data) owner(s)/administrator(s) should specify the detailed requirements a given application has of the underlying platform and IT Infrastructure processes, accordingly. If the company policies require the use of pre-qualified, standardized platform building blocks, the platform requirements take a different format than when platforms are chosen, configured, and perhaps even built for the project.

For GxP applications, the application (system/data) owner has further computer system validation specific responsibilities, see *GAMP® 4* (see Appendix 13, reference 1).

In case the parts of the infrastructure essential to the system in question are installed, tested, qualified, and operated under an SLA, that in itself may be owned by a peer application (system/data) owner or higher management, the application (system/data) owner would be most concerned with the application at hand, and the data it processes.

In relation to the infrastructure, the owner should:

- provide funding as needed, e.g., share of platform SLA costs
- appoint a system administrator as needed to take care of system oriented daily operations, e.g.:
  - resolve issues brought to his/her attention, e.g., level and scope of Platform Qualification Plans
- In many cases, the application (system) owner acts in the role of data owner, see Appendix 1 of this Guide.

In relation to the infrastructure, the system administrator typically would have the following responsibilities:

- creation and maintenance of all required documentation, e.g., copies of platform qualification reports, as required
- performance of required review activities
- liaison with the platform groups and application specialists and ensuring clarity in mutual expectations
- managing system user access profiles and permissions
- managing SLAs with service providers
- managing critical records and specifying any additional requirements to security for the platform groups
- managing or approving system specific changes including those that are initiated from the platform side and may affect application performance or record integrity
- making appropriate use of SMEs, such as application specialists

The administrator should have a deep understanding of the system's functionality and impact on the businesses it supports or automates.

5 Data Owner

In cases where the data that a system stores, displays, manipulates, or transports are not logically owned by the application (system) owner, a company may choose to nominate data owners. For example, when the system or file storage service provides hosting capabilities for a number of users who must account for inputted data over long periods of time, owners of such data need to be aware of their responsibilities, and equipped with adequate means to fill the responsibilities.

Data owners would be responsible for ensuring that the established quality and security provisions are adequate. Considerations should be made for the provision of:

- backup and restoration
- archiving
- change management and audit trails
- access restrictions in general and possibly specific settings
- availability

6 Infrastructure Process Owner/ Administrator/ SMEs

Depending on the size of a company, and thus, the infrastructure, it may be appropriate to assign dedicated staff or organizational units to take care of specific infrastructure processes (see Section 2 of this Guide).

As the objectives for the processes vary greatly so do the responsibilities of the owners, but in all cases, the scope and purpose of the process should be defined and described in SOPs or SLAs, as appropriate. (SLAs usually control outsourced building blocks, but may be used among internal organizational units as well.)

Critical tasks should be described in SOPs and approved by authorized senior staff and IT Quality and Compliance or QA, as appropriate. Ongoing assessment methods should be documented.

Key performance indicators should be established and agreed upon, including adequate reporting and escalation mechanisms.

Infrastructure process owners also may own any supporting IT Infrastructure systems, in which case, they should be aware of any GxP impact that may warrant validation.

Infrastructure process owners should support audits and be trained in good conduct during regulatory inspections within their scope of responsibility.

7 Platform Owner/ Administrator/ SMEs

The role of owning an infrastructure process may coincide with the role of owning a platform, e.g., the server management process may coincide with or include the ownership of a given type of server hardware platforms.

Depending on the company's size, the responsibility for each type of technical platforms would be assigned to dedicated staff or organizational units allowing them to concentrate and specialize on characteristics of each platform type, e.g., servers, networks, clients, peripherals.

If the platform supports one or more GxP applications (business or infrastructure), the platform owner should provide the necessary qualification documentation for inclusion or reference. The platform owner should:

- decide on short and long term strategies for the platforms – in accordance with company policies
- fund the platform operation and maintenance
- appoint a platform administrator or SMEs as needed to take care of daily operations
- act as escalation level for complaints and major problems

The platform administrator/SMEs typically would have the following responsibilities:

- creating and maintaining all required documentation and operating procedures
- qualifying the platforms – including 'building blocks,' and ensuring continued compliance with applicable requirements
- performing required review activities
- managing user access profiles and permissions to shared services
- managing SLAs with service providers
- providing second and third level support
- managing records
- managing the implementation of service and security patches
- conducting ongoing performance management
- managing the configuration and platform specific changes
- providing expertise in the exploitation of the platform and the various versions in operation
- initiating and supporting supplier audits, as appropriate
- presenting the platform documents and justifying all critical decisions to QA and regulators on request

8 Independent Quality Assurance

Quality Assurance, independent of IT, has ultimate responsibility for assessing whether compliance with regulatory and company standards is achieved and maintained.

The degree of technical literacy should be commensurate with defined responsibilities in relation to the IT Infrastructure.

QA should:

- provide governance/oversight
- provide high level company procedures to meet compliance obligations
- develop and maintain policies, processes, procedures, and other guidance documents that comprise the compliance framework
- review and approve documentation/records as appropriate, based on impact to GxP
- plan and perform internal and external audits
- review and approve Periodic Review reports, as appropriate
- host regulatory inspections

9 IT Quality and Compliance

IT Quality and Compliance provides quality and compliance expertise to projects and operations in support of a controlled environment and associated processes that meet the quality and compliance requirements of the company.

IT Quality and Compliance staff need in depth compliance and technical insight, and should:

- provide governance/oversight
- liaise with QA to ensure alignment with the overall company compliance obligations
- liaise with system and platform SMEs
- liaise with appropriate industry groups to leverage and influence industry best practices and standards
- keep abreast of the business, legal, and regulatory environment for interpretation, and assess the impact on IT Infrastructure
- support the development and maintenance of policies, processes, procedures, and other guidance documents that comprise the compliance framework

- review and approve documentation/records as appropriate, based on impact to GxP and business critical elements
- escalate to QA for approval in accordance with company procedures, e.g.:
  - approval of key documents
  - required retention periods for technical records
  - critical changes
- provide education and awareness
- develop and maintain an education program (i.e., training requirements, GxP, regulations, audits)
- train staff as appropriate
- provide guidance/consultancy/validation management/SMEs such as test engineers
- participate in projects, as appropriate, based on risk, to provide quality guidance
- participate in process reviews and support continuous improvement
- perform internal quality and compliance assessments of IT processes
- develop and maintain the assessment programs
- perform periodic assessments/reviews
- conduct supplier audits
- support external audits of the IT Infrastructure organization

The relationship between independent QA and IT Quality and Compliance, including delegation of activities, should be documented.

Appendix 2
Example of Risk Assessment and Controls

1 Background

Risk assessments should be performed at each major life cycle phase of any object or groups of objects (e.g., platforms or data) identified to be important or even critical for a company to fulfill its mission.

Risk Assessment may be taken to comprise two phases: risk analysis and risk evaluation. Note that NIST's *Guide to Risk Management for Information Technology Systems* (see Appendix 13, reference 12) suggests a further refinement into nine steps. *GAMP® 4*, Appendix M3 (see Appendix 13, reference 1) describes a process for performing Risk Assessments of a computerized system in order to ensure design, specification, and test efforts are appropriately focused. This Appendix describes how a combined approach may be adopted for IT Infrastructures.

2 Risk Analysis

The purpose of risk analysis is to provide clarity of the boundaries of the infrastructure under analysis, and review the history of threats (hazards) and vulnerabilities in the light of its potential impact on the company's mission, which for GxP regulated companies includes considerations of public health.

Input to the process should include:

- platform specifications (hardware and software)
- architecture/topology diagrams
- applied or planned security policies and requirements
- requirements from application (system/data) owners
- levels of staff training and experience
- history of attacks, weaknesses, failures, flaws
- any audit or self assessment comments
- current or planned controls that may prevent, detect, or otherwise mitigate harm before irreparable damage occurs

Output from the analysis process would include:

- identification of the infrastructure objects scoped by the process
- the hazards threatening the infrastructure's obligation to meet critical requirements
- the vulnerabilities that may warrant further consideration
- a list of critical controls

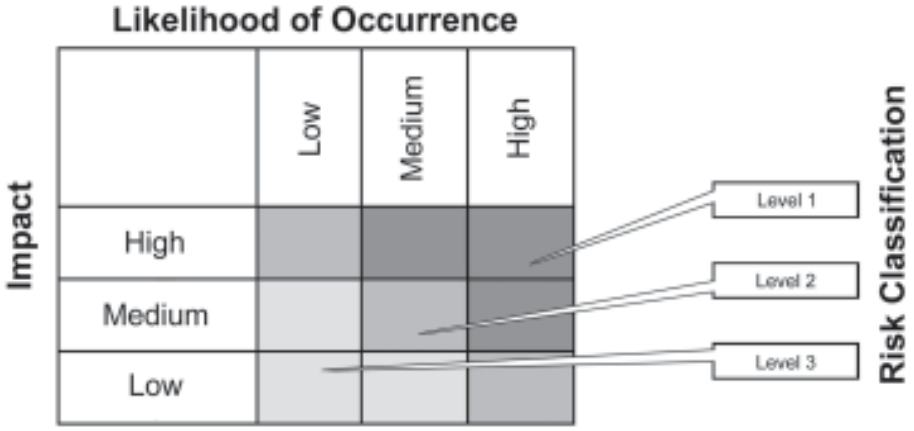
The next step is to determine the likelihood that a given harm occurs, the magnitude of the impact of the harm, and the effect of any identified mitigation factors, e.g., early detection.

Input to this step is largely subjective as little qualitative data typically exists to support the assessment; it is thus important that experienced people with a well balanced conception of the subject matters are involved with the process. Factors to consider include:

- nature of vulnerabilities and motivation for exploitation
- effectiveness of suppliers' quality management system, e.g., design controls
- effectiveness of own quality management system, e.g., qualification
- adequacy of planned or current controls, e.g., vulnerability scans

Each of the factors mentioned above should be rated in relation to each other as high, medium, or low in a two stage process that is described in this Appendix:

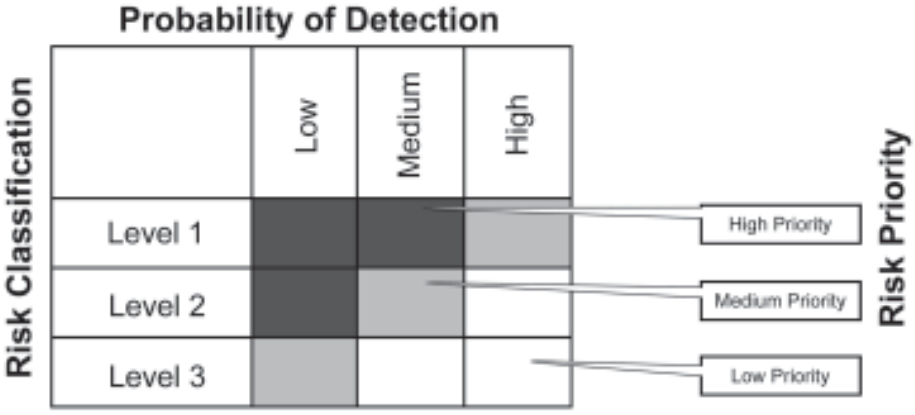
Figure A2.1: GAMP® Risk Assessment, Stage 1



Output from this step is a classification of each hazard in one of three levels: one, two, or three.

The next step in the process is to evaluate the effect of mitigation factors, e.g., probability of detection before any harm to critical aspects occurs. This is depicted in Figure A2.2, GAMP® Risk Assessment, Stage 2.

Figure A2.2: GAMP® Risk Assessment, Stage 2



Output from this stage is the *risk priority*.

3 Risk Evaluation

Once a risk is prioritized, it should be evaluated to determine whether it is acceptable to the company under the influence of all identified factors. If this is not the case, some degree of rework is required to improve the situation, and the Risk Assessment process should be repeated for the change.

The results of the assessment, along with the assumptions made, should be documented.

Note that assessing risks typically is an iterative process, repeated as activities progress and as more information becomes available.

4 Application of the GAMP® Risk Assessment Approach to the Infrastructure

Table A2.1 presents some proposals for considering the scope of typical scenarios/events and shows a broad spectrum of infrastructure components directly related to GxP or business critical aspects.

Table A2.1: Example of Infrastructure Risk Assessment

Hazard	Risk Scenario	Impact	Likelihood of Occurence	Probability of Detection	Risk Priority	Controls
Incorrect physical connection	No function or malfunction	High	Med	High	Med	Network Diagrams IQ
Failure of component, e.g., network interface card	Performance degradation or loss of connection	High	Low	High	Low	Defined Problem Management process Defined alarm logs
Access security compromised	Unauthorized modifications of data/records, potential access to other (GxP) network areas	High	Med	Low	High	Security procedures IQ/OQ Periodic Review

Table A2.1: Example of Infrastructure Risk Assessment (continued)

Hazard	Risk Scenario	Impact	Likelihood of Occurence	Probability of Detection	Risk Priority	Controls
Anti-virus definitions not maintained	Lack of availability Unauthorized modifications Breach of confidentiality Corruption of GxP records	High	Med	Low	High	Security procedures Periodic Review
Firewall incorrectly configured	Lack of availability Unauthorized modifications Breach of confidentiality	Med	Med	Low	High	Specifications maintained for firewall configuration IQ/OQ Periodic Review
Storage capacity limit	Records/data not stored. Applications may halt.	Med	Med	High	Low	Performance monitoring routines
Insufficient network bandwidth/ speed	Applications run slowly	Low	Med	High	Low	Performance monitoring routines
Network diagrams not maintained	Unable to rebuild network in event of a disaster	High	Med	Med	High	Availability of diagrams Change control process Configuration Management Periodic Review
Installation of unauthorized software	Interference with operation of existing software	High	High	Low	High	Security Procedures Periodic Review
Inaccurate or missing configuration records	Inability to restore configuration in case of disaster	High	High	Med	High	Configuration Management process Periodic Review

Appendix 3
Qualification Deliverables

This Appendix provides guidance on specifying life cycle qualification deliverables and deciding which organizational units are involved in preparation, review, and approval. Companies should determine actual involvement required commensurate with the assessed risks. Traceability between requirements, specifications, and qualification should be maintained, e.g., through the use of traceability matrices.

For Table A3.1, the following abbreviations apply:

PO Platform Owner or Administrator

SME Subject Matter Expert/IT Quality and Compliance

QA Independent QA

Table A3.1: Qualification Deliverables

Elements	**Platforms**			
	Clients	Servers	Networks	Hardware/ Peripherals
Qualification Plan	PO, SME, QA	PO, SME, QA	PO, SME, QA	PO, SME, QA
Requirements	PO, SME, QA	PO, SME, QA	PO, SME, QA	PO, SME, QA
Design Specifications	PO, SME	PO, SME	PO, SME, QA[1]	PO, SME
Risk Assessment	PO, SME, QA	PO, SME, QA	PO, SME, QA	PO, SME, QA
Type[2] IQ	PO, SME, QA	PO, SME, QA	PO, SME, QA	PO, SME, QA
Instance[3] IQ	SME	SME	SME	SME
Type OQ	PO, SME, QA	PO, SME, QA	PO, SME, QA	PO, SME, QA
Instance OQ	SME	SME	SME	SME
Type Qualification Report	PO, SME, QA	PO, SME, QA	PO, SME, QA	PO, SME, QA
Instance Qualification Report	SME (via remote management)	PO, SME	PO, SME	PO, SME

[1] Role of QA in ensuring that up to date Network Topology Diagrams are available should be determined

[2] Based on Section 5 of this Guide, the term *type* is used for the generic specifications and derived documents that would relate to building blocks (standard configurations). Qualification of a building block *type* would typically include all the above, except for *Instance IQ and OQ.*

[3] Based on Section 5 of this Guide, the term *instance* is used for the individual documents that would specify qualification details and capture results for instances of building blocks. Qualification of an *instance* would typically include *Instance IQ and OQ* only and these would refer to the associated building block *type* documentation.

Appendix 4
Standard Operating Procedures

This Appendix provides guidelines on addressing the individual aspects that may need to be controlled by SOPs and the quality records that should be produced. Detailed selection and organization of documents depends on the circumstances for each company: size, complexity, geographic layout, impact on critical aspects, etc.

Table A4.1: SOP Requirements

Area or Aspect	Processes Requiring SOPs	Typical Deliverable Documentation
GENERAL		
Roles and responsibilities	• Personnel Development • Job Definitions	• Organization chart • Job description
Training	• Organization of training • Delivery of training • Assessment of effectiveness of training	• CVs • Training curricula • Training records • Competency records
SLAs and Contracts	• Management of Agreements and Contracts, including definition of responsible representatives • Maintenance of Agreements and Contracts • Contract review	• Contractual documents • Contract review records
License management	• License Management • Monitoring software usage	• Licenses • Outputs of monitoring
Records and Documents	• Record and Documentation Management	• Document Control Records
DATA CENTRE MANAGEMENT		
Day-to-day activities	• Data Centre activities • Tape rotation/loading, off-site shipping, general monitoring tasks – backup completion	• Operating Procedures • Logs
Security	• Physical Security access	• Procedures • Approved requests • Access logs and roster reviews
Facilities Management	• Operating environment (temperature and humidity) • Supplies UPS, RFI, EMI, generators • Fire protection and safety management	• Regular service and test records

Table A4.1: SOP Requirements (continued)

Area or Aspect	Processes Requiring SOPs	Typical Deliverable Documentation
PLATFORM MANAGEMENT		
GENERAL		
Hardware and Software installation (including peripheral equipment)	• Physical installation and qualification of new hardware and software • Decommissioning	• Installation and Operational Qualification
Configuration Management	• Maintenance of current and historical configurations • Description of redundancy features (disk mirroring, RAID devices, alternate routing)	• Inventory records • Design and configuration documents • Topology diagrams
Change Management	• Changes to existing hardware and software • Adjustment of configuration parameters • Risk Assessment • Management approval/ rejection	• Change control records • Change control reports
Hardware and software maintenance	• Preventative maintenance and problem resolution • System, application software or firmware and patch installation	• Maintenance plan • Maintenance logs • Change control records
Service start up and close down	• Start up • Shut down • Implementation of service restrictions (e.g., TCP/IP, email, databases access)	• Event logs
System monitoring, event/ problem logging, problem tracking and reporting	• Capacity management • Establishment and recording of performance metrics • Escalation • Help Desk Call Management and Resolution • Trending	• Capacity, usage, availability and performance reports • Event/exception handling reports • Help Desk call records
Retirement	• Decommissioning • Archiving of data • Disposition of equipment • Restoration of archived data	• Retirement records • Data archives

Table A4.1: SOP Requirements (continued)

Area or Aspect	Processes Requiring SOPs	Typical Deliverable Documentation
SERVERS AND MAINFRAMES		
Job Scheduling	• Assignment of batch job priorities • Ensuring proper completion of batch jobs and re-processing when necessary	• Priority lists, especially for validated applications • Deviation reports on failures
NETWORKS		
Third Party networks	• Use of wide area networks • Interfacing of local networks to wide area networks	• Network topology diagrams
CLIENT MANAGEMENT		
Client (including peripheral equipment) hardware and software installation, and changes	• Establishment of initial standard client(s) • Evolution of standard client • Distribution of software upgrades • Maintenance of virus protection including updating and distribution of signatures	• Installation and Operational Qualification • Parameter change control records • Anti-virus software and signature update records
SECURITY		
Physical security	• Means of access to all system and network components (e.g., computer rooms, network rooms/ cabinets, cabling, etc.)	• Access control logs
Logical security	• User account management Password management including functionality rules, changes and related event reporting • Digital signature certificate management • Access rights maintenance • Management of administrator accounts • Management of emergency access	• Logs of creation, deletion, transfers of responsibilities • Logs of password renewals, deletions, suspensions • Security monitoring reports, especially unauthorized access attempts
External influences	• Monitoring of intrusion attempts • Handling of security vulnerabilities	• Security monitoring reports

Table A4.1: SOP Requirements (continued)

Area or Aspect	Processes Requiring SOPs	Typical Deliverable Documentation
DATA MANAGEMENT		
Data Backup and Restore	• Backup scheduling, logging, recorded data verification, problem detection and deviation reporting • Media labeling and storage (on-site, off-site) • Risk analysis • Restore process (including authorization to restore) • Media management • Restoration testing (as part of disaster recovery testing)	• Backup logs • Restoration logs • Risk analysis reports • Event logs
Long term Data Archiving	• Data management (e.g., in-house or devolved, data deletion from active directories, data restoration from archives, archived data expiry and deletion) • Media management	• Archiving and restoration logs • Data deletion logs • Authorization records
QUALITY MANAGEMENT		
Quality Assurance/IT Quality and Compliance	• Compliance with standards and SOPs • Implementation of corrective actions • Process improvement participation • Service Level Agreement performance monitoring	• IT Operational Standards • Internal audit schedule • Audit reports • Process Evaluations • Performance reports
Risk Management	• Use of Risk Model	• Risk Assessment results • Mitigation steps
CONTINUITY MANAGEMENT		
Disaster recovery and contingency planning	• Continuance of service provision in event of catastrophes	• Disaster Recovery Plan (as part of business continuity planning) • Disaster Recovery Test Reports

Appendix 5
Periodic Reviews

For the Infrastructure, a Periodic Review should establish that procedures meeting current applicable GxP regulatory requirements are approved and in use. The review also should establish that qualification and operational records and review reports are complete, current, and accurate.

Companies may choose, for business reasons, to address non-GxP elements of the infrastructure during Periodic Reviews.

Companies should define and agree in advance the topics to cover during specific Periodic Reviews, taking into account possible hazards and risks. The following example checklist may be used when drawing up such a list of topics. Depending on circumstances, companies should select which aspects to include since the complete list will not always be required or appropriate.

Table A5.1: Periodic Review Checklist

IT Management and Organization
Roles and Responsibilities
Are management roles and responsibilities defined (e.g., job description)?
Are quality roles and responsibilities defined (e.g., job description)?
Are technical and support roles and responsibilities defined (e.g., job description)?
Is the organization documented (e.g., organization charts)?
Capability and Competency
Are training plans in place?
Have personnel received training in regulatory expectations (where appropriate)?
Are training records in place to demonstrate that training has been delivered (for both employed and contracted staff)?
Do training records document: • Description of Training • Date of Training • Instructor • Evidence of Attendance
Do training records demonstrate that the attendee understood the training?
Is current documentation in place detailing personnel qualifications, education and experience (i.e., resume or CV)?
Internal Organization Interfaces
Are interfaces between infrastructure organizations defined (e.g., international sites)?
Are service agreements or procedures in place between internal infrastructure organizations?
Are requirements of the business defined?
Are system and data owners defined?
External Support Organizations
Are contracts and/or service agreements/escrow agreements in place for all external service/support organizations?
Have external service/support organizations been assessed (e.g., audited) against contract requirements?

Table A5.1: Periodic Review Checklist (continued)

Is service performance monitored against defined service levels?
Have service providers been trained in your company's procedures where relevant?
Have service providers been trained in your company's security policy?
Are there controls in place to ensure that only authorized personnel from the service organization have access to your network and files?
Is there a mechanism in place to ensure that applicable changes at the external organization will be assessed for any impact on your organization (and vice versa)?
Are your company's records segregated from those of the service provider's other clients?
Quality Systems
General
Are projects managed in accordance with life cycle project management systems?
Is there an overview document (e.g., Quality Manual) describing the quality management system?
Is the quality management system, periodically reviewed for its effectiveness?
Are quality metrics in place to enable measurement of quality system performance?
Are documentation and records management processes, systems and/or procedures in place?
Are infrastructure qualification standards in place including: • Planning • Specification and Design • Risk Assessment and Qualification Test Planning • Procurement, Installation, and IQ • OQ and Acceptance • Reporting and Handover
Are these standards being followed?
Does the QMS address infrastructure operation and maintenance processes e.g.: • Change Management • Configuration Management • Security Management • Server Management • Client Management • Network Management • Problem Management • Help Desk • Backup, Restore, and Archiving • Disaster Recovery • Performance Monitoring • Supplier Management • Retirement
Regulatory
Has impact of applicable regulatory inspection findings been considered and addressed?
Has impact of changes in regulatory requirements, industry best practice, and introduction of other regulations (e.g., financial regulations) been considered and addressed?

Table A5.1: Periodic Review Checklist (continued)

Tools and Infrastructure Applications
Are tools and infrastructure applications compliant with regulatory and company requirements, e.g., SOP systems, Configuration Management, change control, access authorization, etc?
Are the risks of deploying infrastructure tools, e.g., virus protection, backup, performance monitoring, assessed?
Are tools verified to ensure they meet company standards and deliver the required functionality without unexpected side effects?
Is an inventory of tools maintained, such as: • Communication Protocols • Performance Monitoring Software • Virus Protection • Backup and Restoration • Software Deployment Tools
Qualification Planning
Qualification Plans
Are Qualification Plans produced in advance, defining responsibilities, and required activities, procedures, deliverables, timelines, reviews and approvals, constraints, training requirements, critical data being stored?
Are Qualification Plans based upon initial Risk Assessments?
Specification and Design
Hardware
Are inventories of Hardware components in place?
Are specifications, diagrams or other documentation in place to describe the Site Local Area Network including: • Network layout of the site • For each area or building, the location of major network components and cable paths
Are documented specifications in place for each platform component enabling accurate replacement in case of failure?
Network Organization
Are network segregations, domains, etc., documented (including access controls)?
Software and Configuration
Is there an inventory of all applications and data storage areas within the network?
Cable Infrastructure
Are (internal or external) standards used to define cable requirements?
Are cabling diagrams or specifications in place?
Are cables tagged or labeled to aid identification?
Control of External connections
Are connections to WANs defined?

Table A5.1: Periodic Review Checklist (continued)

Are controls in place to ensure that only authorized users can access the system remotely (e.g., secure ID or callback)?
When a remote access link is terminated, is the user automatically logged off the network?
Electrical Supplies
Do electrical supplies conform to earthing, loading, filtering and safety standards?
Are power conditioning in place (prevention of spikes and brown outs)?
Are backup power supplies (e.g., UPS) in place to guard against power loss to critical components?
Are UPS loads determined and monitored?
Is UPS performance verified?
Redundancy and Fault Tolerance
Have redundancy requirements been assessed, e.g., disk mirroring, RAID?
Have requirements for automatic standby systems been defined?
Risk Assessment and Qualification Test Planning
Is the scope of qualification testing based on documented Risk Assessments, carried out by qualified staff?
Procurement, Installation, and IQ
Are suppliers assessed in accordance with documented Risk Assessments?
Are platform components subject to installation qualification in accordance with Qualification Plans? Is adequacy of documentation verified?
OQ and Acceptance
Are platform components subject to OQ in accordance with Qualification Plans?
Reporting and Handover
Is there a summary report, approved by QA, to confirm successful completion of qualification?
Does the approved report enable platform owners to demonstrate compliance to auditors and inspectors and provides assurance to application owner(s) that their platforms are in control?
Change Management
Are change control procedures in place to manage changes to hardware, firmware and software, including impact assessment on any application affected by the change?
Do change control procedures consider the need for testing to be conducted, based on risk, when hardware or software is added, removed or modified within the infrastructure?
Are changes to platform components that support GxP applications qualified?
Do change control procedures address the management of emergency changes, patches, or configuration changes?
Are responsibilities for change management defined (e.g., SME/QA/User)?
Are development, test, and production environments managed in order to ensure that software, hardware and configuration integrity is maintained?

Table A5.1: Periodic Review Checklist (continued)

Are GxP and non-GxP areas segregated or are GxP level controls applied to both?
If GxP and non-GxP items are segregated, is there a documented justification for what is and is not defined as GxP?
Configuration Management
Are adequate means defined to protect configuration items from deletion, removal, or unauthorized alteration or use?
Are specifications, configuration item lists and other documentation updated following changes to hardware and software?
Does the configuration item list enable an accurate restore of critical components in case of break down, by documenting, e.g.,: • Item name or identifier • Serial number • Model or hardware type • Manufacturer • Item location • Storage devices • Operating system software, including version • Layered products, including version • Relevant application software, including version and the application (system/data) owner
Are controls in place to control access to system documentation?
Are retention periods defined for system documentation in line with the site/function record retention schedule?
Security Management
Security General
Are processes, systems and/or procedures in place to address the requirements of the security policy and principles?
Are responsibilities for security management defined?
Is virus detection software in place and maintained up to date?
Are firewalls in place and documented in order to control access to the network?
Are controls in place to ensure that unauthorized software and files cannot be loaded into the network?
Are procedures in place to detect and investigate potential security violations?
Physical Access Controls
Are servers, other critical hardware, backups and archives located in secure areas where access is controlled by key or other security device (e.g., card key)?
Logical Access Controls
Are procedures in place to ensure that users are restricted to those parts of the network required to fulfill their defined role?
Is logical access based on at least two components and is that component combination unique for each person?

Table A5.1: Periodic Review Checklist (continued)

Do user accounts automatically time out after a period of inactivity?
Are user accounts disabled after a defined period of inactivity?
Are users removed from the system when they leave the company or change jobs?
Are there Periodic Reviews of obsolete or dormant accounts?
Do procedures exist to cover both permanent staff and temporary/contract staff?
Are temporary/contract staff accounts set up with an expiry date?
Are there documented rules for password management?
Are unauthorized access attempts detectable, reported, and investigated?
Do procedures exist to manage cards and tokens?
Are User access rights documented?
Server Management
System Time
Are dedicated time servers in place to distribute time traceable to a reliable source, e.g., BIPM (Bureau International des Poids et Mesures).
Are procedures in place to ensure setting of system time does not break sequence of any logging, e.g., always adjust ahead and in small, frequent increments?
Are winter/summer time settings formally managed, and has impact on time stamped logs been assessed?
Environmental Conditions
Are computer rooms and data centers environmentally controlled?
Client Management
Is the standard client defined?
Are local extensions/configurations to standard clients defined?
Are processes in place to manage the deployment of client applications?
Are processes in place to audit client configuration?
Is client configuration documented?
Are processes in place to manage the build of new clients?
Are processes in place to manage upgrades to the client?
Are processes in place to maintain up to date virus protection?
Is the client configuration locked to prevent unauthorized user changes?
Network Management
Is the network management process defined in SOPs or SLAs?
Are network monitoring tools and equipment tested, calibrated, or qualified as per qualification plan?
Have metrics been defined?

Table A5.1: Periodic Review Checklist (continued)

Problem Management
Are procedures in place for reporting, investigating and documenting network faults?
Service Management/Help Desk
Have service start-up and close down processes been defined?
Have processes for implementing and communicating service restrictions been defined?
Are facilities in place for fault reporting, tracking and trending (e.g., Help Desk)?
Are support services defined (e.g., 1st, 2nd, 3rd line support)?
Are escalation procedures in place for management of service shortfalls?
Are continuity plans in place to address critical service outage?
Backup, Restore and Archiving
Backup and Restore
Are procedures in place to assess backup requirements against business and regulatory needs?
Have backup and restoration procedures been formally tested?
Do backup procedures address: • Frequency of backups • Physical labeling of media • Review and retention of backup logs • Periodic testing pf backups to verify that the backup procedure is functioning • On site and off site storage of media. Full backups should be periodically stored off site. • Rotation of backup media • Type of backup (full versus incremental)
Do off-site backup storage considerations include: • Location of facility • Formal processes and controls over physical access to media both on a schedule and “on request” basis? • Storage conditions?
Are procedures in place to assess ability to recover to point of failure?
Do restoration procedures adequately address the retrieval of single files, multiple files, and complex data backups (e.g., database restore)?
Are installed versions of operating systems, communication protocols, applications, etc., archived in order to facilitate backup?
Archive
Are decommissioning processes in place?
Are processes in place for management of data deletion?

Table A5.1: Periodic Review Checklist (continued)

Do archive procedures include: • Identification of archive media • Management of archived media • Documentation of records to be archived • Retention periods • Secure and safe storage of archive media • Frequency of archiving • Periodic evaluation of archive media • Migration following system upgrades • Considerations for data conversion, where appropriate
Do archive restoration procedures provide the ability to read records from the archive (have available appropriate hardware, software, and instructions)?
Do archive restoration procedures address: • Authorization to request records from archive • Procedure for performing restoration
External Data Management Organizations
Are external organizations managing backup and archive facilities subject to appropriate controls including: • Service Definition, including responsibilities, documentation requirements, escalation process • Contacts • Audit • Performance Monitoring
Disaster Recovery
Is the disaster recovery process defined in SOPs or SLAs?
Are key staff identified, available at defined notice, and trained in appropriate procedures?
Is access to archives ensured commensurate with recovery lag times?
Performance Monitoring
Are procedures or automated controls in place to monitor network performance and capacities including: • Speed • Bandwidth • Disk Performance (e.g., fragmentation, thrashing) • Address Clashes
Are event logs created and maintained in support of service performance monitoring?
Supplier Management
Has the supplier management process been defined in SOPs or SLAs?
Have critical suppliers been assessed against quality requirements?
Have purchasing lead times for critical components been agreed upon or have provisions for consignment stocks been made?
Have channels of communication been established?

Table A5.1: Periodic Review Checklist (continued)

Retirement
Have decommissioning plans been made? Including provisions for: • Data/Information Archiving • Transfer of Processes and Data

Appendix 6
Infrastructure Security

1 Introduction

A defined level of infrastructure security is required to meet business purposes and to satisfy external regulations. Lack of security may compromise availability of applications and services, record integrity and confidentiality, reputation with stakeholders, and may lead to unauthorized use of systems that would impact on product quality.

A company should take cultural and practical aspects into consideration when defining the rigor of its approach. Companies may adopt different approaches for specific infrastructure elements, based, e.g., on criticality and risk.

2 Infrastructure Security Management

Infrastructure security management includes all the policies, procedures, requirements, training and audit programs, etc. that a company may define appropriate to safeguard the infrastructure, including information assets.

As a minimum, regulated companies need to satisfy the applicable GxP requirements. Relevant documents include the PIC/S Guide (see Appendix 3, reference 4), which builds on ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6). The 21 CFR Part 11 contains security requirements focused on electronic records and signatures (see Appendix 13, reference 2).

RFC 2196, *"Site Security Handbook,"* is another useful source of information (see Appendix 13, reference 16).

Infrastructure security is a subset of a company's IT Security management plan and companies may elect to extract applicable guidelines from, e.g., ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6), and apply those to infrastructure elements.

Security controls, in general, are considerably cheaper and more effective if incorporated at the requirements specification and design stages.

2.1 ISO/IEC 17799 - Code of Practice for Information Security Management

The international standard ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6) is an internationally recognized set of recommendations for developing security policies and conducting auditing. Many organizations use this standard as a baseline from which to start when developing their policies and their information security programs. Other standards also may be appropriate.

Information security is characterized in the standard as the preservation of:

- **Confidentiality:** ensuring that information is accessible only to those authorized to have access
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods
- **Availability:** ensuring that authorized users have access to information and associated assets when required

Information technology security is achieved by implementing a suitable set of controls, including policies, practices, procedures, organizational structures, and computerized functions.

The ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6) is a risk-based method for assessing, evaluating, and managing risks. It takes a holistic approach to security, and provides a framework for developing a security program. It provides guidelines for organizations on how to develop and implement such a security program and how to improve currently deployed programs.

The ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6) has 10 sections:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. System Development and Maintenance
9. Business Continuity Management
10. Compliance

Not all of the controls described in ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6) will be relevant to all infrastructures, nor to every situation. It cannot take account of local system, environmental, cultural, or technological constraints. Consequently, the use of ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6) as a guide should be adapted to the circumstances of each organization.

2.2 ISO/IEC 17799 and Regulations

Regulatory guidance recommends consideration of these standards, but does not require organizations to be formally accredited.

Companies should define a list of ISO/IEC 17799 issues that are relevant to infrastructure security within their own organization (i.e., define what is business critical, GxP related, and the infrastructure subset). Existing infrastructure policies and procedures should be mapped against the applicable sections of ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (see Appendix 13, reference 6) and an internal audit of these policies and procedures used to demonstrate to regulatory authorities that the organization is in control.

2.3 Technical versus Procedural Issues

Management should establish an administration or individual obligated to define and monitor an infrastructure security program. Administrative, physical, and technical controls should be utilized to achieve management's security directives.

- Administrative controls include the development of policies, standards, procedures and guidelines, security awareness training, incident management, etc.
- Technical controls consist of access control mechanisms, password and resource management, identification and authentication methods, security devices, etc.
- Physical controls consist of controlling individual access into the facilities and different departments, locking systems, removing unnecessary floppy disk or CD-ROM drives from workstations, protecting the perimeter of the facilities, monitoring for intrusion, etc.

2.4 Security Incident Management

To ensure efficient coordination of security incidents, an incident management procedure should be established as effective communication channels are essential in the quick identification and mitigation of a specific threat. Seemingly isolated incidents may not receive an appropriate level of attention unless they are centrally reported. For instance, the seemingly benign situation of an account being locked, e.g., due to a forgotten password, may become more suspicious if the same event occurs repeatedly.

The incident management process can be integrated into problem escalation processes with increased levels of priority to ensure appropriate responses.

2.5 Intrusion Detection

Intrusion Detection Systems (IDSs) in the form of hardware or software are commonly available, enhancing the security of the perimeter of internal networks. Determined intruders may be able to penetrate firewalls, but attacks do not come only from external sources. Depending on the impact and risks involved, companies may decide to use IDS technology to mitigate risks.

By monitoring suspicious activity, alarms can be sounded earlier, giving more time to react to an imminent threat. Although not infallible, they offer an additional level of protection to complement a well-configured firewall. It is important to have incident management procedures in place to ensure no time is lost once an alarm has been raised.

As with firewalls, IDSs are only as effective as their configuration and administration. A well-maintained pattern database and regular review of IDS summary reports ensure their efficacy.

2.6 Vulnerability Management

Vulnerability scanners or adequate manual procedures should be applied to determine weaknesses and gaps in the platforms' security configurations. Corrective actions include:

- application of patches
- changes to security settings

- harnessing the network topology

However, the volume of security alerts can make it difficult to determine which threats are real, and which threats are unlikely to be exploited. A practical approach to vulnerability management is to start with a complete inventory of systems, which permits an assessment of where best to focus available resources. A small number of reliable sources of security alerts should be identified, and the risk of each threat should be assessed, prioritized, and categorized to determine an appropriate response. With numerous new security threats being identified each day, depending on the risk, it is often more appropriate to patch or fix during scheduled maintenance (e.g., weekly or monthly) rather than daily.

2.7 Anti-Virus Shield Update

Most anti-virus applications can initiate totally automatic updates, but some companies prefer controlled daily updates rather than ad-hoc updates throughout the day. In this way, a risk-based approach can be applied very much like security patch management, assessing the threat presented versus the inconvenience of excessive updates. In both cases, Configuration Management practices are required, recording which updates were applied to which systems, and at what date and time.

Servers, and especially clients, that are not office based pose difficulties in distributing virus updates. There are two possibilities for update:

1. updates which are controlled and distributed from the internal IT department

2. automatic updates from the anti-virus supplier which requires no intervention

The first option ensures that Configuration Management processes can be followed, allowing testing prior to deploying the update, but it often inhibits rapid response.

The second option poses challenges for Configuration Management. A Risk Assessment to compare the risk of deploying untested updates versus leaving clients without updates for longer periods may be considered. If this approach is adopted, a Periodic Review of the update process effectiveness should be conducted.

2.8 Public Key Infrastructure

In cases where a company needs to utilize features such as digital signatures, it may consider implementing a Public Key Infrastructure (PKI), or exploit PKI services provided by external organizations, or both.

Digital signatures are employed when the intended use is to secure the authenticity, non-repudiation, integrity, and confidentiality of external messaging over any digital communication channel. Users need to install client programs and to obtain a certificate from a trusted third party, either directly or via the company's own Certification Authority (CA).

2.9 Origin of Software

The origin of all software related to qualified infrastructure platforms should be known in order to avoid quality and security related issues. If a company decides to use *open source software,* it should ensure that a reputable software supplier supports the product and version, and accepts responsibility for maintaining it.

Software downloaded from non-reputable or unknown sources should be avoided.

3 Upgrades and Patches - Balancing Qualification and Security Considerations

Changes to IT Infrastructure platforms require formal change control processes, documentation, and testing. These processes take time, especially where individual application tests are required, and particularly for GxP applications.

Where changes are required to address security vulnerabilities, applying the full change control and testing processes prospectively may present an unacceptable risk to the business in terms of security. However, direct application of any upgrades/patches without change control and testing may compromise the qualified status of the IT Infrastructure and present compliance issues.

First, the scope of the change should be understood, e.g., does it cover:

- Network Operations
- Clients
- Servers
- Firmware/Hardware
- Data Management Software
- Operating System
- Infrastructure Utility Systems or Tools

Second, the urgency of the change should be established.

3.1 Urgency of Security Update

A prerequisite to determining an appropriate course of action is to understand the risks associated with a given security vulnerability. This information should be available from the operating system/application suppliers and confirmed by end user groups.

Generally, this will position the urgency of application of the change into one of three criticality categories:

1. **Emergency Fix:** should be applied as soon as possible, where the security vulnerability presents immediate and real threats to the business
2. **Urgent Update:** probable threat, fix should be applied within a specified time scale
3. **Update:** no immediate threat, consider including within next scheduled platform upgrade

3.2 Compatibility of Security Updates

Security patches are usually available only for a limited number of product versions; suppliers of interacting software may not provide compatible versions which creates a dilemma for system owners. In addition, validation and availability requirements constrain upgrade options. Where critical security patches cannot be installed, system managers may have to resort to procedural controls or even to isolate the system from other systems or from the corporate network. Company security policies should outline strategies to pursue.

Further guidance on managing security upgrades and patches is given in Appendix 7 of this Guide.

Appendix 7
Upgrade and Patch Management

This Appendix presents some risk-based considerations when determining an appropriate approach to upgrades and patches.

1 Fundamental Principles

Regardless of the criticality of an upgrade, the following aspects should be considered:

- **Change Control**
  Change control documentation should be raised to cover application of the upgrade/fix. For emergency changes, this may be retrospective (but within a minimum period of time following application of the upgrade).

- **Configuration Management**
  Configuration Management records should be maintained; documentation recording versions and patch levels of platforms should be accurately maintained. For emergency changes, the documentation may be retrospectively updated.

- **Communication**
  All owners of critical applications should be made aware of the requirement for an upgrade prior to its application.

- **Incident Monitoring**
  An incident monitoring process should be in place. Where emergency changes are applied with minimal or no specific application testing, particular attention should be given to incident monitoring and reporting.

2 Upgrade Strategy

The upgrade strategy should be based on a technical assessment and an impact assessment:

- The IT group should perform a technical assessment of the upgrade, reporting whether the upgrade is minor, medium, or major in nature, based on complexity and possible impact on applications.

- All owners of critical applications should perform an impact assessment on their systems based on the available information.

Issues can arise with applications when implementing patches/upgrades to platforms where the base application and/or operating system have not been upgraded for an extended period of time and lag behind the current version by a number of minor/major releases. Where this is the case, installation of an emergency upgrade may be compromised – resulting in either the application being unable to run or the patch being unable to be applied. In each case, there is a clear business risk, which should be managed by evaluating the risk, documenting conclusions, and where necessary, introducing controls to manage the risk.

Systems that have been removed from operational use, but have been retained as read-only systems for the purposes of record/data retrieval (i.e., partially decommissioned) may present issues, particularly where product support of the base application is no longer available from the system's supplier. In these cases, consideration should be given to isolating or segregating the system to reduce the risk.

Where an update is applied during formal testing, where that testing forms part of the validation of a system, the level of re-testing required should be determined based on an assessment of risks.

Upgrade strategies should be in place for all applications, but especially for business critical or GxP applications.

3 Level of Application Testing

Four general levels of testing that may be applied to applications following a platform upgrade include:

1. **No Testing**

2. **Confirmation Testing**

A minimal level of documented testing to verify that an application runs on an updated platform.

3. **Confidence Testing**

Documented testing against pre-defined specifications that consist of a representative subset of functional tests on the updated platform.

4. **Full Testing**

Full regression testing of the application on the updated platform.

For emergency changes (e.g., critical security update), it is likely that no prospective testing will be applied to applications. For business critical and GxP applications, enhanced incident monitoring should be applied in this instance, and a documented justification made until retrospective testing, or final impact evaluation has been completed.

Where the update is **not** categorized as an emergency, some level of testing should be applied; the level being dependant on the nature of the upgrade and information available.

Where the update is technically assessed to be of a minor nature, then confirmation testing only may be appropriate.

For highly critical business or GxP systems, or where the update is assessed to be significant (or likely to have an impact on applications), then confidence tests should be considered as a minimum requirement.

For an update of a major nature where application impact is likely, and particularly for business critical or GxP systems, then full (regression) testing should be performed.

The two stage Risk Assessment process defined in *GAMP® 4* (see Appendix 13, reference 1) is a good tool for assessing the appropriate level of testing to apply (an example is given in Appendix 2 of this Guide). The process involves assessing three considerations:

- the impact of failure of the system (business and quality risk)

- the likelihood of failure

- the probability of detection of the failure

If an update affects significant platform components, the need for regression testing of the platform also should be considered.

4 Global/Multi-Site Systems

For systems that are used at multiple locations, where the company has a worldwide standardization of platforms, an efficient approach is to perform testing at a single location and then use this as the basis of reduced or no testing at the other locations.

Appendix 8
Outsourcing

1 Definition of Responsibilities

Outsourcing involves the transfer of management and operations of a company's IT Infrastructure to an external company. The scope varies, but some examples include:

- operation of a data center and/or networks
- operation of systems and/or processes (e.g., Help Desk)
- hardware/software component build (e.g., workstation)

The contracted service provider may have staff located on the regulated company's premises or the resource and services may be provided from a remote location (if that location is on a different continent the term 'offshoring' is sometimes used rather than 'outsourcing').

The regulated company remains responsible for the regulatory compliance of their IT operations regardless of whether they choose to outsource/offshore some or their entire IT Infrastructure processes to external service provider(s). Compliance oversight and approvals cannot be delegated to the outsource partner.

The external service provider has the responsibility for ensuring that their service meets the customer's requirements. Critical elements for the external supplier to focus on include:

- regulatory education: ensuring that all staff and contractors provided through the outsourcing agreement understand the regulatory compliance impact of their actions and seek appropriate approvals
- creation and maintenance of Standard Operating Procedures (SOPs) and work instructions
- creation and maintenance of quality records[4]
- Quality Assurance and Quality Control of their IT Infrastructure processes and procedures

2 Special Considerations

The location from which the outsourcing company provides services to the regulated company should be assessed. Services located on the regulated company's site should be managed in accordance with the company's standard security processes. However, services provided from a location outside the regulated company's boundaries may require additional controls to ensure similar levels of security (e.g., in the case of remote management of a data centre or a Help Desk process).

[4] A 'quality record' is evidence that a required quality assurance activity has been performed and the results of that activity.

3 Contracts

The regulated company is responsible for interpreting GxP regulations and defining appropriate requirements for the IT Infrastructure.

These should be provided to the external service provider in terminology that they recognize as requirements for services. It is recommended that the terminology of IT industry best practices be used wherever possible.

Key Performance Indicators (KPIs) and acceptance criteria should be defined by the regulated company governing the level of control required in the operation and maintenance of the IT Infrastructure.

Contracts should handle the ownership and retention of documents and records relating to the service being managed, e.g., if a contract is ended with an external supplier, the regulated company needs to be able to have access to those documents or records at a later date in case of investigation.

Contracts should clearly state the conditions under which the regulated company, or regulators, can undertake on-site audits to verify conformance to agreed provisions. The level of expert support required on site to facilitate inspections, agreed notifications, and alert levels also should be specified.

4 Service Level Agreements

Where services or other deliverables are requested by one organization and are provided by another, consideration should be given to establishing mutual expectations in a formal SLA.

An SLA is especially useful when the service provider is external to the customer; in such cases, the SLA will usually be included as part of a contract, and clearly state KPIs and the associated fees.

Both organizations involved should assign members of their management team to handle the preparation and ongoing performance monitoring of the SLA, price negotiations, complaints, etc. Depending on the complexity and importance of the service involved, a monthly or annual performance report may be warranted.

A typical SLA will specify:

- contacts on either side
- duration of validity and circumstances triggering reviews
- pre-requisites and customer deliverables or involvement
- scope and nature of the required services
- metrics in the form of KPIs
- records demonstrating fulfillment of specified service levels
- pricing arrangements, including penalties in case of shortcomings

- reports, scope, frequency, distribution
- audit provisions, including preparedness to facilitate inspections from regulatory authorities or other regulators

A mechanism should be established to ensure that all applicable changes within one organization are assessed for any impact on the other organization.

See *GAMP® 4*, Appendix O2, for further guidance (see Appendix 13, reference 1).

5 Audits

Before entering into an outsourcing arrangement, a supplier audit should be considered to assess the external service provider's capability to meet regulatory compliance requirements, and pertinent security policies. Staff from the regulated company's QA should be allowed to repeat this initial audit at suitable intervals, or if certain conditions warrant investigations.

The regulated company is responsible for authorizing the appropriate resolution or mitigation of areas of non-compliance that may arise as a result of an audit of the external service provider. The regulated company should include tracking and monitoring of these within its Corrective and Preventative Actions (CAPA) program to closure in order to demonstrate control.

The external service provider should provide a formal written response to audits conducted by or on behalf of the regulated company, and as appropriate develop and execute remediation plans to address these. In many cases this will require a discussion between the regulated company and the external service provider to agree appropriate resolution.

A company should enter into a non-disclosure agreement with the supplier to specify what information the other party has and what may, and may not, be shared with whom. This could be part of the audit plan or embedded in a SLA or other contractual document.

See *GAMP® 4*, Appendix M2, for further guidance (see Appendix 13, reference 1).

6 Training Requirements

Regulations require that personnel have the appropriate combination of education, training, and experience to perform their assigned tasks. This applies to external supplier personnel as well, and the service provider should ensure that their staff is trained, as appropriate, in regulatory compliance. Such training should be documented.

Appendix 9
Server Management

1 Introduction

The objective of the Server Management process is to ensure that specified requirements for operational availability, performance, and security are consistently fulfilled by the server. An important part of the process is to manage the server configuration and changes needed to meet the objectives.

This Appendix provides guidance to a company to assist in deciding schemes for server management, consistent with the individual needs and criticality of server functions and managed data. All quantitative measures provided in this Appendix are derived from actual situations and are meant to assist companies, and **not** to prescribe certain absolutes.

2 Backup and Restore

Failures of computer systems may result in a loss of data. The backup of electronic data from any given computer platform is consequently essential to preserve the integrity and availability of the data contained on those systems and is considered in the following sections. Also see *GAMP® 4*, for additional guidance (see Appendix 13, reference 1).

2.1 Backup

There are two main types of backup, full and incremental/differential.

A full backup consists of a copy of all data on a given system. An incremental backup is a copy of data that has changed since the last backup cycle was completed.

The quantity of data, and the backup solution available, will dictate the type of backup that can be performed for any particular system.

The following minimum requirements are recommended:

- full backup: once per week, one day per week
- incremental or differential – all other days

Historical backups should be taken as appropriate.

Backups should be monitored to ensure successful completion. The following activities should be applied:

- review of backup logs to ensure successful completion
- proactive assessments conducted on a regular basis to ensure that all required systems are included in the scheduled backup operations
- backup media management

2.2 Verification

Most commercially available backup solutions are capable of performing a verification of the data that has been backed up.

Despite the low risk of malfunctioning modern equipment, an extensive verification of the backup should be made when data is considered critical for the business although the quantity of data may prevent a full verification from being performed.

2.3 Schedules

The type of data should largely dictate the backup schedules. At the enterprise level, data actively in use can be considered to be changing each working day with the backup procedure normally taking place overnight.

Defining the schedule for global systems requires careful consideration, as there may be access by users from other locations. All users should be informed of the backup schedule for these systems so they are aware that there may be periods of unavailability.

Certain application data files cannot usually be backed up while they are in use. Backup schedules may require augmented processes, coordinating their actions with the deactivation of the applications in question.

2.4 Restore

When a restore request is received, consideration should be given to whether the person requesting the restore is authorized to do so, and that they are authorized to view the data being restored.

When restoring data, checks should be made to ensure that more recent versions of the files being restored are not overwritten, unless this is specifically requested. Where required, consideration also should be given to enable recovery to the point of failure.

Restoration beyond clearly defined single records or files may pose a challenge in assuring that all related records are brought back to the same state or point in time to retain overall integrity of the set of records. This can be achieved only through carefully planned interactions with the system/data owner representatives.

2.5 Storage

A process for protecting backup data should be established with the aim of preventing loss, damage, and unauthorized access. The procedure should be documented and provide controls to:

- ensure secure storage facilities with proper access controls, and environmental conditions
- provide indexing and labeling capabilities and means to timely retrieval during inspections
- detect the end of the retention requirements for specific records and notify data owner
- ensure that changes are carried out under change control
- securely destroy data given the necessary authorization

Although manufacturers give an expected lifetime for media, in practice the expected lifetime of the media, when it contains data, is considerably less than this figure.

Provisions should be made to ensure that data are refreshed after a defined period of time to ensure the continuing integrity of the data.

To ensure the ability to recover data (electronic records) in the event of a disaster, and based on an assessment of impact and risk, backup media should be stored at a secure ‘off-site’ facility. ‘Off-site’ in this context means geographically diverse from the location where the system is housed.

See *GAMP® 4*, Appendix O6, for further guidance (see Appendix 13, reference 1).

2.6 Testing

The requirement to test the backup process should encompass any off-site storage solutions.

The test should aim to restore data from historical backups, which may require the handling of off-site backups where they exist. This will ensure that the procedure to recall off-site media works as expected.

Restoring actual backups and comparing against the unchanged original file, where possible, gives the opportunity to check that the whole data path from original backup of the data, through to the final restore, maintains the integrity of the data. This periodic activity may, therefore, certify the process of both the backup and restore procedures.

3 Technical Performance and Capacity Monitoring

The performance of devices and services need to be monitored to ensure that stated or implied expectations can be achieved.

Review results or alarms based on this monitoring will trigger maintenance, update, support, or disaster recovery activities, and therefore, form the basis for a fast active/proactive operation and maintenance.

In order to assure that servers perform as required, surveillance procedures should be developed and alert and action limits defined. For infrastructures mainly supporting administrative type applications, server performance can often be considered a statistical entity that on average should provide a certain level of service. In such cases, the platform manager would be concerned with a very high degree of equipment utilization for economical reasons, and the operational key alarm limits would be set around available storage capacity. For time-critical systems, the platform manager would be more concerned with ensuring enough reserve resources to meet surges in demand. Table A9.1 lists sample performance metrics for a process control server, as an aid in deciding metrics and limits in the context of all relevant deciding factors. In some cases, it poses less risk to product quality attributes or required records to allow a higher load, e.g., on a server, than it would to replace it with a new and more powerful one.

Table A9.1: Example Server Performance Limits

Server Metrics (Real-time system)	Unit	Alert Limit	Action Limit
CPU load	%	>60*	>80*
Server Work Queue	#	>2	>4
Available primary memory	MB	<50*	<10*
Memory swops	Pages/sec	>15	>20
Physical memory (disk space)	% disk access time	>60	>80
Physical memory queue length	#	>2**	>4**
Network interface	kB total/sec	>50***	>80***
* Very much dependant on actual system set-up ** Depends on disk array configuration *** Depends on application and network topology			

Monitoring should take place on a daily basis using applicable software tools. A baseline should be created at the time of installation, and actual values should be considered based on those readings.

When using complex Process/System Management Applications, the monitoring and event reaction could be automated.

See *GAMP® 4*, Appendix O5, for guidance on planning and recording monitoring activities (see Appendix 13, reference 1).

4 Remote Management

When servers are remotely managed, e.g., via outsourcing or offshoring arrangements, it is important to maintain the required level of security. Consideration should be given to the use of secure communication channels.

Appendix 10
Client Management

1 Client Types

Personal Computers (PCs) in the form of stationary PC units, laptops, or 'hand-helds' are used by companies in a variety of roles with distinctly different risk profiles depending upon their use. Those that are connected to the company's network may be prepared and maintained according to a set of client types, e.g., unrestricted, restricted, or controlled as described in Section 5 of this Guide.

As part of the client preparation process, companies may choose to prepare and verify installation scripts, or use an image-generating tool, which mirrors an image of a released software configuration onto PCs.

2 Client Management

The Client Management group or designated individual maintains the expertise and resources required to provide adequate client management services to the company. Some of the main responsibilities of the unit are:

- to acquire formal approval by QA and management representatives of significant changes
- to apply change controls in conformance with procedures (see a Section 6 and Appendix 7 of this Guide)
- to maintain controlled standards for approved hardware and software components, and settings in conformance with security requirements and IT Code of Conduct
- to test PC platforms and corporate office packages to ensure an effective and stable client user environment
- to test or qualify clients against all corporate applications
- to provide and verify installation images or scripts conforming to standards to enable cloning of clients
- to detect and correct errors in both hardware and software
- to assemble documents and installation manuals
- to advise and instruct client supporters and others
- to install security patches on clients
- to scan all standard clients for virus
- to ensure timely update of anti-virus software and signature files
- to administrate centralized maintenance processes
- receipt and registration of all IT equipment
- to manage system time (if not managed by servers) (see Section 5 of this Guide)

- installation and set-up of standard clients
- before delivery of the PC or other equipment, to conduct prescribed tests to ensure that all installation and configuration matters are in order
- to implement handling of used hardware for recycling
- to provide User support
- to provide a general contact to suppliers

3 PC Platforms

PCs should possess enough computing power and connectivity to run the client software and other software that is required by the applications. The company will usually have some basic requirements for specific hardware as a result of long term commercial agreements with specific suppliers. Care should be taken to ensure that the chosen PC brands conform to standards for protection against Radio Frequency Interference (RFI) and Electromagnetic Compatibility (EMC) and other applicable codes.

4 Operating System Platform

Client modifications may be managed centrally by the Client Management Group or locally by the user or a local administrator. Modifications to a set of clients have a greater risk level than modifications to a single instance. All modifications should be managed carefully according to SOPs.

As is the case for servers, the configuration of critical items of the client operating system can be grouped into three categories:

- manufacturer supplied default parameters that remain unchanged
- Manufacturer supplied default parameters that will be altered to address specific company requirements for the client. These parameters also may be changed later during the client life time to optimize performance
- parameters that are supplied blank, and should be populated by the company, and without which the client may not work

5 User Modifications

Company policies may dictate whether clients should be **restricted** from user modification (see Section 5 of this Guide). Many applications, especially those that are GxP regulated, will require that PCs running thick client software be *restricted*, or even *controlled* in order to obtain the necessary confidence that data is not lost or modified in an unauthorized way. Other application (system/data) owners may have similar considerations.

PCs running thin client software are less prone to causing data modifications or availability problems, e.g., when using Web-based client technology.

6 Images or Installation Scripts

Client management often includes the creation and maintenance of images or standard installation scripts or both. This ensures easier management of client preparation processes and demonstration of control.

Besides the operating system and standard office packages, an image could include the company's most used client software rendering subsequent requests for installations unnecessary. This approach would improve reinstallation time, but require more time supporting the image, and although user accounts would not be created on a default basis, security policies could be violated.

Before an image can be released for use, it should be tested against the relevant applications and hardware used in the company.

7 Patch Management

Security patches to be installed on clients should be tested for compatibility with the operating system, office software packages, and client software. A test lab with instances of the hardware and software used in the company should be available, and pilot installations in a no-impact live environment should be made as part of the qualification plan. This should discover potential problems with the patch in the live environment before general rollout.

Besides test requirements, security patch information from the supplier should be made available to the organization. This will ensure awareness of the process and allow owners of critical business applications outside the scope of the PC management group to conduct tests before rollout (see Appendix 6 of this Guide).

Appendix 11
Network Management

1 Introduction

The current dominating network technology is based on internet standards, including the protocols: Internet Protocol (IP) and Transmission Control Protocol (TCP). Consequently, this Appendix focuses on providing recommendations based on those standards. Companies that use other technology may still find useful guidance in this Appendix if they look at the information provided as concepts rather than specific for a single technology.

All quantitative measures provided in this Appendix are derived from actual situations and are meant to assist companies, and **not** to prescribe certain absolutes.

2 Goal

The goal of network management is to identify and employ a variety of tools, applications, and devices to assist managers in monitoring and maintaining network performance in support of other platforms and services.

3 Network Management

When establishing the infrastructure network management process, the network administrator should break down the work process into logically separated steps as indicated below. These steps should enable the company to implement controls commensurate with the size and complexity of the infrastructure, and with the risks associated with the network or network segment in question.

Provisioning and Installation

- Planning
- Design
- Analysis
- Facilities Installation and Maintenance
- Network Installation
- Data Gathering and Analysis

Operations and Maintenance

- Trouble Ticket Administration
- Routine Network Tests

Network Operations Center (NOC)

- Upgrades
- Event/Log Management
- Fault Management/Service Restoration
- Change Management
- Configuration Management
- Performance Management
- Security Management
- Account Management
- Report Management

4 Network Provisioning and Installation

Network provisioning involves the following tasks:

- Network planning and design is the responsibility of the network engineering group which keeps track of new technologies and introduces them as needed in conformance with applicable standards and company requirements.
- Identification of bottlenecks through analysis of traffic and performance data provided by the Network Operation Center (NOC) and introduction of modifications to the network to optimize the use of the equipment.
- Keeping track of new network management tools and introducing them where they would be efficient for gathering statistics and showing trends of traffic patterns for tuning and planning purposes.

5 Network Operation Center (NOC)

The function of the NOC, typically headed by the overall network administrator, is to assume responsibility for the daily operation of the network. The responsibility of the NOC is to provide network services in conformance with SLAs and other applicable requirements and standards, this includes:

- establishing a network management system, e.g., based on SNMP
- ensuring that the gathering of data for performance, tuning, and accounting purposes is functioning and kept current
- restoration of faulty services

- analyzing logs and assuring that all manageable network devices respond as required, e.g., via Syslog, an industry standard used to log information for network devices
- assuring that there are current and easily available configuration backups of all network equipment as well as a documented trace of all configuration changes
- providing management with reports and statistics (KPIs) to ensure that the network is performing optimally and the SLAs are within the agreed limits
- ensuring that approved security procedures are followed by tracking all network accesses and by securing that only permitted access to the network is allowed
- applying tools and procedures to ensure that the availability (defined by different parameters such as latency, bandwidth, and availability) is maintained by analyzing trends, planning upgrades, performing preventive maintenance, and fault correction

6 Common Network Protocols and Tools

The following common protocols and tools can be used to support effective network management.

6.1 Simple Network Management Protocol (SNMP/RFC1157)

Network management system contains two primary elements:

1. Manager
2. Agents

The *manager* is the console through which the network administrator performs network management functions, often accompanied by data management systems to store configuration information, logs of alarms/alerts ('traps' in SNMP context), and performance data history.

Agents are the entities that interface to the actual device being managed. Bridges, hubs, routers, or network servers are examples of managed devices that contain managed objects.

SNMP allows *managers* and *agents* to communicate for the purpose of accessing these objects.

The SNMP has become the *de facto* standard for internet work management. Because it is a simple solution, requiring little code to implement, suppliers can easily build SNMP agents into their products. SNMP also separates the management architecture from the architecture of the hardware devices, which broadens the base of multi-supplier support.

6.2 Syslog (RFC3164)

This protocol has been used for the transmission of event notification messages across networks for many years. Its value to operations and management has led it to be ported to many other operating systems as well as being embedded into many other networked devices.

In its most simplistic terms, the Syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as Syslog servers.

One of the fundamental tenets of the Syslog protocol and process is its simplicity. No stringent coordination is required between the transmitters and the receivers.

There are usually many devices sending messages to relatively fewer collectors. This compilation process allows an administrator to aggregate messages into relatively few repositories.

6.3 Remote Monitoring (RMON) (RFC 1757)

Remote network monitoring devices, often called monitors or probes, are instruments that exist for the purpose of managing and/or monitoring a network. A company may employ many of these devices, up to one per network segment, to manage its networks.

RMON also appears as a software capability that is added to the software of certain network equipment, as well as software applications that could run on servers or clients. Despite the variety of these approaches, the RMON capability serves as a dedicated network management resource available for activities ranging from long-term data collection and analysis or for ad-hoc fire fighting.

7 Network Performance Metrics

Table A11.1 represents actual settings for a network segment and may be used as guidance for a company to decide on its own metrics and limits.

Table A11.1: Example Network Performance Limits

Network Metrics	Unit	Alert Limit	Action Limit
Average load over 24 hrs	%	>10	>20
Peak load	%	>40	>80
Collision rate	% of net time	>0.1	>1.0
Discards (lost packages)	% of net time	>0.1	>0.5
BCast/MCast (simultaneous transmission to many receivers)	% of net time	>2	>5
Switch CPU-load	% of max	>50	>70

A monitoring frequency of one to four times a month should be considered; in larger organizations, monitoring would be automated and run almost continuously.

Appendix 12
Glossary

Glossary

1 Definitions

Assessment

Investigation of processes, systems, or platforms by a subject matter expert or by IT Quality and Compliance. An assessment does not need to be independent in contrast to audit.

Audit (ISO/GAMP®)

Systematic, independent, and documented process for obtaining evidence and evaluating it objectively to determine the extent to which agreed criteria are fulfilled.

Building Block

Group of components defined, installed, and controlled by a set of specifications defined by the company to maximize opportunity for re-use.

Certification

The process of confirming that a system or component complies with a specific standard, e.g., a network installation may be certified against the ISO/IEC 11801 standard. In the context of this Guide, 'certification' does not imply involvement of an authoritative body, cf. 'Certification Authority.'

Certification Authority (CA)

A trusted third-party organization or company that creates and manages digital certificates to distribute public keys and other information.

Change Control (Generalized based on GAMP®)

A formal process by which qualified representatives from appropriate disciplines review proposed or actual changes to an object. The main objective is to document the changes and ensure that the object is maintained in a state of control.

Client (in context of Client/Server)

The networked computing device enabling the user to access a client/server system; this encompasses desktops, laptops, palmtops, etc. Note: A thick client performs the bulk of data processing operations locally using software stored on the client, in contrast to a thin client, which has greater reliance on the server. In both cases, data is typically stored on the server.

Compliance

The practice of obeying rules or requests made by people in authority, e.g., adherence to certain specified standards such as regulations, good practices, SOPs, SLAs, or specified (user) requirements.

Computerized System

All of the computers with their associated hardware, software, and documentation needed to satisfy specific user requirements, e.g., Laboratory Information Management System. Note: This Guide does not consider standardized components such as routers and switches to be computerized systems.

Configuration Management

Those activities necessary to precisely define an object at any point during its life cycle, e.g., manage all constituents of a specific server building block.

Data Management Software

All the software in the technology stack between the operating system and the application software, e.g., Database Management Systems, middleware, and application enabling software.

Disaster

Any event (i.e., fire, earthquake, power failure, etc.) which could have a detrimental effect upon an automated system or its associated information.

Disaster Recovery Plan

A plan to resume a specific essential operation, function, or process of an enterprise.

Firmware

Software (firmly) embedded in hardware components. Note: Despite its name, current technology will often permit firmware to be updated post installation.

GxP Application

Software entities which have a specific user defined business purpose that must meet the requirements of a GxP regulation.

GxP Regulation

The underlying international life science requirements such as those set forth in the US FD&C Act, US PHS Act, FDA regulations, EU Directives, Japanese MHLW regulations, or other applicable national legislation or regulations under which a company operates.

Infrastructure Process (Based on ITIL)

A connected series of actions with the intent of satisfying a purpose or achieving a goal in support of managing the infrastructure, e.g., the primary goal of the problem management process is to facilitate the timely collection, trending, and resolution of real and perceived problems.

Infrastructure Services

A computerized part of the infrastructure controlled by personnel, or processes, e.g., printing service, email service, or file storage service.

Infrastructure System

A system designed or configured to support infrastructure processes – in contrast to supporting primary business processes.

Interface (FDA)

A point of communication between two or more processes, persons, or other physical entities.

IT Infrastructure

The aggregation of a company's computer platforms and services including their associated processes, procedures, and personnel.

Logical Access Controls

The features embedded in software programs combined with specific settings (Access Control Lists) that are used to authenticate a user requesting access to computerized resources.

Network

1. An arrangement of nodes and interconnecting branches (FDA).

2. A system (transmission channels and supporting hardware and software) that connects several remotely located computers via telecommunications (ISO).

Network Topology

The specific physical (real) or logical (virtual) arrangement of the elements of a network. Note: Two networks have the same topology if the connection configuration is the same although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types.

Periodic Review (GAMP®/PDA)

A documented assessment of the documentation, procedures, records, and performance of a computer system to determine whether it is still in a validated state and what actions, if any, are necessary to restore its validated state. The frequency of review is dependent upon the system's complexity, criticality, and rate of change.

(Infrastructure) Platform

The hardware and software which must be present and functioning for an application program to run (perform) as intended, e.g., RDBM platforms, network platforms, or server hardware platforms.

Privileged Access

Access to resources or data with the capability of performing administrative tasks, e.g., create, modify, or delete user profiles in contrast to ordinary end-user access levels.

Qualification

Process of demonstrating whether an entity is capable of fulfilling specified requirements. Note: In the context of meeting regulatory requirements, 'qualification' implies adherence to strict documentation requirements, reviews, and approvals.

Quality Assurance (QA)

The planned systematic activities necessary to ensure that a component, module, or system conforms to established technical requirements (ISO).The activity of, or group responsible for, ensuring that the facility and systems meet GxP requirements (based on ISPE).

Quality Control (QC)

The operational techniques and procedures used to achieve quality requirements (FDA). Group responsible for checking or testing that specifications are met (based on ICH Q7A).

Quality Management System (ISO)

The organizational structure, responsibilities, procedures, processes, and resources for implementing quality management.

Risk (ISO)

Combination of the probability of occurrence of harm and the severity of that harm.

Risk Assessment

Overall process comprising a risk analysis and a risk evaluation:

- **Risk Analysis**

  Systematic use of available information to identify hazards and to estimate the risk.

- **Risk Evaluation**

  Judgment, on the basis of risk analysis, of whether a risk which is acceptable has been achieved in a given context. (ISO 14971 definition modified by GAMP)

Risk Management (ISO)

Systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, and controlling risk.

Security

The protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations.

Subject Matter Expert (SME)

A person who possesses a documented deep comprehension of the theory and concepts within his or her field of work.

Supplier

Any organization or individual contracted directly by the customer to supply a product or service.

Testing (IEEE)

The process of exercising or evaluating a system or system component by manual or automated means to verify that it satisfies specified requirements or to identify differences between expected and actual results.

Validation (FDA)

Establishing documented evidence which provides a high degree of assurance that a specific process will consistently produce a product meeting its pre-determined specifications and quality attributes.

Virus

Generic term for all the various types of malicious code that have been designed to breach a company's security measures.

2 Acronyms and Abbreviations

ANSI	American National Standards Institute
BIPM	Bureau International des Poids et Mesures, provider of UTC, the coordinated universal time
BS	British Standard (e.g., BS 7799)
CAPA	Corrective and Preventive Action
CDMS	Clinical Data Management System
CFR	Code of Federal Regulations (e.g., 21 CFR Part 11)
CI	Configuration Item
CIL	Configuration Item List
CM	Configuration Management
CPG	Compliance Policy Guide
CPU	Central Processing Unit
CSV	Computerized System Validation
CV	Curriculum Vitae
DBMS	Database Management System
DS	Design Specification
EIS	Enterprise Information System
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

ERP	Enterprise Resource Planning
EU	European Union
FDA	Food and Drug Administration
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	Good 'x' Practice, where 'x' one of: Clinical, Distribution, Laboratory, Manufacturing
HW	Hardware
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
IQ	Installation Qualification
IS	Information Systems
ISO	International Organisation for Standardization
ISPE	International Society for Pharmaceutical Engineering
IT	Information Technology
ITIL®	Information Technology Infrastructure Library
IVRS	Interactive Voice Response System
KPI	Key Performance Indicator
LAN	Local Area Network
LIMS	Laboratory Information Management System
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
OGC	Office of Government Commerce

OQ	Operational Qualification
OS	Operating System
OSI	Open Systems Interconnection
PC	Personal Computer
PDA	Parenteral Drug Association
PIC/S	Pharmaceutical Inspection Cooperation Scheme
PQ	Performance Qualification
QA	Quality Assurance
QM	Quality Management
QMS	Quality Management System
RFI	Radio Frequency Interference
SAN	Storage Area Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SQL	Structured Query Language
STP	Shielded Twisted Pair
SW	Software
TAI	Temps Atomique International (International Atomic Time)
TSB	Telecommunication Systems Bulletin
UPS	Uninterruptable Power Supply
URS	User Requirement Specification
US	United States
UTC	Coordinated Universal Time (Language independent international abbreviation)
WAN	Wide Area Network
WAP	Wireless Access Point

Appendix 13
References

References

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

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

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

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

5. 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.

6. 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.

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

8. ISO/IEC 14763 Information Technology – Implementation and Operation of Customer Premises Cabling. The Official Web site for the ISO may be visited at http://www.iso.org.

9. ISO/IEC 11801:2002 Information Technology – Generic Cabling for Customer Premises. The Official Web site for the ISO may be visited at http://www.iso.org.

10. 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.

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

12. NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems

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

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

15. "Risk Assessment for Use of Automated Systems Supporting Manufacturing Processes, Part 1 - Functional Risk," ISPE/GAMP® Forum, *Pharmaceutical Engineering*, May/June 2003, Vol. 23, No. 3 pp. 16-26.

16. RFC 2196, "*Site Security Handbook,"* B. Fraser, SEI/CMU, September 1997.

17. ISO 7498 Information Processing Systems – Open Systems Interconnection – Basic Reference Model. The Official Web site for the ISO may be visited at http://www.iso.org.

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