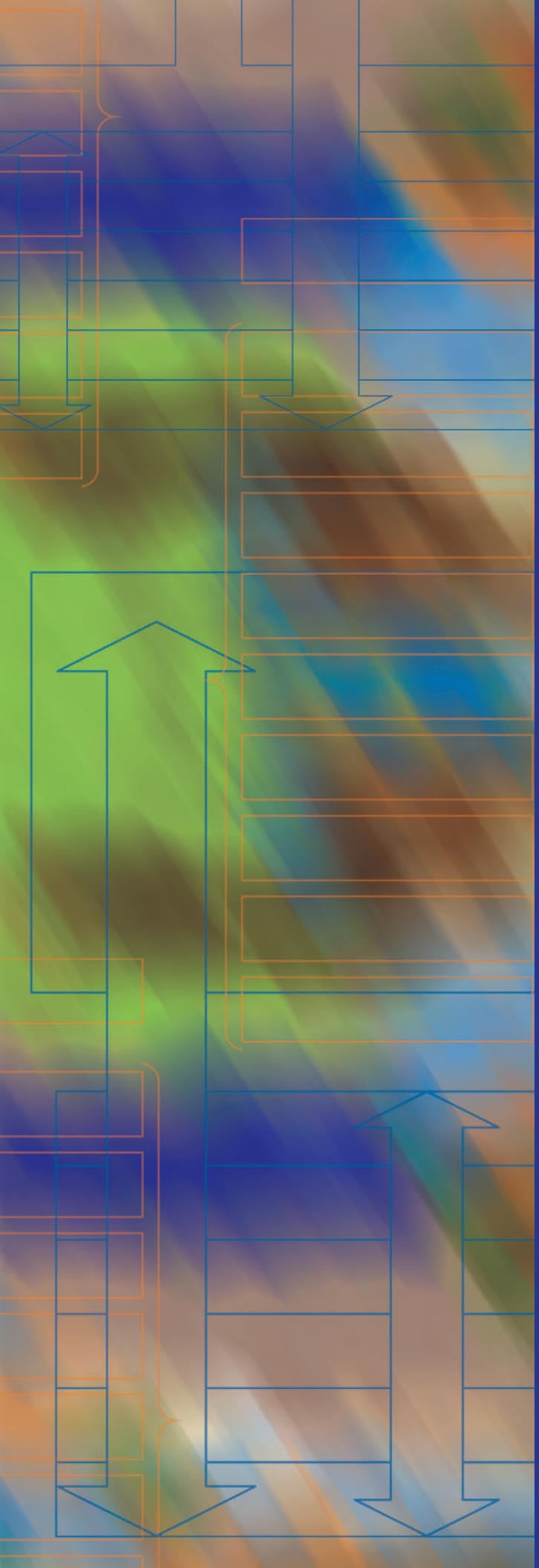


ISPE | GAMP

GOOD PRACTICE GUIDE:

IT Infrastructure Control and Compliance

Second Edition

GOOD PRACTICE GUIDE:

IT Infrastructure Control and Compliance

Second Edition

Disclaimer:
This Guide is intended to provide a structured approach to achieving IT Infrastructure control and compliance, for traditional and cloud-based platforms. ISPE cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

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

All trademarks used are acknowledged.

ISBN 978-1-946964-00-7

Preface

This document, the *ISPE GAMP® Good Practice Guide: IT Infrastructure Control and Compliance (Second Edition),* is intended to be used in conjunction with *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems* and other ISPE GAMP® guidance documents.

This Second Edition was developed by the ISPE GAMP® Community of Practice (COP) and was undertaken to expand the scope of the original Guide to include guidance on the emergence of cloud and virtualized technologies. Updates to this Guide relate to the adoption of virtualized and outsourced infrastructure model.

Acknowledgements

The Guide was produced by a Task Team led by Stephen R. Ferrell, CISA, CRISC (Thermo Fisher Scientific, USA). The work was supported by the ISPE GAMP® Community of Practice (COP).

Core Team

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

Ulrik Hjulmand-Lassen	Novo Nordisk A/S	Denmark
Shana D. Kinney	Canon BioMedical Ltd.	USA
Kevin C. Martin	Azzur Group	USA
Ashish Moholkar	Novartis	USA
Michael F. Osburn	Cornerstone OnDemand	USA
Arthur “Randy” Perez	Novartis (retired)	USA
Mike Rutherford	Eli Lilly and Company	USA
Jason Silva	ByteGrid	USA
Eric J. Staib	PRA Health Sciences	USA
René van Opstal	van Opstal Consulting	Netherlands
Anders Vidstrup	NNIT A/S	Denmark

Other Contributors

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

Chris Clark	TenTenTen Consulting	United Kingdom
Hugh Devine	CompliancePath Ltd.	Scotland
Scott Johnstone	Scottish Lifesciences Association	Scotland
Sion Wyn	Conformity Limited	United Kingdom

Regulatory Input and Review

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

Krishna Ghosh, PhD	US FDA/CDER/OPQ	USA
John F. Murray	US FDA/CDRH/Office of Compliance	USA
Robert D. Tollefsen	US FDA/ORA/OMPTO/OPQO/DPQP/ Pharm. Quality Operations Branch	USA
Jason Wakelin-Smith	MHRA	United Kingdom

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

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

Company affiliations are as of the final draft of the Guide.

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

www.ISPE.org

Table of Contents

1 Introduction

1.1 Background

Since the publication of the first edition of this Guide in 2005, there has been a significant leap in the technologies that make up modern Information Technology (IT) Infrastructure, including:

- The use of virtualization technologies
- The use of cloud computing
- The delivery of GxP applications "as-a-service"
- Outsourcing and the increased use of third-party datacenters

The introduction of virtualization technologies that allow the sharing, combining, and maximization of resources presents the regulated industries with unprecedented benefits. The underlying components of IT Infrastructure, however, have remained hardware centric.

The accelerated use of virtualization technologies has prompted updated guidance from most of the major global regulatory agencies. The EU, via Annex 11 [1], and the most recent Good Manufacturing Practice (GMP) computer Annexes from the Chinese Food and Drug Administration (CFDA) both require that IT Infrastructure is qualified. The US FDA defined "cloud infrastructure" as a computer system in their Draft Data Integrity Guidance [2]. Important changes include:

- The revision of EU GMP Annex 11 [1] and EU GMP Chapter 4 [3] (both adopted for wider use by PIC/S)
- Increased regulatory focus on the wider aspects of data integrity (e.g., the US FDA Draft Guidance on "Data Integrity and Compliance with CGMP" [2])

Two new appendices have been added to this Guide to reflect the increased adoption of virtualization technologies and the engagement of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and suppliers (see Appendix 11 and Appendix 12).

1.2 Overview

Regulated companies have an increasing dependency on computerized systems. The prevalence of new technology has presented regulated companies with significant technological advantages, as well as a changed compliance model.

New technologies include cloud-based infrastructure and three cloud service models:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

These service models are collectively referred to as XaaS for the purposes of this Guide.

For regulated companies seeking to outsource IT infrastructure, the boundaries of the regulated entry and associated risk may be increased, if not adequately controlled.

The validated status of GxP applications that are dependent upon an underlying IT Infrastructure[1] can be compromised if the 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 may be seriously affected whilst a problem is resolved.

Data integrity can also be affected by problems related to IT Infrastructure, leading to increased risks which can in turn affect product quality or patient safety. Aspects of the IT Infrastructure may have a significant impact on data integrity.

IT Infrastructure should be brought into initial conformance with the regulated company's established standards. This can be achieved through a planned qualification (specification and verification) process, building upon recognized industry good IT practices. Once in conformance, this state should be maintained by documented standard processes/procedures and quality assurance activities.

The effectiveness of these Standard Operating Procedures (SOPs) should be periodically verified. Key aspects to consider include:

- Supplier assessment and management
- Installation and operational qualification of infrastructure components (including facilities)
- 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 IT Infrastructure processes
- Service level agreements with XaaS providers
- Service level agreements with third-party datacenter providers
- Security management in relation to access controls, availability of services, and data integrity
- Data storage, and in relation to this security, confidentiality and privacy
- Backup, restore, and disaster recovery
- Archiving

1.3 Purpose

This Guide is intended to provide comprehensive guidance on meeting regulatory expectations for compliant IT Infrastructure platforms (traditional and cloud-based), including the need to identify, qualify, and control those aspects impacted by GxP regulations.

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

[1] Throughout the Guide "IT Infrastructure" and "infrastructure" are used synonymously to indicate a collection of platforms, services, and facilities including their associated processes, procedures, and personnel.

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

This Guide is intended to support the qualification of IT Infrastructure technologies across both the physical and virtualized space including but not limited to:

- Mobile applications
- Wired and wireless networks
- Web portals
- XaaS services and platforms

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 describes a scalable 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 industry best practices for the design, qualification, and operation of an IT Infrastructure with emphasis on the qualification requirements of the major components.

1.4 Scope

This Guide addresses compliance with applicable GxP regulations and considers:

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

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 Food and Drug Administration (FDA) regulations and Compliance Policy Guides [4]
- Relevant parts of EU GMPs, e.g., Annexes 11 and 15 [1, 5]
- PIC/S Guidance [6]
- National Institute of Standards and Technology (NIST) Publications [7]
- FedRAMP [8]

- Cloud Security Alliance [9]

This Guide covers a range of IT Infrastructures, from those found in regulated companies operating globally, to isolated or semi-isolated GxP regulated infrastructures and includes guidance related to XaaS solutions and cloud-based platforms. Additional considerations for XaaS situations are noted where applicable; however, it should be noted that all aspects of the Guide are applicable to XaaS engagements regardless of whether supplemental XaaS information is provided.

This Guide also may prove useful to managers of IT Infrastructure 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 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.

1.5 Benefits

This Guide describes a horizontal, or platform based, approach to qualification and audit of IT Infrastructure in order to avoid unnecessary effort. Benefits of a horizontal approach include:

- Higher level of standardization throughout the entire system 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 traditional IT Infrastructure platforms, and well controlled XaaS platforms
- Cloud-based or third-party service delivered platforms presented to regulated companies.
- 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 [10].
- 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 regulated company

1.6 Objectives

IT Infrastructure Control and Compliance should target those IT related aspects that could potentially affect product quality and public health. Applicable methods also need to be practical and efficient in order to be effective. In support of this, the following guiding principles are applicable to this Guide:

- Provision of a consistent, standalone document that would guide stakeholders to take advantage of current best practices in the field to achieve compliance with applicable regulations
- Definition infrastructure, cloud models (XaaS), and other key terms and concepts referenced or introduced
- Provision of guidance on best practice for network, client, and server qualification and management
- Provision of guidance on security issues in the light of ISO 27001 [11]
- Consideration of change control in regard to virus signature updates and security patches

1.7 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 (QMS)
- 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

- SOPs
- Periodic reviews
- Infrastructure security

- Upgrade and patch management
- Outsourcing
- Server management
- Client management
- Network management
- XaaS models
- Virtualization

1.8 Key Concepts

1.8.1 Traditional Horizontal Platform Based Approach to IT Infrastructure

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

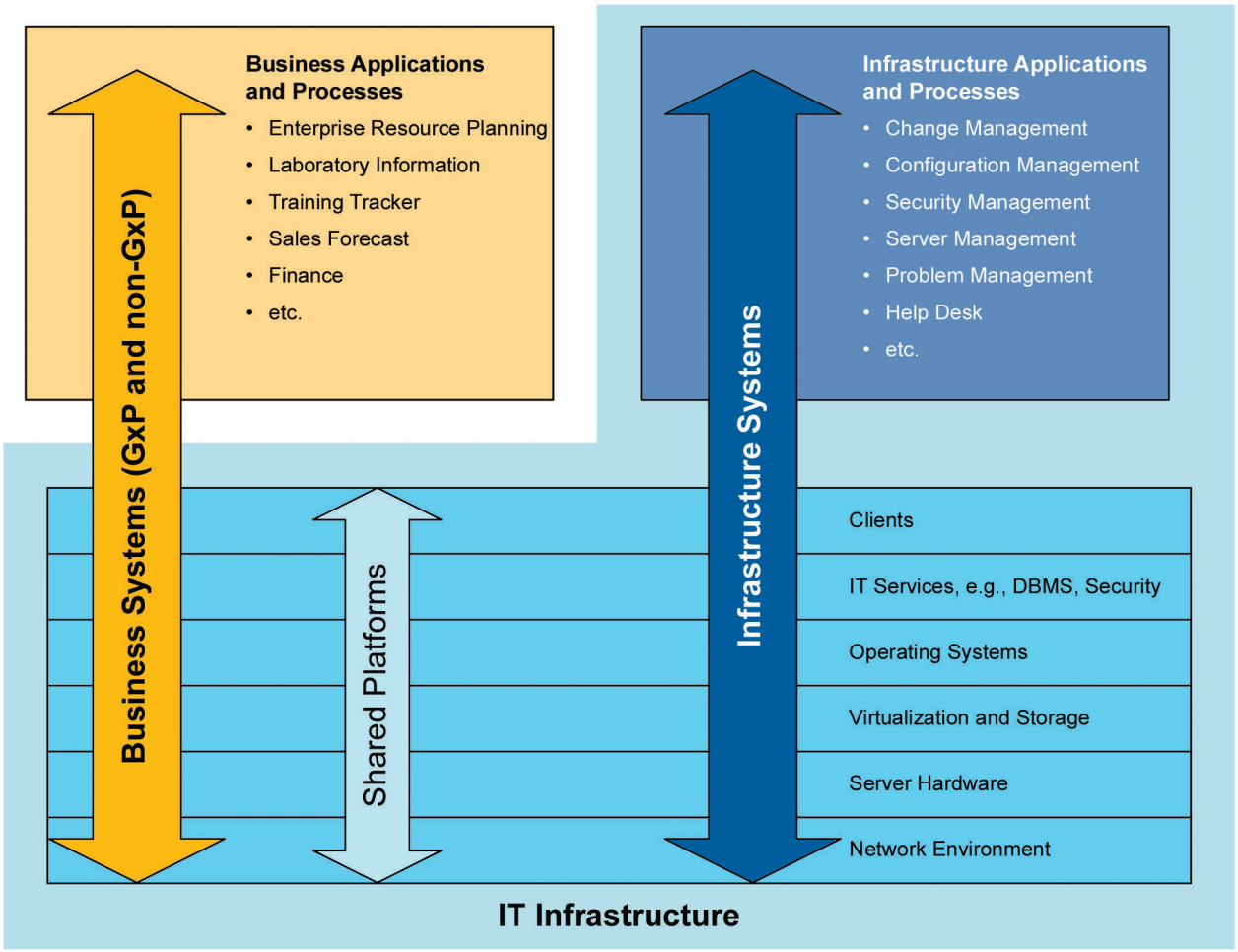
- Platforms to run the business applications[2] (e.g., Clinical Data Management System (CDMS), Interactive Voice Response System (IVRS), Laboratory Information Management System (LIMS), or Enterprise Resource Planning (ERP))
- IT Infrastructure processes that facilitate a capable and controlled IT environment
- 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 regulated company's primary business.
[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, the platform components should be qualified separately from the applications. This can avoid unnecessary duplication of activities and effort and means that:

- Adding or changing a business application would require only the validation of the application
- 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.

1.8.2 Cloud Computing

The NIST definition of cloud computing is:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* [12]

Virtualization and cloud computing may be used together to build a cloud infrastructure. Cloud computing is based on virtualization and is the core component in cloud computing. See Appendix 12 for more information on virtualization.

A quality agreement should be established with the supplier of the cloud services.

The terminology used in this Guide is sourced from the NIST Special Publication 800-145, The NIST Definition of Cloud Computing [12].

1.8.2.1 Service Models for Cloud Computing

Cloud computing is accessed as a service. There are three service models:

1. Infrastructure as a Service (IaaS)

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

2. Software as a Service (SaaS)

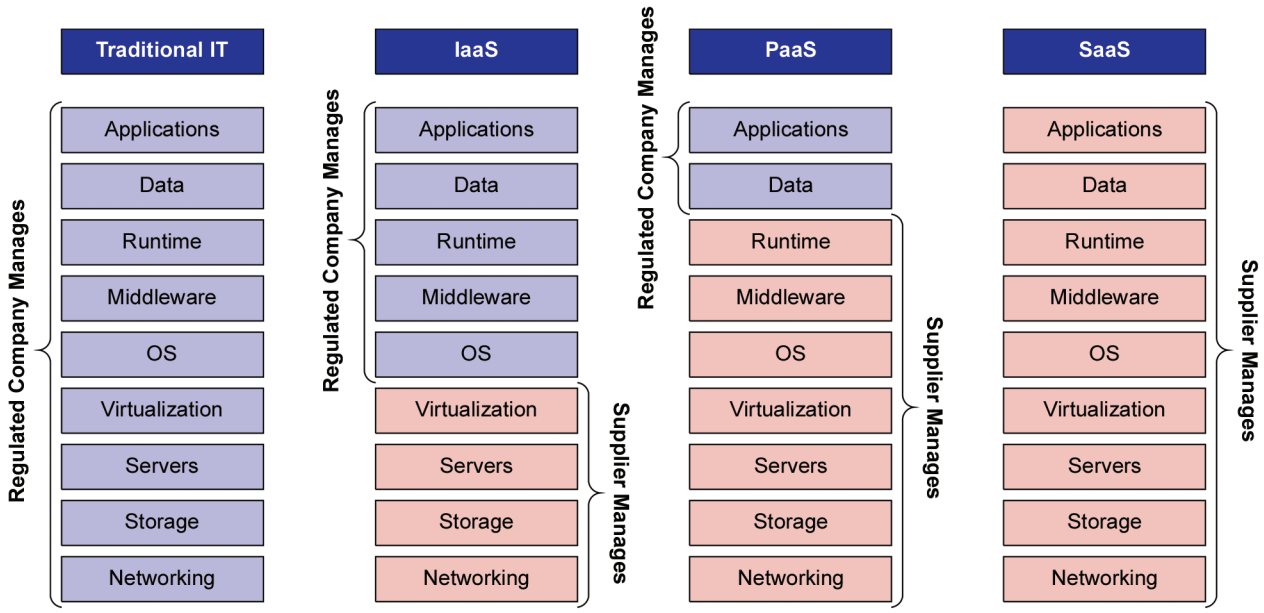
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does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

3. Platform as a Service (PaaS)

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

Figure 1.2 illustrates the three service models in relation to traditional IT Infrastructure.

Figure 1.2: XaaS Management Models



Advantages for IaaS, SaaS, and PaaS solutions include:

- Large flexibility in capacity and services
- Easy to expend or reduce
- Reduced internal hardware foot print
- Reduced capital costs
- Outsourced control and maintenance
- High availability
- Less need for IT knowledge and IT investment

1.8.2.2 Deployment Models for Cloud Computing

There are four deployment models for cloud computing:

1. Private Cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

2. Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

3. Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

4. Hybrid Cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

1.8.2.3 Risks from Cloud Computing

Cloud computing introduces a flexibility in resource capacity, but also introduces new risks to regulated companies. These risks include:

- Less or no control over the datacenter
- Several suppliers working together to provide the infrastructure
- Less control over the infrastructure
- Less control over the data
- Less control over applied services
- Data and systems are outside the companies' network
- Different qualification approach required

Risks need to be assessed and managed.

1.8.3 Key Terminology

Requirements

Requirements for infrastructure platforms and services are usually specified in documents such as Service Level Agreements (SLAs). Requirements are usually described in broad terms. This allows platform management groups to respond and keep pace with platform technology and requests for transmission bandwidth and development in computing power. It is especially the case for larger infrastructures, usually 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, which mostly support real-time applications, such as process control, the requirement specifications may be more precise.

Commissioning

A well planned, documented, and managed engineering approach to the start-up and turnover 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 (ISPE Glossary [13]).

In the context of IT Infrastructure, this concept may be useful for aspects of IT Infrastructure that do not support GxP activities and as part of a wider qualification (specification and verification) approach for all infrastructure.

Qualification

Qualification is the process of demonstrating whether an entity is capable of fulfilling specified requirements (ISPE Glossary [13]).

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) (see Chapter 3). The qualification scope and depth should be determined by a Risk Assessment (see Chapter 4) and planned (see Chapter 5).

Commissioning activities may produce required documentation and help to avoid repeat testing during qualification.

Basic requirements of qualification include:

- Quality Assurance (QA) involvement should be at a strategic level and should provide oversight
- 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 where the focus should be on qualification of components. EU GMP Annex 11 [1] states:

> *"Infrastructure should be qualified".*

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

Verification

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (*ISPE GAMP® 5* [14]). **Note:** monitoring and auditing methods, procedures and tests, including random sampling and analysis, can be used in the verification of the formal system (ISO 14644-6 [15]).

1.9 Specific Aspects and Risks Associated with Infrastructure Outsourcing, Virtualization, and Cloud Adoption

Consideration should be given to specific risks of IT Infrastructure outsourcing, virtualization, and cloud adoption. Appropriate actions should be taken. Table 1.1 presents an overview of risk considerations associated with outsourced infrastructure and identifies sections that provide more comprehensive discussion and guidance on these topics. Table 1.1 uses specific terminology for these risk considerations, so this terminology is described below.

1.9.1 Explanation of Risk Considerations

Willingness to Support Assessment

The willingness to support assessment varies widely between XaaS providers. The need to maintain product and patient safety should be central to the provider selection process. The foundations of a provider's infrastructure are key to understanding their XaaS capabilities, e.g., a disaster recovery site that shares an Internet Service Provider (ISP) or a power grid with a primary site. This type of infrastructure aspect may not be identified as an issue in a traditional audit.

Understanding of GxP Regulations

A XaaS provider's knowledge of GxP regulations should be considered. XaaS providers may already have some understanding of GxP requirements. Awareness and application of traditional infrastructure qualification and controls can vary between providers.

Robustness of Software Development

SaaS/PaaS vendors should be able to provide an overview of their software development approach and associated testing in a similar way to software suppliers. Their approach to change and configuration management is key, as providers may have their own upgrade schedule. The regulated company will not be able to dictate change and configuration scheduling in such cases.

Upgrade Frequency

The upgrade frequency that a SaaS/PaaS provider is following should be understood. This can have a direct impact on the validated state of the system.

Site Qualification Activities

The suitability and effectiveness of specific provider qualification activities should be evaluated.

Data Architecture

Before selecting an infrastructure model, the Data Architecture requirements of the scoped system must be considered. A cross purpose platform may require conformance to multiple Electronic Data Interchange (EDI) standards and so interoperability is a key consideration for the downstream infrastructure.

Deployment Model (from highest to lowest risk): Public, Hybrid, Community, Private

The deployment model applied should be considered when engaging a SaaS/PaaS solution. A properly configured and managed private cloud offers the most control and security; public clouds by their nature are the least secure. Community and hybrid clouds offer a level of control and security in between a private cloud model and a public cloud model.

While the provider may offer a robust service, the regulated company should also consider that public clouds will have a very wide and varied tenant population. It is unlikely that each tenant in a public cloud shares the same risk and security constraints as a GxP regulated company.

Cloud Infrastructure Qualification Activities

The suitability and effectiveness of specific provider qualification activities should be evaluated.

Willingness to Execute a Quality Agreement

The XaaS provider should be willing to enter into a suitable Quality Agreement with the regulated company. As outsourcing has become more commonplace, Quality Agreements between a regulated company and its supplier have taken on additional importance.

Data Location(s)

It can be difficult to establish immediately where data is physically located for a XaaS. The physical and geographic boundaries of a XaaS provider's solution should be understood. Data location can be a good indicator of other performance factors, such as uptime, and can be critical from a data privacy perspective. Local or regional regulations and laws may have specific requirements regarding data location.

Cyber Security

Cyber security is a challenging aspect of a XaaS engagement. It is not the intention of this document to recommend any specific cyber security platforms or approaches, but rather to suggest that a regulated entity ensure that they have fully vetted a provider's cyber security practices. While most SaaS/PaaS providers will provide login methods via an encrypted website (Hyper Text Transfer Protocol Secure (HTTPS), etc.) this does not address the robustness of the underlying cloud infrastructure. It is critical to understand the steps that a Cloud Service Provider (CSP) has taken to guard their solution against cyber-attack, including where the security handoff occurs between the CSP and the SaaS/PaaS vendor.

Geography

Where a datacenter is located can be a key risk factor relative to the likelihood of a major service disruption. Regulated entities should enquire as to the location of proposed datacenter sites paying particular attention to:

- Recent or likely *force majeure* events
- Political stability of the chosen locale
- Robustness of the power grid
- Proximity to flight paths, railway lines, major roadways, and bodies of water

Redundancy (Internet Service Provider(s), Utilities, Generators, Emergency Power Systems, etc.)

The size, complexity, and redundancy profile of datacenters varies considerably. Key factors to consider are the:

- Robustness of the utility providers serving the datacenter
- Number of generators and their prime rating
- Battery and Uninterruptible Power Supply (UPS) systems

- Flood prevention and warning systems
- Building automation and management systems
- Heating, Ventilation, and Air Conditioning (HVAC) and cooling capacity
- Fuel tanks and refueling prioritizations
- Redundant nature of the aforementioned systems
- Number of ISPs serving the datacenter(s)
- Whether blended Internet Protocol (IP) services are an option

Physical Security

Physical security can be a key risk consideration for all XaaS engagements. The following should be considered:

- Crash proof fencing
- Prevalence of Closed Circuit Television (CCTV) cameras
- Who monitors the cameras?
- Where are the videos stored and for how long?
- Biometric, card/key fob systems
- Crush bars
- Dead man doors
- Onsite security personnel (including their rotas and coverage hours)

Capacity

Capacity should be considered from several perspectives, e.g.:

- Does the XaaS track capacity; if not why not?
- How much capacity exists for future growth?
- How often is capacity reassessed?
- How quickly can capacity be increased?
- What are the methods for notifying the regulated entity of physical plant, cloud infrastructure or XaaS deployment capacity change?
- How are such changes controlled?

Staff Training

While training methods records vary greatly, providers should ensure that the personnel providing the XaaS delivery are able to consistently deliver the service in a repeatable fashion. Lack of personnel training can have detrimental effects on cyber security, data integrity, and the overall uptime and performance of a delivered application.

Managed Services (Customer Portal, Virtual Machine (VM)/Service Provisioning, etc.)

Understanding service levels is a key risk factor for any outsourced engagement. It can be particularly difficult in a XaaS relationship given the many combinations of providers who may come together to deliver the XaaS solution to the regulated company. Providers may offer a portal for requests; self-service options all the way up to prepackaged and verified cloud bundles. The level of managed service that can be expected from a XaaS provider should be clearly understood before beginning an engagement.

Uptime

Datacenters and Cloud Service Providers (CSPs) will advertise some level of available uptime. Colloquially referred to as two, three, or four nines, and presented as: 99%, 99.9%, 99.99%, and 99.999%. Enterprise class datacenters may report 100% uptime over extended periods. Regulated companies should be clear within their SLA how much downtime they can expect for their system and make sure that this is acceptable within the intended use of the system(s) in scope.

Table 1.1: Topics Related to Infrastructure Outsourcing, Virtualization, and Cloud Adoption

Topic	Risk Considerations for Outsourced Infrastructure	For Further Information, see
Outsourcing of owned infrastructure to a third-party datacenter	Co-location of IT Infrastructure has become common and can offer a regulated company the lowest risk way to take advantage of a third-party datacenter facility. Considerations for a co-location provider include: • Willingness to be assessed and to provide appropriate information to support risk assessments and quality agreements • Understanding of GxP Regulations • Site Qualification activities • Ability to execute a Quality Agreement • Complementary certifications: SSAE 16 [16], ISO 9001 [17], ISO 27001 [11], PCI [18], EHNAC [19], FISMA [20], FedRAMP [8], HITRUST [21], etc. • Cyber security • Geography • Redundancy (ISP(s), utilities, generators, emergency power systems, etc.) • Physical security • Capacity • Staff training • Hands on services (backup media switching etc.) • Uptime	Appendix 11
IaaS provided by a CSP from their own datacenter(s)	Many regulated companies are using IaaS suppliers to some degree. Depending on the risk factors listed below, CSPs can vary widely from fairly high risk to relatively low risk suppliers. Considerations for a IaaS provider include: • Willingness to be assessed and to provide appropriate information to support risk assessments and quality agreements • Understanding of GxP Regulations • Site Qualification activities • Ability to execute a Quality Agreement • Nature of cloud (from highest to lowest risk): public, hybrid, community, private	Appendix 11

Table 1.1: Topics Related to Infrastructure Outsourcing, Virtualization, and Cloud Adoption (continued)

Topic	Risk Considerations for Outsourced Infrastructure	For Further Information, see
IaaS provided by a CSP from their own datacenter(s) (continued)	• Complimentary certifications: SSAE 16 [16], ISO 9001 [17], ISO 27001 [11], ISO 27017 [22], PCI [18], EHNAC [19], FISMA [20], FedRAMP [8], HITRUST [21], etc. • Certification boundaries (holistic or limited scope) • Cyber security • Geography • Redundancy (ISP(s), utilities, generators, emergency power systems etc.) • Physical security • Capacity • Staff training • Managed services (customer portal, VM/service provisioning etc.) • Uptime • Help Desk support • Change management • Termination of the contract and deletion of data, including avoiding lock-in and ensuring long-term availability of GxP data	Appendix 11
IaaS provided by a CSP from a third-party owned datacenter(s)	Many companies are offering IaaS options from cloud infrastructure located in third party owned datacenters. Regulated companies should fully understand the relationship from a performance and quality perspective when engaging in a multi-partner IaaS delivery. Aspects that should be considered include: **Note:** "C" denotes CSP, "D" denotes datacenter(s) • Willingness to be assessed and to provide appropriate information to support risk assessments and quality agreements – C & D • Understanding of GxP Regulations – C & D • Site Qualification activities – C & D • Cloud Infrastructure Qualification activities – C • Ability to execute a Quality Agreement – C & D • Nature of cloud (from highest to lowest risk): public, hybrid, community, private – C • Data location(s) – C • Complimentary Certifications: SSAE 16 [16], ISO 9001 [17], ISO 27001 [11], ISO 27017 [22], PCI [18], EHNAC [19], FISMA [20], FedRAMP [8], HITRUST [21], etc. – C & D • Certification boundaries (holistic or limited scope) – C & D • Cyber security – C • Geography – C & D • Redundancy (ISP(s), utilities, generators, emergency power systems etc.) – D • Physical security – D • Capacity – C & D • Staff training – C & D • Managed services (customer portal, VM/service provisioning etc.) – C & D • Uptime – C & D • Help Desk Support – C & D • Change management – C • Termination of the contract and deletion of data, including avoiding lock-in and ensuring long-term availability of GxP data – C • Data processing operation • Third party use of subcontractors – C	Appendix 11

Table 1.1: Topics Related to Infrastructure Outsourcing, Virtualization, and Cloud Adoption (continued)

Topic	Risk Considerations for Outsourced Infrastructure	For Further Information, see
SaaS/PaaS (provider using own infrastructure co-located into one or more third-party datacenters)	Some SaaS/PaaS providers have procured their own infrastructure and manage their own cloud from one or more third-party datacenters. In this relationship, the provider is supplying the regulated organization with an application and the cloud infrastructure to run it. They have outsourced the facility management to one or more parties. In addition to the usual software supplier quality assessment, the regulated company should also consider the SaaS/PaaS provider's competency and knowledge related to cloud infrastructure and cyber security. Aspects that should be considered include: **Note:** "aS" denotes the SaaS or PaaS provider, "D" denotes datacenter(s) • Willingness to be assessed and to provide appropriate information to support risk assessments and quality agreements – aS & D • Understanding of GxP Regulations – aS & D • Robustness of System Development Life Cycle (SDLC) – aS • Single or multi-tenant environment – aS • Upgrade frequency – aS • Site Qualification activities – aS & D • Nature of cloud (from highest to lowest risk): public, hybrid, community, private – aS • Cloud Infrastructure Qualification activities – C • Ability to execute a Quality Agreement – aS & D • Data location(s) – aS & D • Complimentary Certifications: SSAE 16 [16], ISO 9001 [17], ISO 27001 [11], ISO 27017 [22], PCI [18], EHNAC [19], FISMA [20], FedRAMP [8], HITRUST [21], etc. – aS & D • Certification boundaries (holistic or limited scope) – aS & D • Cyber security – aS • Geography – aS & D • Redundancy (ISP(s), utilities, generators, emergency power systems etc.) – D • Physical security – D • Capacity – aS & D • Staff training – aS & D • Managed services (customer portal, VM/service provisioning etc.) – aS & D • Uptime – aS & D • Help Desk support – aS & D • Change management • Termination of the contract and deletion of data, including avoiding lock-in and ensuring long-term availability of GxP data • Data processing operation • Third party use of subcontractors	Appendix 11
SaaS/PaaS (provider using a third-party CSP)	In this scenario, the SaaS/PaaS provider is delivering their application or platform from a third party CSP. In this relationship, the provider is supplying the regulated company with an application, but has fully outsourced all aspects of the cloud infrastructure. This may present the regulated company with the highest risk, unless CSPs are transparent and willing to co-operate in an assessment process, and to provide information to support risk assessments and quality agreements. It is important to understand the SaaS/PaaS provider's Service Level Agreement with the CSP regarding planned and unplanned uptime/outages and cyber security boundaries, as well as the service provider's standing regarding their engagement with the CSP (major/minor account). In addition to the usual software supplier quality assessment, the regulated company should consider both the CSP's performance competency and their knowledge of, and willingness to support, compliance with global regulations. Aspects that should be considered include:	Appendix 11

Table 1.1: Topics Related to Infrastructure Outsourcing, Virtualization, and Cloud Adoption (continued)

Topic	Risk Considerations for Outsourced Infrastructure	For Further Information, see
SaaS/PaaS (provider using a third-party CSP) (continued)	**Note:** "aS" denotes the SaaS or PaaS provider, "CSP" denotes Cloud Service Provider(s) • Willingness to be assessed and to provide appropriate information to support risk assessments and quality agreements – aS & CSP • Understanding of GxP Regulations – aS & CSP • Robustness of SDLC – aS • Single or multi-tenant environment – aS • Upgrade frequency – aS • Site Qualification activities – aS & CSP • Nature of cloud (from highest to lowest risk): public, hybrid, community, private – aS • Cloud Infrastructure Qualification activities – aS • Ability to execute a Quality Agreement – aS & CSP • Data location(s) – aS & CSP • Complimentary Certifications: SSAE 16 [16], ISO 9001 [17], ISO 27001 [11], ISO 27017 [22], PCI [18], EHNAC [19], FISMA [20], FedRAMP [8], HITRUST [21], etc. – aS & CSP • Certification boundaries (holistic or limited scope) – aS & CSP • Cyber security – aS • Geography – aS & CSP • Redundancy (ISP(s), utilities, generators, emergency power systems etc.) – CSP • Physical security – CSP • Capacity – aS & CSP • Staff training – aS & CSP • Managed services (customer portal, VM/service provisioning etc.) – aS & CSP • Uptime – aS & CSP • Help Desk support – aS & CSP • Change management • Termination of the contract and deletion of data, including avoiding lock-in and ensuring long-term availability of GxP data • Data processing operation • Third party use of subcontractors	Appendix 11
Multi-tenancy versus single tenancy	Multi versus single tenancy is an important consideration for SaaS/PaaS providers and regulated companies. Multi-tenancy allows a software company to support a single version of an application and roll out upgrades on a scheduled/unscheduled basis. While this presents the SaaS/PaaS provider with a significant opportunity from a portfolio management perspective (e.g., effective installed base of 1 as opposed to 1000), it can present significant challenges for regulated companies that have engaged one or more such providers, as the expectation that such applications are validated is the expectation of the global regulatory agencies. Single tenancy, by contrast, offers the regulated company more control over application upgrades, but is typically more difficult and less cost effective for a SaaS/PaaS provider to manage.	Appendix 11

Table 1.1: Topics Related to Infrastructure Outsourcing, Virtualization, and Cloud Adoption (continued)

Topic	Risk Considerations for Outsourced Infrastructure	For Further Information, see
Applicability of datacenter/CSP certifications to GXP engagements	Datacenters and CSPs may offer one or more third party certifications. The value of each certification should always be considered in the context of the intended scope. Further, a regulated company should understand the boundaries for a particular certification. CSPs may claim certification to a particular standard while not immediately disclosing its limited application within their operation. While some of these certifications and accreditations can provide a level of evidence of IT controls, security, and quality practices, they do not directly address infrastructure qualification activities. Providers should be willing to support quality assessment and to provide appropriate information to support risk assessments and quality agreements, and the provision of certificates on their own may not be sufficient. When considering the applicability of a certification or accreditation the following should be considered: • Applicability to GxP • Original purpose and scope of the certification, e.g., PCI [18], SSAE 16 (Financial) [16], ISO 9001 [17], ISO 27001 [11] • Validity of the certifications (have not expired) • Frequency of surveillance audits • Certification history (lost, gained, etc.) • Audit or assessment history • Prevalence of offered certifications in the market place • Robustness of any self-certifications	Appendix 11

2 IT and Cloud Infrastructure Elements

Ongoing quality management of the IT and Cloud Infrastructure includes assurance that all processes and procedures are in place, to control the life cycle activities of the 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, i.e.:

- Platforms
- Processes
- Personnel

These three 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 definition and guidance on how to identify an appropriate qualification strategy for individual platform components, in accordance with *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems* [14] categories. Infrastructure software components are regarded as GAMP® software Category 1 regardless of whether the component is standard, configurable, or custom. For further information see *ISPE GAMP® 5* [14].

Table 2.1: Definition and Proposed Qualification Strategies for Platform Components

Platform Component	Definition/Proposed 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. **Note 1:** although 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 regulated company, such as the internet, inherently provides a system which adds to the challenge of meeting regulatory and regulated company requirements for security, availability, integrity, confidentiality, etc.
Hardware and Peripherals	Includes all computer equipment (physical and virtual), 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® hardware Category 1.
Firmware	Firmware may be considered an integral part of the hardware component; however, where firmware is updated independently, it should be managed as software in its own right. Infrastructure firmware is typically regarded as GAMP® software Category 1, regardless of complexity and configurability.

Table 2.1: Definition and Proposed Qualification Strategies for Platform Components (continued)

Platform Component	Definition/Proposed Qualification Strategy
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. **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. **Note 3:** an assessment of the operating system's functionality and an impact on other platform components should be performed.
Hypervisor	A virtual platform, which maintains operating systems within its own environment (e.g., Vblock, FlexPod™, Nutanix™, VMware®) The virtual platform should be qualified as an operating system with specific attention focused on the functionality and capabilities of the virtualization software.
Data Management Software	Includes file storage software, database management systems, web services, interface, and communications software, etc. Elements of data management software may support more than one application.
Middleware	Includes software that serves as an interface/integrator, or provides translation between applications, or from the application layer to the operating system, database, etc. **Note 1:** configuration of middleware should be documented. **Note 2:** when used in conjunction with GxP applications, system features and/or functions should be formally qualified as part of the overall validation effort.
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. Server building blocks are usually a combination of GAMP® hardware Category 1 and software Category 1. This is the same for network appliances such as intrusion detectors, etc. **Note:** servers can be physical or virtual components.
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. Client building blocks are usually a combination of GAMP® hardware Category 1, and software Category 1. **Note:** clients can be physical or virtual components.
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® software Categories 3, 4, or 5. The validation of applications is outside the scope of this Guide.

Note: Table 2.1 does not take into consideration datacenter components such as facilities, utilities, computing center areas, etc., as many such items are subject to local building codes and national/international standards.

Based upon the qualification strategies described, validation of XaaS may be able to be focused only on the application layer and using a Category 3, 4, or 5 approach, depending upon the service model and intended use.

Regulated companies should determine which categories apply to platform components. Approaches to making such determinations are described in *ISPE GAMP® 5* [14].

2.2 Processes

The number of IT Infrastructure processes a regulated company decides to implement, and the method of implementation, depends mainly on the criticality of the business processes being supported and on the size of the regulated company. Where a third party (or multiple third parties) has been engaged to provide the underlining infrastructure, the third party should be audited to ensure the existence, and use, of the referenced controls.

There should also be consideration of processes impacted by the method of qualification employed, such as system development, deployment, etc.

The processes listed cover typical aspects that are required for good business practice, as well as compliance. This list, which takes into account the Information Technology Infrastructure Library (ITIL®)[4], is indicative only and regulated companies may view different processes as being sub-processes to other processes:

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

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

[4] Information Technology Infrastructure Library (ITIL®): a set of practices for IT service management that focuses on aligning IT services with the needs of business [37].

2.3 Personnel

Management should define roles and responsibilities (i.e., 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 internal/external roles that may be identified include:

- Executive Management (Project Sponsorship/Strategic Direction)
- Project Manager
- Application/Business (System/Data) Owner4/Administrator/Application Oriented Subject Matter Experts (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 an appropriate educational background and experience, should be available in addition to specific roles already identified.

Provision of training should be planned to ensure that the required skills are developed and maintained to cover all responsibilities. Personnel, including those of external infrastructure providers, should be made aware of any relevant regulatory requirements or guidance, and industry expectations that apply to their duties. Personnel should be trained in the procedures that are applicable to them, and re-trained as changes occur. Consideration should also be given for retaining appropriate levels of subject matter expertise during the operational phase and beyond. Records of training should be maintained and suppliers audited, as required. For further information see Appendix 1.

3 Quality Management System

This Section describes how a Quality Management System (QMS) can assist in providing evidence that an IT or Cloud Infrastructure is in a controlled state. It also describes the key requirements for the QMS to attain this goal. Infrastructure control and compliance aspects should be an integral part of the wider organizational QMS.

3.1 Quality Manual

A quality manual, or equivalent, should set quality objectives in line with a regulated company's quality policy. A top-level document relating to IT Infrastructure should cover:

- Identification of key IT Infrastructure processes (especially those that relate to IT Infrastructure qualification and operational management) and how they interact
- Location of service providers supplying the regulated company with XaaS
- Procedures, detailed work instructions, templates, and other standards that apply
- Required records and documentation to be maintained

Where an external provider is engaged, the corporate supplier management process should be followed. This information can either be included in the quality manual or as a separate document. Quality manuals and top level documents should be developed and approved by QA, with input from executive management. Quality arrangements should also be defined for internal suppliers such as IT departments.

Where an external supplier is hosting or managing all, or some, aspects of a regulated Cloud or IT Infrastructure, typical QMS components that should be considered for evaluation include:

- Quality manual
- Regulatory alignment
- Qualification approach
- Data privacy
- Datacenter management
- Disaster Recovery Plan
- Change and Configuration Management
- Document control
- Training procedure
- Internal audit procedure
- Risk assessment
- Datacenter monitoring

- Emergency response
- Security
- Backup and recovery
- Daily checklists
- Weekly checklists
- Monthly checklists

For further information, see ISO 9000 Quality Management Systems – Fundamentals and Vocabulary [23].

3.2 Roles and Responsibilities

Roles and responsibilities should be defined for all internal and external functions. Job descriptions or other documents should reflect the assignment of roles and responsibilities. When engaging a XaaS provider, a clear understanding of where roles and responsibilities end and begin with respect to the regulated engagement, should be clearly outlined in the SLA see Appendix 11 for further information.

3.3 Data and Records Management

Appropriate controls need to be in place to ensure the retrievability, storage, and protection of records. The controls should provide evidence of the quality levels for the IT or cloud platform, and compliance with regulations. A record management program should consider the definition of a record, its ownership, its location (external/internal), security, and any regulatory retention or privacy laws.

For further information on document management see *ISPE GAMP® 5* [5] and the *ISPE GAMP® Guide: Records and Data Integrity* [24].

3.4 Documentation

Documentation for platforms, processes, test results, etc. (both internal and external), should be maintained in order to meet requirements for inspections by regulatory authorities.

The regulated company 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. Special provisions within SLAs should ensure a third-party datacenter or infrastructure provider to support both customer or regulatory audits.

There should be a consistent approach to documentation across a regulated company. Where an external organization has been engaged to host all or part of a regulated company's infrastructure, the third party's documentation approaches should be understood and agreed to via the Service Level Agreement (SLA) and subject to audit by the regulated company. 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 or 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, including QA and/or IT compliance, or relevant SMEs
- 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 written clearly or made clear by using a computerized tool that supports adequate automatic audit trailing.
- In a XaaS deployment, the provider should be prepared to provide performance testing that supports data integrity, privacy, and security while additionally ensuring that the XaaS product is capable of meeting the needs of the regulated company's user community.

The rigor with which the above requirements are met will depend upon the impact and risks associated with the component being tested and, in the event of an external engagement, those agreed to in the SLA or Quality Agreement. See *ISPE GAMP® 5* [14] section on Testing of Computerized Systems.

Computerized reporting tools may be used for reporting system configuration and installation. The use of these should be encouraged, as they are typically more effective and efficient than paper based methods.

It may be appropriate to use standard checklists or test specifications during testing, e.g., when checking the installation of platform building blocks. For further information on testing GxP computerized systems see *ISPE GAMP® Good Practice Guide: Risk Based Approach to Testing of GxP Systems (Second Edition)* [25].

3.6 Standard Operating Procedures

Standard Operating Procedures (SOPs) or equivalent controls should be prepared (or reviewed if outsourced) and should describe critical processes and services. SOPs should be reviewed periodically 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.

For a suggested list of SOPs that may be considered as part of an IT Quality Management System see Appendix 4.

3.7 Training

Training should be planned and documented. Formal structured training programs, either in-house or external, should be considered. Technical and regulatory training requirements for external service providers and contractors should also be determined. Training records should be maintained for compliance with regulatory authorities.

3.8 Periodic Review and Evaluation

SMEs, or members of IT Quality and Compliance groups, should review processes, systems, or platforms to ensure that they meet specified requirements. In addition, the review can provide 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 can be used to help to maintain the qualification status of the IT or Cloud Infrastructure throughout its operational life. Periodic reviews may be undertaken as a scheduled or event driven exercise, e.g., following a major upgrade to hardware or platform software. For further information see Appendix 4.

Documented periodic reviews of IT Infrastructure components may be referenced from periodic reviews of GxP applications.

The periodic review process should be used when IT Infrastructure services have been outsourced. The frequency of the review should directly correlate to the risk of the system(s) in scope. For further information on periodic reviews, see *ISPE GAMP® 5* [14].

3.9 Audit by QA

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

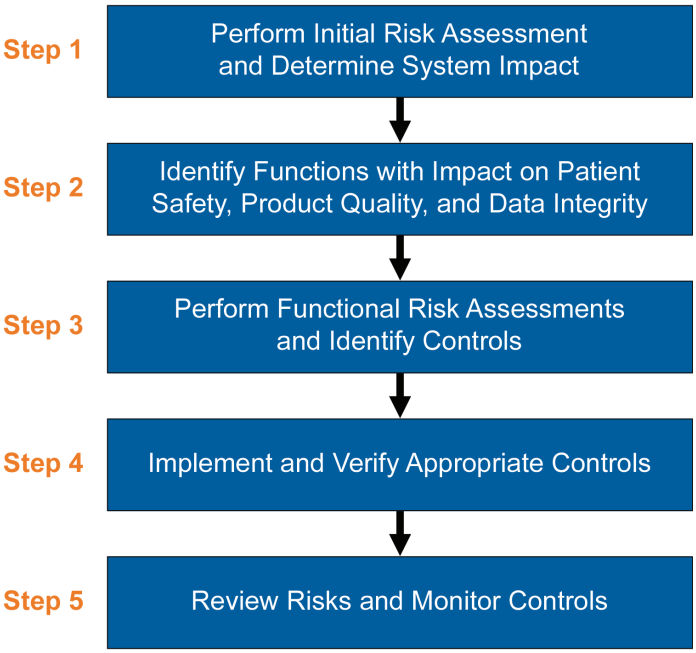
A company may contract external consultants or draw on internal, independent experts to assist the audit.

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

4 Applying Risk Management

ISPE GAMP® 5 [14] describes how Quality Risk Management (a systematic process for the assessment, control, communication, and review of risks) may be applied to GxP regulated computerized systems. This Section considers how this approach may be applied to IT Infrastructure. Figure 4.1 shows the major phases of the Risk Management Process.

Figure 4.1: Risk Management Process Overview



Note: Figure 4.1 can be found in *ISPE GAMP® 5* [14], Section 5.3 Quality Risk Management Process

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 regulated company's business. For example, regulated 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 and systematic way. This involves a number of key activities:

1. *Perform Initial Risk Assessment and Determine System Impact:* Identify the IT and Cloud Infrastructure components that may require qualification, based on an analysis of the applications and processes supported by the IT and Cloud Infrastructure, and the applicable regulations.

2. *Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity:* Assess these IT and Cloud Infrastructure components based upon the identified hazards and vulnerabilities and assessed impact on critical aspects (e.g., data integrity, privacy, and security). This step involves analyzing and evaluating risks to decide if controls are required to manage those risks.

3. *Perform Functional Risk Assessments and Identify Controls:* Implement controls commensurate with the risks identified for the IT and Cloud Infrastructure components. These controls should be documented and justified with reference to the identified risks.

4. *Implement and Verify Appropriate Controls:* Assess changes to qualified components.

5. *Review Risks and Monitor Controls:* Monitor effectiveness of controls by periodic review.

Communication of risks and risk management elements should be provided throughout the process to appropriate groups and/or individuals. Risk management decisions need to be communicated, e.g., between the regulated company and regulators, between the regulated company and end users, and within the regulated company.

Regulated companies may also decide to apply a risk management approach to IT and Cloud Infrastructure components which do not support GxP applications, but which are business critical (e.g., data privacy).

Note: where a XaaS third party engagement is in place, the above activities should be verified to have occurred.

Where external companies are employed, e.g., XaaS providers, datacenter, contract research organizations, regulated companies should communicate risk management requirements.

For further information on Risk Management, see Appendix 2, ISO 14971:2012 Medical Devices -- Application of Risk Management to Medical Devices [26], FDA, Pharmaceutical cGMPs for the 21st Century: A Risk-Based Approach [27], NIST Special Publication 800-30 – Risk Management for Information Technology Systems [28], and *ISPE GAMP® 5* [14].

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 and Cloud Infrastructure components, the criticality of the GxP applications they support should be considered. This applies to both physical and virtualized technologies, along with their potential impact on integrity and availability of data. For further information on security requirements, see Appendix 5.

Platform management groups may assign the same level of criticality to all components and data unless System/Data Owners specify different levels of criticality up front. IT Infrastructure personnel should not be expected to assess GxP compliance independently. A XaaS supplier's capabilities should be considered as part of the regulated company's supplier quality program.

Non-GxP applications operating on the IT Infrastructure may affect GxP applications; these should be identified within the risk assessment process for the GxP applications, and suitable controls included (e.g., to maintain data integrity).

Additionally, results of risk assessments carried out in other areas of the business may influence IT and Cloud 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 through the entire life cycle of the data
  - Confidentiality if required by the company
  - Availability at the right place and time
- Availability of services – affects the business, continuity, and compliance if persistent
- Effectiveness of IT Infrastructure processes, e.g., user access accounting

- Availability and training of key personnel
- Location of data, latency, and performance constraints
- Any third party engaged to support the assessment

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 risk controls. For typical platform building blocks, the risk assessment process may reveal unacceptable risks. In such cases, the regulated company needs to consider elimination by redesign, or mitigation by applying manual, semi, or fully automated controls. Identified controls should be implemented as part of ongoing operation (see Chapter 5 and Chapter 6).

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

4.2 Implementation of Controls

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

- Testing
- Redesign, including incorporation of high availability options
- 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
- Contractual agreements (e.g., SLAs)
- Identification of new or updated roles and responsibilities
- Provision of extra staff, facilities, tools, and office space
- Provision of an alternate XaaS supplier
- Data replication, storage redundancy, and mirroring
- Design reviews
- Procedures
- Clustering at the Operating System (OS) or application level

Successful implementation of the required controls should be verified during qualification, and periodic review (see Appendix 2).

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. Documented low risk operational tasks can be designated as “pre-approved” changes with appropriate control mechanisms in place. Change control is a key consideration for an SLA in an outsourced situation.

Depending on the scope of the change and potential impact to the overall environment, some level of regression testing should be considered to confirm proper functionality of all systems in scope. Changes to a multi-tenancy system should be considered when there is a potential to impact all subscribers. All changes from a customer should be assessed to prevent any impact to other customers on a shared IT Infrastructure. An emergency change process should be defined.

Where a regulated company has procured a suite of XaaS applications from a diverse pool of providers, the impact should be assessed globally, as well as locally, particularly where redundant systems do not exist or data is shared or passed between diverse platforms.

4.4 Periodic Review and Evaluation

During periodic review of IT and Cloud Infrastructure, the regulated company should reconsider the risks and verify that controls, established during IT Infrastructure development and qualification, are still effective, especially where a XaaS relationship exists. The periodic review also should consider whether:

- Previously unrecognized hazards are present
- The estimated risks arising from a hazard are no longer acceptable
- A significant failure/incident has highlighted a risk higher than previously anticipated
- The original assessment is otherwise invalidated
- The XaaS has met its service SLA metrics
- A third-party datacenter has been engaged
- The XaaS has been implicated in quality incidents which have affected the conduct or performance of the regulated activity

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

A platform is infrastructure that includes the operating system and software components, which provide a foundation for the development, configuration and/or deployment of one or more applications.

Platforms may be internal or external, collocated, or cloud-based. This Chapter describes how a platform, or a major addition to an existing platform, can be brought into compliance with a regulated company's established standards by using a planned qualification process.

Note: minor additions to an existing platform are usually managed via change control.

This Guide uses a traditional Installation Qualification/Operational Qualification/Performance Qualification (IQ/OQ/PQ) terminology, as it is still frequently used when dealing with infrastructure, but this is not intended to imply that the use of these terms and activities is mandatory.

5.1 Overview of Process

A Platform Project and Qualification Plan should be created. It should describe the life cycle activities to be undertaken to qualify each platform type. The Platform Project and Qualification 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.

Note: Unique platforms are usually qualified as part of the application validation.

Typically, the qualification strategy is based on one of two scenarios:

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

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

In Scenario 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 Scenario 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 assessed formally to determine how design choices may impact critical aspects. The output of a detailed risk assessment can also determine the scope and extent of the qualification process. For example, if segregation technology is not used to provide effective barriers between components that support GxP and non-GxP activities, the scope of qualification may be greater.

Infrastructure requirements should include regulatory requirements, ensuring that the primary responsibility for understanding and interpreting GxP regulations rests with the QA function, rather than the infrastructure staff.

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

Following procurement, an Installation Qualification (IQ) plan should be created. IQ should provide evidence that all components have been installed and configured as specified. Where appropriate, certification evidence, such as but not limited to SOC 1 [29], SOC 2 [30] and ISO 27001 [11] 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 use of re-usable building blocks (see Appendix 2) is recommended, where feasible, to minimize the need for the introduction of new platform components (e.g., the use of standard, qualified, server, and client platforms).

The qualification strategy should be based on qualifying **types** of building blocks and subsequently running abbreviated qualifications of individual **instances** of those building blocks.

Automation processes for large-scale deployments with automated electronic recording and logging are recommended.

Typical deliverables required when qualifying **types** and **instances** of building blocks are shown in Appendix 2. Appendix 11 provides a comparison of the various XaaS models as compared to a traditional IT Infrastructure scenario.

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 activities described in Table 5.1.

Note: while indicating a general flow of life cycle activities, Table 5.1 is not intended to imply that these are strictly sequential. Typically, overlap and iterations will occur during a project.

Table 5.1: Typical Life Cycle Activities

	Life Cycle Activities	Typical Deliverables
Achieving Qualification	Planning (planning continues throughout)	Project Plans and Project Qualification Plans – these would typically cover: • Project scope • Responsibilities • Deliverables and approvals • Project related risks • Quality and regulatory considerations • Processes • SOPs • Timelines • Training • Funding
	Specification and Design	• 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

Table 5.1: Typical Life Cycle Activities (continued)

	Life Cycle Activities	Typical Deliverables
Achieving Qualification	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	• 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
	OQ and Acceptance	• Operational tests and verification of specifications and agreed deliverables (completed OQ)
	Reporting and Handover	• Summary reports • Approval of acceptance criteria • Transition plans • Transfer of source documents and access rights • Risk review and acceptance • Service contract inauguration
Maintaining Qualification	Operation and Maintenance (see Chapter 6)	• Change Management (internal and external, XaaS provider) • Configuration Management (should be established prior to qualification) • Security Management • Management of servers, clients, and networks • Problem management • Help Desk • Backup, restore, and archiving • Disaster recovery • Performance monitoring of critical IT Infrastructure processes • Supplier management • Periodic reviews
Retirement	Retirement (Decommissioning/ Withdrawal) (see Chapter 7)	• Decommissioning plans • Data/information archiving • Transfer of processes and data • Considerations for long-term data retrieval (reading the actual files) as technologies change – possibly for over 20 years

5.3 Planning

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

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). Platform qualification plans should manage the qualification of platforms.

The validation of GxP applications should be managed by Validation Plans, as described in *ISPE GAMP® 5* [14].

The Platform Qualification Plan should reference:

- Applicable company policies and requirements as well as any third-party supplier policies/requirements
- Any specific requirements derived from the applications or services that the platform is intended to support
- Any existing pre-qualified building blocks in terms of standard platform building block qualification packages, e.g., for specific server types
- Required new or referenced processes
- Any new or modified SOPs

ISPE GAMP® categorization of the platform (see *ISPE GAMP® 5* [14]) can assist with the development of an appropriate qualification strategy. During preparation of the Platform Qualification 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.

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 and resource and time management are outside the scope of this Guide. For further information see *ISPE GAMP® 5* [14].

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. These should be organized to generate building blocks.
- Timelines and interdependencies, e.g.:
    - For a new IT Infrastructure – completion of network qualification before commencing hardware, server, client, and utility qualification.

- Separate teams could perform work in parallel on a given network qualification, using pre-qualified client building blocks. Cloud-based systems could have add-ons to provide additional functionality to a base offering. The additional functionality may be added afterwards.

- 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
- Project risk management
- Need for verification of operational procedures
- Need for evaluation and auditing of platform provider methodologies and QMS

Project risk management is concerned with risks relating to the project, e.g., lack of management commitment, or availability of key staff, equipment, or other resources.

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) should be considered.

Timely coordination with appropriate Application (System/Data) Owners is required, so that they can plan to update their application validation packages accordingly. Application (System/Data) Owners should be encouraged to reference platform qualification packages from each application validation package to benefit from the concept of horizontal, platform based qualification.

Typically, there would be no QA review of the detailed specification, design, and verification of infrastructure. It is a strategic oversight role that does not usually include reviewing and interpreting technical documents, as QA typically do not have the required technical expertise and rely upon appropriate SMEs. The level of oversight by IT QA should reflect the level of maturity of the IT organization. If IT or QA does not have the requisite experience to support the project in scope, a third party should be engaged.

Infrastructure build processes may be automated and can be designed so that errors or problems are automatically flagged and logged. Automated build processes should be appropriately defined and verified. QA normally approve a high-level qualification approach (e.g., for all UNIX® servers), but not the individual documents for the qualification process. SMEs should perform the specification, design, build, and testing processes for individual items.

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

Appendix 2 lists typical deliverables from a platform qualification project and suggested responsibilities for production, review, and approval.

5.3.2 Considerations for Legacy Platforms

A legacy platform is considered to be a platform that has been in use for some time with limited or no formal qualification. This could also include new platforms without appropriate documentation.

Key questions for a legacy 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?

Intensive testing of the system may affect the continued operation of a legacy platform that is already running in satisfactory manner. Production of an Experience Report that summarizes the inventory and operational status, such as service desk records from incident and problem management should be considered. The Experience Report can be used to record a history of the platform, as basis for further planning.

Qualification of legacy platforms should be carefully planned, budgeted, and resourced. IT Infrastructures can also be subject to a high degree of change, which can make qualification more complicated.

A risk assessment should be completed to determine additional documentation and testing needs.

5.3.2.1 Determining Extent of Qualification

Legacy platforms should be audited against the regulated company procedures and regulatory expectations. Gaps should be identified and documented; risk assessments should be used to justify which legacy platforms require qualification to resolve identified gaps. Key regulatory and business drivers for qualifying the legacy platforms should be considered when establishing priorities for the qualification and to help to focus effort. Regulatory and business drivers may include:

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
- Disaster recovery test/plan documents
- Configuration management and change control
- Document management

5.3.2.2 Existing Documentation

Existing documentation should be used, where feasible, to minimize timelines and rework. Effort should be focused on the inclusion of the required document content and on accuracy, rather than document formatting. Relevant information and documentation for the support of platform qualification may already exist within application validation documentation and records. Supplier documentation should be leveraged where possible.

5.3.2.3 Testing

Priority should be given to critical platform components identified by the risk assessment, i.e.:

Basic Installation Verification (IQ)

This should verify that hardware and software items match the documented specifications. Note: re-installing working components only for the purpose of gathering IQ documentation may not be an appropriate approach. This should be highlighted by the risk assessment.

Configuration Verification

This should confirm that the key configuration settings match the documented specification.

Operational Qualification (OQ)

Testing should be geared to identifying potential gaps or issues relating to reliable operation of the platform(s), and may also form the basis for the development of (or assessment of existing) performance, support, and monitoring procedures. The following areas should be considered with baseline measurement where applicable:

- Storage capacity
- Response times, network dependencies
- Concurrent sessions/users
- Availability
- Backup/recovery testing
- Access security processes/procedures

For existing IT Infrastructures that are performing satisfactorily, stress and load testing is not normally a priority, unless there are specific, reported performance issues. Where a platform provider offers cloud-based services, operational testing and documentation may be executed by teams from both the provider and the regulated company.

5.4 Specification and Design

A regulated company should specify requirements for platform components in the form of controlled documents, e.g., reusable, generic requirement specifications, for each type of platform component (building block) and Enterprise IT Solution. Alternatively, requirements for platform components should be embedded in contracts or Service Level Agreements (SLAs).

Inputs to the requirements should include company policies and requirements derived from the applications that will run on a platform, e.g., functionality, compatibility, capacity, and security.

Regulated 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.

Suitable security controls should be enabled to protect data; confidentiality, availability, and integrity should be considered.

5.4.1 Networks

Regardless of whether an internal IT infrastructure has been established, co-location is occurring, or a XaaS relationship exists, network design specifications should be established to:

- Define the topology and diagrams of the network to address segmentation, network performance, and security considerations
- Include any platform provider networking components, as well as connectivity to the provider
- 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 -- Basic Reference Model (OSI Model) [31].

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, wireless access points, 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 IP firewalls usually work on this layer.

Layer 4 End user applications reside on this layer and communicate via software ports. Application level firewall also operates through this layer.

Test and qualification activities should be 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 usually presented as a drawing. The criticality of various network segments may vary, and this needs 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 and non-regulated networks
- The need for built-in redundant networks
- The serviceability of the network (e.g., via Simple Network Management Protocol (SNMP))
- The possible interfaces between segregated networks, such as firewalls and Demilitarized Zone (DMZ) sections
- 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 regulated company should assess the capabilities of the carrier in terms of performance and security (see Appendix 11).

Topology diagrams should provide a high-level representation of the infrastructure. Documentation of the detailed configuration may be kept in dedicated databases, rather than diagrams, due to the dynamic nature of IT Infrastructures. Diagrams should focus on the key components of the IT Infrastructure identified during qualification planning. Diagrams should differentiate between logical and physical depictions where possible.

Platform providers should supply topology diagrams to support internal documentation, as well as auditor requests.

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 IQ.

Redundancy in server building blocks, virtualization, clustering, utilities, and storage building blocks should be considered, based on the results of a 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. Where enterprise infrastructure is linked with platform providers, the sharing of resources becomes an integral component. IT Infrastructure administrators usually apply supplier best practice settings, or settings conforming to corporate or site-specific standards. Application specifications should conform to these settings, unless a deviation is required specifically, justified, and the changes documented.

5.4.2.2 Operating Systems

Operating Systems (OS) usually 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.

Where a cloud or virtualized environment is being utilized, the first layer OS may be an administrative OS designed to provide and establish virtualized environments. Default parameters that will remain unchanged may not need to be recorded. 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, provision for effective time synchronization should be included. This should be 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 some 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 regulated 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, regulated 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.

When a client hosts a "thick" client or an entire GxP application, the application should be validated. For further information, see *ISPE GAMP® 5* [14].

For information on mobile devices utilized in such environments see the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Regulated Mobile Applications* [32].

5.4.4 Support and Diagnostic Tools

Tools should be carefully selected. 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 regulated 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 Datacenters/Server Rooms

Regulated companies may have a variety of demands for their 'internal' or 'external' datacenters/server rooms commensurate with practicalities, costs, and risks in terms of security and quality factors. General considerations include:

- Uptime for third-party datacenters (platform providers) and their ability to comprehend and resolve the requirements of GxP regulated data. A datacenter engaging in the storage, processing or handling of GxP data should offer the regulated company a level of qualification, validation, controls, and transparency commensurate with the level of risk of the application that is being hosted or the infrastructure that has been outsourced.

- Infrastructure ownership is an important and emerging consideration, particularly where SaaS or PaaS are offered. The infrastructure underneath the application may have been outsourced by the software vendor to a third-party datacenter. Regulated companies should understand both the ownership and responsibility for the supporting servers, and the datacenter that infrastructure is housed in to ensure all parties with a stake in the regulated company's infrastructure are fully understood. Data Owner requirements with regards to security, controls, access should be considered.

- 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 regulated companies may choose to double or triple their main datacenters/server rooms to achieve the required assurance of availability.

- Provision of adequate space and environment for the intended purpose. Protection from undesirable outside factors, 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, and alarms. It may be desirable to build datacenter/server rooms inside other buildings on the regulated company campus, to reduce the overall exposure to the outside.

- The use of raised floors and adequate conduits for internal cabling. Uninterruptible Power Supplies (UPSs) and generators should be used to provide the required, filtered Volt-Amps (VA) for specified durations, in case of blackouts or brownouts.

- Grounding and shielding, which are best achieved if planned 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 systems should be considered.

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. **Note:** with an outsourced IT Infrastructure relationship, the risk profile relative to qualification is expanded. Appendix 11 provides example risk considerations for each of the outsourced models. GAMP® software and hardware categories should be taken into account during these assessments.

For individual or groups of components, the extent of qualification should be determined using the approach described in Appendix 2.

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
- Knowledge of all vendors supporting the infrastructure and their sustainability
- 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 I*SPE GAMP® 5* [14].

5.6 Procurement, Installation, and IQ

Components and services should be procured only from suppliers who can demonstrate an acceptable level of quality and effective support, commensurate with the expected life time 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.

5.6.1 Supplier Evaluation

Regulated companies may use a supplier evaluation program to ensure that critical components or services are procured only from approved suppliers. A board of designated experts may evaluate relevant information gathered for a potential or existing supplier, and classify the information accordingly. Examples include “approved”, “conditionally approved”, and “not approved”. Supplier assessments, e.g., as described in *ISPE GAMP® 5* [14], should be leveraged during acceptance testing.

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

Third-party datacenters and cloud platform providers should be fully vetted by the regulated company. 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 (FAT) before transport to the target site.

For further information, see *ISPE GAMP® 5* [14].

5.6.2 Installation and IQ

Installation and integration methods should comply with regulated company standards, and be based on supplier recommendations and the concepts of Good Engineering Practice (GEP), good IT practice, 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 Appendix 2). Once building blocks have been qualified, deployments of these building blocks may be configured with the main focus of qualification being to verify the overall configuration has been completed successfully. 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.

Qualification protocols should follow the building block concept where possible. Generic protocols could be created and reused for building blocks.

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
- Vendor capability and experience relative to sustainable GxP compliance

The configuration management process, including change management, should manage all critical items.

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 that the installation of the server hardware and software has been completed using the parameters and values established in the design stages is needed. 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. Servers can be physical or virtualized.

Regulated companies should consider preparing and maintaining verified server configurations, and use these to duplicate new servers; a Configuration Items List (CIL), or equivalent, is usually needed to achieve this. The use of automated configuration management tools and databases, rather than paper based methods, are encouraged.

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

- Make and model of the server

- Type and amount of memory
- Number of Central Processing Units (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, regulated 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. Clients can be physical or virtualized.

For a SaaS or PaaS delivery where access to the client is achieved through one or more vendor approved web browsers, end point qualification is not necessary. The virtual client would still need the appropriate documentation and testing to verify fit for purpose readiness. Where SaaS/PaaS data is accessed by the physical client, these clients should be qualified.

Individual system specifications may require additional 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.

Virtualized clients offer additional security controls such as setting limitations from where these can be accessed, as well as to which hosts they can connect.

5.6.2.5 Networks

Physical Network Layer

In new facilities or third-party datacenters, customized cabling (copper 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 [33] or ANSI/TIA/EIA 568 [34]. 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 Transmission Control Protocol/Internet Protocol (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 use of security measures such as Virtual Local Area Networks (VLANs) and firewalls should be utilized to separate network traffic, as appropriate.

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.

Note: it is usually verified as an integral part of the system validation effort. Application testing should not commence until the formal handover of the IT 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 risk assessments already performed to verify that the sum of requirements derived from serviced applications, if applicable, are met.

Typical tests to consider 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 OS functionality, e.g., by checking accessibility to defined disk volumes
- Verification of backup and restore process. Long-term data archiving and the ability to both retrieve and access the files should be considered, e.g., can the file be opened in 10 or 20 years, rather than just viewing the data.
- Verification of time synchronization
- Verification of high availability functionality, especially under load
- Verification of security incidents, technical faults, capacity and performance monitoring

For further information on remedial considerations see Appendix 11.

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. Combining IQ and OQ protocols can be inefficient when using generic protocols for building blocks.

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 Quality team.

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). The Quality team should determine the system is fit for the purpose for which it was designed. Any outstanding risks to operations should be documented in this report, with the System Owner accepting these risks with potential mitigation activities documented in either this report, or other risk register.

6 Maintaining the Qualified State During Operation

The IT Infrastructure may change frequently, sometimes on a daily or hourly basis, depending on the size and complexity 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

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, in order to be efficient and cost-effective.

The documented QMS, (see Chapter 3), 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 the impact of changes.

Note: 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.

Where an outsourced relationship is occurring relative to IT Infrastructure, the regulated company should understand how much change management is occurring at the vendor facility. For an outsourced supplier, the agreement should include access to the supplier's change management records (for customer and regulatory inspections, periodic reviews, etc.). Change management procedures should include clear communication lines and responsibilities.

Outsourced suppliers may have a Configuration Management Database (CMDB) to manage the IT Infrastructure components.

A SaaS vendor may offer a homogeneous version of their software across the user community. Before entering into a vendor with this model, the regulated company should understand the vendor's version and change schedule, and ensure that both internal change management and the vendor's associated processes can work in tandem, to maintain compliance.

IT should employ robust change procedures, e.g., those proposed by COBIT® and ITIL® processes. Standardization of changes should be developed to help to ease process and impact assessment. "White lists" may have been established to pre-classify changes. These are intended to define changes that are not critical and could be done as a simple logbook entry, e.g., exchange of identical components or a standard change procedure for changes occurring regularly, such as a pattern update of a firewall which could follow an instruction and does not need additional formal assessment.

For further information on managing upgrades and patches see Appendix 6. Also see *ISPE GAMP® 5* [14].

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 usually 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 are usually defined to the lowest level at which a component can be independently installed, replaced, or modified.

For further information see *ISPE GAMP® 5* [14].

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 would ultimately impact product quality.

Information security may be characterized as the preservation of:

- **Availability:** ensuring that authorized users have access to information and associated assets when required

- **Integrity:** safeguarding the accuracy and completeness of information and processing methods
- **Confidentiality:** ensuring that information is accessible only to those persons authorized to have access

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

- 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

For further information on security controls see Appendix 5. Also see ISO 27000 to 27008 [35].

6.4 Server Management

The objective of the server management process is to ensure that the server consistently fulfills specified requirements for operational availability, performance, and security. 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 server platforms and applications. If the change affects GxP applications, the extent of re-qualification required should be considered.

Virtual and physical servers have different requirements, functions, and risks that should be included in management process.

Server management is further described in Appendix 8.

6.5 Client Management

The objective for the client management process is to ensure that the client consistently fulfills specified requirements for operational availability, performance, and security. 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.

Virtual and physical clients have different requirements, functions, and risks that should be included in management process.

For further information on client management see Appendix 9.

6.6 Network Management

The objective of network management is to ensure that the network consistently fulfills specified requirements for operational availability, performance, and security. 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. Parts of the infrastructure may physically exist outside the vendor premises and may define the involved systems as an open system as defined in 21 CFR Part 11 [36] and enforces requirements.

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.

For further information on network management see Appendix 10.

6.7 Problem and Incident 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. Incident and problem management are often separate processes in IT organizations (see ITIL® [37] and ISO 27001 [11] definitions). These processes should be managed separately.

Problem management should provide users with an adequate method of recording perceived or acknowledged problems. The Help Desk is an important point of contact and may be a valuable source of information.

All filed problems should be tracked and resolved via approved channels; those that require changes should be communicated to the change management group. Quality procedures should be followed in case of GxP impact to ensure root cause analysis and related Corrective and Preventive Action (CAPA) processes.

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. The use of a Configuration Management Database (CMDB) is recommended to collect all IT Infrastructure management information.

6.8 Help Desk

The help desk process should provide day-to-day support to users of the IT Infrastructure for problems, questions, and general support needs. Staff employed in the help desk should be technically skilled with respect to the actual platforms and technology used in the IT Infrastructure to support the business processes in the regulated 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 system as that as used in problem management and can serve as a historical record to facilitate fast response to contacts.

Where a help desk case requires the involvement of SMEs, the help desk service should operate as the liaison between the user and those SMEs.

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.

A given Application (System/Data) Owner defines what is the maximum system break/time to recover the system (Recovery Time Objective (RTO)) and maximum loss of data – 0 minutes, 4 hours, 1 day, 1 week Recovery Point Objective (RPO). These requirements should be translated by an IT specialist to a design of the architecture and backup that will meet these RPO/RTO requirements, e.g., 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 the long-term availability of data by provision 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 regarding whether the person requesting the restoration is authorized to do so, and whether they are authorized to view the data being restored. Procedures should also ensure that the restore process does not inadvertently overwrite data that needs to be maintained subject to regulatory requirements. EU GMP Annex 11 Part 7.2 [1] requires that the integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

For further information on backup, restore, and archiving see Appendix 8. Also see *ISPE GAMP® 5* [14].

The restore process should be initially and periodically verified.

6.10 Disaster Recovery

Loss of vital parts of the IT Infrastructure and business applications may have significant impact on the business of a regulated company. The potentially complex configuration and interdependence of the infrastructure platforms and business applications means that a business can become sensitive to even smaller incidents in the IT Infrastructure and business applications. Disaster recovery should be part of a regulated company's Business Continuity Planning.[5] The primary goal of disaster recovery is to reduce downtime of critical business applications to an acceptable level following an incident.

Modern network architecture can provide the potential for mirroring and redundancy across diverse and geographically dispersed datacenters. When correctly configured close to 100% uptime can be achieved. The mirror infrastructure and datacenter(s) should be subject to the same qualification requirements. For malicious attacks that corrupt data mirroring of systems, including data, means that any data corruption is almost instantaneously replicated to mirrored systems preventing the use of the mirrored system for disaster recovery purposes in such incidents. Therefore, system mirroring must be used in conjunction with traditional backup solutions to maintain records integrity.

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.

The disaster recovery process should be initially and periodically verified. See *ISPE GAMP® 5* [14].

[5] Business Continuity Planning is outside the scope of this Guide.

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 their continued qualification status
- Ensure fulfillment of the 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 life time.

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

Actual metrics and values should be considered by each regulated company in the context of all their business. 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 Performance Qualification (PQ) of a supported software application), and actual values should be considered based upon those readings.

A capacity plan may be used to manage the resources required to deliver IT services, as business requirements of IT Infrastructure is increasing in most regulated companies. The capacity plan should contain scenarios for different predictions of business demand, and options with cost estimates to deliver agreed service level targets.

Appendix 10 lists some typical performance metrics from real life GxP regulated environments, and suggests appropriate alert/actions limits.

For further information on network management see Appendix 10. Also see *ISPE GAMP® 5* [14].

6.12 Supplier Management

The management of services and deliveries to the IT Infrastructure typically follow the general policies of supplier management in a regulated company, including:

- Evaluation of suppliers
- Selection of suppliers
- Management of relationships with the suppliers

Agreements between the regulated company and the supplier should be documented in contracts, or SLAs, and reviewed at appropriate intervals.

Special consideration should be given for supplier management in a XaaS relationship. Appendix 11 provides insight into key considerations by the engagement type.

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

It may be helpful 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 software licenses), to support the rollout and service of IT Infrastructure platforms and to exploit the concept of building blocks.

For further information on the management of outsourced services see Appendix 7.

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.

For further information on periodic reviews see Appendix 4.

7 Retirement of Platforms

Business applications can outlive the underlying platforms, and in such circumstances, data needs to be migrated onto the new platform(s). For example, a validated Laboratory Information Management System (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 regulated 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
- The requirements of the infrastructure needed to support mechanics of the application's data migration are appropriate
- Any specified conversions have consistently produced the expected results

It may be appropriate to apply statistical methods to obtain the required assurance. Alternatively, it may be necessary to devise computerized tools to provide a complete, automated verification. Suppliers may provide verification tools with the update package. The verification method should be determined by assessing and documenting the risks involved.

For further information on the retirement of platforms see *ISPE GAMP® 5* [14], *ISPE GAMP® Guide: Records and Data Integrity* [24], and *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition)* [25].

8 Appendix 1 – Roles and Responsibilities

8.1 Introduction

Regulated companies are organized in a variety of ways that fit their mode of operation, size, objectives, geographic layout, culture, etc. Regulated companies typically identify roles and responsibilities in a similar way; this Appendix discusses their interrelationships and a possible way of grouping them together.

In relation to a regulated company's quality policy or a service provider's quality policy, the word "responsibility" may be described in terms of:

1. Responsibility: who is responsible for doing something

2. Accountability: who is accountable for it being done

The term "owner" is used in this context as:

1. A suggested title for personnel accepting ownership of a given item or process

2. The high level of accountability associated with assuming that role

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 IT Infrastructure platforms, and should commit and empower resources to ensure adherence to relevant GxP requirements, along with other requirements such as those relating to security. In practice these activities are the responsibility of the IT management team.

Key roles may include:

- Executive Management
- Project Manager
- Application (System/Data) Owner/Administrator/SME
- Data Owner, if not coincident with the Application (System) Owner
- IT Infrastructure Process Owner/Administrator/SME
- Platform Owner/Administrator/SME
- Infrastructure Service Owner
- Independent QA (both for processes and technology)
- IT Audit, Quality, and Compliance
- IT Procurement

Specific Roles for Cloud Solutions

- Roles should be organized to ensure that critical objectives are considered
- Job descriptions should be assigned to named individuals
- Such decisions should be justified and documented
- Technical and managerial staff with the appropriate educational background and experience should be available
- Provision of training should be planned, to ensure that 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

8.1.1 Executive Management (Project Sponsorship)

Executive management should appoint members of management to undertake the roles of "sponsoring" projects and defining general requirements for the IT Infrastructure. Key initial activities may 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

Close interaction with QA is recommended in these initial stages.

Whether a regulated company owns its IT Infrastructure, leases services from service providers (co-location, cloud, XaaS, etc.), or engages a combination of both, the regulated company is ultimately responsible for the qualification status. The regulated company should specify expectations and monitor the continuous fulfillment of those expectations, e.g., negotiate, agree, fund, and monitor general SLAs with IT Infrastructure service providers. Final accountability, ownership, compliance, and quality assurance of systems and data cannot be outsourced.

8.1.2 Project Manager

The Project Manager should control all project activities, including:

- Liaison with System, Platform, and Data Owners on working processes and system requirements
- Monitoring compliance of project deliverables with GxP and regulated company standards for documentation, data control, training, software development (if inside the project scope), and technical support
- Preparing the IT Infrastructure project and quality plan, or IT Infrastructure Qualification Plan (in cooperation with a compliance resource)
- Reviewing, approving, and reporting on key project deliverables under the qualification life cycle
- Reviewing and reporting on 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.

8.1.3 Application (System/Data) Owner/Administrator/SME

A system consists of the application plus whatever platforms and parts of the IT Infrastructure that are required to enable the application to run.

The Application (System/Data) Owner/Administrator/SME should specify the detailed requirements that an application has of the underlying platform and IT Infrastructure processes. This can be dependent upon the appropriate approach for a given project. If the regulated company policies require the use of pre-qualified, standardized platform building blocks, the platform requirements can take a different format to when platforms are chosen, configured, and built.

For GxP applications, the Application (System/Data) Owner/Administrator/SME has further computer system validation specific responsibilities, see *ISPE GAMP® 5* [14].

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/Administrator/SME or higher management, the Application (System/Data) Owner/Administrator/SME 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 to take care of system oriented daily operations, e.g., resolve issues brought to their attention, such as the level and scope of Platform Qualification Plans

In many cases, the Application (System) Owner acts in the role of Data Owner.

In relation to IT Infrastructure, responsibilities of the Application (System/Data) Owner/Administrator/SME typically include:

- Creation and maintenance of required documentation, e.g., copies of platform qualification reports
- 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 understand the system's functionality and impact on the business it supports or automates.

8.1.4 Data Owner

A regulated company may choose to nominate data owners where the data that a system stores, displays, manipulates, or transports is not logically owned by the Application (System/Data) Owner/Administrator/SME. For example, when the system or file storage service provides hosting capabilities for several users who need to account for data entered over long periods of time, owners of such data should be aware of their responsibilities, and equipped with adequate means to meet their responsibilities. In a XaaS engagement, data ownership and location should be established, but responsibility for the data ultimately rests with the regulated company.

Data Owners should be responsible for ensuring that the established quality, security, and data integrity 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

8.1.5 Infrastructure Process Owner/Administrator/SME

It may be appropriate to assign dedicated staff or organizational units to take care of specific IT Infrastructure processes (see Chapter 2), depending on the size of the regulated company and the IT Infrastructure.

The scope and purpose of processes 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 Owner/Administrator/SMEs may own supporting IT Infrastructure systems, in which case, they should be aware of any GxP impact that may warrant validation.

Infrastructure Process Owner/Administrator/SMEs should support audits and be trained in good conduct during regulatory inspections within their scope of responsibility.

8.1.6 Platform Owner/Administrator/SME

The role of owning an IT 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 platform.

The responsibility for each type of technical platform should be assigned to dedicated staff or organizational units, depending on the size of the regulated company. This can allow 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/Administrator/SME should provide the necessary qualification documentation for inclusion or reference. The Platform Owner/Administrator/SME should:

- Decide on short and long-term strategies for the platforms in accordance with regulated company policies
- Fund the platform operation and maintenance
- Appoint a platform administrator or SMEs to take care of daily operations
- Act as escalation level for complaints and major problems

The Platform Owner/Administrator/SME typically would have the following responsibilities:

- Creating and maintaining 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

8.1.7 Infrastructure Service Owner

The Infrastructure Service Owner is the owner of services and costs at service providers' site,

The Infrastructure Service Owner is liable for the service description and associated documentation for developing, testing, and releasing the service in the role of System Owner/System Manager, as defined in this Guide.

Each service defined in the Service Providers' Portfolio should have an Infrastructure Service Owner assigned throughout the life cycle of the service. The service should be evaluated periodically.

The Infrastructure Service Owner is usually accountable for:

- Design, construction, testing, and operation of the service

- Aligning and ensuring the service's interface to dependent services (fit for use)
- Required documentation specified through processes defined in the service providers QMS
- Ensuring adequately allocated resources and organizational structure
- Ensuring that appropriate training is in place for the successful delivery of the service
- Profit and loss for the service
- Periodic evaluation of the service

8.1.8 Independent Quality Assurance

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

The role of Independent Quality Assurance is an oversight role, ensuring that an appropriate QMS is in place to cover IT and infrastructure activities, and to monitor adherence to the QMS through audit. Independent Quality Assurance should not be involved in day-to-day IT and infrastructure operations. A quality may be established that delegates specific responsibilities to IT Quality and Compliance.

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

- Provide governance/oversight (both internally and for XaaS suppliers)
- Provide high level company procedures to meet compliance obligations
- Develop and maintain policies, processes, procedures, and other guidance documents that comprise the compliance framework. According to the regulated company policy the term "compliance framework" needs to be defined. It is important to differentiate between IT operational processes owned by IT, and compliance process, e.g., IT Supplier Assessment, IT CAPA owned by QA and/or IT QA and process owners.
- Review and approve documentation/records as appropriate, based on impact to GxP; limited to overall plans/ reports and not necessarily detailed technical documentation
- Plan and perform internal and external audits
- Review and approve periodic review reports, as appropriate
- Host regulatory inspections

8.1.9 IT Audit, Quality, and Compliance

IT Audit, Quality and Compliance should provide 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 regulated company.

IT Audit, 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 regulated 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, IT Audit, Quality and Compliance, and Quality functions at the service provider, including delegation of activities, should be documented.

8.2 Cloud Solutions Roles

Cloud service customer: a party which is in a business relationship for the purpose of using cloud services. In this Guide, it is represented with the System Owner or delegated. See ISO 17788 [38].

Cloud service provider: a party which makes cloud services available. This service could be SaaS, PaaS or/and IaaS. In this Guide, it could be represented with Infrastructure Service Owner. The cloud service provider includes an extensive set of activities (e.g., provide service, deploy and monitor service). See ISO 17788 [38].

9 Appendix 2 – Qualification Deliverables

9.1 Introduction

This Appendix provides guidance on specifying life cycle qualification deliverables and deciding which organizational units should be involved in preparation, review, and approval. Regulated companies should determine the number of deliverables and involvement required, commensurate with the assessed risks, and their own circumstances and policies. The level of oversight by IT Quality and Compliance should reflect the level of maturity of the IT organization. If IT or QA does not have the requisite experience to support the project in scope, a third party should be engaged.

Traceability between requirements, specifications, and qualification should be maintained, e.g., using traceability matrices, and should focus on areas with high potential impact on product quality and data integrity. In relation to infrastructure Commercial off the Shelf (COTS) products the number of deliverables and involvement should be kept to a minimum, based on a risk assessment.

Table 9.1 is intended to be indicative and not prescriptive; the following abbreviations apply:

- **PO:** Platform Owner or Administrator (or Service Owner at service providers' site)
- **SME:** Subject Matter Expert
- **Q&C:** IT Quality and Compliance/Independent QA

Table 9.1: Qualification Deliverables

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

Notes:
1. Role of QA/IT Q&C in ensuring that up to date Network Topology Diagrams are available should be determined.
2. The term "type" is used for the generic specifications and derived documents that would relate to building blocks (standard configurations) see Section 9.2. Qualification of a building block type would typically include all the above, except for Instance IQ and OQ.
3. The term "instance" is used for individual documents that should specify qualification details and capture results for instances of building blocks, see Section 9.2. Qualification of an instance would typically include Instance IQ and OQ only, and these would refer to the associated building block type documentation.

In practice IQ/OQ activities could be combined into one deliverable.

9.2 Infrastructure Building Block Concept

The building block concept is intended to facilitate efficient construction or upgrading of an IT Infrastructure using qualified and commissioned services, via building blocks. The infrastructure building block concept includes the following sub activities:

- IT Infrastructure Plan Stage
- IT Infrastructure Design Stage
- IT Infrastructure Construction Stage
- IT Infrastructure Qualification and Commissioning Stage
- IT Infrastructure Handover to Operation Stage

9.3 IT Infrastructure Planning Stage

A Quality Activity Plan should be established as part of the planning activities. The Quality Activity Plan should state which quality activities need to be conducted, and which QMS will be followed: the service provider's QMS or the customer's QMS.

The Quality Activity Plan should communicate deliverables for the project to project team members. The Quality Activity Plan should:

- Provide the overall qualification and commissioning strategy
- Define the scope
- Describe roles and responsibilities
- List deliverables
- Describe the use of good engineering practices, to satisfy qualification and commissioning requirements according to the QMS

The use of building blocks can help to ensure that the IT Infrastructure build is consistent and that business continuity is aligned across projects. The Quality Activity Plan should contain a list with the release note for each building block.

9.4 IT Infrastructure Design Stage

The purpose of the IT Infrastructure Design Stage is to describe the activities and documentation related to the design of an IT Infrastructure:

- Requirement specifications
- Gap analysis
- Risk assessment
- Technical design specifications
- Design review

9.4.1 Requirement Specifications

Requirements from the User Requirement Specification should be mapped to the requirements for the building blocks used to construct the IT Infrastructure. Discrepancies should be identified using a gap analysis.

9.4.2 Gap Analysis

The purpose of the gap analysis is to identify user requirements that are not fulfilled by building blocks. A gap analysis can identify requirements not fulfilled or described in the building block requirements.

The risk assessment should document handling of any gaps e.g., by describing additional test activities or other mitigating measures.

The identified gaps (requirements) should be implemented during construction. Test plans and test execution should be performed according to the IT Infrastructure Qualification and Commissioning Stage.

9.4.3 Risk Assessment

The purpose of the risk assessment is to:

- Define the correct technical implementations
- Define controls to satisfy confidentiality, integrity, and availability
- Leverage existing operational documents, e.g., instructions and procedures
- Define the right level of the test effort

Risk assessments from the individual building blocks used to construct the IT Infrastructure are used as input for the risk assessment for the IT Infrastructure. An investigation of the interoperability of the service components should be considered during the risk assessment.

9.4.4 Technical Design Specification

The purpose of the technical design specification is to:

- Explain how the IT Infrastructure is built according to the requirement specifications
- Describe the design of the IT Infrastructure architecture, detailing the physical and logical solution, and the interfaces to other infrastructure components (e.g., building blocks)
- Provide a basis for configuration management

An IT Infrastructure specific technical design specification should be developed. The technical design specification should be based on the user requirements specifications and the technical design specifications from individual building blocks.

9.4.5 Design Review Report

The purpose of the design review is to verify that the proposed design is suitable for the intended purpose.

An IT Infrastructure is typically built on already qualified and commissioned services. The design review activities should be focused on interoperability and interfaces of the services and infrastructure components.

9.5 IT Infrastructure Construction Stage

The purpose of the construction stage is to:

- Build the IT Infrastructure and ensure correct implementation of requirements based on the user requirement specification and the technical design specification
- Ensure interfaces to services are implemented, e.g., backup and monitoring
- Perform unit and integration testing: find and fix errors
- Develop documentation for installing and operating the IT Infrastructure

The services, hardware, and software components should be built, implemented, and integrated according to the design documentation. Interfaces to other services, e.g., monitoring or backup should be implemented.

Test scripts and test stubs can be prepared for executing or verifying tests. This code should be subject to code review.

The technical design specification should be updated reflecting deviations that occurred during the construction phase.

The installation guideline not covered by the services should be approved before executing installation quality activities. The operations manual should be approved before executing operation quality activities. The recovery instruction should be approved before preparation of the quality activity report.

9.6 IT Infrastructure Qualification and Commissioning Stage

The purpose of the Qualification and Commissioning stage is to execute tests to:

- Verify and document installation of the IT Infrastructure according to specifications and configuration baseline
- Verify installation methods, tools, and scripts used
- Demonstrate that functional requirements are fulfilled and fitness for intended use of IT Infrastructure is obtained
- Verify instructions and operational procedures

Scripts, e.g., those used for verification of installation or reporting, should be subject to a documented code review. The code review should be documented before executing test activities.

9.7 IT Infrastructure Handover to Operation Stage

The handover to operations should be documented to:

- Ensure correct implementation of IT Infrastructure requirements, based on requirement specification, design documents, and the quality plan
- Verify training of operations staff
- Ensure that documentation for operating the IT Infrastructure is established

The project manager should establish documentation that the IT Infrastructure is released for production and operational use with the IT Infrastructure Process Owner/Platform Owner/Administrator/SME or other relevant personnel responsible for the IT Infrastructure.

The IT Infrastructure Process Owner/Platform Owner/Administrator/SME should be responsible for operation and maintenance of the IT Infrastructure and should ensure compliant operation according to the Quality Management System. Operation includes, but is not limited to:

- Change Management
- Configuration Management
- Daily maintenance, including performance monitoring
- Periodic reviews
- Patch Management
- Decommissioning plans

10 Appendix 3 – 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 regulated company e.g.:

- Size
- Complexity
- Geographic layout
- Impact on critical aspects

Where a XaaS relationship exists, steps should be taken to understand where the vendors SOPs start, and where and how the regulated company picks up and integrates.

Table 10.1: SOP Requirements

Area of 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	• Curriculum Vitae (CV) • 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
Datacenter Management		
Day-to-Day Activities	• Datacenter 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

Table 10.1: SOP Requirements (continued)

Area of Aspect	Processes Requiring SOPs	Typical Deliverable Documentation
Datacenter Management (continued)		
Facilities Management	• Operating environment (temperature and humidity) • Supplies (UPS, RFI, EMI, generators) • Fire protection and safety management	• Regular service and test records
Platform Management		
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 • Retrieval of data from external suppliers	• Retirement records • Data archives

Table 10.1: SOP Requirements (continued)

Area of Aspect	Processes Requiring SOPs	Typical Deliverable Documentation
Servers and Mainframes		
Job Scheduling	• Assignment of batch job priorities • Ensuring proper completion of batch jobs and reprocessing when necessary	• Priority lists, especially for validated applications • Deviation reports on failures
Networks		
Third-party Networks	• Use of wide area networks • Use of wireless networks • Interfacing of local networks to wide area networks	• Network topology diagrams
Cloud		
Third-party Cloud	• Use of third-party cloud(s) • Use of cloud-based applications • Procedure for documenting a risk assessment considering the impact upon data security, integrity, and confidentiality should be available	• Audit/evaluation of provider's IT Infrastructure and handling of customer data regarding quality, compliance and IT security practices and the qualification status of their infrastructure • Risk assessment report
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 • Segregation of duties • 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 10.1: SOP Requirements (continued)

Area of 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 • Periodic reviews
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

11 Appendix 4 – Periodic Reviews

For the IT Infrastructure, a Periodic Review should establish that procedures meeting applicable GxP regulatory requirements are approved and in use. The review should also establish that qualification and operational records and review reports are complete, current, and accurate, i.e., that infrastructure is in compliance with company procedures and policies, and is fit for intended use. This should be stated in the conclusion of the Periodic Review. For a service provider, this should be incorporated in their QMS as control follow up.

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

Regulated 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 (Table 11.1) may be used when drawing up such a list of topics. Depending on circumstances, regulated companies should select which aspects to include, as the complete list may not be required or appropriate.

In the relationship between the regulated company and service provider, it is considered beneficial contractually, to have defined which information the service provider should provide to the regulated company, so that a Periodic Review can be performed, e.g., for use of a cloud solution.

Table 11.1: Example 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)?
Are vendor/provider roles and responsibilities defined (Master and/or Service Level Agreements)?
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)?

Table 11.1: Example Periodic Review Checklist (continued)

IT Management and Organization (continued)
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?
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 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, Hardware and Software Asset Management, Installation, and IQ • OQ and Acceptance • Reporting and Handover
Are these standards being followed?

Table 11.1: Example Periodic Review Checklist (continued)

Quality Systems (continued)
General (continued)
Does the QMS address infrastructure operation and maintenance processes, e.g.: • Hardware and Software Asset Management • 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 and SaaS, IaaS, and/or PaaS Vendor 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?
Tools and Infrastructure Applications
Are tools and infrastructure applications compliant with regulatory and company requirements, e.g., SOP systems, Configuration Management, change control, or access authorization
Are the risks of deploying infrastructure tools, e.g., virus protection, backup, performance monitoring, accessed?
Are tools verified to ensure they meet company standards and deliver the required functionality without unexpected side effects?
Is an inventory of tools maintained, e.g.? • Communication Protocols • Performance Monitoring Software • Virus Protection • Backup and Restoration • Software Deployment Tools • Virtualization and Replication Tools (Physical to Virtual and Virtual to Virtual Replication)
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?

Table 11.1: Example Periodic Review Checklist (continued)

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?
Are controls in place to ensure that only authorized users can access the system remotely (e.g., multi-factor authentication and device authentication)
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?
Is power conditioning in place (prevention of spikes and brown outs) and is preventative maintenance of battery systems considered?
Are backup power supplies (e.g., UPS) in place to guard against power loss to critical components?
Are UPS loads determined and monitored in a structured way
Is UPS performance verified and periodically tested?
Redundancy and Fault Tolerance
Have redundancy requirements been assessed, e.g., disk mirroring, RAID?
Have requirements for automatic standby systems been defined?
Risk Assessment Qualification Test Planning
Is the scope of qualification testing based on documented risk assessments carried out by qualified staff?

Table 11.1: Example Periodic Review Checklist (continued)

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?
Have physical and environmental constraints been considered?
Are safety requirements fully understood? Are remedial plans in place?
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 provide 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 to ensure that software, hardware, and configuration integrity is maintained?
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 breakdown, by documenting, e.g.: • Item name or identifier • 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

Table 11.1: Example Periodic Review Checklist (continued)

Configuration Management (continued)
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 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?
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., Bureau International des Poids et Mesures (BIPM)?
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?

Table 11.1: Example Periodic Review Checklist (continued)

Server Management (continued)
Environmental Conditions
Are computer rooms and datacenters 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 plans?
Have metrics been defined?
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., first, second, third 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 (re-)tested?

Table 11.1: Example Periodic Review Checklist (continued)

Backup, Restore, and Archiving (continued)
Backup and Restore (continued)
Do backup procedures address: • Frequency of backups • Physical labeling of media • Review and retention of backup logs • Periodic testing of 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 to facilitate backup?
Archive
Are decommissioning processes in place?
Are processes in place for management of data deletion?
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

Table 11.1: Example Periodic Review Checklist (continued)

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?
Is the disaster recovery process (re-)tested?
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 and/or Quality Agreements?
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?
Retirement
Have decommissioning plans been made? Including provisions for: • Data/information archiving • Transfer of processes and data
Operation Evaluation
Such evaluations should include: • Deviation records • Incidents • Problems • Upgrade history • Performance, reliability

12 Appendix 5 – Infrastructure Security

12.1 Introduction

A defined level of infrastructure security is needed 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 could impact product quality.

A regulated company should take cultural and practical aspects into consideration when defining the rigor of its approach. Regulated companies may adopt different approaches for specific infrastructure elements, based on criticality and risk, for example. The following infrastructure measures should also be established at external companies (e.g., XaaS providers, datacenters). It is the responsibility of the regulated user to decide which security level is adequate and requested from the XaaS provider.

12.2 Infrastructure Security Management

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

12.2.1 Standards

At a minimum, regulated companies need to satisfy the applicable GxP requirements. Relevant documents include the PIC/S Guide [38], which was originally built on ISO/IEC 27001 [11] and ISO/IEC 27002 [39]). US FDA 21 CFR Part 11 [36] contains security requirements focused on electronic records and signatures.

RFC 2196, *"Site Security Handbook,"* is another useful source of information [40].

Infrastructure security is a subset of a regulated company's IT security management plan and companies may elect to extract applicable guidelines from, e.g., ISO/IEC 27001 [11] and ISO/IEC 27002 [39], and apply those to infrastructure elements.

In addition, general requirements from EU GMP Annex 11 [1] should be considered.

Security controls, in general, are considerably more cost effective and efficient if incorporated at the requirements specification and design stages. The following sections list some standards in a non-prioritized sequence.

12.2.1.1 NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," [41] provides a catalog of security controls for all US federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. The control matrix is comprehensive and provides a full accounting of all relevant IT security control considerations. While there is no statutory requirement for compliance, the NIST guideline is an excellent resource for achieving and maintaining GxP compliance.

12.2.1.2 NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing

NIST Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing" [42], provides an overview of the security and privacy challenges pertinent to public cloud computing.

12.2.1.3 ISO/IEC 27001:2013 Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements

Per ANSI: ISO/IEC 27001 [11] specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001 [11] are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

12.2.1.4 ISO/IEC 27002:2013 Information Technology -- Security Techniques -- Code of Practice for Information Security Controls

Per ANSI: ISO/IEC 27002 [39] gives guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration the organizations information security risk environments.

It is designed to be used by organizations that intend to:

1. Select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001 [11]

2. Implement commonly accepted information security controls

3. Develop their own information security management guidelines

12.2.1.5 Cloud Security Alliance – Cloud Controls Matrix

Per CSA: The Cloud Security Alliance Cloud Controls Matrix (CSA CCM) [9] is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The Cloud Controls Matrix provides a control framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in thirteen domains.

The foundations of the CSA CCM Matrix [9] rest on its customized relationship to other industry accepted security standards, regulations, and control frameworks such as the HITRUST CSF [43], ISO 27001 [11], ISO 27002 [39], COBIT® [44], PCI [18], HIPAA [45] and NIST [7], and will augment or provide internal control direction for service organization control reports provided by cloud providers. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry.

The CSA CCM [9] strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

12.2.2 Regulatory Implications

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

12.2.3 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, segregation of duties, etc.
- Physical controls consist of controlling individual access into the facilities and different departments, locking systems, removing unnecessary external drives from workstations, protecting the perimeter of the facilities, monitoring for intrusion, etc.

12.2.4 Security Incident Management

To ensure efficient coordination of security incidents, an incident management procedure should be established as effective communication channels are needed for 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 example, 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.

12.2.5 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 established 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.

12.2.6 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.

12.2.7 Anti-Virus Shield Update

Most anti-virus applications can initiate totally automatic updates, but regulated companies may 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.

12.2.8 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 should install client programs and to obtain a certificate from a trusted third party, either directly or via the regulated company's own Certification Authority (CA).

12.2.9 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 regulated 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. This also covers internal IT usage of open source software.

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

12.2.10 Origin of Infrastructure

A large infrastructure reseller market exists in the outsourced service space. Vendors offering cloud solutions and infrastructure services should be carefully vetted so that the regulated company understands when the IT Infrastructure is actually resident, and if leased, who actually controls and manages it. Further collocation space, racks, cabinets and cages are easily procurable in third-party datacenters and can then be marketed into the XaaS space. While these types of relationships may not preclude the ability to establish or maintain GxP compliance, they can add several layers of vendor management, security, and infrastructure risks that may not be immediately obvious.

12.3 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.

Firstly, 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

Secondly, the urgency of the change should be established.

12.3.1 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

12.3.2 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.

13 Appendix 6 – Upgrade and Patch Management

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

13.1 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). IT infrastructure changes may be pre-approved, i.e., the change can be made without needing the final QA to approve each one; the QA approves the change as a pre-approved type of change (configuration management records are still updated). These are for expected changes, and helps accelerate the change process.

- **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, attention should be given to incident monitoring and reporting.

13.2 Upgrade Strategy

Regulated companies should implement patch and upgrade management that includes:

- Provision for criteria for providing instructions for determining enterprise impact or threat levels, and the urgency for upgrade
- A defined process that clearly articulates the procedural path for upgrade and patch management
- Allowance for flexibility for applying patches or upgrades based on risk to the enterprise and the validated status of regulated computerized systems
- Generates records that show the version and patch level for a system during any point in the life cycle
- Generates documentation that details the approach to testing and what level of testing was performed

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 scope (level of infrastructure), complexity, and possible impact on applications. The IT group should notify owners of critical applications and provide the results of the technical assessment. This should include the timing of when the upgrade should take place.

- 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 and 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.

13.3 Level of Application Testing

The degree of testing can vary form no testing, limited functional testing to a full validation exercise commensurate with the assessed risk.

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 dependent 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 risk assessment process defined in *ISPE GAMP® 5* [14] can be used for assessing the "Patch Level and Related Risk Strategy" that will assist with defining the appropriate level of testing to apply. 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.

13.4 Global/Multi-site Systems

For systems that are used at multiple locations, where the regulated company has a worldwide standardization of platforms, testing may be performed at a single location and this is then used as the basis of reduced, or no, testing at the other locations.

14 Appendix 7 – Outsourcing

14.1 Definition of Responsibilities

Outsourcing involves the transfer of management and operations of a regulated company's IT Infrastructure to an external company or internal outsourcing, e.g., the centralizing of IT services within an enterprise with support for several economically separated subsidiaries or divisions. See *ISPE GAMP® 5* [14]. The scope varies, but some examples include:

- Use of off-shore, near-shore, or on-shore suppliers
- Use of external supplier resources only
- Use of external supplier computing environments
- XaaS engagement
- Collocation (using a third-party datacenter available for rental to customers instead of self-owned infrastructure)
- Operation of a datacenter and/or networks
- Operation of systems and/or processes (e.g., Help Desk)
- Hardware/software component build (e.g., workstation)
- Hardware/software maintenance and support (e.g., cloud-based infrastructure and XaaS)

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 accountable 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 outsourced service provider is responsible for the day-to-day management of the infrastructure.

The external service provider has the responsibility for ensuring that their service meets the customer's requirements. A regulated company's QMS should be the basis for evaluation when confirming that the service provider meets these requirements. Alignment of responsibilities and expectations between service provider and the regulated company should be clearly reflected in the contract. 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[6]
- Quality assurance and quality control of their IT Infrastructure processes and procedures

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

- Data and system security
- Data privacy

14.2 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 datacenter or a Help Desk process).

Regulated companies engaging in international data transfer and storage should ensure compliance with local and national data privacy regulations.

14.3 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 (e.g., ITIL®).

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 clearly define responsibilities for assuring the control of the infrastructure and the day-to-day management of the 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 facilitating inspections, agreed notifications, and alert levels also should be specified.

Contracts should also define the terms for ending the outsourcing agreement (e.g., bringing an application/outsourced service back in-house).

Contracts should contain conditions for how an exit of services will occur and the roles and responsibilities for each entity. This includes:

- After termination of a contract/service all relevant assets, documentation and data must be transferred back to the regulated company
- Verification (audit) that all relevant assets, documentation and data have been transferred back to the regulated company

14.4 Service Level Agreements or Quality Agreements

Where services or other deliverables are requested by one organization and are provided by another (either internal[7] or external), consideration should be given to establishing mutual expectations in a formal SLA or Quality Agreement.

An SLA can be 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
- Prerequisites 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
- Defined parameters for roles and responsibilities (e.g., maintenance of quality system requirements and controls) as per quality agreements requirements for EU GMP Annex 11 [1]
- Processes to be supported and managed between the two parties, and the service levels including escalation, e.g., parameters for backup frequency, retention periods and retrieval times

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

For further information see *ISPE GAMP® 5* [14].

[7] This is a regulatory requirement for companies who must comply with EU GMP Annex 11 [1].

14.5 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 Preventive Actions (CAPA) program to closure 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 to an appropriate resolution.

A common set-up with large datacenters occurs where the regulated company does not have a contract directly with the datacenter, no direct access for audit, and needs to rely on a service provider contract and SLA with the datacenter.

Datacenter and cloud providers may have independent third-party certifications for IT controls and security, such as ISO/IEC 27001 [11], SOC 2 Type 2 [30], etc. While these certifications provide valuable insight into the daily operations of the company under consideration, they should be carefully assessed to ensure that all of the relevant GxP requirements are being met (e.g., Infrastructure Qualification).

A regulated 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.

For further information see *ISPE GAMP® 5* [14].

14.6 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, according to contract and the regulated company's risk assessment of outsourced activities. Such training should be documented and readily available.

15 Appendix 8 – Server Management

15.1 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 regulated 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 intended to assist companies, and not to prescribe absolutes.

15.2 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. See *ISPE GAMP® 5* [14].

15.2.1 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 backup: all other days
- Historical backups should be taken as appropriate. There can be legal considerations to evaluate that can dictate for how long the regulated company should keep backups. Some regulated companies' legal departments do not recommend keeping backups for long, as they can be subject to investigations. This also depends on the type and content of the data.

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

15.2.2 Verification

Most commercially available backup solutions can perform 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.

15.2.3 Schedules

The type of data should largely dictate the backup schedules. At the enterprise level, data actively in use may 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.

Specific 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.

15.2.4 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.

15.2.5 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.

For further information see *ISPE GAMP® 5* [14].

15.2.6 Testing

Testing the backup process should include any off-site storage solutions and should aim to restore data from historical backups.

Restoring historical backups may require the handling of off-site backups, which should ensure that the procedure to recall off-site media works as anticipated.

Restoring actual backups and comparing against the unchanged original file, where possible, can help to maintain the integrity of data. It also gives an opportunity to check that the entire data path, from original backup of the data through to the final restore, maintains data integrity.

Testing the backup process can certify the process of both the backup and restore procedures.

15.3 Technical Performance and Capacity Monitoring

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

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

Surveillance procedures should be developed, and alert and action limits defined to ensure that servers perform as required.

Where IT Infrastructures mostly support administrative type applications, server performance may be considered a statistical entity that, on average, should provide a particular level of service. The platform manager should consider the degree of equipment utilization (for economic reasons) and the operational key alarm limits should be set around available storage capacity.

For time-critical systems, the platform manager should consider ensuring sufficient reserve resources to meet surges in demand. Table 15.1 lists sample performance metrics for a process control server, as an aid in deciding metrics and limits. Allowing a higher load on a server may present less risk to product quality attributes or required records (e.g., on a server) than replacing the server with a new, more powerful server.

Table 15.1: 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 dependent 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, monitoring and event reaction could be automated.

For further information see *ISPE GAMP® 5* [14].

15.4 Remote Management

The required level of security should be maintained when servers are managed remotely, e.g., via outsourcing or offshoring arrangements. The use of secure communication channels should be considered.

15.5 Server Virtualization

Server virtualization is a technology that makes it possible to run multiple operating systems (virtual servers) on the same physical server at the same time. In regard to e.g., testing, documentation, and operation, there is no difference compared to physical servers: virtual servers should be handled the same way as physical servers. However, virtualization introduces an extra layer of administration compared to the operation of physical servers. The consequence of this extra administration layer is added risks which need to be addressed and mitigated. Examples of risks and mitigating actions are listed in Table 15.2.

Table 15.2: Example Risks and Mitigating Actions

Risk	Mitigating Action
Complexity of the virtualization layer in the infrastructure	• Training • Development of operational processes and procedures • Segregation of duties
Close dependencies to other infrastructure components such as storage and network	Organizational Level Agreements (OLA) between departments in order to determine responsibility
Virtualization puts “many eggs in few baskets”	Disaster recovery plans addressing this

15.5.1 Server Virtualization and Cloud Computing

Server virtualization is the foundation of cloud computing. Cloud computing is a service based on server virtualization and usually offered in three models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), commonly referred to as XaaS. See Appendix 11 for details of these three models.

16 Appendix 9 – Client Management

16.1 Client Types

16.1.1 Traditional

Personal Computers (PCs) in the form of stationary PC units, laptops, or hand-held client devices are used by regulated companies in a variety of roles with distinct risk profiles, depending upon their use. Those that are connected to the regulated company's network may be prepared and maintained according to a set of client types, e.g., unrestricted, restricted, or controlled. The term PC is used broadly to cover client devices such as tablets, mobile technology, and traditional PCs.

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

16.1.2 Virtualized

In a cloud-based environment, where XaaS delivery is part of a regulated company's internal IT Infrastructure, the traditional client may be replaced with a virtualized equivalent. The process by which the client is created and maintained should be documented.

16.2 Client Management

The client management group, or designated individual, should maintain the expertise and resources required to provide adequate client management services to the regulated company. Some of the main responsibilities of the unit include:

- To acquire formal approval by QA and management representatives for significant changes
- To apply change controls in conformance with procedures (see Chapter 6 and Appendix 6)
- 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 viruses
- 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)
- Installation and set-up of standard clients
- Prior to delivery of PCs 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

16.3 PC Platform

PCs should possess sufficient computing power and connectivity to run the client software and other software that is required by the applications. The regulated 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.

16.4 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 according to the applicable SOPs.

The configuration of critical items of the client operating system can be grouped into three categories:

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

16.5 User Modifications

Regulated company policies may dictate whether clients should be restricted from user modification (see Chapter 5). 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.

16.6 Images or Installation Scripts

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

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

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

16.7 Patch Management

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

In addition to test requirements, security patch information from the supplier should be made available to the organization. This can 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).

17 Appendix 10 – Network Management

17.1 Introduction

The current dominating network technology is based on internet standards, including the protocols:

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)

This Appendix focuses on providing recommendations based on these standards. Regulated companies that use other technology may still find concepts described in this Appendix useful.

All quantitative measures provided in this Appendix are derived from actual situations and are intended to assist regulated companies, and do not to prescribe specific absolutes.

17.2 Goal

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

17.3 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 regulated 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
- Risk Assessment
- Design
- Design Review
- Analysis
- Facilities Installation and Maintenance
- Network Installation
- Partitioning of virtual infrastructure components
- Data Gathering and Analysis

Operations and Maintenance

- Incident and Problem Management
- Routine Network Tests

Network Operation Center (NOC)

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

17.4 Network Provisioning and Installation

Network provisioning involves:

- Maintenance of network risk assessments, specifications, topologies and design, and control requirements.
- Network planning and design. This is the responsibility of the network engineering group which should keep track of new technologies and introduce them, as needed, and in conformance with applicable standards and regulated company requirements.
- Identification of bottlenecks through analysis of traffic and performance data provided by the NOC. 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.

17.5 Network Operation Center

Typically, the Network Operation Center (NOC) is headed by the overall network administrator. The function of the NOC 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 Simple Network Management Protocol (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 ensuring that all manageable network devices respond as required, e.g., via Syslog[8], an industry standard used to log information for network devices
- Ensuring 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
- Confirming that approved security procedures are followed by tracking all network accesses and by ensuring 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

17.6 Common Network Tools and Configuration

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

17.6.1 Simple Network Management Protocol (SNMP)

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. Suppliers can build SNMP agents into their products, because it is a simple solution, requiring little code to implement. SNMP also separates the management architecture from the architecture of the hardware devices, which broadens the base of multi-supplier support.

17.6.2 Syslog

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.

[8] In computing, syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

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.

17.6.3 Remote Monitoring (RMON)

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

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

17.7 Network Types

17.7.1 Wide Area Network

A Wide Area Network (WAN) is network that spans a large geographic area (Metro, Region, Global) A WAN is used to transmit data across long distances to connect physically disparate LANs.

17.7.2 Local Area Network

A Local Area Network (LAN) is a computer network that typically spans a small geographic area such as an office, building, or campus to facilitate high speed communication between Ethernet enabled devices. LANs maybe segmented into virtual local area networks for traffic isolation to a specific group of users or roles.

17.7.3 Virtual Local Area Network

Virtual Local Area Networks (VLANs) are networks of computer or Ethernet enabled devices that act as if they are on the same wire, even though they may be geographically dispersed. Segregation of VLANs is performed on the software level of an Ethernet switching device.

One of the main benefits of a VLAN implementation is that it allows the combination of a geographic dispersion of users with the security of isolating communication at the switch level only with other members of the VLAN.

17.7.4 Storage Area Network

A Storage Area Network (SAN) is a high-speed network which allows servers to access remote storage devices on a block level. SANs commonly employ Fiber Channel or high-speed Ethernet based protocols to facilitate wide geographic dispersion for organization wide storage consolidation and simplified disaster recovery management.

Elements that commonly comprise a SAN are storage switches, tape backup devices and disk based RAID storage arrays.

The implementation of SANs in a wide range of organizational sizes has become increasingly more common with the adoption of virtualization technology. The use of a SAN in this environment allows the pooling and transparent expansion of storage resources that would not be attainable with local storage options.

17.8 Network Performance Metrics

Table 17.1 represents actual settings for a network segment and may be used as guidance for a regulated company to decide on its own metrics and limits.

Table 17.1: Example Network Performance Limits

Network Metrics	Unit	Alert Limit	Action Limit
Average Load over 24 hours	%	> 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 at least once daily should be considered for smaller organizations, mission critical infrastructure should be subject to real-time monitoring.

18 Appendix 11 – Traditional versus XaaS Model Comparison

In the following Sections characteristics of the three XaaS types are listed. For a definition of the three types see the definition provided by NIST (NIST Special Publication 800-145: The NIST Definition of Cloud Computing [12]).

18.1 Infrastructure as a Service

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
IT Infrastructure Elements				
Platforms	Physical access to servers no longer possible	• Reduces redundancy – buy only the space you need • The user's peak load capacity increases and efficiency of the user's in-house systems (which are usually underutilized), is improved	• No access to physical hardware • Potential for down time out with control of Platform Owner • Compatibility of IaaS and internal legacy infrastructure	• Audit datacenter, enforce quality practices • SLA • System/process audit
Processes	Change and configuration management under third party control	Requirement for hardware Change Control (CC) outsourced	Limited visibility to hardware changes	• Audit datacenter, enforce quality practices • SLA • System/process audit
Personnel	Hardware personnel under third party	• Reduced labor cost • Costs and resources are shared by IaaS users and the infrastructure is centralized by the provider	No direct supervisory control of key personnel	• SLA • Require up to date training records • Clear definition of responsibilities
Quality Management System				
Quality Manual	• Quality system expanded beyond your door • Providers typically make System and Organization Control (SOC) 1 or SOC 2 or equivalent information available on request, under non-disclosure agreement	Allows focus on core quality functions	• Out of site out of mind • Relying on third party to follow quality processes • Standards do not yet exist: CSA [9], NIST [7], AICPA [46] and DMTF [47] developing a set of standards for cloud computing • Standards will apply to security, operational auditing and compliance • Providers can obtain SOC 2 type 2 certification, but this has been criticized that the set of goals and standards determined by the auditor and the auditee may not be disclosed and can vary widely among providers	The SLA/Quality Agreement with a third party should cover the required certification (e.g. ISO 9001 [17], SSAE 16 [16] / SOC 2 Type 2 [30], ISO/IEC 27001 [11]) to ensure quality, compliance with regulations, and IT security, as well as a non-disclosure agreement on audit results, the right to audit, and the support of audits/inspections at the regulated company site(s) by the service provider.

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Quality Management System (continued)				
Roles and Responsibilities	Hardware installation and maintenance outsourced, only administrative task remains	Refocus resources on other tasks	• Attrition, lack of oversight as to third party hiring/firing methods • Roles and responsibilities are not clearly defined	• SLA • Require up to date training records
Record Management	• Record management requirements remain • There are existing laws and policies in place, which do not allow sending private data onto third party systems • The regulated company is ultimately responsible for compliance to federal and state regulations such as HIPAA [45], SOX [48], US-EU Privacy Shield [49] and other personal medical information for the pharma and insurance industries	None	• Key records stored offsite • Privacy and security concerns • Information is stored remotely, which means that legally (contract and SLA will specify) the IaaS provider is responsible for data	• Periodic audit • Limit access to key records Enforce security policy • Contract and SLA regarding data ownership and privacy • Encrypt, remove, or redact private data
Documentation	Documentation likely resides at third party site	Reduced internal burden on document storage	Third party may not adequately document and account for key hardware	Requires change management configuration specifications for all outsourced hardware
Testing	Testing conducted remotely or at third party site	Testing requirement remains but can be outsourced to third party	• Inadequate tests • Physical verification can only be done by third party	Requires third party to supply IQ documentation for all hosted (shared) infrastructure
Standard Operating Procedures	SOPs must now connect to external group	Potential to learn from/ improve hardware management process from third party	Poor linkage between external and internal policy	• Create a bridge document for internal/ external quality systems • Tie to SLA and ensure shared responsibility
Training	Training now extended to third party	Increased resource pool as needed	• Adequacy of training • Reliance on third party to follow instructions • Limited oversight	• Build training requirements into SLA • Conduct periodic audits to ensure third party enforcement
Periodic Review and Evaluation	Periodic review and evaluation now includes review of third party	Third party has infrastructure management as core competency, likely leading to improved service levels	• More difficult to assess external party than internal • Third party maybe resistant to audit and regulatory inspection	Require audit rights in SLA
Audit by QA	Third party QA now responsible for daily QA function	Reduces burden on internal QA	• Third party QA may not have best interests of hosted party in mind • Auditing IaaS vendors is new to many auditors (auditors may not fully understand the technology, risks, and mitigating controls)	• Audit datacenter • Enforce quality practices • SLA

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Applying Risk Management				
Identification and Assessment of Components	Components are now physically external	• Reduced hardware maintenance costs • Reduced energy costs • Reduced labor costs • Resources are provided on a "scalability" basis • The system is closely monitored, and clients do not have to plan in-house for those times when higher loads will be needed	More difficult to tie one server to one application, particularly in the cloud	Require detailed accounting from third party as to the disposition of all components engaged in the contract
Implementation of Controls	• Hardware IT controls are now the responsibility of the third party • IaaS is a paid-for service, which means that the finance department will want to keep a record of how the service is being used • Some of the new considerations include trans-border information flow as data may be subject to the laws of multiple jurisdictions, impact to large population of unrelated users, new data privacy laws (businesses may be legally barred from placing certain information at the IaaS vendor)	Can benefit from tried and tested controls, third party are SMEs in hardware management	• Inadequate controls • Poor enforcement • Shelfware	• Audit datacenter • Enforce Quality practices • SLA • System/process audit • The IaaS vendors provide audit trail information, but in the case of a dispute it is important to have an independent audit trail
Assessment of Changes to Qualified Components	Change assessment now placed on the third party	As the hardware physically resides with the third party, they are best placed to assess change	Assessment may not fully examine all risks associated with hosted applications or infrastructure	Require internal QA and SME approval on change management process and related risk assessment (e.g., pre-defined changes with risk assessment, risk mitigation actions, involvement of the customer) by SLA/ agreement and/or bridging SOPs as mentioned in Chapter 3
Periodic Review and Evaluation	Periodic review and evaluation now includes review of third party	Third party has infrastructure management as core competency, likely leading to improved service levels	• More difficult to assess external party than internal • Third party maybe resistant to audit	• Require audit rights in SLA • Define roles and responsibilities for both the regulated company and the service provider in SLA/quality agreement

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Qualification of Platforms				
Overview of Process	Third party required to establish internal Computerized System Validation (CSV) policy	Reduces burden on internal validation resources	Adequacy of external CSV policy	• Provide comment and edits to external CSV policy where possible • Ensure adequacy during supplier quality audit and periodic assessment
IT Infrastructure Life Cycle Model	Infrastructure life cycle now at discretion of external party	Reduced hardware cost	Third party may not have adequate insight into IaaS hardware replacement policy	Establish life cycle expectations in the SLA/ contract
Planning	Qualification planning now at the discretion of third party	• Reduces burden on internal validation resources • Agility improves with ability to quickly and inexpensively reprovision infrastructure resources	Plan may fail to address all necessary components for robust qualification	Ensure that internal IT/ QA resources participate in Qualification Planning for any infrastructure components in scope of SLA/contract
Specification and Design Phase	Hardware specifications ownership now resides with third party	Dedicated resources with hardware configuration as core competency	Configuration documentation may fail to capture all necessary static configuration items	Require review of any configuration documentation created for infrastructure components in scope of SLA/contract
Risk Assessment and Qualification Test Planning	Reliance on third party for majority of Risk Assessment (RA) and test planning	Reduces internal validation burden	RA and tests may not be robust	Ensure that internal IT/QA resources participate in RA/test case in scope of SLA/contract
Procurement, Installation, and IQ	Hardware procurement, installation and IQ now conducted externally	• Economies of scale for hardware buys • Shared space and resources • Reduced labor costs • Reduced internal validation burden	Procured hardware may not be adequate from a performance perspective, maybe installed incorrectly and or poorly IQ'd	Supplier quality audit should establish that third party has strong capabilities in the area
OQ and Acceptance	For IaaS, OQ remains an internal task	None	OQ relying of system hosted externally	Ensure enforcement of SLA
Reporting and Handover	IQ summary report prepared by third party	Reduces internal validation burden	IQ summary inadequate or reveals unresolved deviations	Ensure that internal IT/QA resources participate in summary report review in scope of SLA/contract
IT Infrastructure Control and Compliance	IT Infrastructure control and compliance is a shared responsibility with third party	SME team expanded	• Third party may lack knowledge of GxP expectations and regulatory inspection potential • Large organizations using IaaS vendor services may have a need of mirrored IaaS	• Use supplier quality agreement to determine gaps or deficiencies in GxP knowledge Task internal resources with training of third party until that expected by SLA is met • Companies should consider single sign-on between the regulated company and the IaaS vendor

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Maintaining the Qualified State During Operation				
Change Management	• Change management function largely outsourced • Shared responsibility	Dedicated resources with hardware configuration as core competency	• Changes not recorded appropriately or in enough detail (currently it states changes not recorded only) • Appropriate personnel may not be involved in the change control process (particularly if multiple parties involved), oversight of who to involve in the change control process may not be detailed enough	• Require internal QA or IT signature on risk assessments and changes for hardware covered under the scope of the SLA/ contract • Periodic audit
Configuration Management	• Configuration management function largely outsourced • Shared responsibility	Dedicated resources with hardware configuration as core competency	Configuration documentation not kept up to date	Require review of any configuration documentation created for infrastructure components in scope of SLA/contract
Security Management	• Security management function largely outsourced • Shared responsibility	• As infrastructure management is a core competency of third party, security controls are likely more robust and advanced than that available internally • IaaS providers devote their resources to preventing or resolving security problems, which some businesses may not have the SME or may not afford to do	• Reliance on third party to secure data • Unauthorized access to a firm's data and processes: authentication and authorization is controlled at the IaaS and not at/ by the regulated company and it may be difficult to establish effective oversight of permissions changes and controls	• Supplier quality audit • SLA • Periodic Review • Organizations, such as the IaaS Vendor Security Alliance, have been formed in order to provide standards and best practices for security assurance for IaaS vendor computing
Server Management	• Server management function largely outsourced • Shared responsibility	Burden of hardware management outsourced	Reliance on third party to maintain and managed key infrastructure	• Supplier quality audit • SLA
Client Management	Client management remains internal	None	Clients most connect to external servers	• Require connectivity testing • Ensure uptime requirements are included in SLA
Network Management	Internal/external networks commingled	Expansion of network horsepower and capability	Potential exposure to nefarious third parties	• Ensure uptime requirements are included in SLA • Ensure security firewall's an intrusion detection/prevention is acceptable

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Maintaining the Qualified State During Operation (continued)				
Problem Management	• Problem management function largely outsourced • Shared responsibility	Third party has core competency in external customer problem management	Problem prioritization may favor other customers and it may be difficult to establish effective oversight of change requests and Help Desk tickets	SLA enforcement
Help Desk	• Help Desk function largely outsourced • Shared responsibility	• Help Desk function outsourced • Reduced labor cost	Non-responsive help desk	SLA enforcement
Backup, Restore, and Archiving	• Backup, restore, and archiving function largely outsourced • Shared responsibility	Backup, restore, and archiving function can now benefit from dedicated facilities and economies of scale	Inadequate Backup and Restore (B&R) testing could lead to data loss	• SLA enforcement • Test B&R scenarios with third party
Disaster Recovery	• Disaster recovery function largely outsourced • Shared responsibility	• Likely improvement in disaster recovery facilities and reduction in restore time • Due to reliability at multiple sites, IaaS provides business continuity and helps to ensure disaster recovery for the user	Disaster recovery time may be increased	• SLA enforcement • Test disaster recovery scenarios with third party
Performance Monitoring	• Performance monitoring function largely outsourced • Shared responsibility	Third party has core competency in network performance monitoring	• Failure to act on performance dips • Failure to adequately monitor service levels	• SLA enforcement • Stress test for performance
Supplier Management	Supplier management shifts from hardware suppliers to service suppliers	None	Requires significant rethink of supplier management strategy	• Supplier Quality Audit • SLA
Periodic Review		None	Geographical considerations may limit ability to successfully execute periodic reviews in a timely manner	• Supplier Quality Audit • SLA
Retirement of Platforms				
System Retirement	System retirement now a shared responsibility	Cost of retirement hardware spread over all third-party customers reducing cost internally	Potential for data loss if systems are not retired in an orderly fashion	Ensure that internal IT/QA resources participate in retirement planning for any infrastructure components in scope of SLA/contract

18.2 Platform as a Service

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
IT Infrastructure Elements				
Platforms	Physical access to servers no longer possible	• Reduces upfront platform cost: no need to purchase hardware or assign internal resource support • Reduced hardware cost could result in additional funds for platform modules	• No access to physical hardware Potential for down time out of control of platform owner • Compatibility of PaaS with internal legacy infrastructure	• Audit datacenter • Enforce quality practices SLA • System/process audit
Processes	Change and configuration management under third party control	Requirement for hardware CC outsourced	Limited visibility to hardware changes	• Audit datacenter • Enforce quality practices • SLA System/process audit
Personnel	Hardware personnel under third party	• Reduced labor cost • Costs and resources are shared by PaaS users, and the infrastructure is centralized by the provider	No direct supervisory control of key personnel	• SLA • Require up to date training records
Quality Management System				
Quality Manual	• Quality system expanded beyond your door • Providers typically make SSAE 16 [16] / SOC 2 Type 2 [30] or equivalent information available on request, under non-disclosure agreement • An upgrade to new platform modules or administration responsibility may be shared with third party	Allows focus on core quality functions	• Out of site out of mind • Relying on third party to follow quality processes • Standards do not yet exist: CSA [9], NIST [7], AICPA [46], and DMTF [47] developing a set of standards for cloud computing • Standards will apply to security, operational auditing and compliance • Providers can obtain SSAE 16 [16] / SOC 2 Type 2 [30] certification, but this has been criticized that the set of goals and standards determined by the auditor and the auditee may not be disclosed and can vary widely among providers	• Establish quality agreement with third party • Providers obtain SSAE 16 [16] / SOC 2 Type 2 [30] certification
Roles and Responsibilities	Hardware installation and maintenance outsourced, only administrative tasks maybe shared or completely outsourced.	Refocus resources on other tasks	• Attrition, lack of oversight as to third party hiring/firing methods • Reliant on third party security features	• SLA require up to date training records • Ensure datacenter has robust security policy

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Quality Management System (continued)				
Record Management	• Record management requirements remain • There are existing laws and policies in place, which do not allow sending private data onto third party systems • The regulated company is ultimately responsible for compliance to federal and state regulations such as HIPAA [45], SOX [48], and other personal medical information for the pharma and insurance industries	None	• Key records stored offsite • Privacy, Security concerns • Information is stored remotely, which means that legally (contract and SLA will specify) the PaaS provider is responsible for data	• Periodic audit • Limit access to key records • Enforce security policy • Contract and SLA regarding data ownership and privacy • Encrypt, remove, or redact private data
Documentation	Documentation likely resides at third party site	Reduced internal burden on document storage	Third party may not adequately document and account for key hardware	Require change management configuration specifications for all outsourced hardware
Testing	Testing conducted remotely or at third party site	Testing requirement remains but can be outsourced to third party	• Inadequate tests • Physical verification can only be done by third party	Require third party to supply IQ (and potentially OQ) documentation for all hosted platforms
Standard Operating Procedures	SOPs must now connect to external group	Potential to learn from/ improve hardware management process from third party	Poor linkage between external and internal policy	• Create a bridge document for internal/ external quality systems • Tie to SLA and ensure shared responsibility
Training	Training now extended to third party	Increased resource pool as needed	• Adequacy of training • Reliance on third party to follow instructions • Limited oversight	• Build training requirement into SLA • Conduct periodic audits to ensure third party enforcement
Periodic Review and Evaluation	Periodic review and evaluation now includes review of third party	Third party has infrastructure management as core competency, likely leading to improved service levels	• More difficult to assess external party than internal • Third party maybe resistant to audit	Require audit rights in SLA
Audit by QA	Third party QA now responsible for daily QA function	Reduces burden on internal QA	• Third party QA may not have best interests of hosted party in mind • Auditing PaaS vendors is new to many auditors (auditors may not fully understand the technology, risks, and mitigating controls)	• Audit datacenter • Enforce quality practices • SLA • System/process audit

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Applying Risk Management				
Identification and Assessment of Components	Components are now physically external	• Reduced hardware maintenance costs • Reduced energy costs • Reduced labor costs • Resources are provided on a “scalability” basis • The system is closely monitored, and clients do not have to plan in-house for those times when higher loads will be needed	More difficult to tie specific servers to the platform, particularly in the cloud	Require detailed accounting from third party as to the disposition of all components encompassing the platform in the contract
Implementation of Controls	• Hardware IT controls are now the responsibility of the third party • PaaS is a paid-for service, which means that the finance department will want to keep a record of how the service is being used • Some of the new considerations include transborder information flow, data may be subject to the laws of multiple jurisdictions, impact to large population of unrelated users, new data privacy laws (businesses may be legally barred from placing certain information at the PaaS vendor)	Can benefit from tried and tested controls, third party are SMEs in platform management	• Inadequate controls • Poor enforcement • Shelfware	• Audit datacenter • Enforce quality practices • SLA • The PaaS vendors provide audit trail information, but in the case of a dispute it is important to have an independent audit trail
Assessment of Changes to Qualified Components	Change assessment now placed on third party	As the hardware physically resides with third party they are best placed to assess change	Assessment may not fully examine all risks associated with hosted platform	Require internal QA or IT signature on risk assessments and changes for platform covered under the scope of the SLA/ contract
Periodic Review and Evaluation	Periodic review and evaluation now includes review of third party	Third party has infrastructure management as core competency, likely leading to improved service levels	• More difficult to assess external party than internal • Third party maybe resistant to audit	Require audit rights in SLA
Qualification of Platforms				
Overview of Process	Third party required to established internal CSV policy	Reduces burden on internal validation resources	Adequacy of external CSV policy	• Provide comment and edits to external CSV policy where possible • Ensure adequacy during supplier quality audit and periodic assessment

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Qualification of Platforms (continued)				
IT Infrastructure Life Cycle Model	Platform life cycle now at discretion of external party	Reduced platform cost	Third party may not have adequate insight into PaaS hardware replacement policy	Establish Lifecycle expectations in the SLA/ Contract
Planning	Qualification Planning now at the discretion of third party	• Reduces burden on internal validation resources • Agility improves with ability to quickly and inexpensively re-provision platform resources	Plan may fail to address all necessary components for robust qualification	Ensure that internal IT/QA resources participate in qualification planning for any platform components in scope of SLA/contract
Specification and Design Phase	Platform specification ownership now resides with third party	Dedicated resources with platform configuration as core competency	Configuration documentation may fail to capture all necessary static configuration items	Require review of any configuration documentation created for platform components in scope of SLA/contract
Risk Assessment and Qualification Test Planning	Reliance on third party for majority of RA and test planning	Reduces internal validation burden	RA and tests may not be robust	Ensure that internal IT/QA resources participate in RA/test case in scope of SLA/contract
Procurement, Installation, and IQ	Platform procurement, installation and IQ now conducted externally	• Economies of scale for platform buys • Shared space and resources • Reduced labor costs Reduced internal validation burden	Procured platform may not be adequate from a performance perspective, maybe installed incorrectly and or poorly IQ'd	Supplier quality audit should establish that third party has strong capabilities in the area
OQ and Acceptance	For PaaS OQ remains an internal task	None	OQ relying on system hosted externally	Ensure enforcement of SLA
Reporting and Handover	IQ summary report prepared by third party	Reduces internal validation burden	IQ summary inadequate or reveals unresolved deviations	Ensure that internal IT/QA resources participate in summary report review in scope of SLA/contract
IT Infrastructure Control and Compliance	IT platform control and compliance is a shared responsibility with third party	SME team expanded	• Third party may lack knowledge of GxP expectations. • Large organizations using PaaS vendor services may have mirrored solutions	• Use supplier quality agreement to determine gaps or deficiencies in GxP knowledge Task internal resources with training of third party until that expected by SLA is met • Companies should consider a single sign-on between the regulated company and the PaaS vendor

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Maintaining the Qualified State During Operation				
Change Management	• Change management function largely outsourced • Shared responsibility	Dedicated resources with platform configuration as core competency	• Changes not recorded appropriately or in enough detail (currently it states changes not recorded only) • Appropriate personnel may not be involved in the change control process (particularly if multiple parties involved) • Oversight of who to involve in the change control process may not be detailed enough	Require internal QA or IT signature on risk assessments and changes for platform covered under the scope of the SLA/ contract Periodic audit
Configuration Management	• Configuration management function largely outsourced • Shared responsibility	Dedicated resources with platform configuration as core competency	Configuration documentation not kept up to date	Require review of any configuration documentation created for platform components in scope of SLA/contract
Security Management	• Security management function largely outsourced • Shared responsibility	• As platform management is a core competency of third party, security controls are likely more robust and advanced than that available internally • PaaS providers devote their resources to preventing or resolving security problems, which some businesses may not have the SME or may not afford to do	• Reliance on third party to secure data • Unauthorized access to a firm's data and processes: authentication and authorization is controlled at the PaaS and not at by the regulated company and it may be difficult to establish effective oversight of permissions changes and controls	• Supplier quality audit • SLA • Periodic review • Organizations, such as the PaaS Vendor Security Alliance, have been formed in order to provide standards and best practices for security assurance for PaaS vendor computing
Server Management	• Server management function largely outsourced • Shared responsibility	Burden of Platform Management outsourced	Reliance on third party to maintain and managed key platform	• Supplier quality audit • SLA
Client Management	Client management remains internal	None	Clients must connect to external servers	• Require connectivity testing • Ensure uptime requirements are included in SLA
Network Management	Internal/external networks commingled	Expansion of network horsepower and capability	Potential exposure to nefarious third parties	• Ensure uptime requirements are included in SLA. • Ensure Security • Firewalls as intrusion detection/prevention is acceptable
Problem Management	• Problem management function largely outsourced • Shared responsibility	Third party has core competency in external customer problem management	Problem prioritization may favor other customers and it may be difficult to establish effective oversight of change requests and help desk tickets	SLA enforcement

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Maintaining the Qualified State During Operation (continued)				
Help Desk	• Help Desk function largely outsourced • Shared responsibility	• Help Desk function outsourced • Reduced labor cost	Non-responsive Help Desk	SLA enforcement
Backup, Restore, and Archiving	• Backup, restore, and archiving function largely outsourced • Shared responsibility	Backup, restore, and archiving function can now benefit from dedicated facilities and economies of scale	Inadequate B&R testing could lead to data loss	• SLA enforcement • Test B&R scenarios with third party
Disaster Recovery	• Disaster recovery function largely outsourced • Shared responsibility	• Likely improvement in disaster recovery facilities and reduction in restore time • Due to reliability at multiple sites, PaaS provides business continuity and helps to ensure disaster recovery for the user	Disaster recovery time may be increased	• SLA enforcement • Test disaster recovery scenarios with third party
Performance Monitoring	• Performance monitoring function largely outsourced • Shared responsibility	Third party has core competency in network performance monitoring	• Failure to act on performance dips • Failure to adequately monitor service levels	• SLA enforcement • Stress test for performance
Supplier Management	Supplier management shifts from platform suppliers to service suppliers	None	Requires significant rethink of supplier management strategy	• Supplier quality audit • SLA
Periodic Review	Periodic review remains an internal requirement	None	Geographical considerations may limit ability to successfully execute periodic reviews in a timely manner	• Supplier quality audit • SLA
Retirement of Platforms				
System Retirement	Platform retirement now a shared responsibility	• None • Data archival burden still exits • Platform may be retired for the company but not for the outsourcer	Potential for data loss if systems are not retired in an orderly fashion	Ensure that internal IT/QA resources participate in retirement planning for any platform components in scope of SLA/Contract

18.3 Software as a Service

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
IT Infrastructure Elements				
Platforms	Physical access to servers no longer possible	• Reduces upfront platform cost no need to purchase hardware or assign internal resource support • Reduced hardware cost could result in additional funds for software modules	• No access to physical hardware • Potential for down time out with control of software owner • Compatibility of SaaS with internal legacy infrastructure	• Audit datacenter • Enforce quality practices • SLA • System/process audit
Processes	Change and configuration management under third party control	Requirement for software CC outsourced	• Limited visibility to software changes • Potentially limited control over software changes	• Audit datacenter • Enforce quality practices • SLA • System/process audit
Personnel	Software personnel under third party	• Reduced labor cost • Costs and resources are shared by SaaS users, and the infrastructure is centralized by the provider	No direct supervisory control of key personnel	• SLA • Require up to date training records
Quality Management System				
Quality Manual	• Quality system expanded beyond your door • Providers typically make SSAE 16 [16] / SOC 2 Type 2 [30] or equivalent information available on request, under non-disclosure agreement Upgrades to new software modules or administration responsibility maybe shared with third party	Allows focus on core quality functions	• Out of site out of mind • Relying on third party to follow quality processes • Standards do not yet exist: CSA [9], NIST [7], AICPA [46], and DMTF [47] developing a set of standards for Cloud Computing • Standards will apply to security, operational auditing and compliance • Providers can obtain SSAE 16 [16] / SOC 2 Type 2 [30] certification, but this has been criticized that the set of goals and standards determined by the auditor and the auditee may not be disclosed and can vary widely among providers	• Establish quality agreement with third party • Providers obtain SSAE 16 [16] / SOC 2 Type 2 [30] certification
Roles and Responsibilities	Software installation and maintenance outsourced, only administrative tasks maybe shared or completely outsourced	Refocus resources on other tasks	Attrition, lack of oversight as to third party hiring/firing methods Reliant on third party security features	• SLA • Require up to date training records • Ensure datacenter has robust security policy • Third party to inform the contract giver of changes to staff

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Quality Management System (continued)				
Record Management	• Record management requirements remain • There are existing laws and policies in place, which do not allow sending private data onto third party systems. • The regulated company is ultimately responsible for compliance to federal and state regulations such as HIPAA [45], SOX [48], and other personal medical information for the pharma and insurance industries	None	• Key records stored offsite • Privacy and security concernsc • Information is stored remotely, which means that legally (contract and SLA will specify) the SaaS provider is responsible for data	• Periodic audit • Limit access to key records • Enforce security policy • Contract and SLA regarding data ownership and privacy • Encrypt, remove, or redact private data
Documentation	Documentation likely resides at third party site	Reduced internal burden on document storage	Third party may not adequately document and account for key hardware	Require change management configuration specifications for all outsourced hardware
Testing	Testing conducted remotely or at third party site	Testing requirement remains but can be outsourced to third party	• Inadequate tests • Physical verification can only be done by third party	Require third party to supply IQ (and potentially OQ) documentation for all hosted software
Standard Operating Procedures	SOPs must now connect to external group	Potential to learn from/ improve hardware management process from third party	Poor linkage between external and internal policy	• Create a bridge document for internal/ external quality systems • Tie to SLA and ensure shared responsibility
Training	Training now extended to third party	Increased resource pool as needed	• Adequacy of training • Reliance on third party to follow instructions • Limited oversight	• Build training requirement into SLA • Conduct periodic audits to ensure third party enforcement
Periodic Review and Evaluation	Periodic review and evaluation now includes review of third party	Third party has infrastructure management as core competency, likely leading to improved service levels	• More difficult to assess external party than internal • Third party maybe resistant to audit	Require audit rights in SLA
Audit by QA	Third party QA now responsible for daily QA function	Reduces burden on internal QA	• Third party QA may not have best interests of hosted party in mind • Auditing SaaS vendors is new to many auditors (auditors may not fully understand the technology, risks, and mitigating controls)	• Audit datacenter • Enforce quality practices SLA • System/process audit

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Applying Risk Management				
Identification and Assessment of Components	Components are now physically external	• Reduced software maintenance costs • Reduced energy costs • Reduced labor costs • Resources are provided on a "scalability" basis • The system is closely monitored, and clients do not have to plan in-house for those times when higher loads will be needed	More difficult to tie specific servers to the software, particularly in the cloud	Require detailed accounting from third party as to the disposition of all components encompassing the software in the contract
Implementation of Controls	• Software IT controls are now the responsibility of the third party • SaaS is a paid-for service, which means that the finance department will want to keep a record of how the service is being used • Some of the new considerations include transborder information flow, data may be subject to the laws of multiple jurisdictions, impact to large population of unrelated users, new data privacy laws (businesses may be legally barred from placing certain information at the SaaS vendor)	Can benefit from tried and tested controls, third party are SMEs in software management	• Inadequate controls • Poor enforcement • Shelfware	• Audit datacenter • Enforce quality practices • SLA • The SaaS vendors provide audit trail information, but in the case of a dispute it is important to have an independent audit trail
Assessment of Changes to Qualified Components	Change assessment now placed on third party	As the software physically resides with third party they are best placed to assess change	Assessment may not fully examine all risks associated with hosted software	Require internal QA or IT signature on risk assessments and changes for software covered under the scope of the SLA/ contract
Periodic Review and Evaluation	Periodic review and Evaluation now includes review of third party	Third party has infrastructure management as core competency, likely leading to improved service levels	• More difficult to assess external party than internal • Third party maybe resistant to audit	Require audit rights in SLA
Qualification of Platforms				
Overview of Process	Third party required to established internal CSV policy	Reduces burden on internal validation resources	Adequacy of external CSV Policy	• Provide comment and edits to external CSV Policy where possible • Ensure adequacy during Supplier quality audit and periodic assessment

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Qualification of Platforms (continued)				
IT Infrastructure Life Cycle Model	Software life cycle now at discretion of third party	Reduced software cost	Third party may not have adequate insight into SaaS hardware replacement policy	Establish life cycle expectations in the SLA/ contract
Planning	Qualification planning now at the discretion of third party	• Reduces burden on internal validation resources • Agility improves with ability to quickly and inexpensively re-provision software resources	Plan may fail to address all necessary components for robust qualification	Ensure that internal IT/QA resources participate in qualification planning for any software components in scope of SLA/contract
Specification and Design Phase	Software specification ownership now resides with third party	Dedicated resources with software configuration as core competency	Configuration documentation may fail to capture all necessary static configuration items	Require review of any configuration documentation created for software components in scope of SLA/contract
Risk Assessment and Qualification Test Planning	Reliance on third party for majority of RA and test planning	Reduces internal validation burden	RA and tests may not be robust	Ensure that internal IT/QA resources participate in RA/test case in scope of SLA/contract
Procurement, Installation, and IQ	Software procurement, installation and IQ now conducted externally	• Economies of scale for software buys • Shared space and resources • Reduced labor costs Reduced internal validation burden	Procured software may not be adequate from a performance perspective, maybe installed incorrectly and or poorly IQ'd	• Supplier quality audit should establish that third party has strong capabilities in the area • Include relevant provisions in the SLA/ contract
OQ and Acceptance	For SaaS OQ remains an internal task	None	OQ relies on system hosted externally	Ensure enforcement of SLA
Reporting and Handover	IQ summary report prepared by third party	Reduces internal validation burden	IQ summary inadequate or reveals unresolved deviations	Ensure that internal IT/QA resources participate in summary report review in scope of SLA/contract
IT Infrastructure Control and Compliance	IT software control and compliance is a shared responsibility with third party	SME team expanded	• Third party may lack knowledge of GxP expectations • Large organizations using SaaS vendor services may have a need for a mirrored solution	• Use supplier quality agreement to determine gaps or deficiencies in GxP knowledge • Task internal resources with training of third party until that expected by SLA is met • Companies should consider a single sign-on between the regulated company and the SaaS vendor

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Maintaining the Qualified State During Operation				
Change Management	• Change management function largely outsourced • Shared responsibility	Dedicated resources with software configuration as core competency	• Changes not recorded appropriately or in enough detail (currently it states changes not recorded only) • Appropriate personnel may not be involved in the change control process (particularly if multiple parties involved) • Oversight of who to involve in the change control process may not be detailed enough	Require internal QA or IT signature on risk assessments and changes for software covered under the scope of the SLA/ contract Periodic audit
Configuration Management	• Configuration management function largely outsourced • Shared responsibility	Dedicated resources with software configuration as core competency	Configuration documentation not kept up to date	Require review of any configuration documentation created for software components in scope of SLA/contract
Security Management	• Security management function largely outsourced • Shared responsibility	• As software management is a core competency of third party, security controls are likely more robust and advanced than that available internally • SaaS providers devote their resources to preventing or resolving security problems (which some businesses may not have the SME or may not afford to do)	• Reliance on third party to secure data • Unauthorized access to a firm's data and processes: authentication and authorization is controlled at the SaaS and not at by the regulated company and it may be difficult to establish effective oversight of permissions changes and controls	• Supplier quality audit • SLA • Periodic review • Organizations, such as the SaaS Vendor Security Alliance, have been formed in order to provide standards and best practices for security assurance for SaaS vendor computing
Server Management	• Server management function largely outsourced • Shared responsibility	Burden of software management outsourced	Reliance on third party to maintain and managed key software	• Supplier quality audit • SLA
Client Management	Client management remains internal	None	Clients must connect to external servers	• Require connectivity testing • Ensure uptime requirements are included in SLA
Network Management	Internal/external networks commingled	Expansion of network horsepower and capability	Potential exposure to nefarious third parties	• Ensure uptime requirements are included in SLA • Ensure security • Firewalls as intrusion detection/prevention is acceptable
Problem Management	• Problem management function largely outsourced • Shared responsibility	Third party has core competency in external customer problem management	Problem prioritization may favor other customers, and it may be difficult to establish effective oversight of change requests and Help Desk tickets	SLA enforcement

Infrastructure as a Service (IaaS)	How is it different?	Positives	Risks	Mitigation Strategies
Maintaining the Qualified State During Operation (continued)				
Help Desk	• Help Desk function largely outsourced • Shared responsibility	• Help Desk function outsourced • Reduced labor cost	Non-responsive Help Desk, and it may be difficult to establish effective oversight of change requests and help desk tickets	SLA enforcement
Backup, Restore, and Archiving	• Backup, restore, and archiving function largely outsourced • Shared responsibility	Backup, restore, and archiving function can now benefit from dedicated facilities and economies of scale	• Inadequate B&R testing could lead to data loss • Data not being kept for periods of time in line with statutory requirements and best practice requirements (particularly as requirements vary depending on which GxP is concerned) and delay in access to records due to records being stored by an external party	• SLA enforcement • Test B&R scenarios with third party
Disaster Recovery	• Disaster recovery function largely outsourced • Shared responsibility	• Likely improvement in disaster recovery facilities and reduction in restore time • Due to reliability at multiple sites, SaaS provides business continuity and helps to ensure disaster recovery for the user	Disaster recovery time may be increased	• SLA enforcement • Test disaster recovery scenarios with third party
Performance Monitoring	• Performance monitoring function largely outsourced • Shared responsibility	Third party has core competency in network performance monitoring	• Failure to act on performance dips • Failure to adequately monitor service levels	• SLA enforcement • Stress test for performance
Supplier Management	Supplier management shifts from software suppliers to service suppliers	None	Requires significant rethink of supplier management strategy	• Supplier quality audit • SLA
Periodic Review	Periodic review remains an internal requirement	None	Geographical considerations may limit ability to successfully execute periodic reviews in a timely manner	• Supplier quality audit • SLA
Retirement of Platforms				
System Retirement	Software retirement now a shared responsibility	• None • Data archival burden still exits • Software may be retired for the regulated company but not for the outsourcer	Potential for data loss if systems are not retired in an orderly fashion	Ensure that internal IT/QA resources participate in retirement planning for any software components in scope of SLA/contract

19 Appendix 12 – Virtualization: Compliance and Control

This Appendix is based on the article by Ulrik Hjulmand-Lassen "Virtualization – Compliance and Control" from *Pharmaceutical Engineering,* July/August 2010, Volume 27, Number 4 [53].

19.1 Introduction

Over the years as budgets become tighter and data center run out of space, management has increased pressure on IT teams to find solutions on how to accommodate more software applications in less space using fewer resources. By introducing virtualized environments, it is possible for servers to become even more specialized in function, as the cost of separating small or less intensively used applications onto separate virtual machines is significantly less.

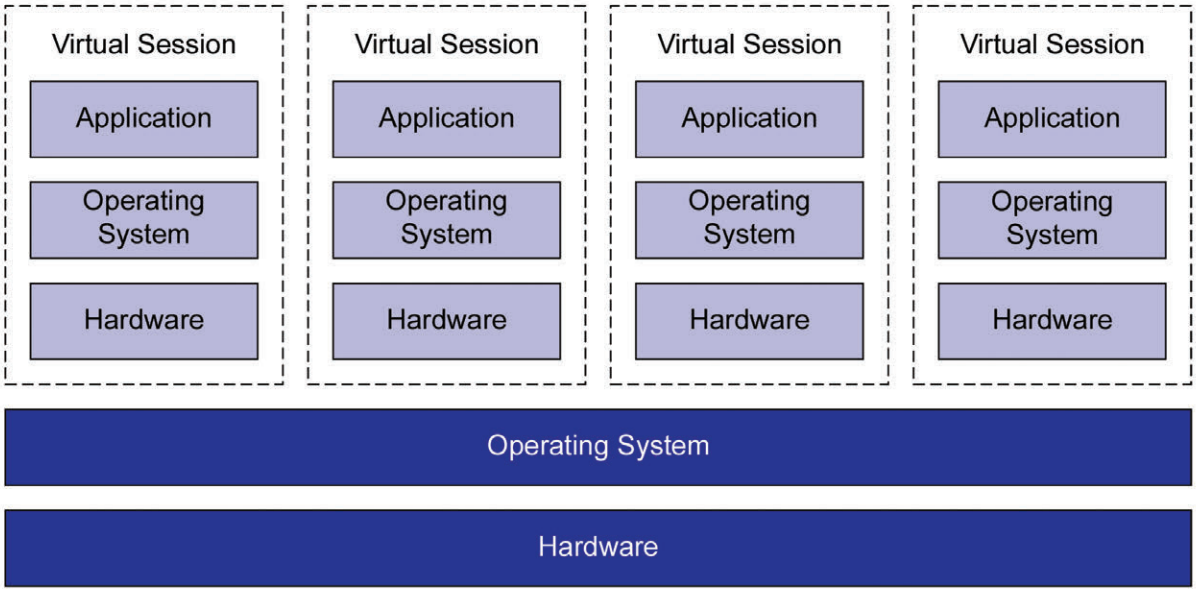
Virtualization simplifies the server build and setup, and allows staff to focus on key issues such as the specific operating system functionalities and security settings (e.g., services and open ports). Managed correctly, this reduces the complexity of the individual virtual machine, enables security settings to be more appropriately defined, and reduces the physical server-count compared to the traditional hardware bound situation.

Before the use of virtualization, the installation of multiple applications on a single hardware server brought potential security and interoperability issues, which meant that sharing hardware had to be either avoided or preceded by significant risk assessment, impact assessment and regression analysis.

19.2 Uses of Virtualization

Almost every infrastructure element is available in a virtual variant, in a large number of competing or complementary variants and proprietary naming-schemes: virtual storage, virtual switch, virtual LAN, virtual firewall, application virtualization, virtual desktop, etc. Most technologies aim to isolate applications from one another, keep data in the data center, and improve centralized administration–but few solutions (or combinations of these) can promise lower complexity, vendor independence, fewer licenses or lower cost at the same time.

Figure 19.1: Virtualized Servers



19.2.1 Application and Desktop Virtualization

Advantages of isolating applications in a Virtual Desktop Infrastructure (VDI) and establishing central administration are: data security and application focused client (e.g., PC, laptop) maintenance. In many situations, commercially sensitive or confidential data (e.g., patient, research, or customer related documents) is better protected if only presented on the workstation on a need-to-know basis rather than in a batch or bulk-copy enabled form.

Maintenance of the client part of corporate applications can become (almost) independent of other applications maintenance and of other client platform maintenance issues, such as upgrade of Java, Adobe or MS-Windows security patches. However, corporate application system administrators will have to take on additional tasks because they will need to specify and maintain the virtualization layer.

As part of introducing any virtualization technology, investigations are required to ensure that the solution is fit for the intended purpose and environment (compatibility) and provides appropriate return on investment. For instance, “thick” clients who traditionally rely on the processing power of the PC or laptop will very likely gain greater advantage from desktop or application virtualization, using the power of the central server.

Centralized solutions obviously require the users to be online (i.e., on the corporate network or internet), which should not pose a problem since corporate applications are usually centralized in a non-virtual environment. However, if users also require offline post processing or similar activities, considerations should be given to these specific requirements (such as the tools and data that must be available when disconnected from the corporate network). This requires the use of emerging application synchronization solutions (where the otherwise centralized virtualized applications are cached locally for offline use) and proves to be a solution with the best from both worlds without introducing any new security issues or other problems.

Centralization generally provides more control capability for IT staff, but the user experience for the communities that use the applications should also be considered. For example, response times may be affected if online transaction patterns for each application conflict. Such usability risks should be considered and managed.

Licensing aspects, capacity needs, security and performance aspects should also be considered. An increasing number of centralized solutions will add to the cost of license per workplace. The central servers must have capacity for all of the concurrent clients. Lost (or “overtaken”) connections should not allow for intruders to gain unauthorized access. Worst case capacity planning becomes more complicated if the processor power is centralized.

19.2.2 Virtual Test Environments

Another advantage to the use of virtualization is the possibility to create entire development or test environments as duplicates of existing physical or virtual systems. In that way, complete server environments and client/server scenarios can be quickly cloned at reasonable cost, to support development and test instances, without having to interrupt production systems or purchase dedicated hardware.

In each case, it is necessary to evaluate the extent to which the clone is sufficiently identical to the production instance and which virtualized environments are suitable for hosting formal verification test cases. The duplicate environment, the tools used for server cloning, and the potential impact of cloning on the production environment should all be evaluated, qualified, and documented.

19.3 Quality Planning and Virtualization

When server virtualization is adopted, it inherently affects the service level attributes and hazard profile of systems and applications migrated to the virtual platform. Some service level attributes of virtualized systems are usually significantly improved (e.g. maintainability, reduced power consumption, portability, and availability) just by establishing the associated working procedures, and this may change risk likelihood and detectability.

However, the nature and complexity of the technology means that a number of new risks need to be addressed in the quality and planning phase for appropriate mitigation. The new risks that need to be considered include: various failure modes for the virtualization software, the potential for interaction between different virtual machines, and human risks due to the increased complexity of the architecture.

Obviously, the specification, implementation, and/or tests of purely physical attributes (e.g. access control, power, temperature, and cooling) are attributable directly to the host which needs to be qualified just once. Virtual machines can trace fulfillment of related requirements to the attributes and qualification of the virtual environment, meaning these tasks need not be considered for the individual virtual machine.

19.3.1 Qualification, Compliance and Control

Based on the approach of this Guide, the infrastructure platforms and components may be qualified independently of the validation of the dependent systems, as long as the infrastructure is properly specified, verified, controlled, and maintained and as long as the infrastructure is not designed to fulfill specific user requirements. Qualification of the virtualized environment and virtual machines should be conducted in such a way as to leverage the strengths of the architecture, while effectively mitigating the specific risks.

Planning should therefore start with clear identification of what and how systems/applications/processes are within the scope of the virtualized environment. The upper bounds for potential risk impact can be set and the effort to qualify the virtualized environment and mitigate risks decided.

In some cases, virtualized environments will be used to group together applications with a similar risk impact and to qualify and control the environments (or virtual machines) accordingly. This naturally implies that controls must be introduced to avoid scope creep or misalignment due to poorly controlled operation and maintenance procedures (e.g., to prevent a high-risk impact application from being installed in a virtualized environment or which is only qualified and controlled to support low risk applications).

19.3.2 Risk Assessment of Virtualized Environments

While considering risks associated with a virtualized environment, some of these risks are the same for all items of infrastructure. However, the complexity of the virtualized environment means that additional failure mode must be considered and that risk likelihood and detectability must be reconsidered.

Other risks are unique to the virtualized environment and will require specific risk assessments to be conducted, at least prior to the introduction of virtualization if not for every build and installation.

Table 19.1 provides examples of the risks, potential causes introduced or exacerbated in connection with virtualization. Considerations should be taken as to what extent it is relevant to select and include them in local risk management processes and where focus should be placed on the technological, procedural or behavioral level depending on a risk evaluation of the given environment.

Table 19.1 Examples of Risks Related to the Potential Impact of Virtualization on Business Processes

Risks	Causes
Corrupt data, lost data, incorrect data	Data corruption in one or the other systems due to Storage Area Network (SAN) confusion, missing backups, restoration to the wrong Logical Unit Number (LUN) because of LUN confusion, LAN intrusion, virtual machine breakout, or misconfigured dualized/failover resources. Root cause examples: Poor backup/restore procedures, poorly trained operators, incomplete design or configuration management, missing LUN masking/zoning, unmitigated host vulnerability, insufficient (implementation of) LAN security policies or missing separation of security zones. **Note:** The term "Logical Unit Number" (LUN) is used for the key (pointer) to data allocation/addressing in Storage Area Networks (SAN's).
Production disruption due to platform malfunction, poor performance, denial of service attack, or server unavailability	Poor performance or failure to operate for otherwise unknown reasons, configuration failures leading to delays or inability to implement changes, virtual machine breakout or Denial of Service attack on host, or insufficient host capacity for peak demands. Root cause examples: Application not fit for chosen virtualization type, poor guidance from vendor, poor vulnerability- or patch-management procedures, patches lost by uncontrolled snapshot rollback, virtualization functionalities (such as migration) unfit for application, poor resource management, or configuration management routines not adapted to virtualized environment.
Lack of application vendor support for virtual environments	In some cases, applications vendors may choose not to support applications that were not designed to operate in a virtualized environment and this may represent a risk to business continuity, where a fault is not acknowledged or corrected by the vendor. This can only be mitigated by the provision of additional resources to provide second and/or third line support and may require the creation and/or maintenance of native physical machine to reproduce problems and demonstrate that the fault is not an artifact of virtualization.

19.3.3 Focus in Qualification and Operation

In building virtualized environments, additional failure modes are created and known failure modes change risk likelihood or risk detectability. Focusing on these issues is a prerequisite when replacing the physical platform with a virtual one. The issues in the list below are directly related to aspects introduced or significantly changed by the nature of virtualization. The complex and transient nature of virtualization allows for new modes of failure or attack, misunderstandings, lack of control, or for malicious individuals to compromise, copy, or break down virtualized systems either invisibly, massively or by incremental changes if not controlled properly. Focus should be placed on these issues when qualifying the set-up.

- **Privileged user access:** All privileged users should be assigned sufficient and specific access rights to perform their duties using their own individual account and have been trained in operational procedures and potential consequences of operational errors or misuse.

- **Assignment of tasks:** Tasks and responsibilities in relation to the virtual infrastructure should be clearly distributed to subject matter units (i.e., between storage-, network- and virtualization-experts).

- **Risk based implementation:** Qualification of all virtualized applications should include risk assessment (and mitigation, where relevant) of specific virtualization risks (i.e. the consequences of being implemented in an environment with variability in available resources).

- **Identification of virtual machines:** All virtual machines should be identified, owned, and documented and only decommissioned in a controlled way according to defined plans.

- **Design of solution:** Assurance should be established that systems with varying criticality, sensitivity, and requirements for control are grouped, clustered, and managed by hosts, personnel, and procedures. Efforts should be targeted at least at the level of the largest common denominator of the group.

- **Configuration management:** The Configuration Management Data Base should be tailored to manage the dynamic nature of virtual environments and support the needs for logical naming schemes and connections.

- **Documented verification:** Verification of configuration baselines, backup/restore processes, and operating procedures should be documented. The intended use of hosts and required functionality (and un-needed functionality) by virtualized applications should also be documented.

19.4 Maintenance

During the operations phase, written procedures should be followed for addition or decommissioning of virtual machines, performance monitoring and capacity planning, on-going maintenance, and the administration and use of privileged access rights. These procedures should be specific to the virtualized environment and periodic reviews should be performed to demonstrate continuous control of the environment.

Their complex and highly configured nature means that virtualized environments can be considered less robust with respect to the likelihood of human errors, which leaves a lot of room for misspellings and logical errors. Since there are relatively few built-in tools to support configuration management and most of the setup is logical, there is an increased difficulty in conducting reviews by traditional or automated methods. Appropriate methods of conducting periodic reviews must be developed.

20 Appendix 13 – References

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

2. FDA Draft Guidance for Industry: Data Integrity and Compliance with CGMP, April 2016, US Food and Drug Administration (FDA), www.fda.gov.

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

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

5. EudraLex Volume 4 – Guidelines for Good Manufacturing Practices for Medicinal Products for Human and Veterinary Use, Annex 15: Qualification and Validation, http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

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

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

8. Federal Risk and Authorization Management Program (FedRAMP), www.fedramp.gov.

9. Cloud Security Alliance (CSA), https://cloudsecurityalliance.org.

10. ISPE/GAMP® Forum, "Risk Assessment for Use of Automated Systems Supporting Manufacturing Processes," *Pharmaceutical Engineering,* May/June 2003, www.ispe.org.

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

12. NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, National Institute of Standards and Technology (NIST), www.nist.gov.

13. ISPE Glossary of Pharmaceutical and Biotechnology Terminology, www.ispe.org.

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

15. ISO 14644-6:2007 Cleanrooms and Associated Controlled Environments – Part 6: Vocabulary, International Organization for Standardization (ISO), www.iso.org.

16. Statement on Standards for Attestation Engagements (SSAE) No. 16, American Institute of Certified Public Accountants (AICPA), www.aicpa.org.

17. ISO 9001:2015 Quality Management Systems – Requirements, International Organization for Standardization (ISO), www.iso.org.

18. Payment Card Industry (PCI) Security Standards Council, www.pcisecuritystandards.org.

19. Electronic Healthcare Network Accreditation Commission (EHNAC), www.ehnac.org.

20. Federal Information Security Management Act (FISMA), US Department of Homeland Security (DHS), www.dhs.gov/fisma.

21. Health Information Trust Alliance (HITRUST), https://hitrustalliance.net.

22. ISO/IEC FDIS 27021 Information Technology -- Security Techniques – Competence Requirements for Information Security Management Systems Professionals (Draft), International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

23. ISO 9000:2015 Quality Management Systems – Fundamentals and Vocabulary, International Organization for Standardization (ISO), www.iso.org.

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

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

26. ISO 14971:2012 Medical Devices -- Application of Risk Management to Medical Devices, International Organization for Standardization (ISO), www.iso.org.

27. Pharmaceutical cGMPs for the 21st Century – A Risk-Based Approach: Final Report, September 2004, US Food and Drug Administration (FDA), www.fda.gov.

28. NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments, September 2012, National Institute of Standards and Technology (NIST), www.nist.gov.

29. SOC 1 – System and Organization Control (SOC) for Service Organizations: Internal Control over Financial Reporting (ICFR), American Institute of Certified Public Accountants (AICPA), www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx.

30. SOC 2 – System and Organization Control (SOC) for Service Organizations: Trust Services Criteria, American Institute of Certified Public Accountants (AICPA), www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx.

31. ISO/IEC 7498-4:1989 Information Technology -- Open Systems Interconnection -- Basic Reference Model: Naming and Addressing, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

32. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Regulated Mobile Applications,* International Society for Pharmaceutical Engineering (ISPE), First Edition, October 2014, www.ispe.org.

33. ISO/IEC 11801:2002 Information Technology -- Generic Cabling for Customer Premises, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

34. ANSI/TIA/EIA 568 Commercial Building Telecommunications Cabling Standards, Telecommunications Industry Association (TIA), www.tiaonline.org.

35. International Organization for Standardization (ISO), www.iso.org,

36. 21 CFR Part 11 – Electronic Records; Electronic Signatures, Code of Federal Regulations, US Food and Drug Administration (FDA), www.fda.gov.

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

37. ISO/IEC 17788:2014 Information Technology – Cloud Computing -- Overview and Vocabulary, International Organization for Standardization (ISO), www.iso.org, and International Electronical Commission (IEC), www.iec.ch.

38. PIC/S Guidance: PI 011-3 Good Practices for Computerised Systems in Regulated "GxP" Environments, September 2007, PIC/S, www.picscheme.org.

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

40. RFC 2196 – *Site Security Handbook,* B. Fraser (Editor), Software Engineering Institute/Carnegie Mellon University (SEI/CMU), September 1997, https://tools.ietf.org/html/rfc2196; Internet Engineering Task Force (IETF®), www.ietf.org.

41. NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, National Institute of Standards and Technology (NIST), www.nist.gov.

42. NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011, National Institute of Standards and Technology (NIST), www.nist.gov.

43. Health Information Trust Alliance Common Security Framework (HITRUST) CSF), https://hitrustalliance.net/hitrust-csf.

44. Control Objectives for Information and Related Technologies (COBIT®), Information Systems Audit and Control Association (ISACA®), www.isaca.org/cobit/pages/default.aspx.

45. Health Insurance Portability and Accountability Act of 1996 (HIPAA), US Department of Health & Human Services (HHS), www.hhs.gov/hipaa/index.html.

46. American Institute of Certified Public Accountants (AICPA), www.aicpa.org.

47. Distributed Management Task Force, Inc. (DMTF), www.dmtf.org.

48. Sarbanes-Oxley Act 2002 (SOX), Public Law 107-204, 107th Congress, United States of America, www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html.

49. EU-US Privacy Shield Framework, US Department of Commerce, https://www.privacyshield.gov/welcome.

50. International Council for Harmonisation (ICH), ICH Harmonised Tripartite Guideline, *Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients – Q7/Q7A,* Step 4, 10 November 2000, www.ich.org.

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

52. Institute of Electrical and Electronics Engineers (IEEE), www.ieee.org/index.html.

53. Hjulmand-Lassen, Ulrik, "Virtualization – Compliance and Control," *Pharmaceutical Engineering*, July/August 2010, Vol. 27, No. 4, www.ispe.org.

21 Appendix 14 – Glossary

21.1 Acronyms and Abbreviations

ANSI	American National Standards Institute (US)
B&R	Backup and Restore
BIPM	Bureau International des Poids et Mesures (France)
CA	Certification Authority
CAPA	Corrective and Preventive Action
CC	Change Control
CCM	Cloud Controls Matrix
CCTV	Closed Circuit Television
CDMS	Clinical Data Management System
CFDA	Chinese Food and Drug Administration
CFR	Code of Federal Regulations
CI	Configuration Item
CIL	Configuration Items List
CM	Configuration Management
CMDB	Configuration Management Database
COBIT®	Control Objectives for Information and Related Technologies (Information Systems Audit and Control Association, Inc. (ISACA))
COTS	Commercial off the Shelf
CPU	Central Processing Unit
CSA	Cloud Security Alliance®
CSP	Cloud Service Provider
CSV	Computerized System Validation
CV	Curriculum Vitae
DMZ	Demilitarized Zone
EDI	Electronic Data Interchange
EHNAC	Electronic Healthcare Network Accreditation Commission
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ERP	Enterprise Resource Planning
EU	European Union
FAT	Factory Acceptance Test
FDA	Food & Drug Administration (US)
FedRAMP	Federal Risk and Authorization Management Program (US)

FISMA	Federal Information Security Management Act
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GEP	Good Engineering Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GxP	Good "x" Practice, where "x" one of: Clinical, Distribution, Laboratory, Manufacturing
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
HTTPS	Hyper Text Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IP	Internet Protocol
IQ	Installation Qualification
ISP	Internet Service Provider
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 (US)
NOC	Network Operation Center
OLA	Organizational Level Agreement
OQ	Operational Qualification
OS	Operating System
OSI	Open Systems Interconnection
PaaS	Platform as a Service
PC	Personal Computer
PIC/S	Pharmaceutical Inspection Co-operation Scheme
PKI	Public Key Infrastructure
PQ	Performance Qualification

QA	Quality Assurance
QMS	Quality Management System
RA	Risk Assessment
RAID	Redundant Array of Independent Disks
RFI	Radio Frequency Interference
RMON	Remote Monitoring
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAN	Storage Area Network
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOC	System and Organization Controls
SOP	Standard Operating Procedure
SOX	Sarbanes-Oxley Act of 2002 (United States)
SSAE	Statement on Standards for Attestation Engagements
TAI	Temps Automique International (International Atomic Time)
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply
UTC	Coordinated Universal Time (Language independent international abbreviation)
VA	Volt-Amps
VLAN	Virtual Local Area Network
VM	Virtual Machine
WAN	Wide Area Network
XaaS	Infrastructure/Platform/Software as a Service

21.2 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 [35] / *ISPE GAMP® 5* [14])

Systematic, independent, and documented process for obtaining audit 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 regulated 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

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

Change Control/Management (generalized based on *ISPE GAMP® 5* [14])

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.

Cloud Services

Infrastructure solutions can be implemented as Cloud solutions. Cloud solutions are managed by an external company and will be accessed via the Internet. Different type of cloud solutions are defined as: Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS).

Colocation

The practice of placing "owned" IT infrastructure equipment in a third-party datacenter.

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

Infrastructure Process (based on ITIL® [37])

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 (US FDA [4])

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 (US FDA [4])

2. A system (transmission channels and supporting hardware and software) that connects several remotely located computers via telecommunications (ISO [35])

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

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 (ISPE Glossary [13])

The 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

1. The planned systematic activities necessary to ensure that a component, module, or system conforms to established technical requirements (ISO [35])

2. The activity of, or group independently responsible for, ensuring that the facility and systems meet GxP requirements (based on ISPE Glossary [13])

Quality Control

1. The operational techniques and procedures used to achieve quality requirements (US FDA [4])

2. Group responsible for checking or testing that specifications are met (based on ICH Q7A [50])

Quality Management System (ISO [35])

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

Risk (ICH Q9 [51])

Combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51).

Risk Assessment (ICH Q9 [51])

A systematic process of organizing information to support a risk decision to be made within a risk management process. It consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.

Risk Analysis (ICH Q9 [51])

The estimation of the risk associated with the identified hazards.

Risk Evaluation (ICH Q9 [51])

The comparison of the estimated risk to given risk criteria using a quantitative or qualitative scale to determine the significance of the risk.

Risk Management (ICH Q9 [51])

The systematic application of quality management policies, procedures, and practices to the tasks of assessing, controlling, communicating and reviewing risk.

Security (IEEE [52])

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)

Those individuals with specific expertise in a particular area or field. Subject Matter Experts should take the lead role in the verification of computerized systems. Subject Matter Expert responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results.

Supplier

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

Testing (IEEE [52])

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 (US FDA [4])

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 requirements/measures.

Virtual Appliance

A pre-configured virtual machine image with a defined function (for example, firewall or network load balancer) that is run on a hypervisor. Installation of software on a virtual machine and packaging that into an image creates a virtual appliance. The key benefit is that virtual appliances can simplify implementation and maintenance of the infrastructure element when compared to traditional deployment methods.

Virtual Machine

A software-based computer that emulates the operation of a physical machine (for example, workstation or server). A virtual machine is implemented on a hypervisor-based physical host machine and uses the processing and memory resources of the host to operate.

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

www.ISPE.org