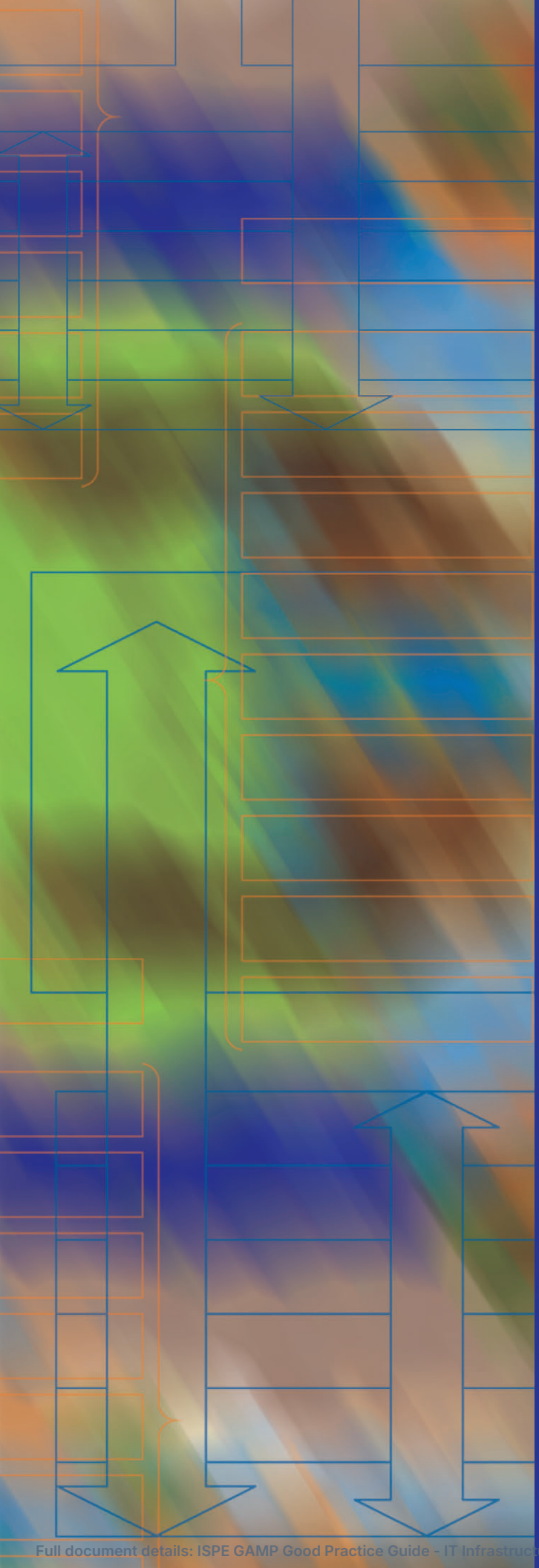


ISPE | GAMP

GOOD PRACTICE GUIDE:

IT Infrastructure Control and Compliance

Second Edition

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

© Copyright ISPE 2017. All rights reserved.

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

All trademarks used are acknowledged.

ISBN 978-1-946964-00-7

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

www.ISPE.org

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

Table of Contents

1 Introduction 9
1.1 Background 9
1.2 Overview 9
1.3 Purpose 10
1.4 Scope 11
1.5 Benefits 12
1.6 Objectives 13
1.7 Structure of this Guide 13
1.8 Key Concepts 14
1.9 Specific Aspects and Risks Associated with Infrastructure Outsourcing, Virtualization, and Cloud Adoption 20

2 IT and Cloud Infrastructure Elements 29
2.1 Platforms 29
2.2 Processes 31
2.3 Personnel 32

3 Quality Management System 33
3.1 Quality Manual 33
3.2 Roles and Responsibilities 34
3.3 Data and Records Management 34
3.4 Documentation 34
3.5 Testing 35
3.6 Standard Operating Procedures 35
3.7 Training 36
3.8 Periodic Review and Evaluation 36
3.9 Audit by QA 36

4 Applying Risk Management 37
4.1 Identification and Assessment of Components 38
4.2 Implementation of Controls 39
4.3 Assessment of Changes to Qualified Components 40
4.4 Periodic Review and Evaluation 40

5 Qualification of Platforms 41
5.1 Overview of Process 41
5.2 IT Infrastructure Life Cycle Model 42
5.3 Planning 44
5.4 Specification and Design 47
5.5 Risk Assessment and Qualification Test Planning 53
5.6 Procurement, Installation, and IQ 54
5.7 OQ and Acceptance 58
5.8 Reporting and Handover 59

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

6 Maintaining the Qualified State During Operation 61
6.1 Change Management 61
6.2 Configuration Management 62
6.3 Security Management 62
6.4 Server Management 63
6.5 Client Management 63
6.6 Network Management 64
6.7 Problem and Incident Management 64
6.8 Help Desk 64
6.9 Backup, Restore, and Archiving 65
6.10 Disaster Recovery 65
6.11 Performance Monitoring 66
6.12 Supplier Management 66
6.13 Periodic Review 67

7 Retirement of Platforms 69

8 Appendix 1 – Roles and Responsibilities 71
8.1 Introduction 71
8.2 Cloud Solutions Roles 78

9 Appendix 2 – Qualification Deliverables 79
9.1 Introduction 79
9.2 Infrastructure Building Block Concept 80
9.3 IT Infrastructure Planning Stage 80
9.4 IT Infrastructure Design Stage 80
9.5 IT Infrastructure Construction Stage 82
9.6 IT Infrastructure Qualification and Commissioning Stage 82
9.7 IT Infrastructure Handover to Operation Stage 83

10 Appendix 3 – Standard Operating Procedures 85

11 Appendix 4 – Periodic Reviews 89

12 Appendix 5 – Infrastructure Security 99
12.1 Introduction 99
12.2 Infrastructure Security Management 99
12.3 Upgrades and Patches – Balancing Qualification and Security Considerations 103

13 Appendix 6 – Upgrade and Patch Management 105
13.1 Fundamental Principles 105
13.2 Upgrade Strategy 105
13.3 Level of Application Testing 106
13.4 Global/Multi-site Systems 107

14 Appendix 7 – Outsourcing 109
14.1 Definition of Responsibilities 109
14.2 Special Considerations 110
14.3 Contracts 110
14.4 Service Level Agreements or Quality Agreements 111
14.5 Audits 112
14.6 Training Requirements 112

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

15 Appendix 8 – Server Management 113
15.1 Introduction 113
15.2 Backup and Restore 113
15.3 Technical Performance and Capacity Monitoring 115
15.4 Remote Management 116
15.5 Server Virtualization 116

16 Appendix 9 – Client Management 119
16.1 Client Types 119
16.2 Client Management 119
16.3 PC Platform 120
16.4 Operating System Platform 120
16.5 User Modifications 121
16.6 Images or Installation Scripts 121
16.7 Patch Management 121

17 Appendix 10 – Network Management 123
17.1 Introduction 123
17.2 Goal 123
17.3 Network Management 123
17.4 Network Provisioning and Installation 124
17.5 Network Operation Center 124
17.6 Common Network Tools and Configuration 125
17.7 Network Types 126
17.8 Network Performance Metrics 127

18 Appendix 11 – Traditional versus XaaS Model Comparison 129
18.1 Infrastructure as a Service 129
18.2 Platform as a Service 135
18.3 Software as a Service 141

19 Appendix 12 – Virtualization: Compliance and Control 147
19.1 Introduction 147
19.2 Uses of Virtualization 147
19.3 Quality Planning and Virtualization 149
19.4 Maintenance 151

20 Appendix 13 – References 153

21 Appendix 14 – Glossary 157
21.1 Acronyms and Abbreviations 157
21.2 Definitions 159

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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 entity and associated risk may be increased, if not adequately controlled.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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]

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

- 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

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

- 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.

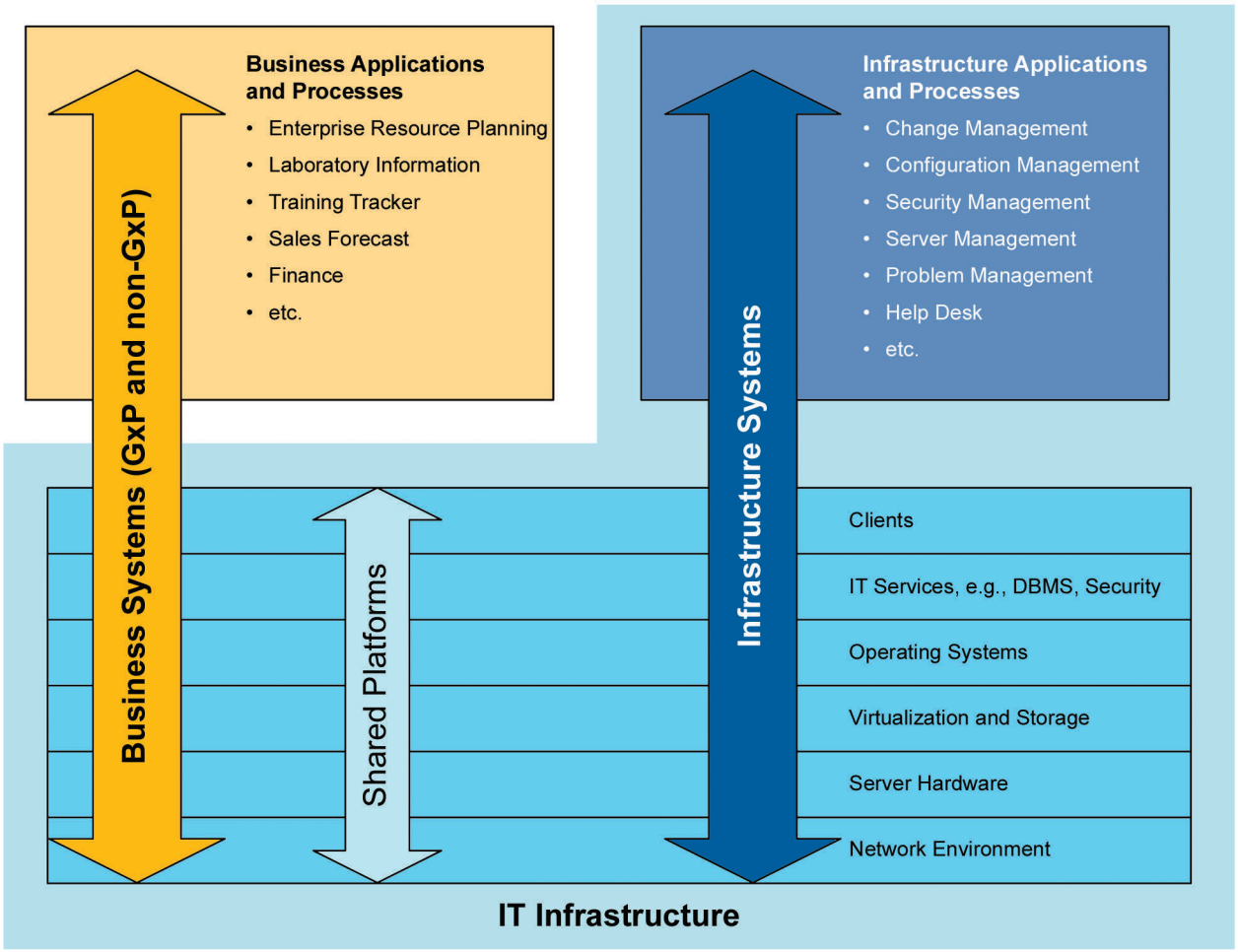
Figure 1.1 shows how the IT Infrastructure elements link together to form an integrated environment for running and supporting applications and services. Figure 1.1 illustrates that computerized systems[3] consist of the applications in question and all the parts of the platforms required making the 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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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)**

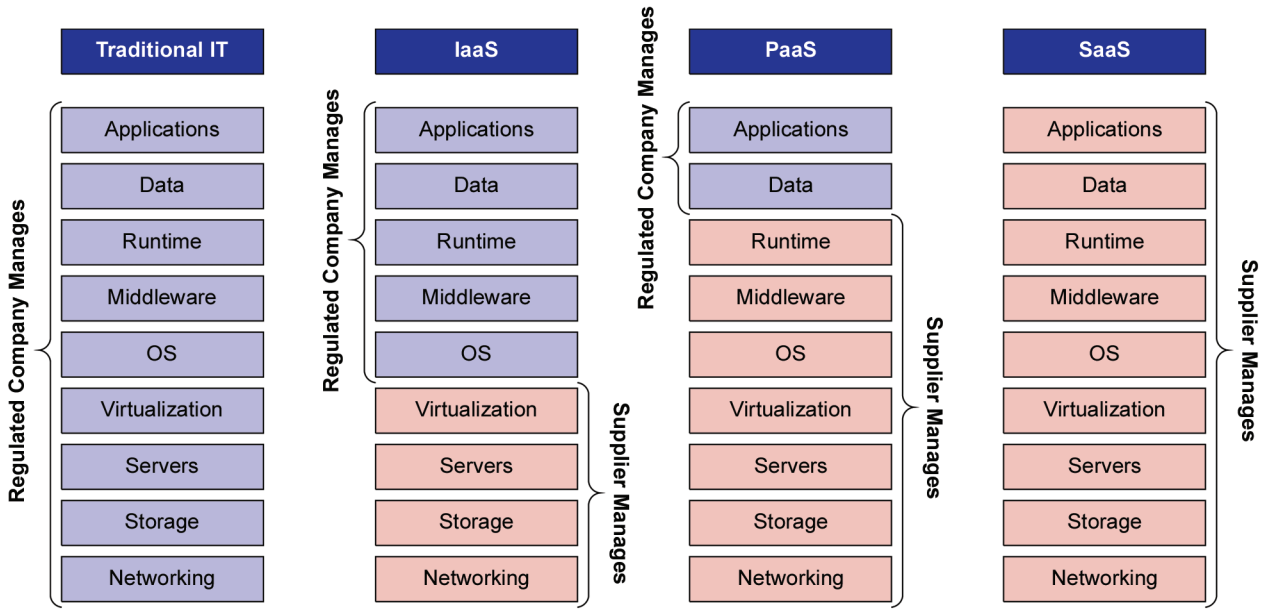
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including 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.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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]).

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

- 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?

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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].

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

- 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).

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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 1.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

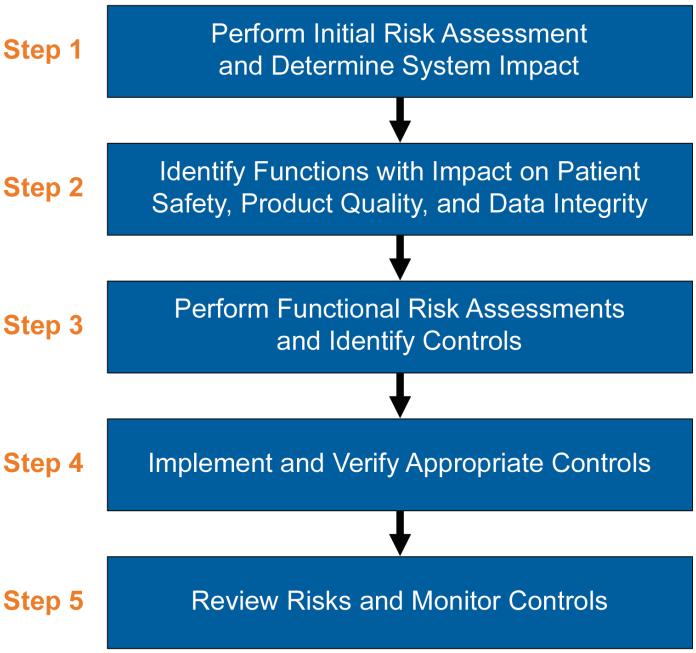
AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

- 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).

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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).

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

- 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.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017

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

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - IT Infrastructure Control and Compliance 2017