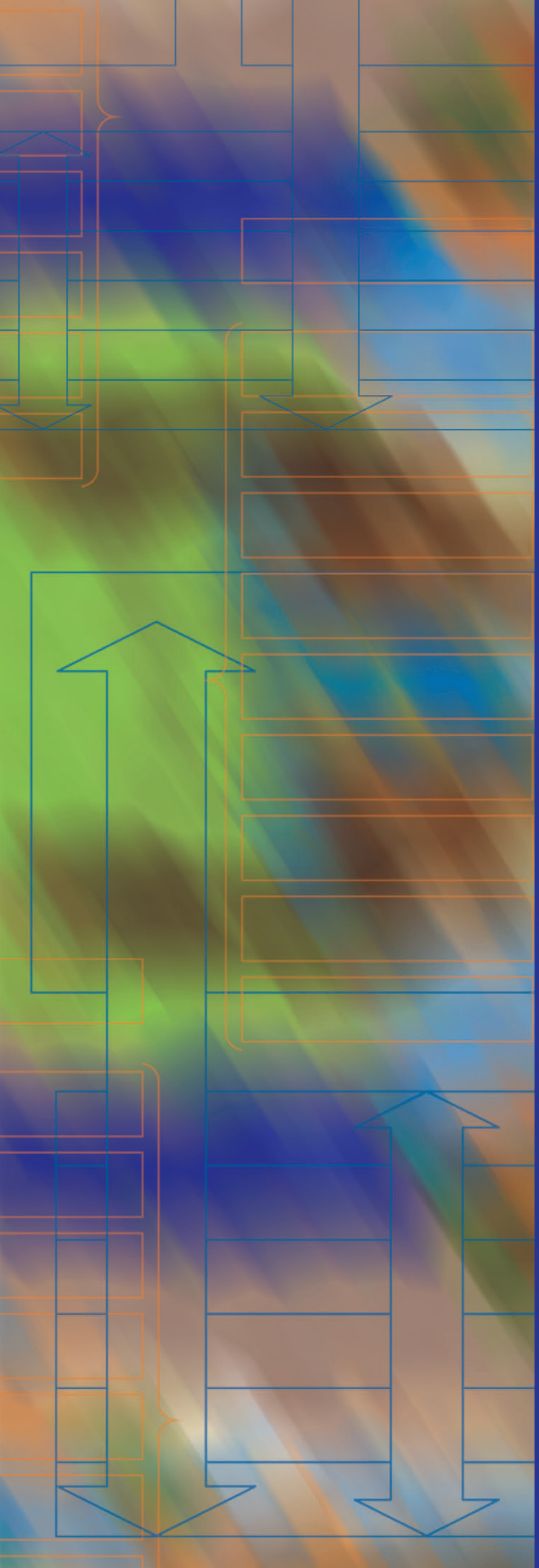

ISPE | GAMP

GOOD PRACTICE GUIDE:

IT Infrastructure Control and Compliance

Second Edition

GOOD PRACTICE GUIDE:

IT Infrastructure Control and Compliance

Second Edition

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

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

ISBN 978-1-946964-00-7

Preface

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

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

Acknowledgements

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

Core Team

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

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

Other Contributors

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

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

Regulatory Input and Review

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

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

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

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

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

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

www.ISPE.org

Table of Contents

1 Introduction 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

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

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

1 Introduction

1.1 Background

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

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

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

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

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

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

1.2 Overview

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

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

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

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

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