Computer Network and Infrastructure Qualification and Validation of Associated IT Applications: A Case Study

By Jeremy Benson and Martyn Smith
Vectura Limited
and
David Mole and R.D. McDowall
McDowall Consulting

Validation of computerised systems generally focuses on the providing documented evidence that a specific software application is fit for its intended purpose. The Food and Drug Administration (FDA) Guidances for Industry such as *Computerised Systems Used in Clinical Trials*[1] or the *General Principles of Software Validation*[2] make no direct mention of computer networks or network infrastructure. Similarly, industry guidelines, such as *Validation of Computer-Related Systems*[3] and the *Good Automated Manufacturing Practice* (GAMP) guidelines[4] concentrate on an application or a process system. However, the emphasis is changing and network infrastructure and the Information Technology (IT) departments that operate them on behalf of the users are now under regulatory scrutiny and this can open a black hole in many organizations.

> **"…the emphasis is changing and network infrastructure and the Information Technology (IT) departments that operate them on behalf of the users are now under regulatory scrutiny and this can open a black hole… "**

During the summer of 2000, two Pharmacia sites (Mälardalen and Strängnäs) in Sweden were inspected over the course of four weeks and some IT-related 483 observations were given. The company and the FDA discussed the issues over five letters, and in January 2001, the FDA issued two warning letters to the company.[5,6] Therefore it appears that a closer focus is coming into the IT Department and the nature of the security via the desktop with respect to access to data outside of the application. The two main issues to consider here is the impact of 21 Code of Federal Regulations (CFR) Part 11, the Electronic Records; Electronic Signatures final rule,[7] and the approaches that the FDA is taking to enforce the regulation. Throughout the whole of the 21 CFR Part 11 regulation only systems are mentioned and never applications. Therefore this regulation means that the IT department, the networks they operate, and the ways that they work must be compliant with this regulation and the applicable predicate rule(s).

Literature Review

There are a few papers in the literature and draft guidance on the qualification of computer networks and these are reviewed below. There is a lack of detailed information in the literature, and it is important that readers understand the background to the approaches that we have used and the rationale for them.

The GAMP Forum has an IT Infrastructure Interest Group that has written a draft guidance[8] where the emphasis is on Quality Assurance (QA) rather than either qualification or validation. This proposed guidance misses the mark as it has tried to convince IT personnel to work to quality assurance principles, rather than include the IT function within the regulatory compliance framework that the rest of the business already uses. The document deals with getting the network infrastructure into control by documenting the design using specifications and, where needed, diagrams. There is also a list of the Standard Operating Procedures (SOPs) required for an IT Department; however during the course of this work we have found the logic to be confusing and it is difficult to get a clear-cut list of SOPs.

This document defines “IT infrastructure” as all of the computer systems with their associated hardware, software and networks used to run the business, other than systems and software dedicated to validatable applications. This definition is only partially effective and needs to be extended. As we will discuss in the network qualification strategy, we incorporated the validation of IT applications, such as network management software, and help desk under the overall qualification of the network.

The PDA *Good Electronic Records Management* (GERM) draft guidance[9] has Section 6 devoted to IT Operations and Infrastructure e.g.:

- Section 6.8: Networks: the emphasis here is on keeping track of configuration and monitoring performance, detecting breakdowns, or conditions that could lead to them.
- Section 6.9: Configuration Management: “configuration management is integrated into the development and validation lifecycles following good engineering practice” and “all software and hardware components that make up the computing environment and infrastructure, including purchased components, are identified as configuration items.”

However, there is no explicit requirement for a network to be designed correctly, only to manage the infrastructure to ensure the continuity and availability of network resources, and the integrity, authenticity and trustworthiness of information assets.

There are two chapters on network and infrastructure qualification in Wingate’s book on *Validating Corporate Computer Systems.* Wilks[10] covers an overview of infrastructure elements that have to be qualified including:

- Computer rooms and environmental control equipment
- Hardware platforms and peripherals
- Networks: physical and logical elements must be defined in specifications with textual descriptions supported by diagrams.
- Desktop

Signorile[11] goes into more detail on the prospective qualification network qualification by presenting a lifecycle model. However, this appears too complex for use in most IT departments and appears better suited to software applications than networks. For example, supplier audits are proposed for simple off the shelf components – where in the authors’ opinions this is not required.

McDowall[12] presented a simplified lifecycle model for infrastructure qualification that consisted of specification, installation, and qualification. This is closer to the way that IT staff normally perform their work, and attempted to put a simple regulatory compliance framework together. This approach is modified slightly in this paper. The debate about network validation or qualification is presented here. Throughout this paper we refer to network qualification and validation of IT applications.

Huber and Budihandojo[13] discuss qualifying network components and validating network applications. The authors suggest that generic network specifications (e.g., cables, security, and vendor qualification) should be part of the Validation Master Plan (VMP), including naming conventions making it easier to identify components and track data flow within a network. However, we believe this to be impractical as the intention of the VMP as defined under European Union GMP Annex 15[14] is a concise document that it updated on a regular basis. Specifications do not belong in the VMP, but in the Network Requirements Specification (NRS) as we will discuss in this paper.

In summary, the literature documents what should you do at a conceptual level, but there is no detailed advice of how networks should be designed and implemented in a regulated environment.

The aim of this case study is to outline the stages of the design and implementation of the Vectura network that highlights the interpretation of the regulations and industry guidance. This is presented in two parts:

❶ Presentation of the overall qualification strategy, plus the control of the qualification and the design of the system in the network requirements specification

❷ Implementation of the design covering the installation and qualification of the components, and the overall network, including the validation of key IT applications

Vectura Limited Case Study

Vectura is a proprietary drug delivery organisation offering contract research facilities to companies in the pharmaceutical and biotechnology industries. The company was moving to a new facility in Chippenham, located in the United Kingdom, and the opportunity was taken to qualify the computer network and infrastructure from design, and installation to the release for operational use. The main advantage in this case study is that the Vectura Chippenham facility is a green field site that allows a structure and controlled approach to the prospective network and infrastructure qualification effort.

Vectura Validation and 21 CFR Part 11 Policy and the VMP

Under the Vectura combined computerised system validation and 21 CFR Part 11 policy, a VMP was written based on the format for European Union GMP Annex 15. This document covers the commissioning of the facility, and includes a section for all of the computerised systems in the organisation to be validated or qualified. This section lists all computerised systems within the company, and whether or not they should be validated or qualified or not.

As the network and infrastructure was a sufficiently large project, it was controlled under a specific network qualification and validation plan that included specification, installation, qualification, or validation and operation of the network and IT applications.

Risk Analysis Used to Define the Network Qualification Strategy

To understand the overall qualification strategy taken with the Vectura network, an appreciation of our thinking and rationale is important. Before starting, the overall approach was discussed, and a risk assessment was documented in the qualification plan as outlined here.

Network Design Strategy

The hardware and software components of the network were standard industry components from suppliers. The intention was to use these straight out of the box, or with a minimum of configuration. Customization of software was not envisioned and there would be no customized hardware developed. This meant that we could install and qualify individual items in a relatively straightforward manner, and build regulatory compliance in at minimal cost. Under this design strategy, the hardware and software was classified as either GAMP software categories 1, 2, or 3 or hardware category 1.[15]

Component Risk Analysis

Using the classification strategy outlined in the GAMP Guideline Appendix M4,[15] all the network components and software can be classified as:

- GAMP Hardware Category 1: Standard Hardware Components

Here the guidance states:

> *"standard hardware components should be documented including supplier details and version numbers. IQ should verify installation and connection of components. The model, version number and where available, serial number, of pre-assembled hardware should be recorded. Pre-assembled hardware does not have to be disassembled if this breaks the warranty. In*

such cases the hardware details can be taken from the hardware's data sheet or other specification material. Configuration management and change control apply."

- GAMP Software Category 1: Operating Systems

"Established commercially available operating system; applications are developed to run under the control of these operating systems. These are not subject to specific validation although their features are functionally tested and challenged indirectly during testing of the application. Change control should be applied to manage upgrades to the operating system. The impact of new or modified or removed features should be determined. Application verification and re-testing should reflect the degree of impact."

- GAMP Software Category 2: Firmware

"Configuration of firmware may be required in order to set up run time environment and process parameters. The name, version number and any configuration or calibration for the firmware should be documented and verified during IQ. Functionality should be tested during Operational Qualification (OQ). Change control should be applied to manage any change to firmware or configuration parameters. SOPs should be established and training plans implemented. Supplier audits should be considered for highly critical or complex applications. Custom firmware should be considered as Category 5."

- GAMP Software Category 3: Standard Software Packages

"The package is not configured to define the business or manufacturing process itself, configuration should be limited to establishing the runtime environment of the package (e.g. network and printer connections). To satisfy validation requirements, user requirements should be documented, reviewed and tested during OQ. Supplier documentation such as user and technical manuals should be assessed and used wherever possible."

Risk Overview

The risk outlined here is based in part on industry guidance, but also common sense. Ask the question: what would the impact be of an error in the network compared with an off-the-shelf application, or configurable off-the-shelf or bespoke applications? This is shown in *Figure 1.* Here the degree of compliance goes up with the level of risk involved with the item.

Qualification Strategy: Scope and Documentation

Scope of the Network Qualification and Validation

As outlined by McDowall[12] and shown in *Figure 2,* the scope of the network qualification in this case study includes the physical components (cables,

Figure 1

Plot of Compound Risk Versus Relative Qualification Effort

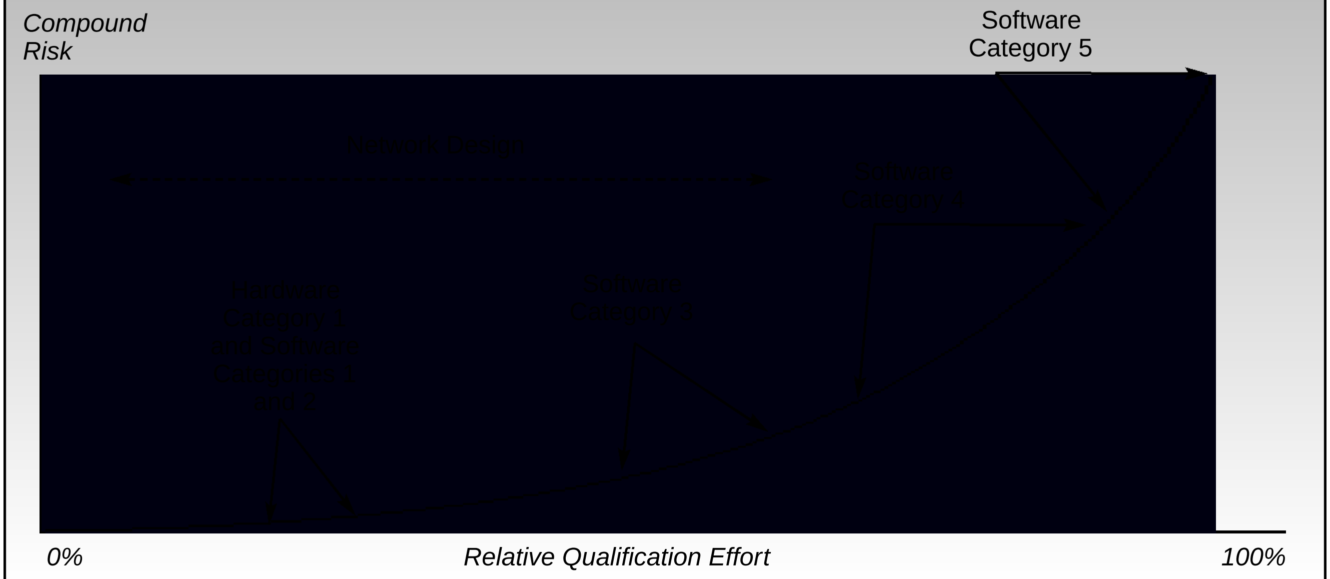
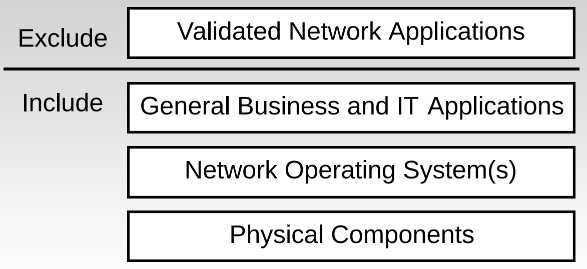


Figure 2

Components of a Network and the Scope of Network and Infrastructure Qualification


Exclude
Validated Network Applications
Include
General Business and IT Applications
Network Operating System(s)
Physical Components

switches, routers, servers etc.), network operating systems (switch software, operating system software), general business applications, and IT applications to be validated.

Good Manufacturing Practice (GMP) applications are excluded specifically from the scope of qualification, and will be subject to separate validation efforts after the network is qualified and released for operational use.

Qualification Documentation

The main documents produced during the qualification are outlined in *Figure 3*, these include the following:

- Network Qualification and Validation Plan
  The controlling document that outlines the steps to be taken that if followed, will result in a qualified network and validated network applications.
- Network Requirements Specification (NRS)
  Specification and unique numbering of each component or application involved with the network to allow traceability from design through installation to qualification of components or validation of applications. There is a provision within this document for cross-referencing documents or diagrams outside of the NRS as will be described later in this paper.
- Installation and Qualification Test Plan
  This document guides the installation and qualification of individual components and validation of the network and infrastructure.
- Network Qualification Summary Report
  Report that summarizes the work performed in the support of the operational release of a qualified network and infrastructure, along with a discussion of any deviations from the plan.

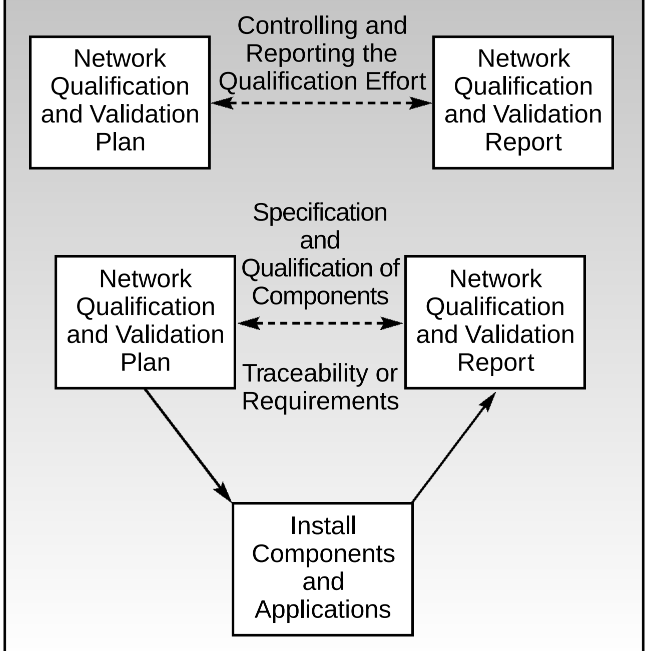
This approach is based on a modified V model for IT infrastructure (*Figure 3*) that is adequate to qualify the network. In this part of the case study, we will concentrate on the network qualification and validation plan, and the network requirements specification, as these are the critical components to our whole approach.

Network Qualification and Validation Plan

An overall qualification plan is needed to define the scope of the qualification activities over the whole of the lifecycle of the network including the roles and responsibilities of all involved including who is going to assure the quality of the work.

Figure 3

Overview of Main Documentation and Simplified "V" Lifecycle Model Approach for Network Qualification


Controlling and Reporting the Qualification Effort
Network Qualification and Validation Plan
Network Qualification and Validation Report
Specification and Qualification of Components
Traceability or Requirements
Network Qualification and Validation Plan
Network Qualification and Validation Report
Install Components and Applications

Similar to a validation plan for a Good Manufacturing Practice, Good Clinical Practice, Good Laboratory Practice (GXP) application, the network infrastructure qualification plan is a controlled document.

The qualification plan covers the tasks involved in getting the network under control, and this consists of the following main activities:

- Write the NRS and System Requirements Specifications (SRS) for IT Applications
- Write the Installation and Qualification Test Plan with associated test scripts
- Install communication racks and patch panels, switches, and cables
- Install the network management PC and software, and validate the application
- Build, qualify, and connect servers
- Install and qualify backup device
- Validate the backup and recovery software
- Qualify environmental controls of the computer room
- Write SOPs and technical documentation
- Qualify workstations and desktop
- Test network capacity and establish configuration baseline
- Write qualification and validation summary report, and release network for operational use

Once operational, the critical area to cover is change control and configuration management, as this is where the operational network and its infrastructure will soon lose compliance if the procedures are not in place and followed. The main stages during the operation of the network are:

- Operate the network
- Install and validate the help desk software
- Write a periodic review SOP and carry out periodic review
- Operate the change control system and maintain configuration management records

The qualification and validation plan is a relatively concise document that covers both the design and installation of the network, plus the operation of it. The format of the document is based in IEEE standard 1012.[16]

Network Requirements Specification

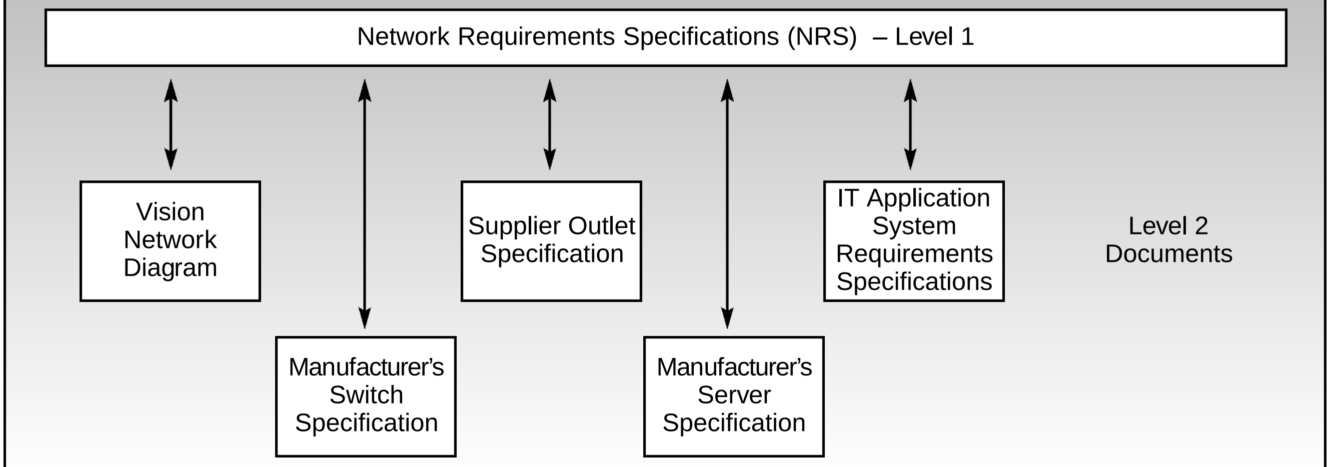
Overview of the NRS Structure

The NRS is a formal and controlled document that uniquely numbers the network components for traceability in the qualification stages. This document is based on a two-level approach as shown in *Figure 4.*

- The first level is the actual NRS that specifies individual components, equipment, or applications under a number of key headings e.g., cabling, outlet sockets, server and workstation build, environmental conditions, etc.

Figure 4

Outline Structure of the Network Requirements Specifications


Network Requirements Specifications (NRS) – Level 1
Vision Network Diagram
Supplier Outlet Specification
IT Application System Requirements Specifications
Level 2 Documents
Manufacturer's Switch Specification
Manufacturer's Server Specification

- The second level is used, where appropriate, for the cross referencing to diagrams, plans, standards, or manufacturer's specifications that are used for further detail outside of the NRS. Also as seen in *Figure 4*, there are also SRS for IT applications that will be validated as part of the network qualification.

This approach puts into practice the use of manufacturer's specifications to define the functions of hardware Category 1 equipment. In addition, Level 2 documentation can be either paper or electronic format, for example switch specifications downloaded from the supplier's web site as a PDF document. Therefore, some of the Level 2 documents can be uncontrolled.

We will now discuss the specification of components, and some of the IT applications to be validated in more detail. We'll start with some of the simpler examples and progress in complexity.

Specification of Level 1 NRS Requirements

An example of how the environmental conditions of the network operations centre were specified is shown in *Figure 5*. The format of the NRS is based on a series of three column tables; the left hand column holds the unique identifier for traceability, the requirement itself in the centre column, and the cross reference (where appropriate) is in the column on the right.

Figure 5

Specification of the Computer Room Environment Control Requirements

Requirement Number	Network Feature/ Specification	Cross Reference
7.2.01	The Network Operations Centre will have controlled temperature in the range 18-22º Centigrade +/- 1ºC	(N/A)
7.2.02	The computer room will have controlled humidity, in the range 40-60% +/- 10%	N/A

The aim is for the whole NRS to be an easily managed size rather than bulky. The size of the NRS level 1 document is approximately 20 pages.

Level 1 and 2 NRS Requirements: Specification of Switches

To see how the two-layer approach works in more detail, an example is the specification of switches used in the network. Within the NRS at Level 1, the switch supplier and model number is specified as shown in *Figure 6*.

Figure 6

Specification of the Network Switches

Requirement Number	Network Feature/ Specification	Cross Reference
9.1.08	Active equipment will be 3 x Avaya Cajun model P334T 48 port	Avaya Cajun Model P334T specification

The cross-reference column takes the reader to the Level 2 document that is a PDF document of the switch specification downloaded from the supplier's web site.This an uncontrolled document that will be stored on a CD-ROM that forms part of the overall qualification documentation package.

Switches are configured during their installation, however, the switch configurations are not specified in the NRS, but will be documented when the switches are installed in the installation and qualification test plan.

Level 1 and 2 NRS Requirements: Validation of IT Applications

The backup and help desk software will be validated as part of the overall installation, as they will be backing up or undertaking problem management of validated GMP applications. The approach here is for the NRS to specify the names and suppliers of these software applications and then cross-reference to SRS for each application. These controlled documents cover the functions of each application in more detail to enable specific test scripts that test these functions to be written and executed under the installation and qualification test plan.

Validation of Network Management Software

The approach to diagnostic tools as outlined in the GAMP Guide Appendix M4[15] is rather vague, but as the network was deemed critical to the success of

Vectura, the network management software applications used within the network to monitor its operation and to hold configuration records were classified as GAMP category 3.

The strategy was to validate these applications at the same time as the network was qualified, and accordingly, these were included under the network qualification and validation plan. Similar to the approach taken with backup and help desk applications, an SRS and test scripts for each were written and approved.

Summary

The approach to the specification of the requirements of the network is one of managed risk. By using standard components, minimum configuration, and no customisation, the design and control of the qualification of a network, and the associated infrastructure can be accomplished in a very cost-effective manner. ❑

About the Authors

Dave Mole is currently a Senior Consultant for McDowall Consulting, Bromley, UK. He has 30 years experience working in the pharmaceutical industry with Wellcome Research covering a wide variety of roles, including automation project, computer validation, data migration, and system retirement.

Bob McDowall is the Principal of McDowall Consulting with nine years experience in this position. Prior to that, he held positions in the pharmaceutical industry for 15 years. Bob has published and presented widely on a number of topics, including computerized system validation. He can be reached by phone at 44-20-8313-0934.

References

1. FDA. *Computerized Systems in Clinical Trials*. FDAGuidance For Industry. 1999.
2. FDA. *General Principles of Software Validation*. Guidance For Industry, 2002.
3. PDA. *Validation of Computer-Related Systems, Pharmaceutical Drug Association Technical Report 18*. 1995. Baltimore MD
4. ISPE. *Good Automated Manufacturing Guidelines Version 4, 2001*. Tampa, FL.
5. FDA. Pharmacia Warning Letter, FDA Warning Letter 320-01-07. January 11, 2001.
6. FDA. Pharmacia Warning Letter, FDA Warning Letter 320-01-08. January 11, 2001.
7. FDA. "21 CFR 11, Electronic Records and Electronic Signatures Final Rule." *Federal Register*. Vol. 64. (1997). Pp. 13430-13466.
8. The GAMPForum, Compliance for Information Technology (IT) Infrastructure. *Pharmaceutical Engineering*. November/December 1999, pp 34, 36-39.
9. PDA. Good Electronic Record Management, draft document. Baltimore, MD. March 2002.
10. Wilks, P. "Compliance for the Corporate IT Infrastructure." Chapter 11 in G.Wingate (Editor). "Validating Corporate Computer Systems, Good ITPractice for Pharmaceutical Manufacturers." Interpharm Press. 2000.
11. Signorile N. "Validating Local and Wide Area Networks." Chapter 12 in G.Wingate (Editor). "Validating Corporate Computer Systems, Good IT Practice for Pharmaceutical Manufacturers." Interpharm Press. 2000.
12. McDowall, R.D. "Qualification of Computer Networks, American Pharmaceutical Review." Summer Issue. 2001.
13. Huber, L. and Budihandojo, R. "Qualification of Network Components and Validation of Networked Systems." *Biopharm*. October 2001. Pp18-20, 22, 24-26, 46, 47.
14. Annex 15: Validation Master Plan. European Union.
15. Appendix M4 – Guideline for Categories of Software and Hardware. GAMP Guide for Validation of Automated Systems. Version 4, 2001. GAMPForum.
16. IEEE 1012-1998. Standard for Validation and Verification Plans, IEEE Software Engineering Standards. IEEE Press. Piscataway, NJ, 1999.

Article Acronym Listing

CFR:	Code of Federal Regulations
FDA:	Food and Drug Administration
GAMP:	Good Automated Manufacturing Practice
GERM:	Good Electronic Records Management
GMP:	Good Manufacturing Practice
GXP:	Good Manufacturing Practice, Good Clinical Practice, Good Laboratory Practice
IT:	Information Technology
NRS:	Network Requirements Specification
OQ:	Operation Qualification
QA:	Quality Assurance
SOP:	Standard Operating Procedure
SRS:	System Requirments Specifications
VMP:	Validation Master Plan