Qualification of Computer Networks and Infrastructure

R.D.McDowall
McDowall Consulting

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 The FDA Guidance for Industry such as Computerised Systems Used in Clinical Trials[1] or the draft guidance General Principles of Software Validation[2] make no direct mention of networks or network infrastructure.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

In this paper, I would like to discuss some terms and definitions, the scope of the regulations and some recent regulatory actions and finally outline some approaches to aid qualification of computer networks and the associated infrastructure. This is not intended to be an all encompassing article but to simulate thought within IS departments.

Definitions

The following definitions will be used in this paper:

Network and Infrastructure:

- Network: A system (transmission channels and supporting hardware and software) that connects several remotely located computers via telecommunications[5]. In practice this means the physical items such as cables, switches, hubs, servers as well as the network operating system, ne work management software, switch software that allows the transmission of data on the network.
- Network Infrastructure: This comprises both the desktop and general support services. The desktop will be the general office or business applications and utility programs (but not GXP applications) available when a user logs onto the ne work. Backup, recovery, disaster recovery, help desk and problem management typifies the support services that comprise the second part of network infrastructure.

Qualification and Validation

- Installation Qualification (IQ): Establishing confidence that process equipment and ancillary systems are compliant with appropriate codes and approved design intentions, and that manufacturer's recommendations are suitably considered[5].
- Operational Qualification (OQ): Establishing confidence that process equipment and sub-systems are capable of consistently operating within established limits and tolerances[5].
- Validation: Establishing documented evidence which provides a high degree of assurance that a specific computer related system will consistently meet its predetermined specifications[3].

Validate or Qualify Networks?

This is an interesting question but the answer is very simple. The network is essentially a transport mechanism that is used to move data and information from one location on the network to another. As such, it should be qualified as equipment rather than validated as an application. Other than the data transport mechanism what is the main function of a network?

The GXP application that utilises the network is validated explicitly for the functions that it will automate and when this is done to include the full operating range of functions and worst case capacity, then the network can be considered implicitly validated as part of that process.

Regulatory Perspectives

The two main issues to consider here is the impact of the electronic records and electronic signatures final rule[6] and the approaches that the FDA are taking to enforce the regulation.

Impact of 21 CFR 11 (Electronic Records and Electronic Signatures)

Throughout the whole of the 21 CFR 11 regulation[6] only systems are mentioned and never applications. This means that the whole of the computerised system is encompassed by the regulation and this includes:

- GXP Application (currently the main focus of validation and inspectional activity)
- Utilities and tools necessary to operate the application
- Desktop (including Windows Explorer that could allow access to data outside of the application and permissions that allow others to access data)
- Applicable infrastructure support functions such as backup etc
- Network components

The whole operation of the system is now impacted, however not all IS departments may appreciate the situation.

Regulatory Actions

During the summer of 2000, two Pharmacia sites (Mälardalen and Strängnäs) in Sweden were inspected over the course of four weeks and some IS 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[7,8].

The significant issues, from an IS perspective, were that:

- Wide Area Network diagrams (WAN) and Local Area Network (LAN) with appropriate definition documentation identifying corporate sites on the network that use the GXP application were not included in any validation documents.
- The WAN and LAN were not validated (this should be qualified, as noted above) as there were no complete definition documentation available
- The Quality Unit failed to have any procedures in place to define, control and maintain approved network diagrams such as site diagrams
- Lack of training by the IS service provider (outsourced IS) in GMP regulations and the written procedures referred to by the regulations

Therefore, lack of overall network design and documentation coupled with a lack of GMP training were the focus of the inspectional observations.

Recently, a 483 observation quoted in GMP Trends[9] noted that:

- The configuration of the client server systems enables each user to access functions, which can have a serious impact on the integrity of data stored in the server. Data edit authorization rights were not only available to the system administrator but to all users. Analysts have access to operations, which can modify data files, delete data, add or remove users, corrupt data files and reconfigure the entire system
- Insufficient security measures were in place to maintain data integrity. The firms software security procedures cannot prevent unauthorised program changes and deletion of data. Analysts have read-write access to all computer resident data, which was used to release products and to determine the stability of products during their shelf life. Analysts have assess to File Manager and the DOS command prompt, which can be used to edit text files and to cut, copy and paste data from document to document. Each terminal has a floppy disk drive which can be used to copy data files and may inadvertently introduce a virus.

Therefore it appears that a closer focus is coming into the IS Department and the nature of the security via the desktop with respect to access to data outside of the application.

Quo Vadis Network and Infrastructure Qualification?

From the regulations and the emerging evidence of enforcement, GXP regulations have now arrived in the IS Department, where in many organisations there were no formal procedures in place or even GXP training. Moreover, networks now have to be designed, installed, qualified and controlled using trained personnel; likewise the same requirements apply to the infrastructure. I will discuss some outline approaches based on my experiences qualifying networks.

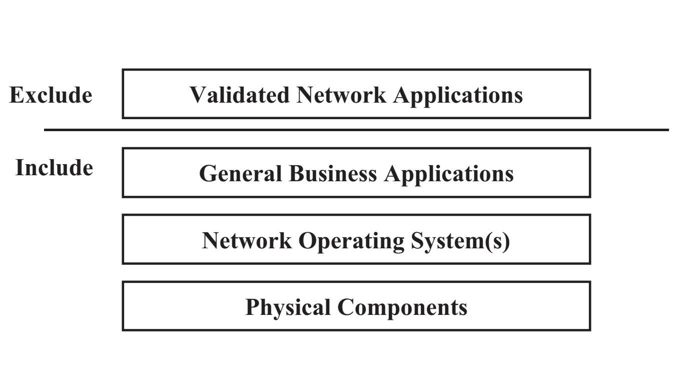
Qualify Network Separate from Validation of an Application

(Figure 1) shows that network qualification is separated from GXP application validation.

One could argue why not include the network qualification with a specific application validation? As this approach would mean bundling two jobs into one. This is feasible for a single GXP application running on a local area network serving a single department, but consider when you have more than one GXP application over several departments what then? Does this mean every application validation needs to include the network and repeating work again and again?

Figure 1

Components of a Network and the Scope of Network Infrastructure Qualification


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

Consider the approach where the network is first qualified and is in a "validation ready" status. New GXP applications can be added relatively easily knowing that the network and infrastructure are under control and qualified. We will explore this approach in more detail below.

Life Cycle Model for Network Components

A traditional system development life cycle model, such as the ISO V model, can be adapted for network qualification. Instead of a detailed process of requirements definition, functional and design specification before the build and test phases, consider what is actually happening in designing and installing a network.

There are number of physical components such as the cables, switches, servers etc. These are usually not unique items but they are manufactured standard components such as a specific vendor network switch or server that are usually purchased as off the shelf components. Cabling is specified as either fibre optic 10 or 100Mbit or 1Gbit or category 5 unshielded twisted pair (UTP) cable and is installed to a map within a building or site. Using this concept, the life cycle model can be considerably reduced to a simple three stage V model for each network component as shown in (Figure 2).

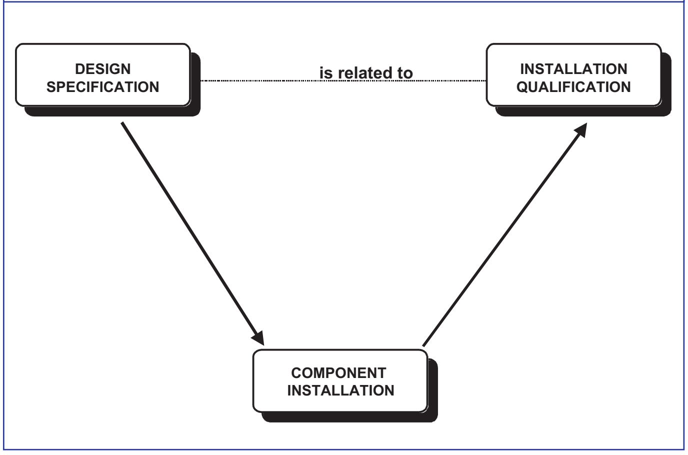
The emphasis is on a structured approach to collecting documented evidence of activities:

- Design Specification: what do you want and where will the equipment be placed?
- Component Installation: Has it been installed correctly
- Installation Qualification: Does it work as designed?

This approach takes a balanced approach to regulatory risk, a more cautious company can increase the level of work if required. Note an operational qualification of the network to demonstrate that all components are functioning correctly is also needed, but this will be discussed later.

FIGURE 2

Simplified V Life Cycle Model for Network Components



Write Qualification Plan

An overall qualification plan is needed to define the scope of the qualification activities over the whole of the life cycle of the network including the roles and responsibilities of all involved including who is going to assure the quality of the work. Similar to a GXP application validation plan the network infrastructure qualification plan will be a controlled document. The critical area to cover is change control and configuration management as this is where the operational network and its infrastructure will soon if the procedures are not in place and followed. However, if you are starting from scratch, then there may need to be some elements of retrospective qualification to include in the plan.

Specify, Install and Qualify Components

Each network component should be specified; this will include servers, cables and switches etc. Often the manufacturer's specifications can be used as the basis for the design, although there will be some custom elements such as cabling runs where diagrams will be needed for specific sites. When diagrams are needed, these may be drawn in a CAD package or similar application, you'll be creating electronic records that will need to be version controlled and approved as noted above[7,8].

After the specification is approved, the ordered components will be installed against the specification and then tested, both activities producing documented evidence of activities. For example, cables in many organisations are installed by a specialist company, the staff of which will not be trained in GXP regulations. Therefore the onus is on the IS department to ensure that adequate records of the installation and testing stages are obtained and preserved.

Some components can be configured after IQ such as servers and switches, it is important to record this information so that in the even of failure or disaster the configuration can be recovered relatively easily. One advantage that 21 CFR 11 allows is that this information can be kept electronically, therefore providing it can be saved outside of the equipment unit, alternatively the configuration can be documented on paper.

OQ Network

Once all components are installed and have been tested individually, then the network segment or the whole network needs to be operationally qualified. Given the complexity of many of the components such as a hub or switch, many permutations can be tested but this would take a lifetime. A defined subset is one way of qualifying the network based on the assumption that standard components are the same having undergone the manufacturer's design and testing. Qualification should include load testing to show that the network can handle the anticipated traffic and the performance once operational should be monitored to ensure that traffic is within the design limits. The test plans and scripts need to be written and approved before they are executed.

Desktop and Non-GXP Applications

In the sections above, we have looked at the components of the network, now I would like to turn our attention to the desktop and non-GXP applications. As a large number of non-GXP applications could be installed on the network, an important element must be control and standardisation of applications: have one application rather than several for the same function. This reduces the impact of .DLL hell that may be found in uncontrolled networks where shared files can be overwritten by either earlier or later versions with differing results. The non-GXP applications should be engineered and tested centrally (formally documented!) and distributed over the network to the users.

One issue here is that the configuration of the operating system and the engineering of the applications, software engineers traditionally do not like documenting what they have done. This must change.

Define Baseline Configuration

With all network and infrastructure components installed, the configuration of the network must be defined and maintained during operation. This is key to demonstrating control of the network, we will return to this in a later article as the discussion requires more depth than space allows here.

Write Procedures for Network and Infrastructure

Operating procedures for the staff running the network and the infrastructure will need to be written if not already available. The important point to note is that many IS operations will generate electronic records of automated procedures e.g. backup, restore etc how will the IS department manage these records and review them to ensure they are working properly? Many IS groups have procedures for activities but may not always concentrate on producing documented evidence that those activities have occurred, furthermore what happens if the activity fails e.g. backup, does the procedure cover this eventuality?

Train Personnel

Once the procedures are written the IS staff must be trained in their use as appropriate to their jobs. Training records in the procedures is important but also required is training in GXP regulations and Part 11. This is important to show the IS personnel how they fit into the pharmaceutical organisation and the data repository that they are responsible for.

I have had not had space to cover some of the issues such as change control, configuration management and qualification of applications such as the help desk and problem management software. We will return to these issues in a later article.

Summary

GXP regulations cover the Information Sciences (IS) Departments in all pharmaceutical organisations who operate and maintain computerised systems for users. The impact requires IS to design and qualify networks and the associated infrastructure and operate them in a compliant manner. This can mean a culture shift within many IS departments as traditionally there was no need to comply with regulations in the past. ■

References

1. Computerized Systems in Clinical Trials, FDA Guidance For Industry, 1999
2. General Principles of Software Validation, draft FDA Guidance For Industry, 1997
3. Validation of Computer-Related Systems, Pharmaceutical Drug Association Technical Report 18, 1995 PDA, Baltimore MD
4. Good Automated Manufacturing Guidelines Version 3, 1998, International Society for Pharmaceutical Engineering, Tampa, FL
5. Glossary of Computerised System Validation Terminology, FDA 1995
6. 21 CFR 11, Electronic Records and Electronic Signatures Final Rule, Federal Register, 64 (1997) 13430-13466
7. Pharmacia warning letter, FDA Warning Letter 320-01-07, 11 January 2001
8. Pharmacia warning letter, FDA Warning Letter 320-01-08, 11 January 2001
9. 483 Observations for laboratory controls, GMP Trends, Issue 578 p3, 15th February 2001, GMP Trends Inc, Boulder, CO