The 5Ws of Network Infrastructure Qualification

May 12, 2014 4:41 pm EDT

Network infrastructure qualification is a rapidly evolving, multi-faceted practice. As desktops, servers, network services, networks, and data centers continue to evolve, there are consistently reoccurring questions that they continue to be raised during qualification. Adapted from Sharon Strause's presentation at IVT's Computer and Software Validation conference, the following are the five "Ws" that need to be answered during network infrastructure qualification.

1. Who are the Stakeholders?

Today, the stakeholders of a network infrastructure qualification will include management, the user community, project team, technical team, power users, and support team. As computers and infrastructures become more specialized and complex, the skills needed for the project can rarely be provided by one individual.

The network infrastructure qualification should therefore be undertaken by a team, with assistance from consultants, system analysts, end users, operations, quality assurance, technical services, and vendors. From a regulatory perspective, there are numerous agencies with guidances that would thereby consider them stakeholders of a network infrastructure qualification project.

2. What are the Elements?

The makeup of a network infrastructure can be seen in Figure 1.

Figure 1: Makeup of a Network Infrastructure.
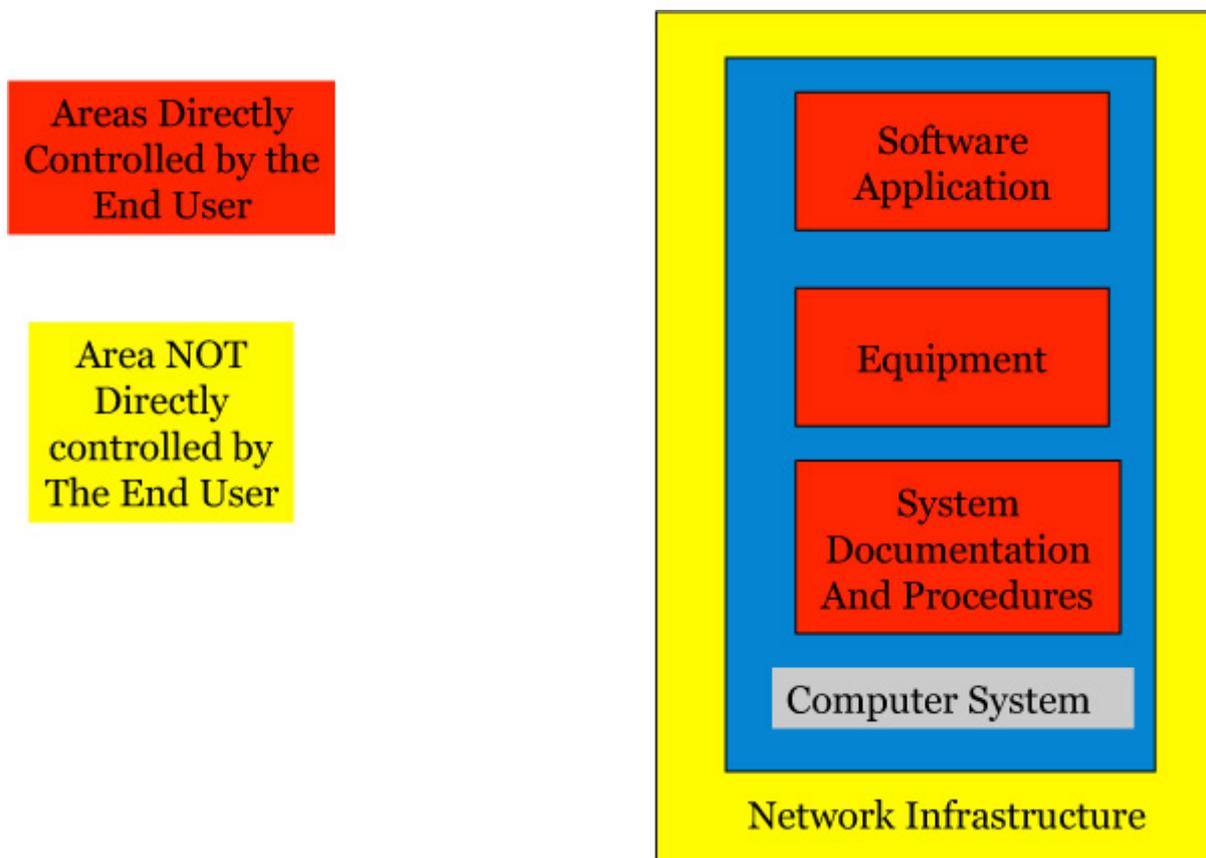
The key elements qualification project that a team will need to be knowledgeable include:

- Equipment Hardware
- Computer Hardware
- Network Components
- Operating Systems
- Application Software
- Specifications
- Qualification/Validation status
- Documentation.

The project team must understand information on each component and how they interact—at any time.

Two more important elements of network qualification are data management and business continuity. Data management should include procedures for:

- Back-up scheduling, deviation logging reporting
- Media labeling and on-site & off-site storage
- Restoration processes
- Documentation minimization.

Business continuity will include a disaster recovery plan in the face of a catastrophe and a business continuity plan in event of less serious contingencies.

3. When Should it Be Completed?

The nature of computer infrastructure has dramatically changed in the last few decades, as shown by Figure 2.

Figure 2: Evolution of Computer Infrastructure.

Dedicated Environment	One Client One Server	Multi-Client One Server	Multi-Client Multi-Server	Compute Abstraction
OS/390	Unix Client/Server	PC Client UNIX Server	Web Client Db. App. Server	SAN. Grid

1970s	1980s	1990s	Today	Tomorrow

Nevertheless, when the qualification should be completed will be determined by the risk management process. Risk management should follow the steps found in GAMP 4, GAMP 5, and ISO 14971-1:1998.

A step-by-step risk assessment strategy can be seen below:

1.
2. Determine potential risks of the process relative to intended use
3. List critical control points for each identified hazard
4. List critical limits for each of the critical control points
5. List procedures used to monitor each of the critical control points.

4. Where Can I Find Information?

Both GAMP and the IT Infrastructure Library (ITIL) are resources that can assist in compliance and efficiency in support of your network infrastructure. A list of additional guidance can be found below:

- Agilent
- Lab Compliance
- PDA
- ISPE
- FDA.

5. Why is Network Infrastructure Qualification Necessary?

IT professionals are responsible for the company's network—the infrastructure must be qualified (servers, routers, storage area, networks, etc.). Because IT records are subject to regulatory inspection, IT personnel control, maintain, and support systems that must be compliant. Therefore, the documentation that must be immediately available upon inspection include:

- Network qualification plan
- Descriptions, specifications
- Vendor qualification documents
- Qualification documentation

Installation, test protocols, summary report:

- User access lists, signed and updated
- Security procedures, password policies
- Change control procedures
- Change logs
- Monitoring charts
- Audit documentation.