

COMMITTEE MEMBERS

Committee Lead

Warren Campbell
*Consultant CSV, SDLC,
QA, Regulatory Affairs*

Jerry Anderson
*Watson Pharmaceuticals
Director Corporate
Computer Systems*

Michael Byrd
*Aventis
Sr. Manager, Infrastructure
Quality Compliance*

Edward Crosson
*Aventis
Sr. QA Specialist*

Ellis Daw
*GlaxoSmithKline
Director, Operational Compliance
Support*

Ludwig Huber
*Agilent
Worldwide Compliance
Program Manager*

Anita Morrison
*Lilly
Manager, Infrastructure Quality
Program*

Michele Pontinen
*IBM Global Pharmaceutical
Strategy Practice
IBM Business Consulting Services
Managing Consultant*

Sharon Strause
*formerly McNeil
Validation Manager, SAP Support
Team*

ADVISOR

Paul Motise
*FDA/ORA
Consumer Safety Officer
Office of Enforcement*

SPONSORS

Glenn Melvin
*Institute of Validation Technology
President*

John Kirchner
*Institute of Validation Technology
Vice President*

*Thanks to Corey Schneider and
Jeff O'Neill for their early participation.*

The Institute of Validation Technology (IVT) Network Infrastructure Qualification (NIQ) Committee was comprised of industry representatives from pharmaceutical, biotech, laboratory, and services organizations. An FDA representative participated in an advisory capacity. The initiative was started in order to bring Information Technology (IT) infrastructure concepts, methodology, and experience of IT professionals, along with the participation of regulatory and quality professionals in order to propose a qualification standard.

The NIQ meetings were held via teleconference every two weeks for approximately 10 months. Additionally, there were two face-to-face meetings. At an IVT's Network Infrastructure Qualification conference in 2003, a draft of the paper was field tested during panel discussions and presentations. The results of the field test were evaluated within the scope of the committee.

Sections of the paper were written by sub-teams based upon the committee agreements on the scope determined by several early meetings. It was the committee's desire to write a practical approach to network infrastructure qualification. There were many discussions on who our audience would be. The committee decided that IT professionals responsible for the infrastructure should

be the primary focus. Additionally, the committee did not want to write a rehash of what has already been published on the subject of validation and compliance. However, it was felt that, in terms of network infrastructure, there was a need to clarify what the IT professional does in order to support a regulated industry.

It was agreed that the context of discussions regarding network infrastructure would be with the understanding that all the IT infrastructure activities were to take place within a framework of quality. Management of IT infrastructure would require policies, procedures (SOPs), guidelines and/or work-instructions. The IT professionals would have documented training requirements. IT personnel should have training and understanding of their job function. Thus, it was felt that the committee would show the relationship of a qualified network infrastructure in support of the validated processes and applications.

Whatever the IT organization calls the documentation was determined not to be the issue, as long as the information or documentation is useful to support regulatory compliance. For example, if the IT infrastructure group has installation instructions or scripts for a server, and work instructions for technology dependent elements within the context of qualification, then the documentation may be considered applicable as a traditional Installation Qualification (IQ) protocol, in the context of validation of processes and applications.

Tools are available in the marketplace to help with infrastructure management, and are also beneficial for qualification efforts. There are also enterprise network monitoring software, help desk, and other software enablers that would be of benefit for qualification and maintenance efforts. However, it is not the intent of this paper to recommend or endorse specific tools.

The evolution of information technology continues. However, the fundamentals of regulatory compliance and quality issues remain constant with the management and control of processes. The committee researched many sources

Background

for specific network infrastructure information. The sources included the Department of Defense (DoD), Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), and the Information Technology Infrastructure Library (ITIL).

IT methods and activities are not an unknown in today's technological environment. Technology continues to evolve, yet fundamentals on IT management have been written about at length. It was suggested that IT infrastructure best practices from other industries should be considered. The concepts and knowledge should be transferable to the pharmaceutical arena.

Another decision was made to write the paper with the primary audience being the practitioner. Thus, the amount of references, citations, and cross-references would be kept to a minimum. A bibliography and suggested reading list has been included.

During the final meetings of the committee, there were several discussions regarding installation instructions within the context of IT infrastructure that would be considered an IQ protocol within the computer system validation context. The result of the discussions was that IT should call its documentation whatever it is. If the information will support regulatory compliance, then an organization could make a table to show the relationships of information or documentation between different organizations. The benefit would be that there would be fewer cut and

paste exercises into another format that may not provide any value. The content and accuracy of the information is more important.

The result is the committee suggests that the effort for qualifying the network infrastructure and its components, within a framework quality, will enable focus to be applied to the validation of the processes and applications. It doesn't matter whether it is (Good Manufacturing Practice (GMP), Good Clinical Practice (GCP) and Good Laboratory Practice (GLP)) GxP or non-GxP; it is difficult to separate and, in the context of IT, the methodology may be the same.

Management processes are important to the successful implementation of infrastructure qualification. In order to establish a qualified state, the network organization should utilize a risk-based approach to document the strategy for the implementation. Roles and responsibilities of infrastructure versus applications may need to be discussed regarding the boundaries to be agreed within organizations after one has read the proposed standard.

The committee tried to provide clarification, and in some cases, raise questions, for the importance of implementing a network infrastructure qualification program. The committee hopes that we have met the objective given us by IVT.

WARREN CAMPBELL

Committee Lead

IVT Network Infrastructure Qualification Committee

IVT Network Infrastructure Qualification Proposed Standard

Purpose

The purpose of the proposed qualification standard is to provide those who have the responsibility for the computer network infrastructure within FDA regulated industry, specific information and guidance to effectively support both business and regulatory compliance expectations. The information should enable the reader and network infrastructure practitioner to create a framework to mitigate regulatory risks, while also providing the infrastructure foundation to enable the company to meet its network communication, information, and security needs. In addition, the management and related activities for Network Infrastructure Qualification (NIQ) are enabled to be more information centric, rather than document centric.

Target Audience

The intent is to target two specific audiences within regulated companies:

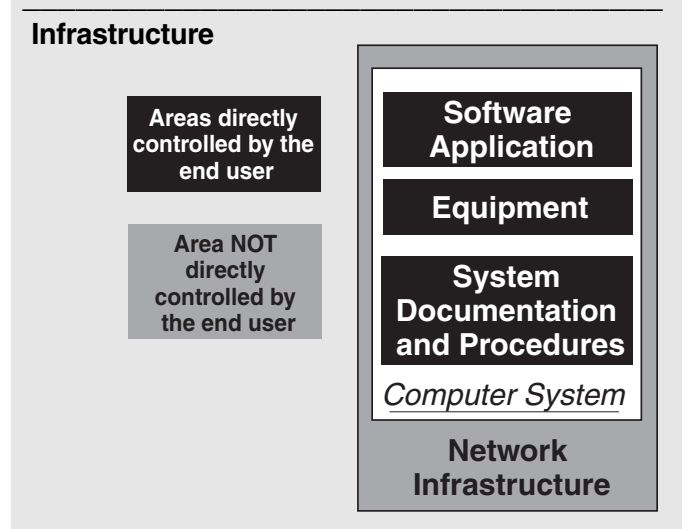
The first are personnel whose responsibility it is to develop, implement, and maintain the infrastructure that provides support for the transmission and storage of information for an organization. These professionals are called infrastructure practitioners. They may be employees of a company, or an external organization providing contracted support services. For these individuals, the intent is to provide information that will help them control and generate information that will assist them, as practitioners. Also, it will help increase both the efficiency of their jobs or compliance in providing information that will allow the processes and applications utilizing the infrastructure to operate in a validated and compliant state of control.

The second are personnel who build, maintain, and use applications and processes utilizing the infrastructure. It is important for them to understand the nature and control of the infrastructure in order to support the systems they put into place. The intent is to provide information on what to expect from the processes of implementing and maintaining the infrastructure in terms of evidence in the form of records and documentation to support their processes and their processes' validation.

Scope

In terms of the computer network, infrastructure is composed of the underlying hardware and software components that must be present and functioning in order for network communications and applications to work (see Figure 1).

Figure 1



As defined within the scope of this document, infrastructure includes such elements as infrastructure hardware (e.g., servers, workstations, etc), network components (e.g., routers, switches, hubs, cables, etc.), and supporting software (e.g., operating systems, monitoring tools, backup/recovery software, configuration management tools, etc.). Also addressed within this scope are facilities (e.g. data centers, etc.) in which critical infrastructure equipment is maintained and managed.

The focus of this document is on the IT network infrastructure and the related network components. In keeping to this focus, the intent is to identify the processes associated within the IT world for installation and deployment of infrastructure components that meet the needs of the business, which includes regulatory compliance. This publication will not address software applications, their interactions with each other, or discussion of business processes not directly related to network infrastructure.

Infrastructure Concepts

The basic concept proposed for the network infrastructure is that it is managed and controlled as equipment. As such, it is installed, qualified, and maintained in alignment with an organization's governing management procedures. Maintenance in this fashion serves two key benefits to the company:

1. From the perspective of the business, there is better documented functionality and reduced maintenance and rework costs. From the perspective of regulatory compliance, the documentation serves as one of the foundations for validation of the regulated systems and processes uti-

lizing the infrastructure.

2. The foundation of good infrastructure management is predicated on the use and application of industry standards and IT best practices. In providing the framework for qualification and management of the infrastructure, this paper “builds” on the framework from published standards that are already in wide use within other industries (e.g., financial, defense, etc.).

Equipment Qualification versus System Validation

“Qualification” and “Validation” are two closely related terms. They are often used interchangeably. However, while there is some overlap in use, their meanings are distinctly different used in the context of network infrastructure.

- Qualification demonstrates that a component or equipment works, or that an application functions as it was designed. Qualification is the result of direct measurements and observations that prove a piece of equipment was installed correctly (more properly in compliance with the requirements of the manufacturer), or that it functions in conformance to a design parameter. It can readily be shown that the infrastructure functions as designed, in terms of hardware, data transmission capabilities, and bandwidth. It can be shown that, for example, to meet an anticipated influx of capability that data storage, memory, Central Processing Unit (CPU) cycles and bandwidth were increased. Measurements can be made (e.g., packet collisions, etc.) showing that the capability is retained. In simpler terms, “qualification” supports validation through the presentation of direct measurements or evidence.
- Validation focuses on the requirements of the users or on a process. Validation is normally a statistical exercise that is used to show that a process that is consistently applied and under control, will reliably produce a consistent and predictable output. In other words, validation shows that a system or process functions according to its intended use (i.e., that a computer system meets the requirements of the users and their processes).

Qualification looks back at what was done to demonstrate that it was conducted according to design or specification, while validation looks forward and provides evidence that a system or process, based on past performance, will perform reliably in the future. Qualification stands on

its own merits. Validation stands on the exercises performed in the context of specific, business-focused objectives.

General Requirements

As part of the systems that contribute to the development, manufacture, testing, holding, and distribution of drug product, the infrastructure needs to be controlled, and information documented consistently with consideration of the applicable regulations that may be impacted.

What is required is simply the application of good engineering practices following industry accepted or sound company standards. To assure consistent performance, these practices need to be formalized with written procedures for maintaining the infrastructure. This formalization includes the information or documents that control the system and its processes.

The regulatory compliance requirements of a Quality Management System (QMS) are evidenced in the documents that control the system and its processes. These are the written procedures (SOPs) and internal reviews. The compliance requirements are also evident in the equipment documentation itself. These are the network diagrams, change logs, maintenance logs, qualifications and parameter settings, problem tracking, and management improvements.

This information is maintained under revision control. They are the working documents that provide information to share technical awareness and expertise required to maintain and troubleshoot the infrastructure.

IT Risk Assessment and Management

Introduction

The complexity of today’s information systems and their interactions, which depend on the reliability of the infrastructure, becomes ever more critical. It is absolutely necessary that a company allocate effective resources to protect revenue and product safety by the implementation of infrastructure tools that monitor and enable stable infrastructure management. With such tools, the ability to assess and mitigate risks would be a benefit both for business and regulatory compliance.

Risk analysis is one of the tools that can be used in quantifying the controls required and avoiding adverse situations caused by failures. To a large extent, failures, or their impacts, can be reduced at reasonable costs by applying modern risk management strategies. In performing risk analysis,

possible hazards and subsequent harms are identified, the probability of occurrence and the potential severity or costs of impact are estimated, and actions to mitigate the risks can be determined. The FDA has increased their focus on risk assessment, management, and pharmacovigilance.

It is not the intent of this publication to provide a treatise on assessment and management of risks. Risk assessment and risk management practices have an abundance of published books and articles. However, to discuss the concepts involving NIQ without mentioning the value of risk assessment and management may leave the network practitioner to conclude that such assessments were incidental to infrastructure qualification.

Definition of risk and risk factors, impact of risk levels

Risk is defined as the combination of the probability of harm and the severity of that harm. Severity in general means how much damage the problem can cause if it occurs. Probability is the likelihood that a problem or event will occur. These two components allow risk to be quantified. The severity of risk can be categorized as high, medium, or low, based on the degree of compliance/public health and business risks.

In the pharmaceutical industry, failures that impact compliance or generate potential health risks (e.g., harms that could arise from release for distribution and use of products that are adulterated or misbranded, etc.) are normally considered critical in severity. Other issues that would be considered critical would be continuity of business issues. Risks are generally classified as high (=critical), medium (=major) and low (=minor) in both categories, although some organizations choose other schemes of categorizing the classification.

A risk assessment for the network infrastructure components should be documented, along with the risk mitigation strategy. Such an assessment may be the determining factor in decisions for purchase of network components and external suppliers. Network infrastructure is the foundation for multiple applications which may be found to have different risk levels. At first glance, network infrastructure may be seen as a high risk level. However, network infrastructure may not be in the high risk level if the IT procedures and management of the infrastructure are found to be in control.

Probability should answer the question: What is the likelihood that the network infrastructure or component fails? The probability of occurrence would be classified as high, medium, or low.

The resulting risk level information is used for other considerations, such as:

- How extensively do we test and monitor the network components and communication? For example, although all systems should be tested under normal and high load conditions, such testing would include a greater number of load conditions for a higher risk level based upon the risk assessment.
- How much hardware component inventory should be on hand? For high risk infrastructure, should we have qualified component inventory for all hardware components? For medium risk infrastructure, an inventory of the most critical components is enough, and for low risk systems, there is no need for hardware inventory.
- How frequently do we have to back-up data from the network database?
- How stringently do we handle change control for workstations? For example, for high risk workstations, should all changes be approved?
- How much detail and redundancy do we need to plan for data centers (e.g., redundant power, Heating Ventilation Air Conditioning (HVAC), and environment monitoring equipment, etc.)?

Typical risks associated with design, installation, operation, and change of network components are listed in *Appendix 1*.

Risk Analysis

The first step in the risk management process is the risk analysis, sometimes also called risk identification or Preliminary Hazard Analysis (PHA). The output of this phase is the input for risk evaluation.

Inputs for compliance-related risk analysis are:

- Specifications of equipment/hardware/software
- Users experience with the same equipment already installed
- Users experience with similar network equipment
- IT staff experience with the same or similar network equipment
- Network qualification and system qualification reports
- Internal and external supplier or quality audit results

Inputs can come from operators, the validation/qualification group, IT administrators, or from QA personnel, (e.g., as

a result of findings from internal or external audits, etc).

Typical problems and harms with network infrastructure with possible impact on compliance risks include, but are not limited to, the following:

- Inadequate or absent verification of the accuracy of a file transfer can cause inaccurate results
- Inadequate or absent verification of security access functions can result in unauthorized access to the network
- An insufficient or absent plan for system back-up can result in data loss in case of system failure.
- An insufficient or absent plan for rollbacks if updates don't work as expected may cause severe infrastructure downtime through reinstallation and reconfiguration.
- Inadequate corporate quality assurance policies and procedures, or inadequate reviews may result if procedures are implemented and followed.

Risk Evaluation

This phase is used to categorize and prioritize the risk in business and compliance/health risks.

Risk Mitigation

This phase covers what is documented to mitigate risks. There are different methods and approaches to mitigate risks. They can range from process and system design changes to personnel training. Typically, the most effective methods are also the most expensive and take the longest amount of time.

Design/Process Change

This could entail installing new types of equipment, such as servers having higher capacity and new functionality. Typically, this requires expenditures for purchasing, installation, qualification, and familiarization. It also may require development of new SOPs and additional training.

Extended Testing

This does not remove the problematic network component, but shows weaknesses of the component and conditions under which component failures can be identified. This only helps if procedures and workaround solutions can be developed and implemented to avoid known critical conditions. A typical example would be to test a system under increasingly high loads, and to always operate the system

below the point when it started to fail in the test phase. It is suggested that a development or test environment be available for such exercises.

Extended Monitoring and Warnings

This is useful when the results are graphically presented, and warning and action limits have been defined. Operators should have clear instructions on what to do if critical limits are approached.

Better Personnel Qualification

The idea here is to avoid risk situations that are caused by human errors. Alternatives are to better train existing staff or hire additional personnel who have more experience with the same or similar systems. Compared with other approaches, it can be quite cost effective, and mitigation can be achieved in a relatively short time if current personnel can be trained. However, it can take longer if additional personnel have to be hired.

It is extremely important that the rationale behind the decisions be well justified, thoroughly documented, and approved by high levels of management. In the event of a major problem that harms the public and generates litigation (e.g., on a class-action basis, etc.), the discovery process could disclose risk management documentation that shows the responsible firm was well aware of the risks, yet failed to take prudent or reasonable measures to mitigate the risk. The responsible firm could be portrayed in a very damaging light as a company that puts profits before people and public health. Once the decision to mitigate has been made and the strategy identified, a plan should be developed documenting the strategy and plan elements.

Ongoing Control

Once the plan is in place, the effectiveness of the plan should be monitored and adjusted, if necessary. The risk monitoring program should also help to identify previously unrecognized issues. These could have been introduced by changing processes or introducing new technologies.

The risk monitoring program should check to determine if risk factors have changed to either higher or lower values. If factors exceed the previous specified risk limits, mitigation strategies should be reevaluated. If higher risk values decrease below the threshold of acceptable risk levels, further mitigation may not be necessary.

Documentation

Regulatory agencies strongly suggest basing decisions on a justified and documented risk assessment. Documentation is also important to justify investments needed to meet business requirements. Complete documentation for risk management should include:

- Risk Management Master Plan. This shows the organization’s approach towards risk assessment and risk management. It is a framework that is used to derive project-specific risk management plans.
- Risk Project Management Plan. Defines approach, responsibilities, deliverables, and time tables for a specific project, or alternatively as sections in a network qualification plan.
- Lists with description of risk categories, ranking criteria, and results of ranking.
- Justification for mitigation strategies.
- Risk mitigation plan. Includes actions with time tables, deliverables, and responsibilities

Initial Versus Retrospective Qualification

Qualification should be completed before infrastructure components are deployed for use in the production computing environment. This type of qualification is sometimes referred to as an “initial” qualification. However, an organiza-

tion may find network infrastructure that was never qualified, has been in place, and functioning for some time. Because networks change frequently over time, it may not be possible to identify and qualify a previous “initial” configuration of the current network infrastructure. Nonetheless, it is important to qualify the current network. In doing so, certain selective information from the network’s past performance may still be relevant and considered “retrospectively” as part of that effort.

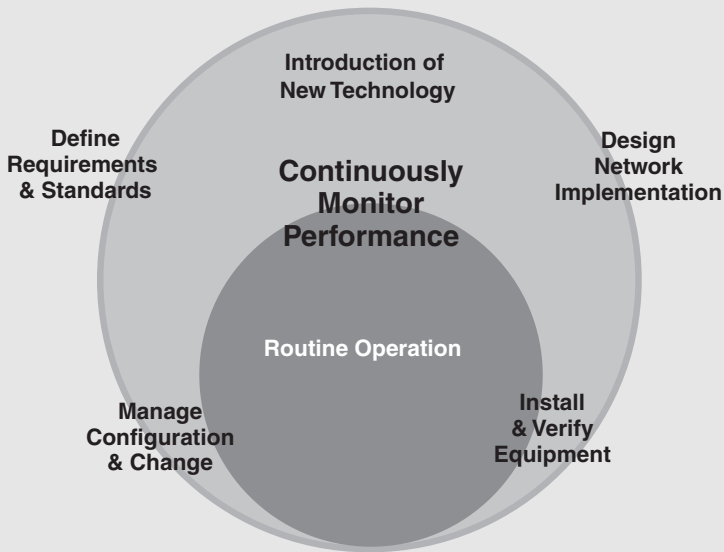
Initial qualification simply means having written proactive processes in place, and following them for all of the phases described above. The concept of having a well-defined and controlled network infrastructure management process from concept to retirement mirrors the widely understood expectations for prospective validation of automated or computerized systems. Satisfactory “initial” qualification is achieved when a written process (e.g., procedures, guidelines, and/or work instructions, etc.) is understood and followed to cover these elements. It is understood that information is available to demonstrate that the process has been followed, and show that network infrastructure components meet specifications and requirements.

Organizations that are new to NIQ recognize that processes are already being followed, even if completely undocumented, and have begun to capture qualification activities in written form. Creating a “snapshot” baseline of the network infrastructure with changes from the baseline documented via change control is an excellent starting point. Another approach is to focus on one discrete area of the network infrastructure (e.g., routers, switches, etc.), and identify who should be allowed to update or change components, conditions under which the changes may occur, and document (or reference) repeatable instructions that are needed to perform and verify those changes. The instructions should be written at a level that the technical staff considers helpful and appropriate to ensure tasks are performed in a repeatable manner (see Figure 2).

The same type of approach mentioned above - “observe and capture” - should be incrementally expanded to steadily develop established written processes covering all aspects and components of the infrastructure. For example, once the process for controlling changes to network infrastructure components, such as routers is established, move on as a logical next step to capturing the process for purchase and installation of other network components. In order to minimize redundancies, documentation can collectively cover identical network infrastructure components and elements common to the infrastructure. Expand the NIQ program, ad-

Figure 2

Network Qualification Cycle



addressing the most critical components (as defined in the risk assessment) first in a prioritized manner, until all elements of the network infrastructure are covered by written processes, and any required configuration data is captured. New purchases and installations should follow the newly defined and documented processes.

Retrospective qualification, the review of historical operating performance to determine the acceptability of current performance and capability, is generally not applicable to network infrastructure components, due to the rapid rate of change and reconfiguration virtually all organizations experience as the infrastructure evolves. Once the processes described above are established, much of the existing infrastructure may lack historical documentation (e.g. bandwidth requirements or initial router configuration, etc.) required by the current processes. In these situations, it is appropriate to capture or reference as much of the information required by the applicable process as possible to facilitate change control or possible disaster recovery. However, attempting to “look backwards” and explain historical performance, document initial configuration, or explain all changes that have occurred since initial installation provides little or no value. It is best to document and test what you have, and then move forward in strict adherence to your new procedural processes (e.g., SOPs, procedures, guidelines, work instructions, etc.).

Good Engineering and Quality Assurance Best Practices

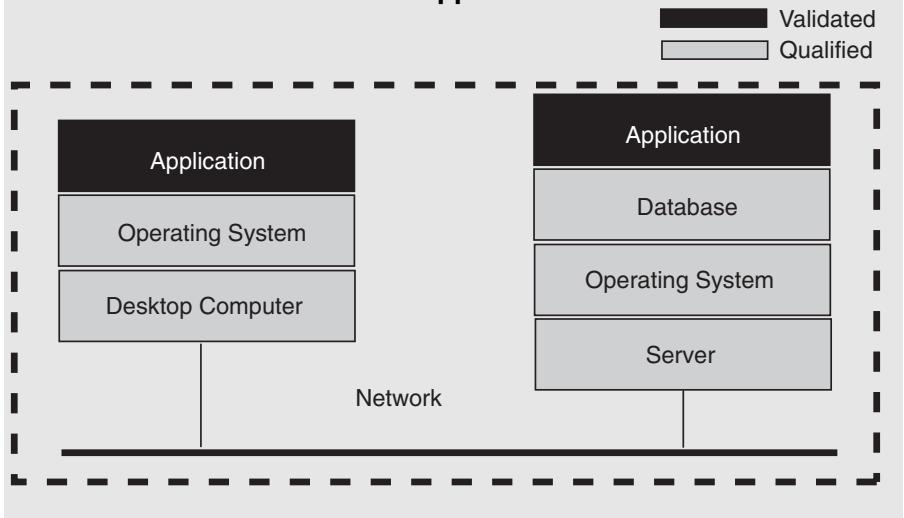
Hardware and Software Standards

Selection of infrastructure technologies is driven by evaluation of industry trends, system requirements, and corresponding industry infrastructure hardware and software standards. Standards form the basis for controlled, uniformly applied technical solutions. This, in turn, is the first step in providing a qualified network infrastructure. Standards should be defined, approved, and maintained through a documented and managed process.

The use of standard technologies helps reduce complexities of maintenance and support. Standards should be available for servers, operating systems, database management

Figure 3

Qualified Network - Validated Application



software, desktop workstations, base desktop utilities, network hardware, network operating systems, and other key infrastructure components.

Standards will address important requirements for infrastructure support of a company’s business applications and systems. Verification of compliance to existing standards may be accomplished through internal periodic reviews, self-inspections, or periodic audits by qualified resources (see Figure 3).

Staff Qualifications and Training

Evidence of qualified infrastructure support staff begins with documenting job requirements for individual roles. This may take the form of job descriptions for various support functions within the infrastructure organization. Individual staff members should have documented evidence that they are qualified to provide the services called for in job descriptions. This should not only focus on a list of credentials or educational background, but should also reflect expertise gained through ‘in the field’ experience.

Specific training requirements for infrastructure support staff, both internal and third-party suppliers providing support in any infrastructure areas, must be defined to ensure competent delivery of infrastructure services. Training is to include exposure to GxP and other relevant regulatory requirements related to infrastructure implementation and support, as well as specific SOPs that are applicable to an individual’s area of responsibility. Training records must be maintained and available for review, along with general

qualifications identified above.

Supplier Management

Technology and service suppliers should be selected based upon suppliers' capabilities to meet well-defined technical requirements matched against supplier capabilities. In many cases, this will be evaluated through structured processes. Supplier relationships should be carefully managed contractually, and in the case of service arrangements, contracts should include specific Service Level Agreements (SLA's), which clearly outline performance criteria and expectations.

In some cases, supplier audits can help determine if quality programs play a part in supplier services and products. This would include evaluation of supplier product and company viability over time. Selection of a limited number of technology suppliers, based upon well-established industry standards, can simplify management of the infrastructure environment and associated quality impacts.

Configuration and Change Management

The cornerstone for infrastructure compliance is a well-documented configuration and change management process. Configuration management procedures ensure that the current state of the configurable portions of the infrastructure are known and controlled. Key aspects of configuration management include component identification, configuration control, status accounting, and configuration auditing. Configuration management is facilitated with well-documented and managed inventories of important infrastructure equipment and operating environments. Infrastructure components that require configuration management would include:

- Network Devices
- Server Hardware and Operating Software
- Desktop Client Configurations
- Network Topology
- Data Center Systems (HVAC, power, fire suppression)

Any change should be evaluated in terms of business and technical risk, impact to the current business and regulatory environment, and implementation considerations. Change documentation requirements may vary for specific types of infrastructure changes. Replacement of identical hardware components may require only creation and approval of a change control record, while upgrades to the operating sys-

tem or layered software may require additional documentation, and include re-execution of the original installation work-instructions (verification). Change control procedures should outline how various categories of change will be documented and approved, and how the impact of the change on the rest of the environment is analyzed and tested, if appropriate. Any change process must include considerations for handling situations when a change does not provide the desired result (i.e., procedures for restoring the modified environment to its original state), and documenting and resolving the problems that were encountered in implementing the change.

Effective change control procedures ensures that properly designed, implemented, and maintained technologies continue to effectively support business applications. Components of effective change processes may include the following, depending upon the impact and criticality of the change.

- Complete business and technical analyses of proposed changes
- Specific implementation plans for individual changes
- Development of associated test plans
- Identification of steps required to reverse the change if problems arise (back-out contingencies)
- Review and approval of proposed changes by key stakeholders (including the change owner, system owners, technical representatives, and quality organizations for changes impacting regulated environments)
- Tracking the implementation of the change
- Analysis of success or failure.

Qualification Methodology

The qualification methodology used in the remainder of this paper is intended to closely follow the normal lifecycle of IT infrastructure components. The goal and focus of qualification is to understand, clearly define, and control good infrastructure business practices. Qualification should be a natural outcome of these business best practices.

A model lifecycle for IT infrastructure components is outlined below. Note that this model is general, and not every activity will be applicable in every situation. In later sections of this paper, specific examples using this model are given.

Qualification Methodology and Deliverables

For each phase in the qualification lifecycle model, the outputs of the activities described by the model must be captured. Infrastructure qualification will result in documents that capture this activity. These documents should be the natural result of the activities in that phase.

An important practice is that these documents be controlled. In other words, they should have approvals (i.e., signatures) and version control. They should also be stored in a protected area so that they can be easily retrieved or located, especially by those performing the work. A document management system is desirable to help achieve this goal.

For each phase in the qualification lifecycle model, the outputs of the activities described by the model must be captured.

The table in *Appendix 2* captures the types of documents that may be produced during a particular qualification phase. Not every type of document will be applicable in every situation. This table captures suggested outputs, but it is not all-inclusive, nor is it the only way to appropriately document activity. This approach is not in conflict with the information centric versus document centric approach. The content of the information or documentation is more important than the document title. If the IT installation instruction fulfills the requirement of an IQ protocol, the suggestion is to leave the IT terminology in place. If a work instruction fulfills the requirements for documenting that an activity has been completed, in the context of the IT network infrastructure domain, then this should be acceptable within the management of the IT organization, and provide evidence to other organizations. Information and documentation should be clear in the context for which it exists.

Planning Phase Deliverables

Qualification Plan

A qualification plan is a document that captures the steps to be taken in order to qualify the network infrastructure.

Typical contents of a qualification plan are roles and responsibilities, tasks to be accomplished, timeframe for task completion, and responsible persons for the work.

An organization might have several layers of qualification plans. For example, a high-level plan may exist below the higher-level document.

Content for a qualification plan is often driven by the output of a risk analysis. Any applicable corporate policies and procedures should be considered when building the plan. A qualification plan should be appropriate for the complexity of the infrastructure components being qualified. For example, a qualification plan for a new highly-available super-computer class system that will host a corporate large Enterprise Resource Planning (ERP) solution will likely be complex. In contrast, the qualification plan for an infrastructure area that routinely installs standard infrastructure components will be much simpler, and may describe processes that cover a large number of infrastructure components.

Service Level Agreements

A Service Level Agreement (SLA) documents the services that the infrastructure support teams will deliver in order to meet application requirements. Content of a SLA normally includes a list of services provided, response times, and uptime requirements. An infrastructure service area may have one document that covers all customers, or may have agreements that cover individual customer areas, as appropriate. Customers for a SLA may include IT application support teams, application end users, or both.

Standard Operating Procedures

Infrastructure support teams have high-level processes that must be defined in order to professionally manage their services. Such processes likely include change management, problem resolution, backup/restore, training, configuration management, performance monitoring, and security management. In the planning phase, such key processes must first be identified, and then documented and approved prior to their implementation in later phases. Standard Operating Procedures (SOPs) are the documents often used to describe such processes.

These SOPs capture processes that are normally used by an entire team for all the components supported. For example, one change control process could be documented in an SOP, and used by an entire team for every infrastructure component they support.

Design Phase Deliverables

Design Documentation

Most infrastructure teams should already have processes in place to help determine what infrastructure pieces need to be acquired. In fact, infrastructure teams typically either make purchase recommendations, or are responsible for making the purchases themselves. Infrastructure teams also determine how the components will be configured initially. A design document captures the output of such purchase and configuration decisions in a readily accessible manner.

In many cases, the demands of applications (such as number of users, data storage estimates, application-level restrictions, such as Operating System (OS) estimates and application dependencies, etc.) will directly drive design decisions. When these factors are known, they should be captured and documented. In other cases, such as networks or data centers, design may be driven based on projected growth and/or historical trends of accumulated applications.

A design document will vary, depending on the type of infrastructure being managed. For example, design documents could be vendor-supplied configuration specifications (often produced in the purchasing process) that have been verified by the infrastructure team, internally-created drawings, such as network diagrams, or text descriptions of key configuration options. The level of detail that is captured for design should be appropriate to business use, amount of customization, and type of infrastructure. For example, a network design will likely include diagrams or drawings that show the connections between network components. A design for a standard server could be a purchase order or shipping invoice that captures the details about the components purchased (e.g., number of processors, amount of memory). Note that where such information is contained in scattered source documents, they should be extracted and retained where they can be collectively retrieved.

Architecture or Standards Documents

A good infrastructure business practice is to develop standards, which may also result in an infrastructure architecture. An architecture or standards document captures these standards in one location. Such a document should describe the standards, scope for such standards (e.g. corporate, departmental, etc.), and any process for requesting and approving any deviations from standards.

Build and Test Phase Deliverables

An important task of network infrastructure support teams is the installation of infrastructure components. The build and test phase includes all steps necessary prior to the actual installation into a production environment. Build and test phase activity includes the development of installation instructions, the development of test scripts that will be used to determine if the installation succeeded, and preliminary execution of these instructions and tests, when applicable. It is suggested that the tests be performed in a separate test environment.

Installation Instructions

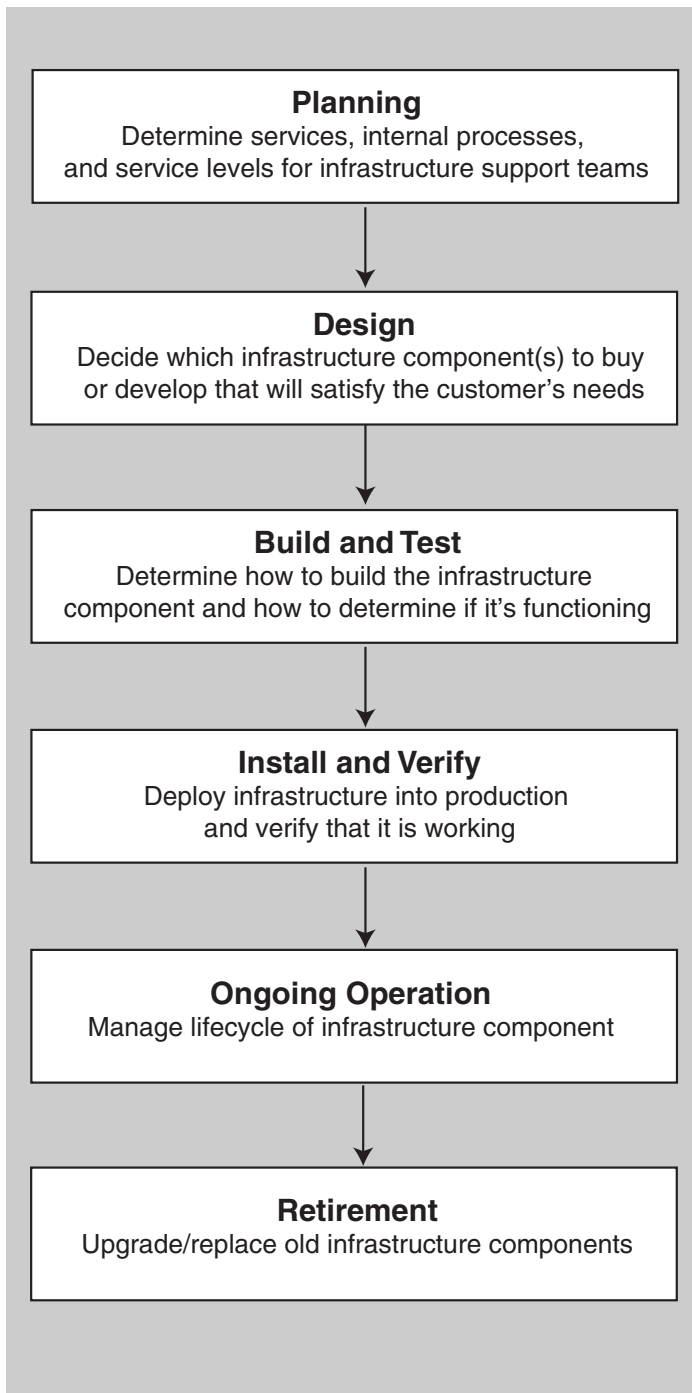
Installation instructions outline the steps trained network infrastructure personnel would use to perform an installation. These instructions should be documented, reviewed for technical accuracy, approved prior to their use, and easily accessible. The purpose of such instructions is not to rewrite the vendor manuals, but to instead capture any local settings, processes, or conventions. In many cases, the instructions will reference (but not repeat) the steps documented in a vendor manual. The complexity of the instructions and the level of detail should be appropriate for the complexity of the asset. Checklists may be an appropriate format for such instructions. Good installation instructions play an important role in providing consistency across installations, reducing errors, and training new staff in local processes.

Depending on the infrastructure type, installation instructions may be executed once, and captured into a “build” that is later deployed into production, or the installation instructions may be performed at the actual time of the installation. In most cases, a given set of installation instructions will be used for the installation of many “like” infrastructure components (e.g., UNIX operating system installation instructions would be used repeatedly to install many UNIX servers).

Test Scripts

Test scripts are used to ensure that what was installed in the live environment is working properly. Testing each and every potential function of an infrastructure component may not always be practical or feasible. Teams should carefully consider what to test, and ensure that their test scripts are technically sound, well-designed, and capable of properly challenging the component’s functionality.

In some cases, additional testing in the live environment may be needed beyond the initial verification of successful



installation. For example, a newly installed component may not be intended to operate in a stand-alone fashion. In addition, proper performance under stress (e.g., simulated high load) may be critical. Any additional steps needed to verify appropriate operation in a given operational environment or under stress should be documented.

Testing methods and the documents that record them should be versioned and maintained. Test scripts will vary with infrastructure type. Some infrastructure teams may write automated scripts to verify an appropriate installation. Others

may verify the installation through interactive inspection of the infrastructure component. In either case, the verification method should be documented with approvals, if appropriate.

Test Environments

A test/development environment is highly desirable when developing installation instructions and test scripts. Whether it is a sub-set or a simulation of the production environment, the ability to utilize a test environment to work outside of production is an important consideration.

Prototype Testing

New or non-standard types of infrastructure or unique configurations of infrastructure may require prototype testing to ensure that the components will function as planned. This type of testing should be done outside of a production environment, if possible. In many cases, such prototype testing is performed prior to adding the infrastructure component to the approved architecture list. Examples where prototype testing is desirable include the introduction of a new technology (GB Ethernet) or major software version release (e.g., database software, operating system, backup software).

Installation and Verification of Phase Deliverables

Installation Record

Once the infrastructure component is ready for production use, the installer will deploy it into production by using the previously established installation instructions, or by migrating an established build into a production environment, as appropriate. The infrastructure support team should retain some record of the installation. Installation records typically capture the unique identifier of the infrastructure component installed, installation date, and versions of the build installed and instructions used for the installation.

Test Script Execution

Verification of proper installation is performed using the test scripts developed in the prior phase. An infrastructure component is ready for production use once the test script has been executed and any problems resolved. If possible, the person performing the verification should be different from the person who performed the installation, if required by a company's procedures.

Ongoing Operation Phase Deliverables

Records of Standard Operating Procedure Execution

Infrastructure teams provide lifecycle support to their installed infrastructure base. These teams should be following the process as documented in their SOPs. Records that demonstrate this behavior should be defined and retained. For example, a team's change control SOP will likely produce change records when the process is executed. Such records provide evidence that the team is following its processes. Additional benefits of such records include an historical trail (e.g., what was the last change made to this infrastructure component, etc.), and the ability to identify systemic issues by collectively examining records.

Technical Instructions

In addition to the processes described in their SOPs, support teams may produce detailed technical instructions for ongoing activities. For example, the purpose of a technical instruction document may be to ensure repeatable steps for operational tasks, such as daily monitoring. These documents are not intended to duplicate instructions that exist in vendor manuals. In fact, many qualification attempts have failed because teams have attempted to rewrite all their vendor manuals. This approach is flawed, due to the enormous volume of material covered in manuals, the likely introduction of error when rewriting so many manuals, and the lack of value for the time invested for cases when vendor manuals are sophisticated, accurate, and easily accessible online. Instead, infrastructure support teams should create technical instructions where value is added and risk reduced. Local methods that are likely to be, or need to be, repeated should be documented, especially those processes unique to a given local environment. Technical instructions should also be produced when vendor manuals are insufficient, inaccurate, or inaccessible. Technical instructions should be accurate, clearly written, updated as needed, and readily accessible to the support team.

Another critical component of ongoing operation is keeping both SOPs and technical instructions current. Teams should have a process for reviewing and updating these documents.

System logs are likely used throughout the qualification lifecycle. Monitoring of critical functions, such as system access security, backup success/failure, and performance levels may all rely upon system logs. An area that SOPs should address are which logs are reviewed, how often they are reviewed, and by whom.

Retirement Phase Deliverables

Retirement Procedure

Infrastructure equipment is often obsolete after only a few years of usage. Infrastructure support teams should have a defined process for handling obsolete equipment. A retirement procedure should be produced which captures the methods that an infrastructure team will use to handle aged equipment. The procedure should address the team's approach for migration of data to new equipment, as well as hardware disposition, and removal of any sensitive data from the old equipment.

Given that infrastructure components may be retired long before the end of the life span of the applications hosted, the scope of the retirement procedure should be for the infrastructure components only. For example, a server hosting a given application may be retired and replaced with a new server several times over the application's life, due to the limited technological life of the server. Be aware, however, of any interdependencies between the applications and the network components that might be candidates for retirement; such interdependences should be evaluated as part of infrastructure risk assessment and change control procedures. A team's retirement procedure will likely cover all similar components supported by a team.

Qualification Methodologies

Data Centers

Data centers house and support infrastructure components, that in turn, host a company's applications. Key aspects of managed data centers that should be considered relative to qualification activities are included below.

Planning Phase

Qualification Plan

A qualification plan for a new data center is likely to be very complex. It should describe the roles and responsibilities of those associated with the project, timetables and milestones to build the facility, install the necessary electric, air handling (HVAC), and fire suppression equipment, and verify the operation of this equipment. In addition, the qualification plan should address the timetables for formation and institution of formal processes for critical data center operations, such as equipment add/move/changes, environment monitoring, and security management.

If the facility is already built and operational, then the

qualification plan should describe the roles and responsibilities of those associated with the project and timetables for collecting existing documentation (or creating documentation if none exists) for the current configuration. In addition, the plan should include the timelines for producing any missing documentation for existing processes for critical data center operations, such as equipment add/move/changes, environment monitoring, and physical security management.

Service Level Agreement

The SLA for a data center should address the necessary uptime and redundancy requirements for cooling, power, and space. Any agreements for monitoring, 24x7 operation, disaster recovery, or security access should also be addressed.

Design Phase

For a new facility, design of the data center will rely on the output of a risk analysis to determine its availability requirements. Considerations weighed in the risk analysis should include business criticality of systems housed in the data center, and the collective impact if the systems were off-line due to problems with power, cooling, or fire. Once this is understood, appropriately redundant power, HVAC, environment monitoring equipment, and fire suppression features can be selected and documented. A facility expert normally completes this work. For an existing facility, these features should be documented as they exist in their current state.

Once the facility is ready to host infrastructure equipment, a floor layout (which should include the location of equipment within the data center) should be produced and maintained throughout the operating life of the data center.

Installation Phase

Installation, verification, and maintenance for facilities-related equipment is usually completed by groups external to the IT data center support organization. Such installations are normally governed by building, fire, and safety codes, as well as the equipment manufacturer's specifications. IT data center organizations should ensure that these external organizations are qualified to professionally perform these installations. The IT data center support organization should provide oversight for any redundancy testing done by facilities professionals, and should perform additional testing on security-related data center features (e.g., card access, etc.). Upon completion of data center construction and installation work, facilities professionals should complete and sign

documents indicating compliance with all applicable codes, standards, and equipment manufacturer recommendations.

Once the facilities are ready to host infrastructure equipment, IT data center professionals should provide formal processes for adding, deleting, or removing equipment from the data center. Data center layout documents should be kept current with these changes.

Ongoing Operation

Data centers should have SOPs that address critical data center activities, such as:

- Physical Security – addresses how physical access to the data center is granted and tracked. Includes the process to periodically review the access roster, and how authorization is verified before data center entry. Also includes handling of transient personnel, such as maintenance workers and the processes to ensure access rights are appropriately revised or revoked as staff are transferred or terminated.
- Environment monitoring – documents the monitoring that will detect and alarm for problems with power, HVAC, fire, water leaks, or other environment issues. Includes the frequency of monitoring, and the process used to notify appropriate personnel if a problem is detected.
- Change and Capacity Management – documents the process to add to or remove equipment from the data center. Also documents the data center capacity tracking and monitoring

Technical instructions may be produced for commonly repeated operational tasks, such as:

- Maintenance – documents the maintenance activity for data center support equipment, and specifies who is responsible for oversight of maintenance delivery
- Other critical data center activities, which might include backup tape rotation, log file monitoring, etc.

Server Hardware and Operating Systems

Server hardware and associated operating system software products support a number of functions, including business applications, e-mail, databases, inter/intranet web, network management, print, and general file services. Risk factors, as well as the definition and application of hardware standards, should be applied in evaluating qualification re-

quirements for servers and operating system software. This section focuses on specific server-related aspects of the general infrastructure qualification approach.

Planning

Typically, infrastructure organizations, working in conjunction with supported application groups, will attempt to standardize around key server platforms to support specific services. Standardization enables streamlining of all server-related support requirements, including qualification. Server standards should be documented and published. Documented, controlled installation instructions should exist for each standard server type and operating system supported. Standardization of platforms will also allow for creation and approval of standardized installation test scripts that can be applied on a routine basis.

For high risk complex systems having specialized performance requirements, supplemental verification testing may be required beyond standardized protocols. This should be identified in the planning phases of a project, and appropriate test protocols may be required that are specific to the project. If a project has special requirements that require a server solution outside of defined standards, the reasons for the use of non-standard equipment should be documented in project planning documentation. Again, this may require development of verification test scripts that are specific to the planned non-standard solution.

Risk factors to be considered in qualifying server platforms would include the types of services or environments that they support. For example, servers supporting general services, sandbox, or development activities, are viewed as lower risk than those supporting critical production environments, and may warrant different levels of testing, change management, and monitoring. These factors, and any differences in server verification based upon such risk evaluations, should be outlined in a server qualification plan or SOP.

Design

While basic platform criteria may be defined through the adoption of server standards across an organization, application requirements will drive specific hardware configurations during the design phase of a project. Specific hard-

ware requirements should be documented in project design documentation to form the basis of hardware acquisition and specific verification activities during installation of the equipment. Server supplier specifications covering environmental and power requirements are included implicitly with the selection of specific equipment, and will also be referenced in the installation verification process.

Build and Test/Installation

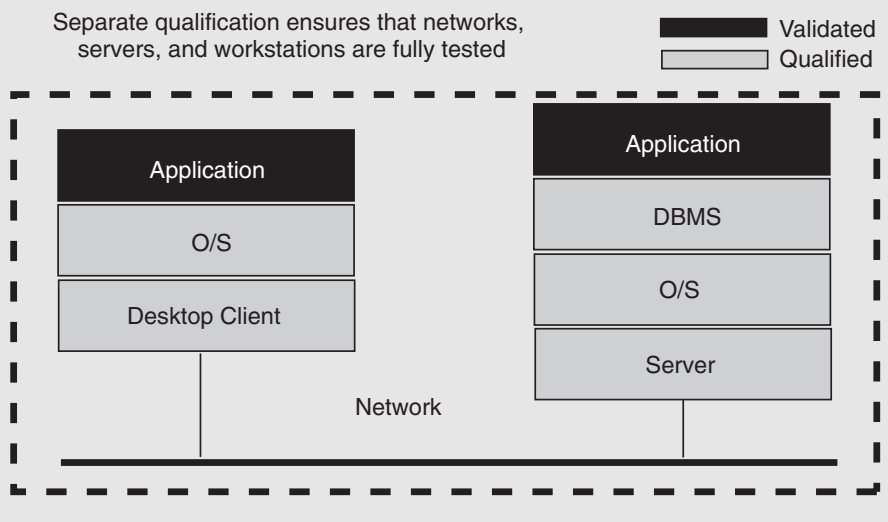
Upon receipt of specific server equipment, documented installation instructions will be used to perform server builds and installation activities. For routine server installations, standardized test scripts or installation checklists would be executed covering verification of:

- Specific hardware and operating system configuration against application requirements
- Environmental conditions against hardware supplier specifications
- Version of documented installation instructions used
- System log files containing no error conditions on initial startup and operation
- Existence of key operating and support procedures
- Network connectivity and controlled access

For more complex high-risk server installations, customized test scripts may be required to verify specific performance requirements, such as clustering and fail over capabilities, data replication services, and synchronized backup and restore capabilities across multiple platforms.

Figure 4

Business Continuity



These types of test protocols would be executed in addition to the type of standard verification for basic server installation (see Figure 4).

Ongoing Operation

As with other infrastructure components, documented, controlled operating procedures are necessary to provide adequate ongoing support for server platforms. These should include server monitoring and capacity management. A number of tools are available today to support basic server monitoring, as well as enhanced monitoring of individual services and processes running on each platform. Automated monitoring of server resources should be considered for critical systems.

For high risk complex systems having specialized performance requirements, supplemental verification testing may be required beyond standardized protocols.

Change management for servers should cover all aspects of server updates, including hardware component replacement, operating system patches, full upgrades to operating systems, and expansion of existing hardware configuration. Each change should be evaluated relative to its impact to business functionality, technical complexity and risk, and qualification status of the server. Higher risk changes should include documented testing, verification, and back out plans that have been approved prior to change execution.

PC's, Workstations, Laptops, and Handheld Devices

Personal devices like PC's, workstations, laptops, and handheld devices are used in large quantities, and often connected to corporate networks. Some companies have thousands of PC's, many times with different hardware configurations, various versions of operating systems, and application software. The large variation of hardware and software,

combined with the ease of adding and changing modules without following strict change control procedures, make it difficult to bring and keep these devices in a state of control, a requirement not only by the FDA, but also for effective business continuity.

In this section, we describe how these personal devices can be brought into and maintained in a controlled status.

Planning for Standardization

Half of success for efficient qualification and control is development and implementation of a plan for purchasing, installing, and qualifying personal devices. The main objective is standardization of hardware, operating software, and application software to the extent possible. Such a plan should include

- Guidelines for purchasing personal devices
- Listing of minimal configurations
- Listing of possible suppliers for hardware and software
- Listing of possible standard configurations and options
- Guidelines for installation and documentation
- Guidelines for changes to the devices, e.g., adding or upgrading hardware, operating systems, and application software

Selecting specifications, suppliers, hardware, models, and software

Standardization of hardware and software helps with qualification. One problem is that the lifetime of computer hardware is relatively short, which also limits standardization. The recommendation is to work with hardware suppliers, and to standardize on models that have a relatively long lifetime. Specific recommendations include:

- Define minimum specifications for hardware, e.g., processor speed, memory, hard disk capacity, CD/DVD-ROM.
- Define a minimum set of application software
- Select a supplier and model that meets specifications.
- Take the most recent model and obtain a commitment from the supplier for delivery of the selected model over the foreseeable timeframe, e.g., two years
- Allow employees to only purchase this model with approved options
- Allow employees to order approved operating systems and application software
- Specify the approved version of operating and application software

Testing

The approach for qualifying PCs and workstations is to:

1. Build one reference system that contains all specified hardware, operating software, and application software
2. Test and qualify this reference system
3. Create many duplicates of this qualified system for use in production

Once qualified, the reference system forms a configuration baseline for workstation qualification. This baseline should be preserved by capturing a snapshot of the qualified software image (e.g., using Ghost or tar) and a configuration record of the qualified hardware. Once this has been done, any number of additional workstations may be qualified simply by loading a copy of the qualified software image onto a copy of the qualified hardware configuration, then performing minimal acceptance testing (e.g., does it boot, etc.).

Software that comes with the operating system, but is not needed by end users, should be removed (e.g., games, etc.). The reference system should be tested extensively by following test scripts and previously defined acceptance criteria. Test cases should include correct start up, user access, and testing of applications (e.g., Internet Explorer, Outlook, MS word, printing, and file storage, etc.), retrieval, and network connectivity.

It should be noted that if the architecture of the organization's validated applications requires the permanent installation of "fat client" program code on the workstation, the interoperability risk is higher, and testing must therefore be more rigorous than if all validated applications are accessed via "thin footprint clients" (e.g., web browser, Citrix, etc.).

Installation and testing at end users site

Workstations may be pre-configured prior to delivery to the user, or configured after delivery through the use of installation scripts or electronic software distribution tools. After delivery and installation, basic acceptance testing (e.g., proper startup, network connectivity, etc.) should be performed. A record of the successful installation and acceptance testing should be retained by the organization.

Change control

There is a high likelihood that end users will wish to make changes to "their" qualified workstations and/or PCs. The organization must plan for this, and determine how the pressure for changes will be balanced against the desire to maintain a

qualified state. A risk-based approach should be used to determine what types of controls should be put in place.

Factors to consider:

- How is the system being used? A desktop PC that occasionally launches a validated change control application may require less stringent configuration management than a PC that is used to automate product manufacturing or testing.
- Are technical controls (e.g., user profiles, login scripts, change notification and rollback software, etc.) available to secure the desktop and/or prevent uncontrolled changes? If not, must procedural controls and written documentation of changes be used?
- What is the real consequence of an uncontrolled change? Example: assume that all validated applications are accessed via a web browser. If a user makes an uncontrolled change to a PC's configuration, the web browser may stop functioning. This situation will result in a help desk call and a loss of productivity, but is there any real quality risk or compliance risk?

The organization should identify quality and compliance risks, and determine which risks must be mitigated and which will be accepted. This will determine whether the organization's configuration management and change control process for workstations and/or PCs will be restrictive or permissive, procedural, or technical. Different processes can be used for different scenarios: for example, the high-risk PC used in the lab can be secured by requiring written change procedures, configuration records, post-change testing, and approvals from Quality; whereas the average desktop PC can perhaps be allowed to change more often and with fewer controls.

Wireless Equipment and Software

Wireless networks and devices are finding increased utilization in regulated business areas. Some popular business uses are: data collection, supply chain management, email, general communications, database input systems, and on-site analysis of data

We can categorize wireless equipment as long distance RF or microwave systems, short-range small office or building-wide systems, and wireless receiver equipment that is integral to the user's computer or data collection tool. All wireless components should have reasonable controls in effect to ensure performance and security within expected parameters.

Hardware installation

The most important aspect to be aware of when installing wireless equipment is the fact that RF transmits/receives in all directions on some devices and two-way direction in other cases. If it is located too close to another network, you may get electromagnetic interference limiting performance, even in the case of unidirectional transmitters. (This effect is sometimes called scatter though better systems will filter for it.) Multiple transmitters should be placed away from one another in order to avoid cross-talk and to improve the wireless coverage area. The transmitter/receiver must always be installed by qualified technicians per instructions of the manufacturer of the equipment, or even better, by the manufacturer.

Layered Software

A myriad of software products is typically used within even the simplest of infrastructure computing environments to support common application service requirements, such as user authentication, backup, and software distribution. There is also a growing volume of software for monitoring and analyzing infrastructure performance (e.g., network monitoring). These support and monitoring software packages are collectively referred to in this article as layered software. Consideration should be given to determining the rigor of qualification appropriate for layered software based on the potential impact to validated applications.

Planning

While it is impossible to identify and provide qualification guidance for all examples of support software available in the marketplace, categorizing the potential impact on validated applications, as either direct or indirect, provides a good starting point for determining the qualification needs of layered software products within the context of infrastructure.

Layered software, whose installation, configuration, use, or ongoing maintenance activities must consider requirements of specific validated applications, can be considered as having a direct impact on those validated applications. For example, most software distribution tools require configuration (script development) for each application remotely installed over the network. Since the integrity of the script will directly

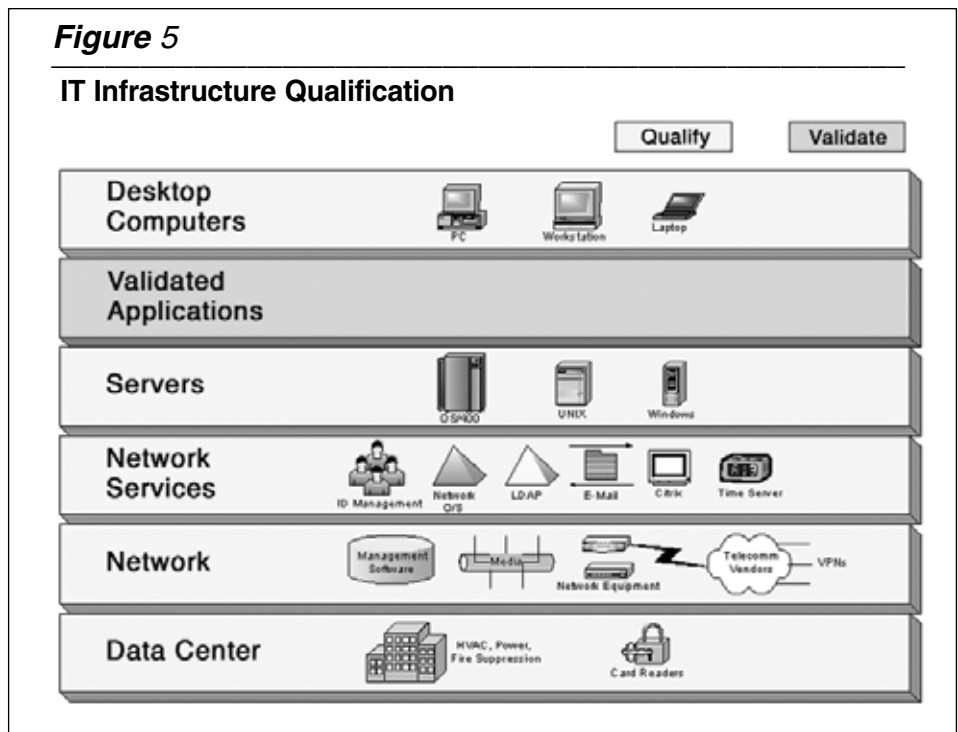
determine the success or failure of attempts to distribute and install the validated application, the impact of the distribution software on the validated application is considered direct. Conversely, network monitoring tools generally have an indirect relationship, as they can generally be installed and operated with no impact on, or consideration of, validated applications operating on the network, and should follow the generic lifecycle approach.

Planning for layered software with potential direct impact on one or more validated applications should explain the relationship between layered software and specific validated applications. This explanation should include identification of the requirements fulfilled or services provided on behalf of the validated application(s), and any modification that will be required, as those validated applications change or applications are added or removed from the environment.

Design

Since layered software is almost always bundled with other software or purchased off-the-shelf with no customization, the design documentation can be limited to a simple listing of requirements the software is intended to address, and any configuration settings/instructions necessary to achieve the required functionality in the intended environment.

Consider mapping the requirements to specific sections of supplier materials, such as user or technical manuals for functionality that is critical to a business operation or directly impacts validated applications. The primary value of



such mapping is that staff can more easily locate detailed guidance regarding correct operation, configuration, and maintenance of software.

Build and Test

Since layered software is rarely built, this phase consists of developing work instructions to ensure local staff can install and configure the software in a test environment (if possible) and testing to determine if the requirements will be achieved. Generic installation instructions are usually provided with layered software, so these need only be referenced, not repeated, with incorporation of local information or amendments needed to setup the software in your environment. The goal is a process that will be readily understood by the staff that will use the instructions.

Once successfully installed and configured, the software should be tested to determine if the requirements identified in the planning phase are satisfied.

Installation Phase

Verification of proper installation can be as simple as a quick version check on a splash screen, or as complicated as a daily backup integrity check spanning multiple weeks for mission critical or high-risk validated applications that includes completion of a detailed checklist each day. The detail and extent of the final installation verification should be commensurate with the potential impact of failure of the software to perform as required. Pay particular attention to layered software requiring configuration changes, as either applications or hardware is deleted or added to ensure all required service needs are covered (e.g., ensuring all disks are included in the nightly backup script, etc.).

Ongoing Operation

Layered software is often implemented to provide a service for multiple applications (e.g., backup for LIMS and MRP systems, etc.). Implement processes that will keep configuration and operation of the layered software synchronized with future changes to applications and hardware that can be affected by the layered software.

Retirement

As layered software is retired or replaced, consider the possible need for later restoration. Copies of retired software and associated support materials, such as internal documentation and supplier materials, should be retained when that software would be needed to process or restore archived data. The software and documentation should adhere to the

same retention schedule as the pertinent archived data.

Infrastructure Applications

Certain application software is used by infrastructure organizations to manage various business processes within the infrastructure environment (*see Figure 5*). Examples of software that might fall into this category would include:

- Inventory/Asset/License management systems
- Problem and change management systems
- General document management applications supporting the creation, approval, and control of items, such as
 - Standard Operating Procedures
 - Installation guidelines and checklists
 - Network diagrams

While the information managed within these types of applications does not directly impact the development, manufacture, and distribution of pharmaceutical products, some of this information may be subject to review during audits by regulatory agencies, e.g., change records that show the controlled change history of a qualified server. As a result, they may be viewed in the same validation context as business applications supporting regulated areas. Such considerations are outside the scope of this paper, which focuses on infrastructure equipment qualification, but such applications should be reviewed with the company's business Quality Unit for potential applicability of internal validation requirements. □

About the Authors

The full IVT NIQ committee is responsible for authorship of this proposed standard. The opinions expressed are their own, and not necessarily those of their employers. Comments and questions should be directed to Warren Campbel. He can be reached at (610) 715-4741, by fax (610) 933-9413, and by email at campbmw@attglobal.net

Suggested Reading

- Garwood, R. and Motise, P. FDA's Guide to Inspection of Computerized Systems in Drug Processing. Reference Materials and training aids for investigators. (The Blue Book). Feb. 2000.
- Institute of Electrical and Electronics Engineers. IEEE Standards Collection: Software Engineering. 1994 Edition.
- Myers, G.J., Ed. "The Art of Software Testing." John Wiley & Sons: New York. 1979.

- International Society of Pharmaceutical Engineering. "GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture: Version 4.0."
- TickIT.A Guide to Software Quality Management System (Using 9001:1994) – The TickIT Guide. ISBN 0-580, Issue 3.0, 1994.
- Parenteral Drug Association. "Validation and Qualification of Computerized Laboratory Data Acquisition Systems, Technical Report #31." PDA Journal of Pharmaceutical Science and Technology.
- Parenteral Drug Association, "Network Management in an FDA-Regulated Environment", PDA Journal of Pharmaceutical Science and Technology, Vol. 53, No. 6 / November-December 1999.
- Black, Uyless - Network Management Standards, McGraw-Hill, Inc., 1994 - Second Edition
- Carnegie Mellon University Software Engineering Institute (SEI) – Case Study: Computer Supplier Evaluation Practices of the Parenteral Drug Association (PDA), Technical Report CMU/SEI-2003-TR-011, May, 2003
- Crosby, P. B., Completeness: Quality for the 21st Century, Dutton, 1992
- Davis, P. T., (editor) - Securing Client/Server Computer Networks, McGraw-Hill, Inc., 1996
- Dertouzos, M. - What Will be, Harper Edge, 1997
- Freedman, D. P. & Weinberg, G. M. - Walkthroughs, Inspections, and Technical Reviews, Dorset House Publishing, 1990 - Third Edition
- Gause, D. & Weinberg, G. M., Exploring Requirements, Dorset House Publishing, 1989
- Goglia, P. A. - Testing Client/Server Applications, QED Publishing Group, 1993
- Kochan, S. G. & Wood, P. H., (eds) UNIX Networking, Hayden Books, 1989
- Marks, D. M. - Testing Very Big Systems, McGraw-Hill, Inc., 1992
- Miller, M. A. - Internetworking, M&T Books, 1991
- Silverberg, I. - Source File Management with SCCS, Prentice Hall, 1992
- Kaaranjit, S. & Hare, C. - Internet Firewalls and Network Security, New Riders Publishing, 1995
- Smith, M. R. - Commonsense Computer Security, McGraw-Hill, Inc., 1989
- Sodhi, J. - Computer Systems Techniques, TAB Professional and Reference Books (PTR), 1990
- Yourdon, E. - Yourdon Systems Method, Yourdon Press, 1993
- Yourdon, E. - Death March, Yourdon Press, 1997
- Yourdon, E. - Rise and Resurrection of the American Programmer, Yourdon Press, 1996
- Weinberg, G. M. - An Introduction to General Systems Thinking, John Wiley & Sons, Inc., 1975
- Weinberg, G. M. - Quality Software Management, Volume 4, Anticipating Change, 1997.
- Bouman J., Trienekens J., and van der Zwan, M. Specification of Service Level Agreements, clarifying concepts on the basis of practical research. In Proceedings of the SoftwareTechnology and Engineering Practice conference, Pittsburgh, Pennsylvania, USA, August 30 - September 2, 1999.
- Central Computer and Telecommunications Agency. Best Practice for Service Support. IT Infrastructure Library. The Stationary Office, London, UK, 2000.
- Curtis, B., Hefley, W. E., and Miller, S., Overview of the People Capability Maturity Model. Technical Report CMU/SEI-95-MM-01, Software Engineering Institute/Carnegie Mellon University, September, 1995.
- Curtis, W., Hefley, W. E., and Miller, S. People Capability Maturity Model. Technical Report CMU/SEI-95-MM-02, Software Engineering Institute/Carnegie Mellon University, September, 1995.
- Office of Government Commerce. IT Infrastructure Library Online, April 2003. <http://www.itil.co.uk>.
- The Capability Maturity Model: Guidelines for Improving the Software Process. SEI Series in Software Engineering. Addison-Wesley Publishing Company, 1995. Carnegie Mellon University/Software Engineering Institute.
- Journal of Systems and Software, July, 1997. CMMI Product Team. Capability Maturity Model Integration (CMMI)
- Engineering and Software Engineering. Technical Report CMU/SEI-2002-TR-01, Software Engineering Institute/Carnegie Mellon University, December, 2002.
- Adrion, W.R., Branstad, M. A., Cherniavsky, J. C. NBS Special Publication 500-75, Validation, Verification, and Testing of Computer Software, Center for Programming Science and Technology, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Department of Commerce, February, 1981.
- Powell, P. B., Editor. NBS Special Publication 500-98, Planning for Software Validation, Verification, and Testing, Center for Programming Science and Technology, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Department of Commerce, November, 1982.
- Wallace D. R. , Editor. NIST Special Publication 500-235, Structured Testing: A Testing Methodology Using the Cyclomatic Complexity Metric. Computer Systems Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, August, 1996.
- ANSI/ANS-10.4-1987, Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry, American National Standards Institute, 1987.
- ANSI/ASQC Standard D1160-1995, Formal Design Reviews, American Society for Quality Control, 1995.
- AS 3563.1-1991, Software Quality Management System, Part 1: Requirements. Published by Standards Australia [Standards Association of Australia], 1 The Crescent, Homebush, NSW 2140.
- AS 3563.2-1991, Software Quality Management System, Part 2: Implementation Guide. Published by Standards Australia [Standards Association of Australia], 1 The Crescent, Homebush, NSW 2140.
- 1999 IEEE Standards Collection, Software Engineering, Institute of Electrical and Electronics Engineers, Inc., 1994. ISBN 1-55937-442-X.
- ISO 8402:1994, Quality management and quality assurance – Vocabulary. International Organization for Standardization, 1994.
- ISO 9000-3:1997, Quality management and quality assurance standards - Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software. International Organization for Standardization, 1997.
- ISO 9001:1994, Quality systems – Model for quality assurance in design, development, production, installation, and servicing. International Organization for Standardization, 1994.
- ISO 13485:1996, Quality systems – Medical devices – Particular

- requirements for the application of ISO 9001. International Organization for Standardization, 1996.
- ISO/IEC 12119:1994, Information technology – Software packages – Quality requirements and testing, Joint Technical Committee ISO/IEC JTC 1, International Organization for Standardization and International Electrotechnical Commission, 1994.
- ISO/IEC 12207:1995, Information technology – Software life cycle processes, Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 7, International Organization for Standardization and International Electrotechnical Commission, 1995.
- ISO/IEC 14598:1999, Information technology – Software product evaluation, Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 7, International Organization for Standardization and International Electrotechnical Commission, 1999.
- ISO 14971-1:1998, Medical Devices – Risk Management – Part 1: Application of Risk Analysis. International Organization for Standardization, 1998.
- Technical Report No. 18, Validation of Computer-Related Systems. PDA Committee on Validation of Computer-Related Systems. PDA Journal of Pharmaceutical Science and Technology, Volume 49, Number 1, January-February 1995 Supplement.
- Beizer, B., Black Box Testing, Techniques for Functional Testing of Software and Systems, John Wiley & Sons, 1995. ISBN 0-471-12094-4.
- Beizer, B., Software System Testing and Quality Assurance, International Thomson Computer Press, 1996. ISBN 1-85032-821-8.
- Beizer, B., Software Testing Techniques, Second Edition, Van Nostrand Reinhold, 1990. ISBN 0-442-20672-0.
- Deutsch, M. S., Software Verification and Validation, Realistic Project Approaches, Prentice Hall, 1982.
- Dunn, R. H., and Ullman, R. S., TQM for Computer Software, Second Edition, McGraw-Hill, Inc., 1994. ISBN 0-07-018314-7.
- Dustin, E., Rashka, J., and Paul J., Automated Software Testing – Introduction, Management and Performance, Addison Wesley Longman, Inc., 1999. ISBN 0-201-43287-0.
- Gilb, T., Graham, D., Software Inspection, Addison-Wesley Publishing Company, 1993. ISBN 0-201-63181-4.
- Grady, R. B., Practical Software Metrics for Project Management and Process Improvement, PTR Prentice-Hall Inc., 1992. ISBN 0-13-720384-5.
- Herrmann, D. S., Software Safety and Reliability: Techniques, Approaches and Standards of Key Industrial Sectors, IEEE Computer Society, 1999. ISBN 0-7695-0299-7.
- Humphrey, W. S., A Discipline for Software Engineering. Addison-Wesley Longman, 1995. ISBN 0-201-54610-8.
- Humphrey, W. S., Managing the Software Process, Addison-Wesley Publishing Company, 1989. ISBN 0-201-18095-2.
- Jones, C. Software Quality, Analysis and Guidelines for Success, International Thomson Computer Press, 1997. ISBN 1-85032-867-6.
- Juran, J.M., Gryna, F. M., Quality Planning and Analysis, Third Edition, McGraw-Hill, 1993. ISBN 0-07-033183-9.
- Kan, S. H., Metrics and Models in Software Quality Engineering, Addison-Wesley Publishing Company, 1995. ISBN 0-201-63339-6.
- Kaplan, C., Clark, R., Tang, V. Secrets of Software Quality, 40 Innovations from IBM, McGraw-Hill, 1995. ISBN 0-07-911795-3.
- Kit, E., Software Testing in the Real World, Addison-Wesley Longman, 1995. ISBN 0-201-87756-2.
- Myers, G. J., The Art of Software Testing, John Wiley & Sons, 1979. ISBN 0-471-04328-1.
- Neumann, P. G., Computer Related Risks, ACM Press/Addison-Wesley Publishing Co., 1995. ISBN 0-201-55805-X.

APPENDIX 1

Risk associated with design, installation, operation, and change of network components

Action	Risk Issues	Documentation	Primary Factors
<ul style="list-style-type: none"> • Install Router 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity • Capacity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals 	<ul style="list-style-type: none"> • Engineering Considerations • Physical Security
<ul style="list-style-type: none"> • Replace/ Upgrade Router 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals • Problem/maintenance logs 	<ul style="list-style-type: none"> • Engineering Considerations • Physical Security • Current Application and Data Communication
<ul style="list-style-type: none"> • Install Firewall 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals 	<ul style="list-style-type: none"> • Engineering Considerations • Physical Security • Logical Security • Current Application and Data Communications
<ul style="list-style-type: none"> • Install New Server 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals 	<ul style="list-style-type: none"> • Physical, logical security • Testing
<ul style="list-style-type: none"> • Replace/ Upgrade Server 	<ul style="list-style-type: none"> • Security • Communication integrity • Potentially Impacted Applications • Data Integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals • Problem logs 	<ul style="list-style-type: none"> • Physical, logical security • Testing • Change control
<ul style="list-style-type: none"> • Install Workstation 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals 	<ul style="list-style-type: none"> • Logical security
<ul style="list-style-type: none"> • Replace/Upgrade workstation 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals • Problem logs 	<ul style="list-style-type: none"> • Change control
<ul style="list-style-type: none"> • Install Printer 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals 	<ul style="list-style-type: none"> • Confidentiality

APPENDIX 1 (continued)

Risk associated with design, installation, operation, and change of network components

Action	Risk Issues	Documentation	Primary Factors
<ul style="list-style-type: none"> • Install Disk Drive(s) 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity • Data integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals 	<ul style="list-style-type: none"> • Testing
<ul style="list-style-type: none"> • Replace / Upgrade Disk Drive(s) 	<ul style="list-style-type: none"> • Security • Compatibility • Communication integrity • Data integrity 	<ul style="list-style-type: none"> • SOPs • Protocols or Checklists • Executed Protocols or Checklists • Approvals • Problem logs • Backup/Restore Procedures • Backup/Restore Logs 	<ul style="list-style-type: none"> • Change control • Confidentiality

APPENDIX 2

Qualification Phase	Activity	Qualification Deliverable
<p>Planning</p>	<ul style="list-style-type: none"> • Develop or align with corporate policies or guidelines • Determine support team’s approach for managing services <ul style="list-style-type: none"> • Integrate outcomes of risk assessment into an approach • Align with corporate enterprise architecture • Define roles and responsibilities • Identify and define fundamental services and processes • Develop service level agreements between infrastructure support teams and their customers • Document support team’s process as identified in step above. Processes that are common to most infrastructure support teams include: <ul style="list-style-type: none"> • Change and Configuration Management • Backup, Restore, Disaster Recovery • Security • Problem and Incident Management • Monitoring • Training • Document Management 	<ul style="list-style-type: none"> • Qualification Plan • Service Level Agreements • Standard Operating Procedures (SOPs)
<p>Design</p>	<ul style="list-style-type: none"> • Determine infrastructure functionality that is needed, based on customer needs, and steps that will be taken to select and implement the component • Develop standards and architecture • Determine capacity and performance needs 	<ul style="list-style-type: none"> • Design Documentation • Architecture or Standards Document
<p>Build and test</p>	<ul style="list-style-type: none"> • Acquire or develop appropriate infrastructure components • Develop or reference repeatable instructions for installation in the local environment, along with any configuration details. • Execute installation and configuration instructions to determine if required functionality has been realized • Develop test scripts which verify proper installation • Develop test scripts which verify functionality of components under stress, if appropriate 	<ul style="list-style-type: none"> • Installation Instructions • Test Scripts – Develop and Execute

APPENDIX 2 (continued)

Qualification Phase	Activity	Qualification Deliverable
Install and Verify	<ul style="list-style-type: none"> • Install infrastructure components into production environment, utilizing established installation instructions • Verify correct functioning of infrastructure equipment in live environment <ul style="list-style-type: none"> • Execute test scripts and resolve any problems 	<ul style="list-style-type: none"> • Installation Record • Test Script Execution
Ongoing Operation	<ul style="list-style-type: none"> • Monitor uptime and performance • Manage lifecycle of component through execution of: <ul style="list-style-type: none"> • Change and Configuration Management • Backup, Restore, Disaster Recovery • Security Management • Problem and Incident Management • Monitoring • Training • Document Management 	<ul style="list-style-type: none"> • Records which show output of the processes defined in SOPs • Change records • Backup logs • Security authorizations and reviews • Trouble tickets • Technical Instructions
Retirement	<ul style="list-style-type: none"> • Migrate data from old system to new • Ensure proper disposition of old media • Remove old infrastructure components from environment 	<ul style="list-style-type: none"> • Retirement procedure