Technology Update

Validating Computer Systems, Part 4

The QA Role in Computer Validation

Teri Stokes

QA staff members can help develop a computerized system validation policy and SOPs that meet regulatory standards for GCP computer systems.

Quality assurance professionals have important roles to play in computer validation work—roles that do not require them to be technology experts. The QA role in computer validation is to assess and support the quality practices surrounding the computerized system during its development, installation, and use in a GCP work process. The QA focus is not on the details of technology, but on the documented evidence used to prove to an inspector that the GCP system is under management control, that it reliably operates as expected, that it protects the integrity of electronic data during handling, and that its quality is auditable.

The first three articles in this series describe the creation of computer system validation packages for user acceptance of a software application, IT/IS validation of a platform infrastructure, and the software supplier's verification of software development. This fourth, and final, article in the series discusses the quality assurance role in the process, including package audits and system inspections.

Quality roles—QA and QC

Quality professionals must be careful to structure their involvement in validation activities so that their participation is appropriate for the role they intend to play. As quality assurance (QA) professionals, they can lead the effort to develop a computerized system validation (CSV) policy for their organization. They can develop general standard operating procedures (SOPs) for conducting computer validation activities under the CSV policy. They can support line managers in developing and administering a systems QA plan for implementing the CSV policy in their own regulated area. They can instruct system teams in the SOPs for validation and audit CSV packages for their compliance to policy, SOPs, regulations, and validation plan directives. QA personnel can also audit internal and external suppliers for a CSV package. In the end, QA can host regulatory inspections that include review of CSV packages.

When quality professionals participate on the actual CSV package team as package manager, test coordinator, or site QC, they perform a *quality control* (QC) function for the CSV package and are not eligible to audit the same CSV package. In the act of building quality into the CSV package, quality professionals can be very helpful on the package team with the writing of user SOPs and system SOPs to company standards. They can audit internal and external suppliers for a CSV package. Before testing, quality professionals can check the test documentation for its compliance with standards and completeness of coverage for all test cases described in the test plan. They can play a witness role for formal testing and/or review the test records right after testing. As the package QC personnel, however, the same quality professionals cannot provide the QA signature or make a QA audit for the validation plan or validation package summary report, because they are no longer independent of the CSV package effort.

QA and CSV policy

The corporate director of quality assurance joins the chief executive officer, chief information officer, and vice presidents of regulated areas (research, development, manufacturing) as a member of the senior management team that sponsors development of a (CSV) policy for the organization. It is important that QA not write the policy by itself, because then people in line functions will lack the sense of "ownership" in the policy, and that is where resources must be committed to achieve compliance.

The goal of QA in this policy effort is to integrate computer validation practices into the normal

Abbreviations

CSV	computerized system validation
EU	European Union
GCP	good clinical practice
GLP	good laboratory practice
GMP	good manufacturing practice
GXP	good [pharmaceutical] practice
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
ISO	International Organization for Standardization
MHW	Ministry of Health and Welfare, Japan
MVP	master validation plan
QA	quality assurance
QC	quality control
SDLC	software development life cycle
SLA	service level agreement
SOP	standard operating procedure
SQAP	systems quality assurance plan

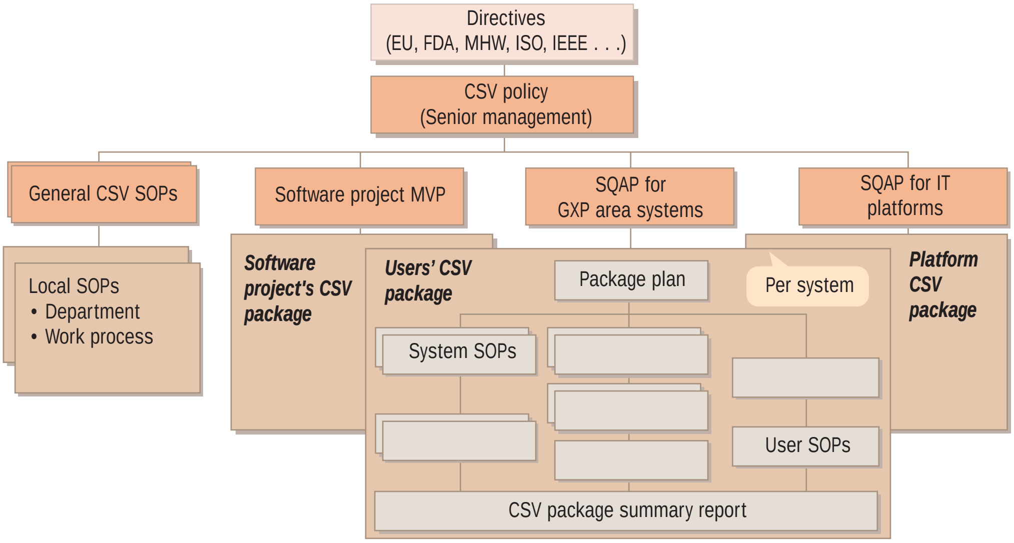


Figure 1. The policy framework for users' CSV documents. Senior management uses the CSV policy to translate regulatory directives and external standards into the local corporate culture and to establish the company's standard approach to CSV documentation.

business activities of regulated work processes just as GCP, GLP, and GMP process validation have been integrated into regulated business areas. As shown in Figure 1, senior management uses the CSV policy to translate regulatory directives and external standards into the local corporate culture and to establish a standard approach to CSV documentation across the organization for software development projects, user applications, and platform infrastructure systems.

QA further supports the policy team by helping to write general standard operating procedures (SOPs) for performing CSV work consistently across the organization. Such SOPs reduce redundant efforts per system and make it easier to train system teams how to keep their computerized process in compliance. Some basic topics for general SOPs include

- CSV package development, package team roles and responsibilities, and documentation standards.
- formal testing practices, types of testing, and testing documentation.
- system change control practices and ongoing testing.
- management's role—the business decision group and area systems QA plan.
- audit and inspection response for computerized systems.

QA and systems QA plans

In each GXP-regulated (GCP/GLP/GMP/e-records) area, the local QA organization should participate on the team of area managers that develops a business strategy for addressing compliance to the CSV policy for systems in their area. The systems QA plan (SQAP) is the document used by functional line managers to apply the CSV policy directives to area systems in a way that is integrated into local business and system knowledge.[1] For example, the clinical research area is subject to GCP system compliance and must harmonize its CSV resources across the departments of clinical data management and biostatistics, and with the system in pharmacovigilance for data management and reporting of serious adverse events.

The SQAP for GCP systems also has to consider the CSV implications for its various external suppliers of GCP data, such as investigator sites, CROs, central laboratories, and subjects' electronic diaries. Since clinical studies are usually conducted on a global basis, the harmonization and CSV control of worldwide applications, databases, platforms, and network communications broaden the scope of the SQAP considerations. Management control and the mandate of "due diligence" for the accuracy of GCP data in this new century have moved beyond people and paper to the electronic process itself. Clinical QA's support of management in developing and administering a SQAP for GCP systems is the most direct way to address business control of electronic process quality and achieve documented evidence of management's due diligence for audits and inspections.

QA as trainers

Corporate and area QA professionals are a logical choice for instructing system users and CSV package teams about the content of the CSV policy, general CSV SOPs, and the regulations related to the specific system area and type of technology being used (such as electronic signatures). A well-trained organization will be able to conduct CSV work more efficiently. When users understand the reasons and methods

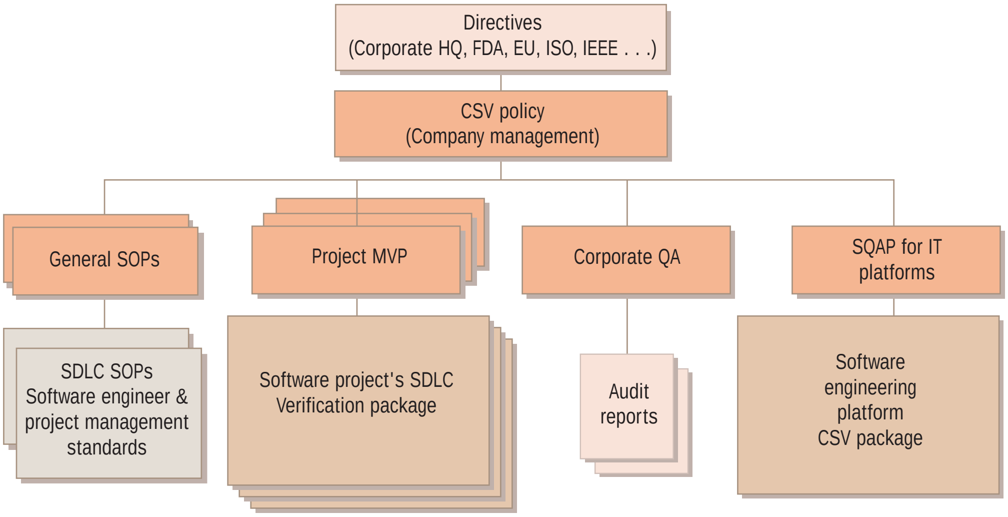


Figure 2. The software supplier's quality management system. A team that audits a software supplier can use the ANSI/ISO/ASQ quality standard (Q9000-3-1997) as a guide when examining this system.

behind CSV work—as explained in the CSV policy and general CSV SOPs—they will be able to better understand its benefits and fulfill their role in keeping a GCP system in compliance throughout its whole life cycle.[2]

This same knowledge helps IT/IS organizations better organize their approach to regulated platforms and ongoing preparation for audits and inspections.[3] Such training can also help internal suppliers of custom programs to understand the benefits of reliability and data integrity that come with good development practices.[4] Current and new members of the QA organization itself can benefit from a program to train the trainers on the CSV policy and general CSV SOPs.

QUALITY reference documents

International Organization for Standardization, Geneva, Switzerland, www.iso.ch	
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 software	Good description of quality items for service level agreement (SLA) contracts and for quality systems in software supplier organizations. Requires independence of auditors from the product or process audited.
American Society for Quality, Milwaukie, WI, USA, www.asq.org	
ANSI/ISO/ASQ Q9000-3-1997 Quality management and quality assurance standards—Part 3: Guidelines for the application of ANSI/ISO/ASQC Q9001-1994 to the development, supply, installation and maintenance of computer software	Same good description as in ISO 9000-3, but with enhanced discussions of many points. The extra detail is very useful. Calls for independence of auditors from the product or process audited.
U.S. FDA Rockville, MD, USA, www. fda.gov	
21 CFR 820—Quality System Regulation	Directly applied to and mandatory for medical device manufacturers, but still a good regulatory view of expected components in a strong quality system. Requires independence of auditors from the product or process audited.
21 CFR 11—Electronic Records; Electronic Signatures; Final Rule	Section 11.10 gives validation concerns in brief, and Subpart C addresses electronic signatures.
Guidance for Industry—General Principles of Software Validation	In-depth discussion of validation practices for medical device software. Useful to assess regulated software applications generally. Requires independence of auditors from the product or process audited.
Guidance for Industry—Computerized Systems Used in Clinical Trials	Describes the basic computer quality principles endorsed by sites and applicable to sponsor systems as well as to CROs, central laboratories, and other end-user application systems.
The Institute of Electrical and Electronics Engineers, Inc., Piscataway, NJ, USA, www.ieee.org	
IEEE Std. 1062-1993 Recommended Practice for Software Acquisition	This international standard includes a number of useful checklists for evaluating software suppliers during the purchase process.
IEEE Std. 1028-1988 for Software Reviews and Audits	Describes a variety of audit types and the audit process and gives a standard structure for audit reports. Calls for independence of auditors from the product or process audited.

QA audits of system suppliers

When a user group is selecting a GCP software application or preparing a CSV package, QA is usually asked to perform a supplier audit. QA professionals are often concerned about their ability to audit computer technology vendors, because their background is not in computers. It is important for them to remember that they are going to examine the supplier's quality management system, so their audit team should include an IT/IS representative to look at the technology practices and a user group representative to discuss the product's fit with the group's work process. QA should not be expected to carry the full audit burden alone.

Figure 2 shows a view of the supplier's quality management system with key items to examine during the audit. QA auditors can use the ANSI/ISO/ASQ quality standard (Q9000-3-1997) as a guide for specific concerns. In general, however, auditors are advised to look for

- a corporate policy on building quality into software to meet the needs of regulated clients.
- general SOPs for customer support, disaster recovery with escrow protection, and producing user training materials.
- a standard approach to producing a package of quality documentation during the software development life cycle (SDLC).
- standard practices for documenting software engineering activities.
- an independent QA structure within the supplier's organization.
- logs for internal audit reports performed by the supplier's QA group.
- documented control (configuration management) of the platform system and software tools used during product development.

QA professionals can study and use several industry and regulatory standards to develop more specific points for auditing a computer technology supplier either internal or external to the auditor's organization (see Quality Reference Documents box).

Any supplier to the pharmaceutical industry should know that regulations such as good clinical practice (GCP) and 21 CFR 11 for electronic records and electronic signatures apply to computerized systems. The supplier should be able to discuss how the company has applied the principles of these regulations to its product design and development.

The description of the software supplier's CSV package in part 3 of this series can be used as another guide to the type of documented evidence that should be in place for a software supplier.[4] Often, the key challenge for QA auditors is to find the same level of compliance in their own company's internal software organization as they see at external suppliers. The standards of performance should be the same for internal groups developing software for regulated environments. When it comes to GCP compliance, internally developed software has to be audited to just

QA Audit Questions

The QA audit of any CSV package should include at least the following questions:

□ **How do this system and this CSV package fit into the organization's strategy for GCP compliance?** The validation plan should state its relationship to the CSV policy, general CSV SOPs, local systems QA plan, and GCP regulations. Any team member should also be able to articulate this message.

□ **What is the content of the CSV package and how does each item relate to the GCP quality of the computerized system?** The validation task list should match policy and SOP requirements for a CSV package of its type—application user, platform system, or software development. Each item should address one or more of the following—management control of the system, system reliability, protection of data integrity during electronic handling, and/or auditability of the system.

□ **Have all the tasks in the validation plan and the test plan been completed according to their planned status for the day of the audit? If not, why not?** When package teams are not given sufficient time and resources to perform needed work, it is important that QA provides an independent audit view of the situation so that management can decide to accept a delayed go-live of the system or add more resources to finish on time. The degree to which test cases and test script documentation have been prepared under an approved test plan is a good indicator of a team's progress to plan.

□ **What is the testing strategy for this system at start-up and ongoing? How well do test cases and test scripts address the real work process using the system? How do they relate to the system requirements?** The test plan should give a coherent description of how the system is to be tested. It should include a traceability matrix between the system requirements, the test case descriptions, and the test scripts used for system testing. Both normal and problem data and system stress situations should be included in testing. The "rule of three" should be applied to show consistent performance across three examples of system use. There should be a test script document for every test described in the test case description. When automated testing tools are used, reports should be generated to show how the system was tested and how the tests are traced back to system requirements.

□ **Where is the system description? How are changes to the system being documented? How are problems with the system being reported, addressed, and recorded?** The configuration management log binder should have documents and forms to answer these questions.

□ **What happened during testing and during the whole CSV effort? How does the team support its final conclusion about the GCP status of the system?** At the final audit of the package, there should be a summary report for every plan in the CSV package. A summary report should identify its related plan and describe the strategy of the activities performed, the size and scope of the effort, the problems encountered and their resolution, any deviations from the related plan, the results of the effort, and a judgment made on the quality of the outcome with a recommendation to management for approval or other action with the system.

□ **What plans does the team have for disaster recovery of the computerized system? Have they been exercised?** If an external disaster recovery service is to be used, there should be a record confirming the continued existence of this supplier and of its preparedness to support the system. The user requirements for disaster recovery should be documented to include the user procedure for checking the data integrity and data management operations of the system once recovered.

as high a quality standard as software from external sources.

QA audits of CSV package teams

When a user group is validating a major system, it is helpful for QA to audit the CSV package twice. Because large project CSV packages usually take 12–14 weeks to complete, the first audit should occur at 6–7 weeks—or halfway through the package process. The focus of this midway audit is to ensure that the validation plan, test plan, and general approach of the package team are sufficiently rigorous to meet policy, SOP, and regulatory requirements. This first audit also provides a checkpoint for the team to prepare its best effort, see how it is performing to project schedules, and identify any major issues or concerns arising that could prevent compliance or delay the go-live schedule of the system. QA's audit report to the system sponsor then becomes a midstream assessment of the efficiency and effectiveness of the system team's CSV package effort.

The second QA audit of the CSV package should be performed at the end, just after the CSV package summary report has been written and before it goes to the system sponsor for approval. This last audit should be used to provide the CSV package team with a practice "inspection" response experience. It is the team's opportunity to present and defend its package and it is QA's opportunity to make a serious assessment of the system's ability to pass regulatory inspection. It is also a good time to make any suggestions for improvement needed to ensure that ongoing change control, user support, and supplier service level agreement (SLA) practices are in place to keep the system compliant during its use in the work process. The system sponsor receives an unbiased evaluation of the inspection-readiness of the package and the system, and the audit report becomes QA's contribution to the CSV package.

Depending on the size and scope of the platform system and the experience of the CSV package team, QA may conduct one or two audits of the IT/IS platform CSV package. When multiple GCP applications are being put on the same server platform configuration, common sense dictates a full CSV package for the first application with QA audits—then minor efforts to address any changes for the rest. The QA involvement is also reduced in proportion to a change control audit. The QA Audit Questions box lists some basic questions and expected responses for any CSV package.

An excellent description of the audit process can be found in section 8 of the IEEE standard 1028-1988 for Software Reviews and Audits (see Quality Reference Documents box). That standard explains how to plan, prepare, conduct, and report an audit (key points are shown in the CSV Audit Report box).

CSV Audit Report[a]

□ **Audit identification.** Report title, audited organization, auditing organization, date of audit.

□ **Scope.** Scope of the audit including types of items audited, standards used, auditing practices, and metrics for decisions.

□ **Conclusions.** A summary and interpretation of the audit findings including the key items of nonconformance. This is an executive summary of the "bottom line" for the audit.

□ **Synopsis.** A listing of all the audited elements and their associated findings. This can be concisely done using a table format.

□ **Follow-up.** The type and timing of audit follow-up activities—for example, expected written responses or further audits.

Additionally, when applicable, recommendations can be reported to the audited organization or the group that initiated the audit. *Recommendations are reported separately from results.*

[a] *Based on IEEE Std. 1028-1988 for Software Reviews and Audits*

Inspection Checklist

"Dos" for QA audits

□ Check CSV packages for match of package summary report to tasks in validation plan.

□ Review test plans and test summary reports.

□ Check backup tapes, system logs, training records, SOPs.

□ Check sponsor's control of system for ongoing GXP use.

□ Train teams with internal audits of CSV packages.

"Don'ts" for package teams

□ Do not meet inspectors unless QA is present.

□ Do not re-create missing documents, lie, or argue issues with inspectors.

□ Do not volunteer "war stories" about fixing the system.

□ Share only the log of prior audits.

□ Do not give system access to auditors or inspectors.

QA hosts regulatory inspections

Corporate QA in a GCP-regulated company or service provider usually has a standard procedure for hosting a regulatory inspection—it should be followed for computer audits and inspections as well (see Figure 3).

QA manages the logistics of the inspectors' workspace, interview schedule, and documentation review. The inspection visit starts with the QA host asking participants to complete the form for an audit/inspection log (reference the audit log example) and notifying the respective user and platform CSV package teams.

Team presents CSV package. The CSV package team then presents its documented evidence for the quality of the GCP system to the inspectors and answers any queries about the system.

Inspectors query CSV package. The inspectors review the package and write an inspection report.

Sponsor receives inspection report. For U.S. FDA inspectors, the visit report is on a Form 483 that is presented to management (system sponsor) at an exit meeting. The regulatory authority expects a written response to any critical issues raised in the inspectors' report.

Sponsor responds to inspection report. It is usually the QA host who tracks down answers to inspection concerns and writes a formal response.

Every audit report with findings should have a written response. For internal QA audit reports with findings, the system team responds in writing to QA and the system sponsor. For inspections, the QA host collects responses from participants and prepares a written report for the company to send to the authority. When QA audits a supplier, it should request a written response to critical findings from the supplier's organization through its QA department. Follow-up audits and inspections may then check on how the replies have been implemented.

The Inspection Checklist box shows some general guidelines for QA auditors and package teams having an inspection. The inspector sees only what you have documented. Remember that you get credit only for those quality practices for which you can present documented evidence that supports their existence. As noted in the list, auditors can use internal package audits as training to prepare package teams to present and defend their documented evidence during an inspection. The package team also must protect system security and recognize that auditors and inspectors are not authorized to use a GCP system. An auditor or inspector who asks to see database material can watch an authorized user query the database and make a printout.

If the inspector and the package team have a difference of opinion about the system, it is very important to avoid arguing with the inspector. A polite statement of the package approach and an expression of willingness to consider the new information are

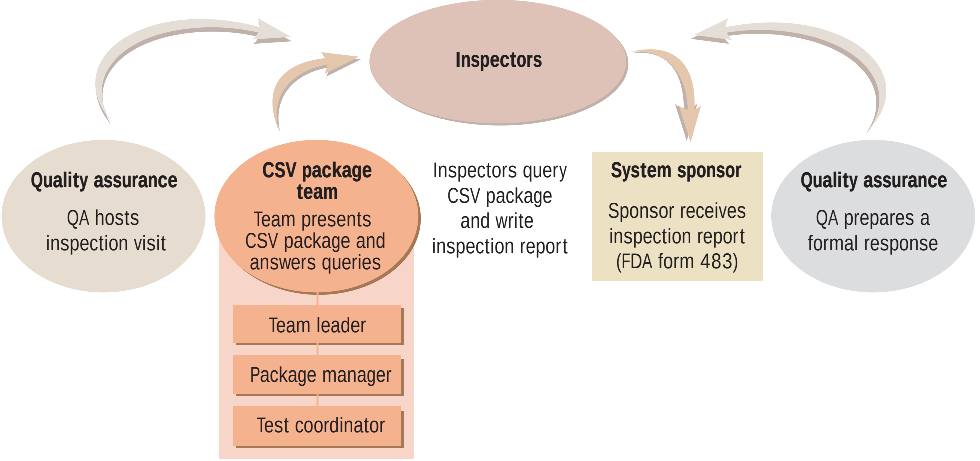

Inspectors
Quality assurance
QA hosts inspection visit
CSV package team
Team presents CSV package and answers queries
Team leader
Package manager
Test coordinator
Inspectors query CSV package and write inspection report
System sponsor
Sponsor receives inspection report (FDA form 483)
Quality assurance
QA prepares a formal response

Figure 3. An inspection response model. The QA team hosts the inspection visit and prepares the formal response to the findings.

Audit and Inspection Log

Date of audit/inspection:

This is an audit (yes/no) ________ or an inspection (yes/no) ________.

Reason for audit/inspection:

Company initiated (yes/no): ________ Authority initiated (yes/no): ________

Internal QA (yes/no): ________ Pre-approval (yes/no): ________

Follow-up to prior audit (yes/no): ________ For cause (yes/no): ________

Other (specify):

Name(s) & organization(s) of audit/inspection team: Signature(s) and date:

Site host for audit/inspection:
(Name/title)

(Signature) ______________________________________ Date: ___________

Summary report in company confidential file (yes/no): ________

Document ID for initial report: ________________

Document ID for follow-up report: ________________

Interviewee name & title	**Signature**	**Date**

Audit and Inspection Log (cont'd)

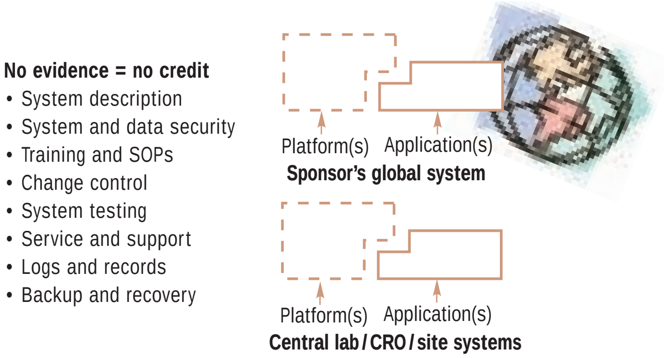
Documents copied for reference of auditor/inspector

sufficient. ("This has been our approach, but we are always looking to improve it.")

Although it is not permissible to re-create a missing document, a clearly labeled "history" of the system is allowable, and can document known experiences by a person in a position to witness such experiences. The author should sign and date it as a current history document and provide credentials that indicate the author is a relevant and credible witness to the information it contains.

Quality control of the CSV package

A quality professional who participates on a CSV package team can make a valuable quality control contribution by examining documents as they are produced to ensure the audit- and inspection-readiness of the package as it is being developed. When a quality professional is not available to make a QC check of the package, it is the package manager who performs the quality control role for all documentation as it is prepared.



No evidence = no credit

- System description
- System and data security
- Training and SOPs
- Change control
- System testing
- Service and support
- Logs and records
- Backup and recovery

Figure 4. Audit and inspection topics of interest. Any computerized system handling GCP data requires these areas.

The quality professional working as QC on one system CSV package can be QA auditor for a different system's CSV package in the same company or can be QA auditor at any supplier site. This concept of independence from auditing one's own work is described in many regulatory and standards documents and must be followed for CSV work (see Quality Reference Documents).

For global systems used by multiple sites, it is important to include the local QA organization as site QC on the extended package team to ensure that system-related SOPs, test cases, and test scripts appropriately reflect regulatory requirements and work processes at its site. The SOPs, work instructions, and other documented evidence for inspection topics noted in Figure 4 can have variations depending on location and the way user groups at that site operate the system in their work process.

For computerized systems used in clinical trials, auditors and inspectors can look at systems used in sponsor sites and external suppliers to the trial such as laboratories, CROs, and investigator sites. As the conduct of clinical trials has become more technology-intensive, the concern for auditable quality of electronic data has produced more regulatory guidance. Figure 4 identifies the areas for which documented evidence is needed at any location using a computerized system to handle GCP data. The FDA has stated its basic concern for auditable system quality this way: "Persons using the data from computerized systems should have confidence that the data are no less reliable than data in paper form."[5]

QA success in validation

The first computer validation goal of the QA role is to ensure the quality of electronic data, records, and systems related to the safety, efficacy, and quality of work processes and regulated products. The second goal is to pass audits and inspections on the first visit. The CSV activities for quality professionals described in this article are designed to achieve both goals.

The four parts of this series can be read as a suite of material that fits together as a practical view of CSV work. The material in this series is based on more than 10 years of hands-on consulting experience with CSV projects large and small in sponsor firms and supplier organizations around the world. The practices in this series have focused on GCP, but are equally applicable to and have been used for GLP, GMP, and e-records projects as well as by technology and service suppliers to such projects.

As discussed in part 6 of the 1996–1997 series of articles on computer validation audits and inspections, good CSV work is all about taking pride in your system and its ability to support your work process. Passing audits and inspections is just a by-product of that pride in system perfor-

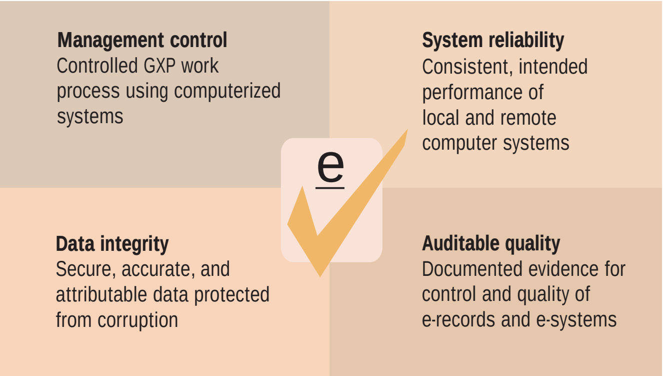

Management control
Controlled GXP work process using computerized systems
System reliability
Consistent, intended performance of local and remote computer systems
e
Data integrity
Secure, accurate, and attributable data protected from corruption
Auditable quality
Documented evidence for control and quality of e-records and e-systems

Figure 5. Auditor and inspector goals for GXP systems.

mance.[6] The auditor/inspector goals shown in Figure 5 are also good business goals for the QA department, for senior management, and for the CSV policy.

References

1. Teri Stokes, "Computer Systems Validation, Part 4: Operating GCP Systems at Investigator Sites," Applied Clinical Trials, April 1997, 54–60 (available at www.pharmaportal.com/articles/ stokes.cfm).
2. Teri Stokes, "Validating Computer Systems, Part 1: A GCP Computer System Is a Lifetime Responsibility," Applied Clinical Trials, August 2000, 38–43 (available at www.pharmaportal.com/articles/).
3. Teri Stokes, "Validating Computer Systems, Part 2: GCP Validation of Platform and Infrastructure Systems," Applied Clinical Trials, September 2000, 55–66 (available at www.pharmaportal.com/articles/).
4. Teri Stokes, "Validating Computer Systems, Part 3: GCP Software Verification," Applied Clinical Trials, November 2000, 48–58 (available at www.pharmaportal.com/articles/).
5. Food and Drug Administration, Guidance for Industry: Computerized Systems Used in Clinical Trials (FDA, Rockville, MD, April 1999).
6. Teri Stokes, "Computer Systems Validation, Part 6: A Survive and Thrive Approach to Audits and Inspections," Applied Clinical Trials, August 1997, 40–44 (available at www.pharmaportal.com/articles/stokes.cfm).

Teri Stokes, *PhD, is senior consultant and director of GXP International, 131 Sudbury Road, Concord, MA 01742, (978) 287-4393, fax (978) 369-5620.*