Regulatory authorities require life cycle management for GCP systems both during the systems' development (referred to as the software development life cycle, or SDLC) and for the rest of their existence through to retirement and replacement. The initial validation plan prepared by users for user acceptance of a new GCP system must include provisions for the “care and feeding” of a validated system for the rest of its life—after startup through to retirement. The computerized system validation (CSV) package developed at system launch must also establish the ongoing validation environment to keep the system “fit” and performing as expected over the years it is being used. Such long-term planning requires the involvement of management to ensure a supply of user resources to support the system over time.

This first of a series of articles on the subject of system validation discusses the user’s role in the process. Later articles describe the roles of the software supplier and of the system installers.

Anatomy of a GCP system
In the 1980s, the computer validation committee of the Pharmaceutical Manufacturers Association produced a diagram to help define terms for validation work.\(^1\) Figure 1 shows an updated view of that classic drawing using an adverse event (AE) system as an example. In this view, a computer system is composed of hardware and software, and a work process is composed of people, standard operating procedures (SOPs), and often equipment or instrumentation.

When a computer system is used to support a work process, the two together become a computerized system—in the example, a serious AE management system. The computerized system performs in an operating environment such as pharmacovigilance (in the example) or

**Figure 1.** An example of the configuration of a system designed for serious adverse event management.
product safety. To make user acceptance validation work practical, however, it is necessary to add to the basic diagram two new concepts. The software that performs in the work process and that users see and “touch” with a keyboard, mouse, or bar code wand is the software application system. Everything else that is required for the software application to perform as expected is part of the platform system. The platform system includes the hardware, operating systems, databases, query and other software tools, and network communications for server and desktop configurations that supply the infrastructure support to the regulated application.

The software application cannot function without its platform system support and users cannot reach the software application without desktop or handheld systems and network communications. One platform system can, however, support more than one software application system if it is large enough and the infrastructure requirements are the same for both applications.

Creation of validation packages

Figure 2 shows the full life cycle of a regulated software application and its platform system. As shown in the figure, there are three separate CSV packages to be prepared at the startup of a new computerized GCP system: the performance qualification (PQ) package, the installation qualification (IQ) package, and the operational qualification (OQ) package.

Software application: The PQ package. Preparation of the performance qualification pack-age for the software application system is the responsibility of the user acceptance team. This process focuses on how the application performs in its operating environment. It consists of a package of documented evidence that “paper trains” your system to behave itself in the work process. Regulatory authorities hold users responsible for GCP validation of both the application and its platform. Because a user team is seldom equipped to address platform issues, the users normally depend on subcontracting development of the platform CSV package to the information technology/information systems (IT/IS) department. An internal or external service level agreement (SLA) is then used to define roles and responsibilities for the startup validation support and the ongoing service and success of the system over time.

Platform system: The IQ package. The installation qualification package for the platform system includes startup testing, backup, recovery, contingency planning, SOPs, change control, maintenance, configuration management, and ongoing services. This platform CSV package process is like preparing the yard so your pet dog can play in safety and comfort (invisible fencing, dog house, water dish); it is the subject of Part 2 in this series.

This formal division of validation labor allows the respective teams to focus on what they know best. An IT/IS team cannot know the work process as well as the user team and thus cannot conduct performance testing that fully exercises the application in the same way users can. It is also important that real users have the chance to work with the system to prepare their working materials (SOPs, work instructions, guidelines) and fine-tune their work process to the idiosyncrasies of the system and vice versa before the application goes live. Software problems arising during user acceptance testing can then be resolved without interrupting GCP operations, which can lead to a troublefree launch of the system.

Figure 3 illustrates the division of labor between the user acceptance team and the platform package team.

Software supplier testing: The OQ package. Yet a third team involved in the startup of a new software application system is that of the software supplier and/or configuration provider, who perform the operational qualification of the system. Regulatory authorities also hold the users responsible for the quality of work and testing performed by this third team, whether the team is internal or external to the user’s organization. Thus, the “pedigree” of your GCP system must be as well documented as the kennel registration of your purebred pet, including what kind of “shots” (testing) it has had to ensure good health and immunity to known diseases.
Management’s role in lifetime system validation

Buying a purebred pet requires taking on daily responsibility for the animal during its lifetime, and purchasing a strategic GCP system requires a similar level of care and attention. For management to be in control of a computerized work process, the organization must be set up to support lifetime validation for a regulated system. Figure 3 shows how a sponsor or CRO can be organized to support lifetime validation for strategic GCP systems.

The business decision group, senior management—such as the director of clinical research and the directors for clinical data management, biostatistics, pharmacovigilance, and clinical quality assurance—has ultimate regulatory responsibility for GCP data in the clinical trial work process. This group of managers forms the logical composition for a business decision group (BDG) to plan and provide resources for compliance efforts for strategic GCP systems.

The BDG addresses broad issues, such as: Can we add another country of users to the system? Should we add another application to the same server or get a new server? How many users can we send to the supplier’s user training this quarter? Which work process gets the next upgrade to its computerized system? When do we retire this system, and do we upgrade with the current supplier or move to a new vendor or new technology at retirement? How much do we redesign our work process to fit the system? Who is responsible for keeping the system in a validated state?

The system sponsor is the senior manager responsible for a particular computerized work process such as clinical data management or pharmacovigilance. The system sponsor carries the local responsibility for funding and approving the validation effort of computerized systems in that work process.

The system sponsor addresses such issues as: Who will I appoint as system owner to lead a CSV package team? How can I locate others to help the three key package team members with regular tasks so that they have time to develop the startup CSV package on time? How do I budget and gauge their ongoing duties for training new users, troubleshooting, and keeping the system validated after the system goes live and they return to their full-time jobs?

The system owner is usually the key user in the operating environment who is held responsible for having the system available for users in the computerized work process. This person assigns a package manager who drives the documentation process and a test coordinator who manages the testing activities. The system owner leads this core team in developing and maintaining the CSV package. Other users are included in an ad hoc capacity as testers and witnesses, and specialty resources may be added as necessary to provide specific expertise.

The quality assurance role stays outside of the package development process to be able to audit the CSV package. QA audits of the CSV package midway and at the end of development give the team and the BDG an independent view of the ability of the package to pass compliance inspections.

The user acceptance CSV package

Once the need for a new GCP system has been established, the needs analysis document itself starts the application life cycle and becomes the first document in a users’ CSV package. The request for proposal (RFP) becomes the second document in the package. When a system is chosen, it is time to identify the package team and write a validation plan. The Institute for Electrical and Electronics Engineers, Inc. (IEEE) gives a document outline and explanation of expected content for a validation plan in its standard 1012-1986.2.

The user acceptance package for computerized system validation is designed by the validation plan to provide documented evidence for:

- management control of the system, its users, and its regulated data.
- reliability of the system to perform as intended every time.
- protection of data integrity...
The validation plan developed by a user acceptance team includes more than just testing. The boxes on the left side of Figure 5 focus on control of the physical and logical environment for the application and the two boxes on the right address control of user interaction and the human interface to the system. Each of these items is discussed briefly below in order of appearance in the figure.

**Control of physical/logical environment**

Application administration SOPs. Descriptions of user types and their privileges on the system, procedures for system administration, backup and restore activities.

Application configuration management logs. A logbook binder used on an ongoing basis to keep a current description of the application, its backup log, maintenance records, support actions, change control decisions and actions taken, ongoing testing, problem tracking, release notes, supplier correspondence, the service level agreement (see below) with the platform supplier and/or with the application provider, record of user training events, and list of authorized users.

Change control log. A change control SOP for the system and monthly change control reports for system changes made by user, platform, and/or supplier actions. Report should include the extent of repeat testing performed and/or updates made to relevant CSV package items.

QA audit log. A record of any QA audits performed on the CSV package itself or on behalf of the CSV package, such as QA audits of suppliers.

Supplier reports. This log includes any walkthrough reports developed by the users when reviewing the platform CSV package or other supplier activities. It also includes follow-up reports on supplier milestone performance under service level agreements.

BDG minutes. The business decision group, consisting of line managers responsible for the operating environment and its computerized work processes, documents its financial, operational, and resource decisions about the regulated system in meeting minutes that are a part of the system’s CSV package.

**Control of user interaction**

Needs analysis. The initial document examining the work process and describing the type of computerization it might benefit from.

Request for proposal (RFP). A formal document sent to prospective suppliers describing the work process needs and requesting a response from vendors showing how they could meet those needs with their products and/or services.

Test plan(s) start-up & ongoing

Test cases, scripts, data & results logs

Test summary report & updates

Needs analysis, RFP, contract, URS, SLAs

User manuals, CVs & training records, dept. SOPs, problem/help logs

Users’ CSV package summary report

Figure 5. A standard user acceptance CSV package, prepared and maintained by a user department’s team.

Contract. A legal document describing the roles, responsibilities, and financial elements in the business relationship (purchase, lease, rental) between system users and external suppliers of systems or services.

User requirements specification (URS). A formal, approved document describing the users’ needs for a computerized system from a work process perspective, such as the types of data to be handled, the flow of data across the work process, data inputs and outputs to the work process, size and location of user groups, types of user roles, and access privileges needed.

Service/success level agreements (SLAs). Formal, approved documents between system user BDGs and internal or external suppliers to describe roles and responsibilities on both sides for keeping the regulated system in successful operation and continually validated.

User manuals. Printed materials from system suppliers instructing users how to work with the regulated system.

CVs and training records. Curriculum vitae showing the users’ educational backgrounds and work experience that indicate competence to perform in the work process, and training records showing formal and on-the-job training given to ensure that a user is qualified to use a regulated system in the work process.

Department SOPs. Department standard operating procedures, guidelines, and/or work instructions that are specific for using the computerized system in the GCP work process.

Problem/help logs. Logbook binder to record user problems as they arise and their resolution as they are settled. A standard incident report form might be used to facilitate this recording. Department should have work instructions for how to report problems and where to go to get help with the system. Records describing problems and resolution should be reviewed monthly for trends and training issues.
Figure 6. The ongoing test plan illustrates management control through to retirement.
Change Control Test Summary Report

- Test summary report identifier. Unique ID traceable to associated ongoing test plan.
- Summary. Describes change(s) being tested. Describes items tested (application version), test environment (platform system), and test approach (test cases used).
- Variations. States any deviations from test case or test scripts and reasons for deviations.
- Comprehensive assessment. Discusses assumptions and limits to scope of testing. Were scope of testing and results obtained sufficient to assess system reliability for change(s) made? Discuss reasons for limits chosen.
- Summary of results. Gives table of testing results per test case. Table of anomalies and their resolutions. List of outstanding issues and risks (unresolved anomalies).
- Evaluation. Pass/fail conclusion based on test results and criteria in the ongoing test plan.
- Summary of activities. Describes tester/witness staffing, testing location(s), and test documentation preparation and approval process.
- Approvals. Names, titles, signatures, dates with meaning of signatures.
- Appendix. Table of contents list for test documentation produced.

dated requires keeping all of its relevant documentation up-to-date as the system is tuned to a changing work process or a problem is resolved, or when a supplier provides a new feature. User training and user instructions in manuals and SOPs may have to be adjusted to ensure proper use of the system. Management needs to be kept informed of trends in changes and the scope of changes over time.

System change requires repeat testing to some extent determined by the ongoing test plan, and all formal testing documentation must be kept for audit purposes. The reuse of startup test scripts provides a degree of “regression testing” that checks for consistent results with prior findings. Some startup test scripts can also be used for training new users on the system. Such training test experience can also be used for periodic checks of the system, and so should be kept and recorded for “double credit” whenever possible.

Test summary report. When any formal testing is performed, a test summary report must be prepared to give management a review and analysis of the experience and assessment of the testing’s impact on the validation status of the system tested. A pile of test result logs remains just a pile of paper until a responsible person who understands what the testing means has analyzed it and reported the conclusions. A good test summary report includes the points outlined in the Change Control Test box (adapted from the IEEE Standard for Software Test Documentation).

As Figure 7 shows, many changes can occur with a GCP system after startup. The longest part of a successful system’s lifetime is during its operational phase in the work process.

The user team continues to focus on the GCP software application system by training new users, resolving issues and problems with the system, and keeping the configuration management logbook binder up-to-date with system activities. The user team also managers the SLA.

GCP system, and management should provide the strategic focus and ongoing resources needed to achieve the goal of expected performance with lifetime system validation for its essential GCP systems.

References

Teri Stokes, PhD, is senior consultant and director of GXP International, 131 Sudbury Road, Concord, MA 01742, (978) 287-4393, fax (978) 369-5620, gxpintl@ma.ultranet.com.
Part 1 in this series discussed the user acceptance validation of application software as a lifetime responsibility to ensure its ability to perform as intended in a good clinical practice work process. The metaphor of buying a dog was used to compare the ongoing responsibilities for keeping a family pet healthy and fit to the need to provide ongoing care to keep a computerized GCP system fit during its lifetime.

Part 2 now addresses the other half of the system operation story that is often hidden from the users’ view. Like the tip of an iceberg, however, multiuser and global GCP applications sit atop a huge, unseen, but necessary, mass of support. Below the application software tip is the rest of the system “iceberg”—a collection of server, desktop, and peripheral hardware, operating systems, database engines, query/reporting tools, and the communications networks needed so the application will work as intended. These components make up the platform and infrastructure systems usually supplied to users by the information technology/information systems (IT/IS) department.

Often the phrase “Out of sight, out of mind” can be used to describe the typical validation focus for such platform and infrastructure systems. To meet regulatory requirements, however, what is needed is a focus for computer validation in the IT/IS department that documents the health and fitness of the platform systems and network infrastructure for the way they are used to support GCP applications.

**Platform system life cycle**
The life of a platform system begins when the user group decides to purchase a particular application software to perform a certain set of GCP work process tasks—clinical data management, adverse event reporting, electronic subject diaries, statistical analysis, Web-based clinical data entry. For major applications, an IT/IS person often consults with the user team to provide technical expertise in the purchase process. This person also advises about how well the technical requirements of the application software candidates fit into the current IT/IS setting and whether any new platform/infrastructure components will need to be purchased to handle a particular application.

Figure 1 shows the traditional life cycle for application software with a division between the steps performed by the user group purchasing the software (1,2,6–9) and the steps performed by the supplier that develops the application software (3–5). The life cycle of the platform system is also shown in Figure 1, operating in support of the user group during steps...

**Figure 1.** The platform system life cycle in detail, and how it fits with the rest of the application development cycle.
The life cycle of the platform system requires that the IT/IS platform team configure, install, test, operate, maintain, and—eventually—retire the system. Details of each stage follow.

Configuration. The IT/IS platform team must first define the hardware, software, and network components to be assembled for server and desktop systems to be used for access to and operation of the application. Platform configuration must meet the specifications of the application software supplier, the platform component suppliers, the user group’s work process, and the IT/IS department’s work process.

Installation. The team assembles and installs all platform components according to relevant manufacturers’ specifications.

Testing. Team members perform an installation qualification (IQ) test to ensure that the many components work properly as a platform system unit. They install the GCP application and ensure that platform functions are accessible to the application—for example, that the desktop can reach both the database engine and the printer to produce a report.

Operation. The IT/IS platform team then performs ongoing operations using standard operating procedures (SOPs) to meet the user group GCP needs stated in a service level agreement (SLA)—for example, nightly or weekly backups, security checks, system administration, disaster recovery, support for new user groups. The team performs periodic testing of the platform for ongoing quality control.

Maintenance. The IT/IS platform team is responsible for installing patches and upgrades from the application supplier. Team members service, repair, replace, and install new components to the platform system as needed over time. They perform problem resolution, maintenance, and repeat testing, as dictated by a documented change control SOP.

Retirement. When the time comes, the IT/IS platform team will plan and execute the orderly decommissioning of the platform and its infrastructure components—in part or as a whole—when new technology decisions are made for the application itself or for platform support.

Platform system CSV package

The first regulated application installed on a new or existing platform system automatically makes the entire platform subject to regulatory inspection, even though the rest of the applications on that platform are not regulated. Thus, it is smart for an IT/IS department

The documentation required for a platform system CSV package also helps the IT/IS department to be organized in its operations.
to plan its platform environments with a realistic strategy for establishing and maintaining a documented approach to system operations. Grouping several GCP applications on the same platform system configuration can minimize IT/IS work by requiring only one computerized system validation (CSV) package for the common platform.

In many ways, the documentation required for a platform system CSV package also helps the IT/IS department to be organized in its operations. The CSV package makes it possible for new hires and backup operators to work with the system and to take a knowledgeable approach to resolving issues that arise.

The platform CSV package is very similar in content to the users’ CSV package outlined in Part 1, but reflects the particular responsibilities of the platform package team. The IT/IS platform package needs to reflect the work process in the data center and infrastructure support functions. It also needs to have a practical approach that eliminates redundant work and allows for a response to multiple applications and user support for all regulated applications—GCP, GLP (good laboratory practice), GMP (good manufacturing practice), Rule 11—collectively referred to as GXP. Goals for the platform CSV package are the same as for user acceptance. The platform system must have documented evidence to show that it is under IT/IS management’s control, that it operates reliably, that its database engines and communications networks protect the integrity of GXP data being handled, and that documentation is in good order for audit purposes.

Validation plan
The Institute for Electrical and Electronics Engineers, Inc. (IEEE) publishes a standard for software verification and validation plans that can easily be adapted to the purpose of writing a platform system validation plan (see Platform Validation Plan Outline box).1

Every plan in the CSV package—validation plan, startup test plan, disaster recovery plan—must have a defined task list stating just what actions are to be taken to execute the plan’s strategy. Figure 2 and the Platform CSV Package give an itemized description of each component of the package to be addressed by the validation plan.

Every plan must have its own summary report written to explain to management the outcome of the planned tasks. The package summary report includes the outcome of individual tasks as well as the highlights of summary reports from subordinate plans. The Platform Package Summary Report box shows an outline for such a summary report.

A collaborative effort
The GCP application software cannot function without its plat-
Platform CSV Package

- **Validation plan.** Document describing the purpose, scope, approach, resources, and schedule of intended validation activities. It identifies the CSV package items: the tasks, roles, responsibilities, and schedule for developing package items; and the standards, methods, and procedures used to quality assure a computerized system throughout all phases of its life cycle (Figure 2).
- **Configuration management (CM) log.** First section in a CM logbook binder that contains a written description of the platform system configuration in text and in diagrams. Section includes a list of all major components of the platform with relevant identifiers, such as server identifiers, associated disks, software versions, overall network topology.
- **System manuals.** Supplier documentation for major components of the platform such as server hardware, operating system, database engine, network management.
- **System SOPs.** System administration standard procedures and/or department work instructions for operating the platform, performing backups, providing security.
- **Disaster plan.** Document describing exactly how the platform system can be reconstructed in case of its destruction by fire, flood, theft, or other catastrophe.
- **Change control log.** Section of CM logbook binder where records are made for the approval, implementation, and repeat testing of changes to the platform system. It is expected that IT/IS has a department level change control SOP and that records in this log conform to the department’s procedure.
- **Backup log.** CM log record of performing daily, weekly, monthly backups for the regulated applications on the platform system.
- **Archive log.** CM log record of off-site storage location for any backup media stored that relate to the platform system or its regulated applications.
- **Supplier records.** CM logbook binder section(s) for filing any correspondence or visit reports from component suppliers. Should also include an area for logging telephone conversations with supplier support desks.
- **Audit log.** CM logbook binder section to record date, time, and participants in any audits or inspections of the platform system by internal QA, external clients, or regulatory authorities.
- **Test plan.** Document that describes the technical and management approach to be followed for testing a system or component. Typical contents identify the items to be tested, tasks to be performed, responsibilities, schedules, and required resources for the testing activity (see IEEE standard1).
- **Startup test plan.** Document describing the strategy for testing at the time of the initial installation of a platform system.
- **Ongoing test plan.** Document describing the approach for testing performed under change control throughout the operational life of a platform system.
- **Test case.** Document specifying the details of the testing approach for a platform feature or combination of features and identifying associated test scripts, such as system power up/down, system backup/recover, server connectivity to desktops/printers/remote sites across a network.
- **Test script.** Document specifying inputs, predicted results, and a set of execution conditions for an individual test. Includes one or more step procedures that describe keystrokes or other tester actions and provide log space for recording system response to test activity.
- **Test summary report.** Document summarizing testing activities and results. It also contains an evaluation of the platform system tested.
- **Service level agreement(s) (SLAs) with user groups owning a regulated application on the platform system.** Document that describes the respective roles and responsibilities of IT/IS and the user group for successful support of the GCP application on the platform system.
- **SLA monthly reports.** Brief notes describing ongoing milestone results and important decisions/actions taken for the platform system in supporting a GCP application and its user group.
- **Security log.** Section of CM logbook binder that defines security levels for the platform system and records any incidents of security breach and their resolution.
- **Help desk log.** Record of platform system issues arising and their resolution.
- **IT/IS department SOPs.** Standard operating procedures should be defined for physical-logical security of the data center and platform systems, change control for applications and platforms, installation/operation of a regulated platform system, performing system backup procedures, actions for disaster recovery, and training of personnel.
- **Curriculum vitae (CVs).** Resumés of education and professional experience related to current work assignment.
- **Training records.** All IT/IS department personnel working on a platform system supporting GCP applications should have CVs and updated records for ongoing training relevant to their work. Training in the regulatory requirements for computerized systems is also expected.
- **CSV package summary report.** Document summarizing all CSV package activities initiated under the validation plan and the results of those activities. It also contains an evaluation of the platform system’s readiness to perform and be operated in compliance with regulatory requirements (see Platform Package Summary Report outline).
For GCP systems, the user team and the IT/IS team must work closely together for the life of the system. The need for collaboration is usually quite clear during the excitement and attention paid to the initial project for startup of a new system. But as time goes on, it is often overlooked that both teams must continue to exist and must continue to work together to operate, maintain, and fine-tune the computerized system to its GCP work process while keeping it in a validated state. Ongoing activities and updates to the CSV package items of each team must continue.

The SLA. The businesslike way to address a lifetime partnership is to develop a service level agreement (SLA) between the parties. The SLA needs to clearly describe the expectations on both sides for application and platform activities to ensure the success of the computerized system in the GCP work process and its ability to have uneventful audits and inspections. Developing the SLA is the start of a long-term partnership between the users and the platform support group. As with any lifetime partnership, it is important to be clear about roles and responsibilities, to set specific expectations with measurable milestones, and to have a problem resolution process defined and understood. Platform support can come from IT/IS departments that are internal or external to clinical research or to the company as a whole, and the SLA process is the same for any source of platform support. Figure 4 shows the partnership process.

There are many topics to consider when developing a service level agreement. Topics will vary depending on the size and complexity of the role the application plays in the GCP work process. The following items are given as examples of the types of questions to be discussed between the platform team and the user team.

The application user’s GCP work process needs. Size and scope of user population. How many users? At how many locations? Across how many time zones and countries? Likely number of concurrent users? Are users internal or external to the organization? Who approves adding new users? What is the expected expansion rate for adding new users—CRA laptops, investigator site entry systems, subject palm diaries? What types of physical-logical security are needed?

Type of user activities to be performed. How does data get into the database? Batch upload/download of data from internal/external sources, manual data entry from what locations, data acquisition from instruments? How is data retrieved from the database? Who manages the database? What kinds of reports are needed requiring what types of printers? Location of specialty printers? Is the application expected to communicate with other applications or databases? How? Diary upload to CRA laptop followed by upload to platform server? CRO SAS (statistical analysis system) tapes to platform server? Instrument data to lab server followed by upload to platform server?

IT/IS platform support process needs. Support services. What kind of system and data backup schedule is needed? When can maintenance be performed without disrupting the users’ work process? What hours will help desk response be available for user support with desktop and server issues? For what time zones? Is special technical expertise needed to support this application? How much support...
is the application supplier providing—for users and for IT/IS? What is the application supplier’s process for contacting support services?

**Support training.** Is special training needed for platform operators? How and when is training available? Can the application supplier provide backup for the IT/IS help desk? Who delivers the special training? How will installation and training for remote site users be handled?

**User and IT/IS roles and responsibilities.** *Business partnership.* Who speaks for the user group and who speaks for IT/IS on platform system issues? Who manages contact with the application supplier and for what purposes? Who approves change requests? Who pays for what? What notices will be given and to whom when application changes are made that require platform changes and vice versa? What is the problem resolution process? How are unsolved problems escalated for resolution? What are the GCP audit/inspection response roles?

**Monthly progress.** Lifetime partnership success is measured by application success each month. **SLA success milestones.** Does every SLA requirement have a measurable outcome? If the user group or IT/IS expectation cannot be measured, it is a “wish,” not a requirement, and it should be omitted from the SLA.

**IT/IS view.** How many help desk calls are handled and closed per month? Length of continuous platform server and network uptime for the application without any interruptions in work process operations? Number of printer or desktop problems reported and resolved for the application versus number of printers or desktops in use for the application? Any changes to platform system components resulting in updates to the configuration management logbook binder? Any change control and repeat testing records for the month? Any updates to the platform’s CSV package? Any new announcements from the platform component suppliers for upgrades, enhancement patches, or new versions of product coming soon that could affect the application?

**User group view.** Number of new sites or new users added per month? Number of application supplier’s fixes or updates installed and retested? Number and type (system/data/application, daily/weekly/monthly) of backups performed for the application? Any audits or inspections expected for the CSV packages? Any application training needed for system fixes and/or new hires for IT/IS or user groups? What is the training, who delivers it, and when?

As with any lifetime partnership, it is important to be clear about roles and responsibilities, to set specific expectations, and to have a problem resolution process defined.
ers it, and how is it recorded? Any new announcements from the application supplier for upgrades, enhancement patches, or new versions of product coming soon that could have an impact on the platform configuration? Any security issues arising—server, database, network?

It is important for all parties to remember that the goal of the SLA is the successful operation of the application software in the GCP work process. The ultimate measurement of SLA success is the controlled, reliable handling of GCP data in clinical research and protection of the integrity of such data throughout its processing, storage, and retrieval by the application software.

**Lightening the IT/IS load**

To make life simpler, many IT/IS departments identify one standard desktop configuration of PC and core applications to be used across the clinical research organization. This standard desktop configuration is then validated on its own in a single desktop CSV package. The CSV package for the standard desktop is then referenced across multiple application platforms with only a brief installation qualification (IQ) test performed per new application.

In similar fashion, many IT/IS departments identify standard server configurations for certain types of server technologies (HP/UNIX, for example) and database environments—such as Oracle—that are often used by regulated applications. The standard server configuration is then validated on its own in a single CSV package to support the first regulated application being used. Subsequent GCP applications going on to the same server configuration would reference the first platform CSV package and just add package updates for the specific needs of the new application. Updates might include testing new printer types, network communications to new user sites, and special data backup requirements.

For platform servers dedicated to a single application, the IT/IS CSV package is performed separately on the one platform system. The platform CSV package should be completed before the time for formal testing by the user team. A test environment is then built on the platform system in time for the user team to execute test scripts in a simulated production environment.
Management support
It is important that IT/IS management provide an organizational framework for developing CSV packages for regulated platform systems. The framework includes SOPs for how to develop a CSV package, for how to perform formal testing in a documented fashion acceptable to regulatory inspection, and for describing a standard approach to service level agreements with parties that are either internal or external to the company.

In addition to SOPs for performing CSV work, IT/IS management should agree or approve a systems quality assurance plan (SQAP) for data center operations that provides an overall strategy for ensuring the quality of system operations. The IEEE Standard for Software Quality Assurance (IEEE Std. 730-1989) can be adapted to this purpose. All platform system CSV packages would then operate under the auspices of the approved IT/IS systems QA plan (see Systems QA Plan box).

CSV package team
Just as we described for the user CSV package team in Part 1, a business decision group funds and approves the IT/IS work process for providing platform systems to clients with regulated applications (Figure 5). A data center manager is appointed as sponsor of a particular platform system and then assigns a team of IT/IS operations personnel to develop and maintain the CSV package for the platform. The quality assurance function stays independent of package work and

Platform CSV Team Roles

System sponsor (CIO/head of IT/IS function)
The IT/IS dept. manager owning the regulatory responsibility for the GXP platforms. Provides personnel, budget, and equipment. Approves CSV package validation plan and package summary report. Assigns a team leader.

System owner and team leader (senior manager, IT dept.) Person responsible for ensuring the system functions as intended for platform purposes. Functions as team leader for CSV package effort. Identifies and leads a package team. Approves test plan and test summary report. Drives the package preparation process and identifies ad hoc members as needed.

QA auditor (IT or GCP QA) Trains the team on regulatory requirements for the system and audits the package for progress toward plans and compliance with regulations.

Package manager (senior administrator, IT dept.) Systems analyst trained in CSV package documentation practices. Drives item preparation, manages package archive, and checks the quality of documents in production for their ability to pass audits.

Ad hoc members Provide administrative support, specialty expertise, consulting, training, testing, or other support as needed. Platform size and scope determine the size of this component.

Test coordinator (support specialist) Systems analyst who understands the specific use of the platform by the GXP application. Develops test plan and other test documentation. Identifies and trains testers and witnesses in formal testing practices. Manages formal testing process.

Test script writer Individual with a technical understanding of the configured platform system to be tested. Creates specific conditions to test the platform and writes instructions for how the platform system is to be used to operate to those conditions.

Tester(s) Trained platform specialist who executes the directions in the test script. A tester observes system response and records it in a testing log or by capture of a screen or by printing an expected report. The writer of a test script can never be the tester for that same script.

Witness Responsible individual trained in GXP testing practices (testing SOP). Ensures that GXP practices are followed and that test logs contain all the items requested by the test script. The writer of a script can witness its testing.
audits the CSV package for compliance to company and regulatory standards.

The various CSV roles and responsibilities for the package team effort are described in the box, Platform CSV Team Roles. Given the high turnover rate in many organizations, it is wise to always keep the CSV package team populated by at least three roles—the system owner, the package manager, and test coordinator. Thus, several knowledgeable people are available who know the system and its package and can defend both in case of an audit or inspection.

Developing a CSV package for a platform system takes time, costs money, and requires a team of people. It is not a casual experience and must be planned for as an ongoing business responsibility for organizations supporting regulated application software with platform systems and infrastructure. Good practices for computer validation can, however, be integrated into normal good practices for running stable, unsinkable operations in the IT/IS department. Lifetime system validation goals are also good business goals for IT/IS services.

References


Teri Stokes, PhD, is senior consultant and director of GXP International, 131 Sudbury Road, Concord, MA 01742, (978) 287-4393, fax (978) 369-5620.
Validating Computer Systems, Part 3
GCP Software Verification

Teri Stokes

Writing software for GCP use is serious business. Applications must be tested and retested to ensure that they actually do what they are designed to do.

Software suppliers have a tough job. Writing software for use in a GCP work process adds an extra complication: preparing for many audits of the software engineering process itself as well as the software application produced. Part 1 of this series (August 2000) discussed a user acceptance package for computerized system validation (CSV) to prove that the “right” software was built for the user requirements in the GCP work process. Part 2 (September 2000) addressed the IT/IS department’s CSV package to document that the software was installed on the “right” platform of components and infrastructure. Part 3 explores the software supplier’s CSV package that documents the way the software was “built right” to meet its design specifications.

The life of a software application, as shown in Figure 1, has nine steps, beginning with a system idea and needs analysis and continuing through to retirement. The software development life cycle (SDLC) portion is shown in detail in steps 3 through 5 (design, build, test). These steps are the focus of the supplier’s computer system validation (CSV) package.

Figure 1 also illustrates the areas of close coordination with the user group for refining the user requirements specification (URS, step 2), being audited in the commissioning step (step 6), and providing ongoing support and enhancements under a service level agreement (SLA).

Showing these steps in a flat, two-dimensional picture with arrows going in one direction is misleading, because there is usually a lot of cycling back and forth and refinement of specifications between steps 2 and 3, when users are shown demonstration or prototype versions of an application. At some point, however, the URS must be frozen so that the functional requirements can be finalized and the software design description made for the programmers to use as a blueprint for building the software application.

Requirements. The Questions on the Path to a URS box lists questions for defining requirements on any size of software application. The key factor here is that the user’s work process requirements are written down and agreed to by all parties before the start of building the software. Extra time taken to refine the URS with the supplier can pay huge dividends, because the rest of the development process evolves as a response to the URS. Any error at the start builds error into the rest of the process and the final product. The cost to fix errors in specifications grows exponentially through each succeeding step of the development cycle. Unclear

Figure 1. The software development life cycle in detail, and how it fits with the rest of the application development cycle.
Questions on the Path to a URS

- Who are the sponsors and intended users?
- What job is the system expected to do in the work process? Which tasks?
- Where is the documentation to describe in detail the user’s GCP work process?
- When is the software to be released, updated, fixed, tested, and maintained?
- Why does the work process need this software? Is it safety- or efficacy-related?
- How are users to be trained and problems resolved during ongoing operations?

Extra time here pays off in a smoother design process.

- User requirements, functional specifications, and design specifications must represent actual requirements of the work process and its platform system.
- All requirements must be testable.
- Testing must exercise all GCP aspects of specifications, including:
  - Functions
  - Limits
  - Invalid entries
  - Error messages
  - Access control
  - Online help messages.

Good requirements document lends itself to direct translation into test scripts. If a user, function, or design requirement cannot be stated in a clear and precise way so that it can be objectively tested, then it is a “wish” and not a “requirement.”

Building. Well-defined requirements also smooth the path for the team building the software. The software application can be built in two ways.

- Programming. The supplier can use a programming language or object tool to write source code for a unique software application such as SAS (SAS Institute, Cary, NC) or Excel (Microsoft, Redmond, WA).
- Configuration. The supplier can configure an application by setting preprogrammed variations in a configurable system and writing small routines to adapt it to the user’s specific needs. Examples of such applications are a macro for randomizing treatments and a spreadsheet for scheduling patient visits.

Testing. As different levels of software code are built, tested, adjusted, and retested, there is frequently a great deal of recycling between development steps 4 and 5 (Figure 1). Testing is conducted in several ways. Peer review is informal testing; a programmer gives the code to another software professional to try out and asks for comments and suggestions. Formal types of testing are defined below as per IEEE Standard 610.12:1990.

- Code review. A meeting at which software code is presented to project personnel, managers, users, customers, or other interested parties for comment or approval.
- Unit testing. Testing of individual hardware or software units or groups of related units.
- System testing. Testing conducted on a complete, integrated system to evaluate the system’s compliance with its specified requirements.
- Integration testing. Testing in which software components, hardware components, or both are combined and tested to evaluate the interaction between them.
- Regression testing. Selective retesting of a system or component to verify that modifications have not caused unintended effects and that the system or component still complies with its specified requirements.

Although this formal development and testing process is clearly needed for large systems—such as a sponsor’s clinical data management system and high-end statistical system—many people question its usefulness for spreadsheets, macros, and small applications used at investigator sites. In fact, the same nine steps shown in Figure 1 need to be traversed for the life of any software used for GCP purposes, but the size and scope of each step is scaled to the size and scope of the software application. The CSV package documents are also scaled to fit the size of the software. A small software systems development form can be designed to cover steps 2 through 6 using two sides of one sheet of paper.2

Software supplier CSV package

Producing a good CSV package in software development is good business and exercises the standard practices for good software engineering. A well-defined and well-documented software development life cycle provides the software supplier with management control of the engineering process. Clear requirements and documented coding standards lead to efficient and effective building of software and the ability to bring new programmers into a project with minimal ramp-up time and reduced risk of errors.

Documented formal testing of a product under development provides traceability for changes and a measure of the reliability of the software and its capacity to protect the integrity of data it handles. It lays a strong foundation for problem resolution when the application is out on the market or future enhancements are considered. Test summary reports give developers and testers the opportunity to present objective evidence for how good they are at creating robust, reliable software. Good online and off-line user documentation facilitates user training, increases customer satisfaction with the application, and
Software Verification Plan

Purpose and scope
☐ Inclusions, exclusions, and limitations.
Reference documents
☐ SOPs, manuals, and policies referenced by the plan.
Definitions
☐ Terms required to understand the verification plan.
Verification overview
☐ Organization and master schedule for the software verification effort.
☐ Resources summary and responsibilities for verification tasks (usually a three-column table listing verification tasks, role[s] responsible, and due date).
☐ Tools, techniques, and methodologies used in the verification effort.
Life cycle validation tasks at each phase until retirement
☐ Management of verification process. Control procedures of quality management system requirements for SDLC.
☐ Concept phase. Market analysis of user needs.
☐ Design phase. Development of and approval for system design description. Perform design traceability analysis, design evaluation, and design interface analysis. Develop test plans.
☐ Implementation phase. Perform source code traceability analysis, evaluation, interface analysis, and documentation evaluation.
☐ Test phase. Execute test scripts for test plans and write test summary reports.
☐ Installation and checkout phase. Audit software installation package and check replication process for accuracy. Write CSV package summary report.
☐ Operation and maintenance phase. Establish help desk and any other support/maintenance activities. Develop bug fix, release, and upgrade plan for software product.
☐ Retirement phase. Plan for product retirement in original design.

Establish the off-site archive with access and retrieval SOP.
Software verification reporting
☐ Required and optional records/reports to be written.
Verification administrative procedures
☐ Anomaly reporting and resolution. Problem/issues handling.
☐ Task repetition policy. Criteria for when to repeat testing or any other verification task when its input changes.
☐ Deviation policy. How to report actions taken that differ from the plan.
☐ Control procedures. How the software application and engineering system(s) are configured, protected, and stored—SOPs for backup/retrieval, disaster recovery, change control, and system testing.
☐ Standards, practices, and conventions for verification work—policies, procedures, and templates for logs, reports, and other items in the CSV package.

☑ Adapted from IEEE Standard 1012-1986.3

reduces the volume of help desk support calls.

Experienced software suppliers to the clinical trials marketplace understand that their clients are responsible to the authorities for the validation of software they use. To meet that responsibility, suppliers will be subjected to client QA audits to assess the way quality was built into the software during development. A well-organized supplier CSV package that emerges from the normal good engineering practices of the supplier’s business will reduce audit time and audit follow-up work.

The Software Supplier CSV box lists the items in the package. Whether each item is covered by a sentence, a paragraph, a page of text, or a manual of information will depend on the size and scope of the software product being developed and the size of the effort being described.

Verification plan
The Institute for Electrical and Electronics Engineers, Inc. (IEEE) publishes a standard for software verification and validation plans that can easily be adapted.3 The Software Verification Plan box shows a sample of an outline for this purpose.

Every plan in the CSV package—verification plan, master test plan, subordinate test plans—must have a defined task list stating just what actions are to be taken to execute the plan’s strategy. Every plan must also have its own summary report written to explain to management the outcome of the planned tasks. The package summary report includes the outcome of individual tasks as well as the highlights of summary reports from subordinate plans. After all the tasks in the supplier’s verification plan have been completed, a package summary report is written (see the Software Package Summary Report box for an outline).

☑ Adapted from IEEE Standard 1012-1986.3

Software Package Summary Report

☐ Plan identifier. ID number indicating system associated with the plan.
☐ Summary of all verification SDLC tasks and their status.
☐ Summary of all CSV package items and their status.
☐ Summary of unexpected problems/issues and their resolution.
☐ Summary of deviations from the verification plan and rationale for deviations.
☐ Assessment of overall software quality based on package documentation, test summary report, and QA audit report.
☐ Recommendations. Release statement to management for the release status of the software application system.
☐ Approval signature(s) and date(s).
☐ Appendix A. Update report form for recording major system changes with related regression testing.
☐ Appendix B. Table of contents for CSV package.

☑ Adapted from IEEE Standard 1012-1986.3

November 2000
APPLIED CLINICAL TRIALS
Software Supplier CSV Package

- Verification plan. Document describing the purpose, scope, approach, resources, and schedule of intended verification activities for a specific software development project (see Software Verification Plan box).
- Software engineering SOPs. Standard procedures for naming conventions, application interfaces, database calling conventions, documenting source code, testing practices, writing system manuals, release notes, online help formats, debugging process, change control.
- Code and tools management log. The first section in this tools management logbook binder contains a written description in text and in diagrams of the software engineering system configuration. It also includes a list of all major components of the development environment—server identifiers, associated disks, versions of database, language, and software tools, code management and testing tools, and overall network topology.
- SDLC. A written and approved description in text and diagrams to describe the software development life cycle with documented input and output requirements per phase and the roles responsible for review and approval to allow software to progress from one phase to the next.
- Programmer training records. CVs and training records to show that everyone on the software development team has experience and training appropriate to his/her role.
- Software upgrade plan. Documented business process for developing and releasing enhancements to the software in a controlled manner after first release to the market. Includes archive process for past versions with retention times suitable for regulatory requirements.
- QMS. Documented quality management system with management commitment to a corporate quality policy and QA organization to conduct independent internal audits of the SDLC activities for compliance with engineering SOPs and corporate quality policy and practices.
- Audit logs. Configuration management logbook binder section to record date, time, and participants in any audits or inspections of the supplier by internal QA, external clients, or regulatory authorities. Audit reports per se are kept company-confidential by QA department.
- Master test plan. Document that describes the technical and management approach to be followed at project level for testing a software product. Typical contents identify the items to be tested, tasks to be performed, responsibilities, schedules, and required resources for the testing activity. Document also describes the number and type of specific test plans to be developed for a given software product—unit test plan, system test plan, integration test plan, regression test plan.
- Test case. Document specifying the details of the testing approach for a platform feature or combination of features and identifying associated test scripts—system power up/down, system backup/recover, server connectivity to desktops/printers/remote sites across a network.
- Test script. Document specifying inputs, predicted results, and a set of execution conditions for an individual test. Includes one or more step procedures that describe keystrokes or other tester actions and provide log space for recording system response to test activity.
- Test summary report(s). Document(s) summarizing testing activities and results per test plan under the master test plan. Include(s) an evaluation of software quality based on testing results.
- SDD. Software design description—a blueprint or written model of the software system created to facilitate analysis, planning, implementation, and decision-making in building a software system.
- Application code. Computer instructions and data definitions in a form suitably designed to fulfill the specific needs of a user.
- SDLC documentation. All QMS documentation associated with the SDLC process—signed phase review documentation, testing documentation, code annotations.
- Support contract (SLA). Service level agreement(s) with clients purchasing a regulated application from the software supplier (see Figure 4).
- Application manuals. Instruction manuals to train IT/IS and/or system administrators in how to install and manage the software application system and instruction manuals to train users in how to operate the software in their GCP work process.
- User training. Online or hard copy training courses and materials for the client’s users and their system administrators working with the software application in the GCP work process.
- Problem help. Documented process with defined escalation procedure for help desk technical support to resolve user problems with the software application.
- Supplier’s CSV package summary report. Document summarizing all CSV package activities initiated under the verification plan and the results of those activities. It also contains an evaluation of the software application system’s readiness to perform as intended and be operated in compliance with regulatory requirements. (See Software Package Summary Report box for recommended outline.)

Figure 2. The software supplier’s CSV package.
The quality assurance department will audit the CSV package process and its documentation for compliance with the firm’s quality management system and software quality standards. The package sponsor is usually the senior manager responsible for the product’s development effort. The team leader is assigned by the package sponsor and is usually the individual who carries the engineering responsibility for building a quality product. The team leader selects the rest of the team. The CSV package roles and responsibilities are shown in the Software Supplier CSV Team Roles box. These roles apply to the software supplier during development and also to the CSV package teams of the user group and their IT/IS department for validation of the software product in the work process. It is extremely unwise to give in to the temptation to reduce the number of CSV package team members from three to one. With turnover in the workforce, it is only good business sense to have more than one person understand the software product and its CSV package well enough to defend it in audits and inspections. It is also good to assign roles to people whose jobs in the project are associated with creating key items in the CSV package—for example, project manager as team leader, quality control secretary as package manager, and software tester as test coordinator. In this way, package items can flow out of the direct work activities in the project rather than being seen as added overhead at the end. For very small projects, the team leader can choose to also carry one of the other two roles—but not all three.

**Software development platform**

Software applications are created using various configurations of hardware, operating systems, networks, databases, programming languages, design and coding tools, graphical user interfaces (GUIs), and testing tools. When developing critical software applications, it is important to document this platform and to check the application for any effects from changes made to the development platform.

Changing a database version, for example, may interfere with the performance of some database calls already programmed into the application, and these would have to be rewritten. Changing automated testing tool versions may result in certain prior test cases not executing as expected. Moving to a new GUI version may cancel the action of or hide the view of certain buttons previously programmed.

Replacing like-for-like components in a platform should not cause problems, but—as with generic replacement of branded drugs—some unexpected variations can emerge. Installation qualification testing should be performed on all components of the development platform. Checklists can be used to verify and document that all key aspects of the installation adhere to the specifications and recommendations of the component’s manufacturer and that the component is appropriate for the development platform’s configuration. The configuration itself should be documented and changes tracked in a configuration management logbook.

As the Documenting the SDLC Platform box illustrates, platform security, maintenance records, backup and recovery logs, and the disaster plan are to be documented in an organized way for software development platforms. It should always be possible to trace the logical and physical environment used for creating critical software.

The escrow process is one major difference between user platform systems and software development platforms. The escrow process goes beyond the usual archive activity to specify that an official third party will have secured custody of a master copy of the firm’s software product. In the event that the software supplier goes out of business, its customers have a defined legal right to contact the third party and access a copy of the source code for use in ongoing support of their operations.

**Supplier and user SLA partnership**

The service level agreement (SLA) for a critical software system used for GCP purposes is more than a commercial contract. It is a commitment from both sides for supporting the success of the application in its operational environment and compliance with regulatory standards. The more direct impact the software application has on the safety, efficacy, and quality of subject care or the integrity of safety and efficacy
Documenting the SDLC Platform

The software development platform must be traceable through careful documentation.

- Configuration management logbook binder
  - Configuration. System components and versions of hardware, software, languages, and tools.
  - Platform security. Access rights, user privileges, software code manager, training.
  - Maintenance and support records. Change records, service visit logs.
  - Backup and recovery log. Disaster plan—daily, weekly, monthly, yearly.
  - Archive and escrow process. Control of master copy of software and updates.

In Figure 4 the service level agreement (SLA) defines the ongoing partnership between the users and the software supplier over the life of the application.

-软件开发平台必须通过仔细的文档进行追踪。
-配置管理日志本
  -配置。系统组件和硬件、软件、语言和工具的版本。
  -平台安全。访问权限，用户权限，软件代码管理，培训。
  -维护和支持记录。更改记录，服务访问日志。
  -备份和恢复日志。灾难计划—每日，每周，每月，每年。
  -存档和托管过程。控制主版本的软件和更新。

图4展示了服务级别协议（SLA）定义了用户和软件供应商之间的持续合作伙伴关系。
CSV packages described in the series. To be or not to be involved is the QA question. How to be involved will be the series’ answer.

References

Teri Stokes, PhD, is senior consultant and director, GXP International, 131 Sudbury Road, Concord, MA 01742, (978) 287-4393, fax (978) 369-5620.
Validating Computer Systems, Part 4

The QA Role in Computer Validation

Teri Stokes

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.

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
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 the company’s standard approach to CSV documentation.

QA further supports the policy team by helping to write general standard operating procedures (SOPs) for performing CSV work consistently across the organization for software development projects, user applications, and platform infrastructure systems. QA further supports the policy team by helping to write general SOPs for performing CSV work consistently across the organization for software development projects, user applications, and platform infrastructure 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. 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 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.

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.

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

<table>
<thead>
<tr>
<th>QUALITY reference documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Society for Quality, Milwaukie, WI, USA, <a href="http://www.asq.org">www.asq.org</a></td>
</tr>
<tr>
<td>ANSI/ISO/ASQ Q9000-3-1997 Quality management and quality assurance standards—Part 3: Guidelines for the application of ANSI/ISO/ASQ Q9001-1994 to the development, supply, installation and maintenance of computer software</td>
</tr>
<tr>
<td>U.S. FDA Rockville, MD, USA, <a href="http://www.fda.gov">www.fda.gov</a></td>
</tr>
<tr>
<td>21 CFR 820—Quality System Regulation</td>
</tr>
<tr>
<td>21 CFR 11—Electronic Records; Electronic Signatures; Final Rule</td>
</tr>
<tr>
<td>Guidance for Industry—General Principles of Software Validation</td>
</tr>
<tr>
<td>Guidance for Industry—Computerized Systems Used in Clinical Trials</td>
</tr>
<tr>
<td>The Institute of Electrical and Electronics Engineers, Inc., Piscataway, NJ, USA, <a href="http://www.ieee.org">www.ieee.org</a></td>
</tr>
<tr>
<td>IEEE Std. 1062-1993 Recommended Practice for Software Acquisition</td>
</tr>
<tr>
<td>IEEE Std. 1028-1988 for Software Reviews and Audits</td>
</tr>
<tr>
<td>IEEE Std. 1016-1993 This international standard includes a number of useful checklists for evaluating software suppliers during the purchase process.</td>
</tr>
<tr>
<td>This 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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
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 do 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.

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’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).
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

---

**CSV Audit Report**

- 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.

*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.
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.

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): |

<table>
<thead>
<tr>
<th>Name(s) &amp; organization(s) of audit/inspection team:</th>
<th>Signature(s) and date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site host for audit/inspection:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Name/title)</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary report in company confidential file (yes/no):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document ID for initial report:</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interviewee name &amp; title</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.”

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...
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**