Technology Update

Validating Computer Systems, Part 2

GCP Validation of Platform and Infrastructure Systems

Teri Stokes

The IT/IS team not only implements the platform system that delivers the GCP application to the work process, but is responsible for its continued care.

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

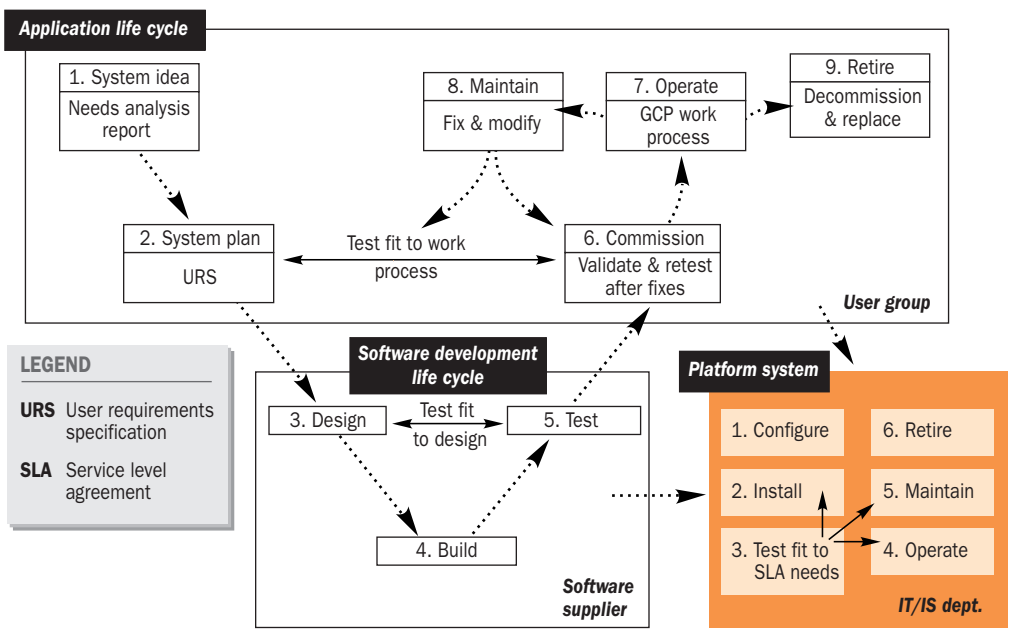


Figure 1. The platform system life cycle in detail, and how it fits with the rest of the application development cycle.

6–9, but also depicted next to the software supplier that specifies the physical and logical requirements of the application for the IT/IS department to use when configuring the platform system.

The documentation required for a platform system CSV package also helps the IT/IS department to be organized in its operations.

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

Platform Validation Plan Outline[a]

Purpose and scope
- ☐ Inclusions, exclusions, and limitations.

Reference documents
- ☐ SOPs, manuals, and policies referenced by the plan.

Definitions
- ☐ Terms required to understand the validation plan.

Validation overview
- ☐ Organization and master schedule for the validation effort.
- ☐ Resources summary and responsibilities for validation tasks (usually a three-column table listing validation tasks, role(s) responsible, and due date).
- ☐ Tools, techniques, and methodologies used in the validation effort.

Life cycle validation tasks at each phase from purchase/install to retirement
- ☐ Concept phase. SLA based on user's needs analysis, URS, and application supplier's specifications for platform requirements.
- ☐ Development phase. CM logbook description of platform system.
- ☐ Installation and checkout phase. Test and validation summary reports.
- ☐ Operation and maintenance phase. SOPs, logs, audits, and training.
- ☐ Retirement phase. Archive plan and transition plan to next platform system.

System validation reporting
- ☐ Required and optional records/reports to be written.

Validation administration procedures
- ☐ Reporting and resolution process for system and user problems and issues.
- ☐ Task repetition policy. When and how to repeat testing and other validation tasks.
- ☐ Deviation policy. How to handle actions that differ from the plan.
- ☐ Control procedures. How software application and platform system(s) are configured, protected, and stored—SOPs for backup/retrieval, disaster recovery, change control, and system testing.
- ☐ Standards, practices, and conventions for validation work. Template formats for logs, reports, and other items in the validation package.

[a]Adapted from IEEE Standard 1012-1986.[1]

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 box 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 Package Summary Report[a]

- ☐ **Plan identifier.** ID number indicating system associated with the plan.
- ☐ **Summary of all validation life cycle tasks** and their current status.
- ☐ **Summary of all CSV package items** and their current status.
- ☐ **Summary of unexpected problems/issues** and their resolution.
- ☐ **Summary of deviations** from the validation plan and rationale for deviations.
- ☐ **Assessment of overall system quality** based on package documentation, test summary report, and QA audit report.
- ☐ **Recommendations.** Release statement from management for the GXP status of the platform system.
- ☐ **Approval** signature(s) and date(s).
- ☐ **Appendix A.** Update report form for recording major system changes with related regression testing.
- ☐ **Appendix B.** Summary reports for periodic quality control testing.

[a]Adapted from IEEE Standard 1012-1986.[1]

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.

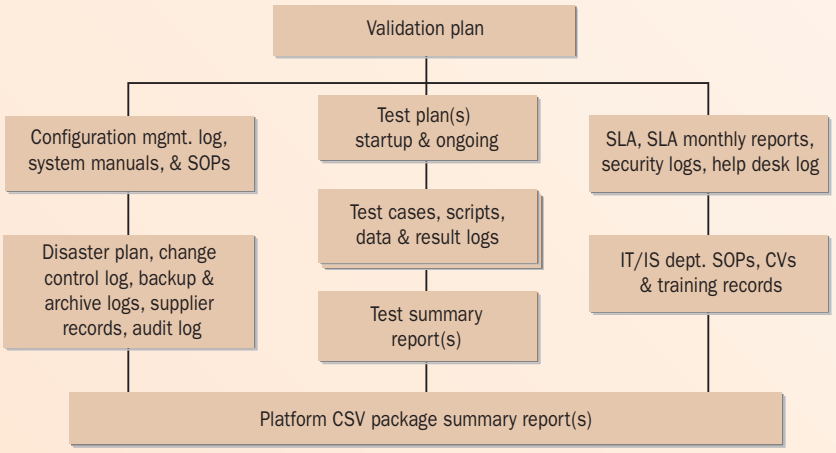


Figure 2. The platform CSV package.

- ☐ **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 standard[1]).
- ☐ **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 deptartment 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).

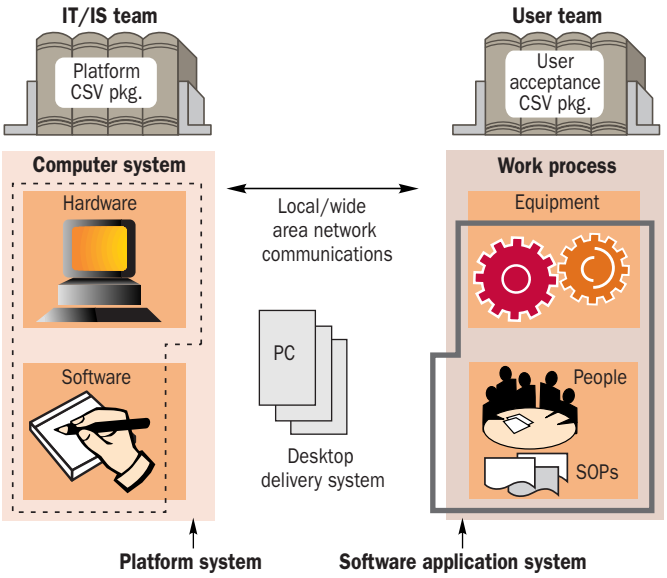


Figure 3. The IT/IS team delivers the system to the desktops of the users.

form system support, and users cannot reach the application without desktop or handheld systems and network communications. The size and complexity of a platform system varies with the design of the application software and the size and diversity of the user population.

Validation of the computerized system requires the collaboration of two teams—the user acceptance team and the IT/IS team (Figure 3). The user acceptance team is responsible for the CSV package that documents whether the software application performs as intended during the GCP work process. The IT/IS team is responsible for the CSV package that documents the assembly and validation of the platform system configuration to deliver the application to the work process. The platform system configuration will include the components of the server system(s) hosting the software application, the components of the desktop delivery system (PC/laptop/device) bringing the application to the users, and all network communications required for the application to operate as intended in the work process.

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

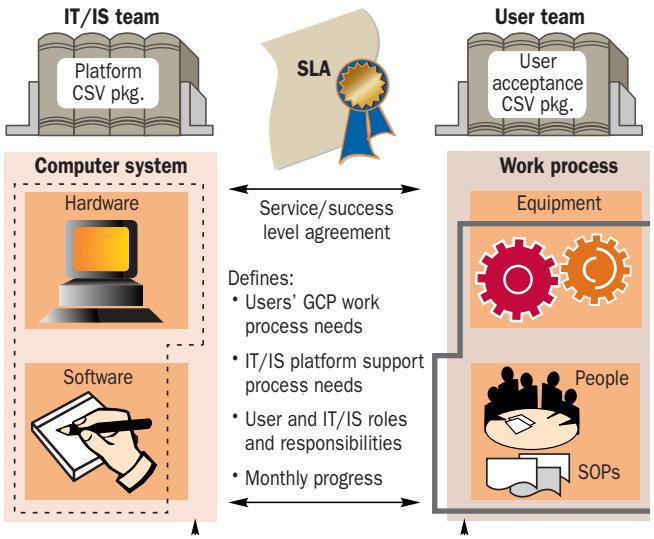


Figure 4. A service level agreement (SLA) defines the ongoing partnership that must exist between the user team and the platform team over the life of the application.

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 to be 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?

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.

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 deliv-

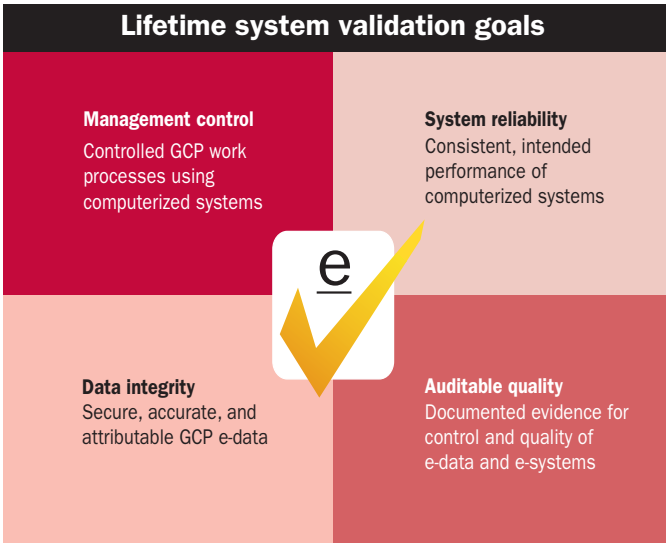
ers it, and how is it recorded? Any new announcements from the application supplier for upgrades, enhancement patches, or new versions of product coming soon that could have an impact on the platform configuration? Any security issues arising—server, database, network?

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.

Systems QA Plan[a]

Purpose of plan
- ☐ Business, regulatory, and technical purposes.

Scope of systems QA plan (SQAP)
- ☐ Inclusions. Types of platform systems to be validated.
- ☐ Exclusions. Internals of platform system components.
- ☐ Limitations. Shared systems controlled elsewhere.

Reference documents
- ☐ Regulations, company policies, department SOPs.

Management
- ☐ Organization. Roles defined for CSV package team.
- ☐ Tasks. Validation package activities described.
- ☐ Responsibilities. Role responsibilities identified for package activities.

Documentation for quality control of systems
- ☐ Logs, plans, reports.
- ☐ Minimum documentation requirements are defined for standard system packages and special types of systems.
- ☐ Standard formats and templates are referenced in appendices.

Standards, practices, and metrics
- ☐ SOPs for responsible installation, maintenance, and support of validated platform systems, company policies, and external regulations applied to SQAP scope.

Reviews, audits, and inspections
- ☐ Type and frequency of system reviews.

Testing
- ☐ Formal testing practices required for validating systems.

Problem reporting
- ☐ Problem reporting and corrective action process.

Code and media control
- ☐ Security, archival, and retrieval.

Supplier control
- ☐ Content for quality and service level agreements (SLAs).

Records collection
- ☐ Records collection, maintenance, and retention practices.

Training
- ☐ Materials and instruction for system support personnel.

Risk management system
- ☐ Risk management, data security, disaster recovery, legacy systems.

Approvals
- ☐ Authorized signatures for this plan.

[a]Adapted from IEEE Standard 730-1989.[2]

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.[2] 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.

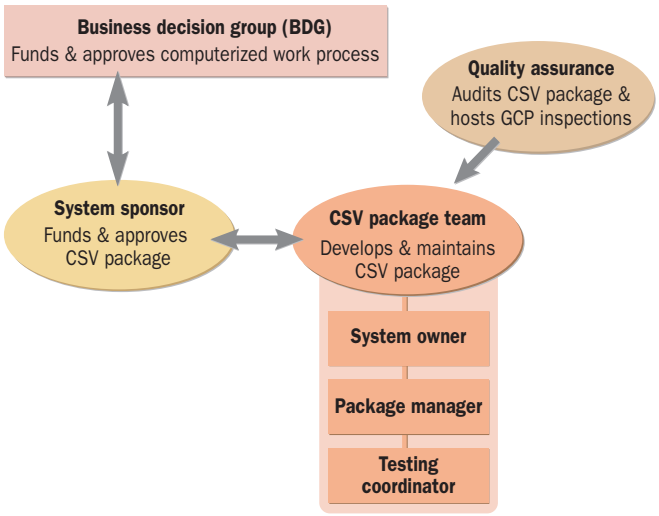


Figure 5. The CSV package team.

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

1. Institute for Electrical and Electronics Engineers, Inc., IEEE Standard for Software Verification and Validation Plans, Standard 1012-1986 (IEEE, Piscataway, NJ, 1993), pp. 12–19.
2. Institute for Electrical and Electronics Engineers, Inc., IEEE Standard for Software Quality Assurance Plans, Standard 730-1996 (IEEE, Piscataway, NJ, 1993), pp. 9–12.

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