Applying Part 11 to the Implementation of Quality Management Software

Chet Shemanski* and Gregg F. Clyne

COMSTOCK

This article describes the Part 11 requirements that companies must address when automating their quality management processes and offers practical tips for compliance.

Chet Shemanski is the director and **Gregg F. Clyne** is a senior consultant of manufacturing systems and equipment practice at Taratec Development Corporation, 1170 US Highway 22, Suite 302, Bridgewater, NJ 08807, tel. 610.725.8790, fax 908.725.8999, chet.shemanski@taratec.com.

*To whom all correspondence should be addressed.

The use of quality management software (QMS) to automate manufacturing quality processes quickly is becoming an industry-wide initiative. Companies are turning to commercial off-the-shelf systems (COTS) to simplify implementation and validation efforts. Regardless of the system selected, the automation of these critical quality processes is subject to electronic records and electronic signatures (ER/ES) requirements, as set forth in the 21 *CFR* Part 11 regulation (1). Therefore, companies must adopt a comprehensive but manageable approach to Part 11 compliance as they begin to automate the processes that support product quality and efficacy to ensure they meet the requirements of good manufacturing practices and all predicate rules.

This article describes the compliance requirements that companies must address when automating their quality management processes and gives insight into practical, risk-based recommendations for compliance with Part 11.

Ensuring safety and efficacy for consumers is the single most important outcome of the manufacturing process. To that end, the quality challenges that pharmaceutical companies face during product manufacture continue to evolve. It is estimated that compliance with internal quality systems and applicable regulations consume almost 25% of total site operating budgets industry-wide. Considering these costs, even modest improvements in quality management efficiency will have a significant financial effect. Because of increasing competition throughout the industry, manufacturers of pharmaceuticals, biologics, and medical devices are looking for innovative ways to improve their margins and maintain their market shares. Increasing the effectiveness of quality management is one of the first places to start.

Virtually every commercial quality management software vendor will claim that its systems "are 100% 21 *CFR* Part 11-compliant" or "meet all Part 11 requirements." Although these systems may provide 100% of the application-specific technical functionality to enable Part 11 compliance (*e.g.,* audit trail, user-based access control, and electronic signatures), the implementation of these systems requires additional consideration and controls to guarantee compliance.

Because the best software will only satisfy a portion of the systemic Part 11 requirements, strategic organizational and procedural controls must be addressed.

A life cycle approach

To ensure compliance with Part 11, one needs a holistic view of the QMS implementation life cycle. It is important to recognize the various components that must be addressed before deeming a quality management system "Part 11 compliant."

Requirements definition. The first step in any automation or computerized effort is to define the requirements. Following a methodical analysis of user, predicate rule, and Part 11 requirements, companies must document the necessary system components and controls for the process to become automated. These requirements will be the basis for designing a risk-based testing strategy, selecting and configuring the chosen software solution, and developing standard operating procedures (SOPs).

Companies must understand the requirements set forth in the predicate rules such as those regarding the follow-up of production control, laboratory record review, and investigation of discrepancies (21 *CFR* Part 211.192). As defined in its subparts, the regulation requires the documentation of investigation, root cause, and signatures for both the investigator and batch disposition approver. Thus, the electronic system must control how this information is captured, reviewed, reported, secured, and maintained.

Software selection. Selecting the appropriate technical solution is an important factor when complying with the regulations, but it also has more far-reaching consequences.

The selection of a system that best fits the company's needs and quality management process can reduce the time, effort, and cost needed to become compliant. Companies should select software with application-specific technical controls for Part 11 and should select software vendors that comply with applicable quality standards and Part 11 procedural controls. This effort will not only solidify the product selection process, but also could help reduce the burden of the company's test strategy and organizational controls.

Companies often use requests for proposals (RFPs) to measure the risk and/or necessity of technical features, vendor practices, or architectural integrity before selection. By using a company-applied weighting system, each requested function can be ranked according to the vendor's ability to comply with applicable regulations. Therefore, a measurable approach will allow a company to select a software package that not only fits its business needs, but also meets applicable regulatory requirements.

Process development. Because configurable COTS will not completely adapt to company-specific processes, external controls are required. Organizations must make use of clear and understandable language in SOPs to close the gaps that software functionality does not address. SOPs that dictate how predicate rules are ensured can help document the system's use and "work-arounds."

Administration. Companies are leveraging Web-based QMS software to promote harmonized quality processes at multiple sites, and also globally. This strategy offers several benefits, including supporting global trend analysis, remote approval, and reduced costs.

A global QMS installation can be difficult to administer without a good plan that ensures compliance with Part 11 mandates. Failure to ensure integrity and consistency in administration could be detrimental to data reliability or system stability. Thus, each company must determine how the administration will be controlled and monitored through:

- a central administration approach which decreases the risk of variation from procedures but clearly is difficult for large implementation;
- a decentralized administration approach that allows for local support but increases the risk of variation in carrying out processes that may affect global data integrity;
- a hybrid of the two.

Although each model has its benefits and risks, one constant exists: the administration of the system must be consistent and integrated to ensure the reliability and integrity of data and control. With this point in mind, procedures should clearly lay out guidelines for user and system access, change management, documentation, and backup and recovery, for example.

A global QMS usually requires that well-trained, decentralized information technology (IT) person-

nel administer user accounts, application access, and necessary local configuration. All individuals' responsibilities and boundaries are verified through a corporate administrator and global system SOPs. Thus, procedures supporting the deployment of a global deviation and corrective and preventive actions (CAPA) system should indicate the processes by which user privileges are granted and removed, equipment code lists are updated, and employees are adequately trained to use the system.

Implementing and validating. Although software may provide tools that are needed to comply with Part 11, the implementation and validation processes will ensure the system is configured properly and operates according to requirements. As previously mentioned, these requirements stem not only from the organization, but also from the predicate rules and Part 11. By using qualification and verification test protocols, companies make every attempt to ensure expected functionality is configured as intended, procedures are approved, and all requirement gaps are closed.

The performance qualification (PQ) protocol is especially important because it verifies that the designed system configuration maps to the process, and therefore meets the requirements of the predicate rules, Part 11, and users. For example, while executing the protocol and traversing through a deviation or investigation workflow, the PQ test scripts will ensure that the root cause and investigational information can be captured and an investigation and final batch disposition electronic signature are required. In addition, the PQ protocol should ensure that only authorized individuals can perform these functions, thus ensuring the stability and integrity of captured data.

Change management. Managing change to any regulated system, process, or piece of equipment is critical to ensure continuous compliance. In the case of a multisite QMS implementation, change management must be well coordinated, and impact analysis must be critically performed. It is important to assess the potential effect on global facilities when making changes to user requirements, design, or system architecture. Failure to coordinate such efforts could leave the organization out of compliance with the user requirements, predicate rules, or Part 11.

Although companies use various tools to manage change, they all attempt to create harmony between the flexible administration of change and ensuring system/data integrity and stability. Thus, many companies use a three-pronged approach to manage change within the systems.

First, system-specific procedures are used to manage routine and daily administration that may have been qualified during functional testing. These types of changes include, but are not limited to, modifications of field code lists, updating system time for changes to Daylight Saving Time, managing cosmetic

changes to reports, or performing user administration.

Secondly, the addition of new modules, workflows, or role configuration changes requires more formal procedures. Processes that assess the impact of the change such as site or IT change control procedures serve this purpose. These mechanisms ensure that thorough change analysis is performed to assess the adequacy of regression testing, system stability of regression testing, or effect on product.

Lastly, the rationale behind a hierarchical change management process can be documented in a detailed fashion and managed accordingly with a well-defined and "living" system validation plan.

COTS functionality

The selection of the appropriate software package cannot only make or break Part 11 compliance, but also can help reduce costs, simplify procedures, and ease the training burden.

None of the quality management software available in today's marketplace will perfectly meet the technical requirements of Part 11 when implemented within the company's workflow to support predicate rule requirements. Therefore, when procuring such a system, it is important to understand the main requirements. As previously mentioned, by clearly defining the required functionality in an RFP based on process and organizational needs, companies can mitigate the risk inherent in the Part 11 software selection process.

Audit trail (plus some). The intent of an audit trail in regulated systems is to determine what data were created, changed, or deleted; who created, changed, or deleted the information; when the data were created, changed, or deleted; and to retain a full record history of those changes or deletions. Some software packages accomplish this task with audit trail fields that are independent of the record itself. This configuration makes it cumbersome and difficult to recall a record at a given point in time. Thus, software packages that offer record revision control will make it easier to display records as they originally appeared.

Companies also must understand the importance of an administrative audit trail. Although this technical control is not required by the regulations and can be accomplished procedurally, it will enable production record data to be reviewed in the context of the system's "once was" configuration more easily. Therefore, it is of the utmost importance that the system's configuration be revision-controlled in some way.

Imagine that an auditor must understand how a batch was errantly released six months ago using the company's deviation system. Since then, the company upgraded the system, changed the security role, and revised the workflow. The technical audit trails discussed are one way to review how Parts 11 and 211 address change. Understanding the record and configuration in the context of the process, the validation

and system life cycle may, however, be more important.

Electronic signatures. The use of electronic signatures during quality processes often raises concerns, but should it? Companies must clearly define their processes and electronic signature requirements before configuring their systems. Milestones for electronic signature acquisition should be clear when using the current predicate rule standard operating procedures.

Part 11 enables companies to use electronic signatures in place of handwritten signatures, but it is important to remember that the purpose of signatures and the signature requirements remain the same and are based on the predicate rules.

As with a paper signature, an electronic signature establishes accountability and ensures authenticity. It should also ensure that those who review the records or documents in the future can determine that the appropriate person signed the record.

In some systems, clearly indicating the lines of authority is nearly impossible. Thus, companies turn again to procedures to document where signatures are required during the process and system workflow, and what that signature signifies. For example, Am I giving authorization to take the lot off quarantine and ship? Am I agreeing that this CAPA plan is sufficient to address the investigation root cause? Am I authorizing a change control that I have reviewed and understand?

Role-based permissions. QMS, such as those that help to control workflow-type events, often allow for the configuration of multiple "roles" (*i.e.,* security levels, groups). Although predicate rules do not establish the specific responsibilities for individuals or groups (other than quality assurance), the industry has determined best practices for these logical, role-based authorities. They are documented in paper processes in the SOPs' "responsibilities" and "procedure" sections.

To facilitate the use of roles and role-based configuration in QMS, companies first begin by understanding the knowledge, training, and limitations of their personnel that are assigned to perform specific tasks. Role-based configurations often drive workflow and approval authority and the ability to view and modify data fields. These functions are critical to the process's integrity by defining which groups can: add, modify, or delete in fields; approve or reject work; or access specific quality records.

Therefore, most companies spend countless hours with vendors understanding the limitations of their systems and investigating how their employees and processes operate. At a minimum, documenting the requirements for a company's role-based permissions is a great learning experience for how its work is completed.

Ensuring compliance

At the end of the day, the strategy for ensuring Part 11 compliance for quality management software is sim-