A Tangled WEB

Does internet-based software **have a place** in **highly regulated industries?**

by Jim Dougherty
and Wylene Lengel

In 50 Words Or Less

- Software as a service (SaaS) applications are growing in popularity because of their ease of use, but they present significant issues for FDA-regulated organizations.
- By managing SaaS providers as they would other outsourced services, FDA-regulated organizations can ensure compliance.

ANYONE FAMILIAR WITH purchasing and implementing business application software for organizations regulated by the U.S. Food and Drug Administration (FDA)—pharmaceutical, medical device or biotechnology companies in particular—knows the effort is not a small one.

After an application has been selected and purchased, the validation approach required for conventional software implementation can take weeks or even months of effort from IT and other resources. These requirements, however, are well-known and understood.

Some companies are moving away from conventional software and adding software as a service (SaaS) applications, which use a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over the internet.

Developed and maintained by the software vendor at its locations, SaaS applications are typically purchased as a subscription based on the number of users or number of transactions.

In simple terms, SaaS is on-demand access to software via the internet. It seemingly eliminates the installation and testing of the software by the customer—or does it?

And how do FDA-regulated organizations prove they have validated these systems when the installation and testing are done at the software vendor's site? How do those organizations provide the proper documentation to regulatory authorities for SaaS-supported operations?

SaaS benefits

The breadth of available SaaS applications is rapidly expanding to encompass a variety of business applications, including many that fall under FDA regulations. Examples of SaaS applications that typically don't fall under FDA regulations include project management, customer relationship management, HR management and sales automation.

Examples that fall under FDA regulations include electronic laboratory notebooks, clinical trial data management, employee training, inventory control, distribution and pharmacoviligance—the study of data surrounding a drug's adverse effects. In addition, many organizations are now using SaaS applications for backup storage of their network data, some of which fall under FDA regulation.

Given their compelling business case, it's no surprise that SaaS applications are growing in popularity. Customers are shifting to SaaS for a variety of benefits, such as:

- Easy leveraging of the application from the internet to support a mobile workforce or a workforce located in multiple locations.
- Immediate availability of the latest version for all customers, eliminating the need for multiple installations or to roll out upgrades across multiple sites.
- Advantages of scalability with subscription use, which makes it easier to accommodate changing business needs.

Perhaps the most significant benefit is lower overall cost of ownership to each customer because of:

- Accelerated software deployment.
- Hardware requirements handled by the vendor.
- Operational and maintenance costs incurred by the vendor.
- Fewer IT and quality assurance resources required for deployment, testing and maintenance.

On the rise

As SaaS rapidly increases in popularity—*InformationWeek* Analytics recently found that 60% of companies use SaaS solutions, 13% more than last year[1]—the question of validation presents challenges to firms in FDA-regulated industries. Can regulated companies take advantage of this new wave in business applications?

FDA-regulated organizations are responsible for ensuring that any software used to help manufacture or manage data about a product—or other software used in any regulated application—is typically validated using the approach in Figure 1.

This validation approach puts in place documentation that can be audited by the FDA or other regulatory agencies. The documentation provides evidence the software meets applicable regulations, such as part 11 of the FDA's Code of Federal Regulations Title 21.[2]

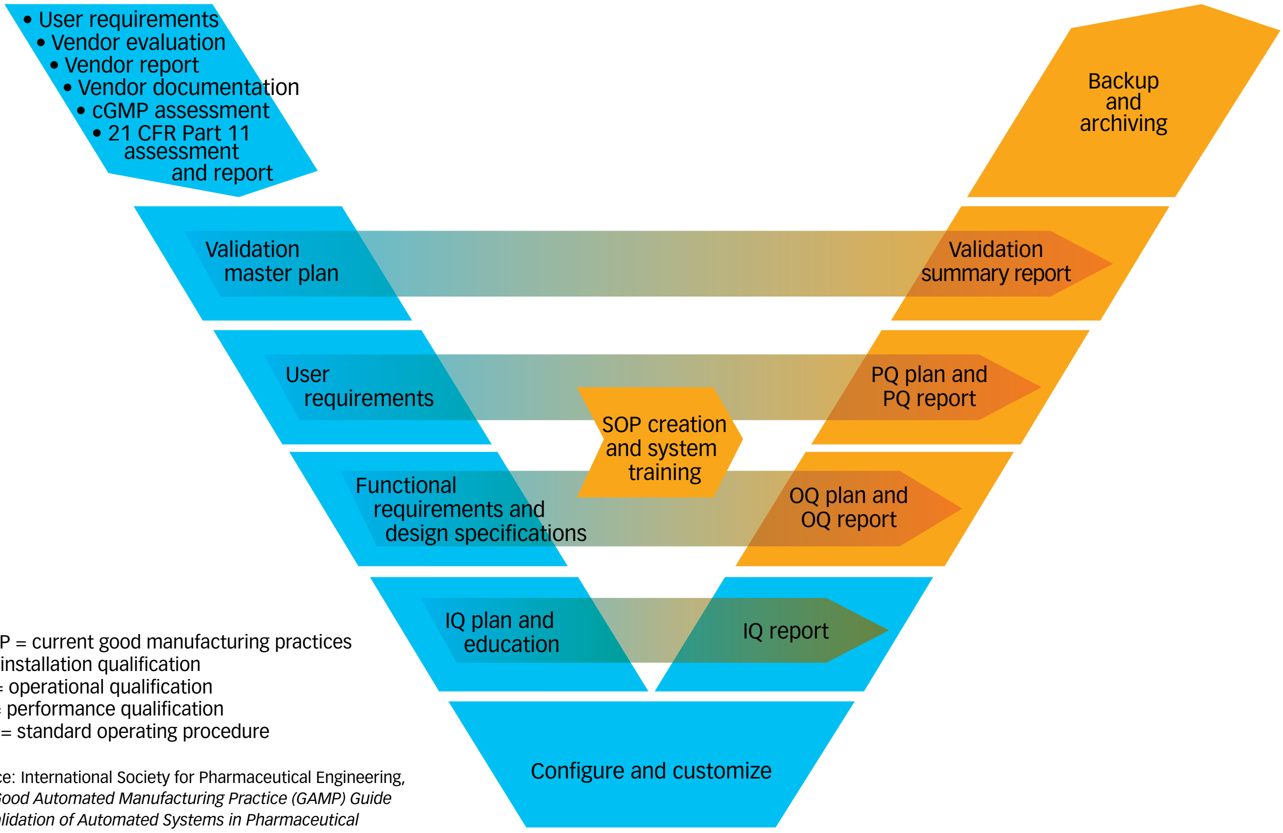
For example, one requirement is that an audit trail can be generated to record all changes made in the system, including the change itself, the user who made the change and the date of the change. A test protocol would be written and executed to verify that this requirement could be met and the actual test result matches the expected result defined in the test protocol. This provides evidence that the audit-trail requirements are indeed met.

Outsourcing comparison

A significant concern for organizations regulated by the FDA—or any comparable international agency—is the loss of direct control that occurs with the implementation of a SaaS system. Similar concerns exist regarding the outsourcing of other activities, such as engaging with a contract manufacturer.

These regulated organizations typically conduct

Computer system validation model / FIGURE 1



cGMP = current good manufacturing practices
IQ = installation qualification
OQ = operational qualification
PQ = performance qualification
SOP = standard operating procedure

Source: International Society for Pharmaceutical Engineering, *The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture,* version 5, January 2008.

an initial validation and subsequent related activities, such as change control and upgrades in their own facilities with their own trained personnel so the activities can be closely controlled and documented.

In a SaaS environment, most of these activities are conducted at the supplier's site with supplier personnel and without client personnel present. This loss of direct control is new and disconcerting to most regulated organizations.

Using and overseeing a SaaS system is analogous to overseeing other regulated outsourced activities. Outsourcing across the value chain has been increasing among life-sciences companies, and many regulated companies are moving toward virtual manufacturing, providing a framework for SaaS.

The general concept is that experts in a given arena provide the services they do best. The critical part is how these regulated companies leverage and manage the expertise. It is important to note that the regulated company—not the SaaS provider—is ultimately responsible for compliance with the applicable regulations.

Do your homework

A common practice among regulated companies is to perform an audit of the potential supplier's quality systems prior to the selection of a software system for traditional implementation.

Pre-selection and ongoing audits are of greater significance to SaaS suppliers than conventional software vendors because greater reliance is placed on a SaaS supplier's quality systems. So, in addition to the pre-selection audit criteria, a SaaS supplier audit should emphasize areas in which the SaaS supplier maintains control of specific processes, such as:

- Location and control of data centers used to store the software and client data.
- Change control of hardware and software for ongoing updates or upgrades.

- Data security—protection of data used by more than one organization from corruption and unauthorized access.
- Physical and logical security, such as user identification, passwords, and roles and privileges.
- Backup and recovery.
- Communication methods and timelines for customer notification of software updates or upgrades.

The history and past performance of the SaaS supplier also should be considered, along with the number and types of other customers successfully using the system. This is often a challenge because most SaaS applications for regulated operations are relatively new and therefore don't have an extensive history.

Given their **compelling business case,** it's no surprise that SaaS applications **are growing in popularity.**

Procedural updates

Site and corporate computer system validation procedures should be reviewed for compatibility with the SaaS model well in advance of initiating a SaaS project. These procedures would have been written to address conventional software applications and likely contain elements that are incompatible with a SaaS project and lack elements necessary for the validation of a SaaS system.

Procedures should be revised to include a framework for the management of SaaS providers and validation requirements for SaaS applications based on a risk assessment. Ample time must be allocated for revision, review and approval of the procedures to avoid a state of noncompliance with approved procedures.

Validation considerations

In many respects, the validation approach for a SaaS system is similar to that of a conventional system. The organization would still apply an overall risk-based approach, documenting business and regulatory risks, and areas needing more robust validation.

Factors contributing to the risk analysis include results of the vendor audit, criticality of the data and processes captured in the SaaS system, and the degree of customization—as opposed to configuration—of the SaaS application.

Perhaps the most significant concern regarding the validation and ongoing maintenance of SaaS systems is software updates. In FDA-regulated organizations, changes are reviewed and made, the version number of the software is advanced, and the testing is completed to maintain the validated state of the software.

The testing is performed using a computer system validation method depicted in Figure 1. Industry practice is to update software in a development environment, perform validation testing in a quality assurance environment and transfer the update to the production environment after successfully completing testing.

It's common for this process to occur annually for a specific software upgrade because it is a large undertaking. In contrast, SaaS suppliers commonly perform periodic software updates, often at specified times. For example, minor changes are made to the software weekly, while major changes are made quarterly.

Out of the loop

The reality of SaaS systems is that upgrades are performed by the supplier at the supplier's facilities, and they often occur with no regard for any validation activities that may be required by the client.

Indeed, the client typically does not have any input into when or how often upgrades are performed. Because of this, procedures must be established describing the update process, and should include how and when proposed changes are communicated to the client prior to the upgrade.

The procedure also should include a description of how the evaluation of proposed changes will be handled and documented by the client, and how feedback regarding supplier testing of the proposed changes will be handled. Test results can be either directly shared with the client, shared only if there was an issue or be available for review during an audit.

One area that may result in a contentious situation is customer evaluation of proposed software changes. Many SaaS providers are accustomed to operating in an environment in which changes are designed, planned and implemented internally with no or minimal communication with their customers. FDA-regulated organizations will require that the proposed change be reviewed and tested, and the results documented in a manner that complies with the applicable regulations and supporting procedures.

Many SaaS providers have a variety of customers, most of which are not regulated by the FDA and are not accustomed to meeting these requirements. The SaaS suppliers may view the specific requirements of one—or a very small percentage—of their customers to be excessively burdensome and may resist.

In compliance

Organizations that must comply with a set of regulations must have some degree of creativity and mutual understanding to reach an agreement that satisfies the SaaS provider and the regulated customer.

In most cases, qualification of infrastructure—hardware such as servers and cables—can be performed in a manner similar to that of traditional applications. Many SaaS suppliers maintain a robust infrastructure qualification and change-control system, but potential red flags for FDA-regulated clients include cases in which the provider does not and will not perform adequate infrastructure qualification.

For example, the supplier may move data from one server to another at a different location without proper qualification or may not maintain adequate documentation. These types of issues present challenges similar to those encountered when dealing with suppliers of conventional software systems that do not understand the needs of regulated customers.

Physical and logical security, backup, recovery and disaster recovery can be addressed in the same way as conventional software validation. The important distinction is that these elements be addressed at all relevant locations and properly documented. Some SaaS suppliers use secondary or backup locations in addition to their primary location, and there can be a tendency to overlook procedures at the backup locations.

Conventional software validation occurs when an organization's personnel follows its procedures at its own facility. SaaS validation typically occurs off site with SaaS supplier personnel performing much of the work. Diligence must be exercised to ensure the SaaS supplier personnel are properly trained in the applicable validation procedures, whether these procedures are provided by the SaaS supplier or the client.

For situations in which SaaS supplier procedures are used, the adequacy of these procedures should be verified during the vendor audit. These procedures should be referenced in the project validation plan.

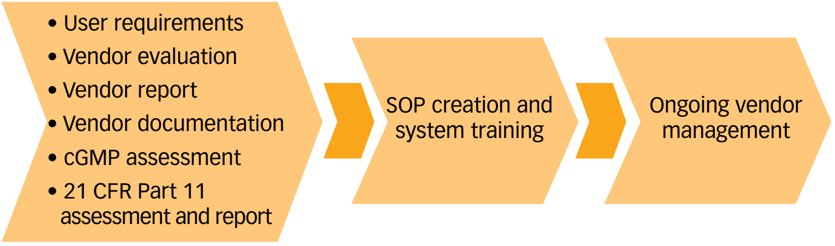
Working together

One last validation consideration is the interfaces between a SaaS system—regardless of whether it contains FDA-regulated information—and a customer's validated systems. These interfaces must be identified and validated.

For example, an organization may interface its own learning management system with a SaaS human capital management application. The learning management system contains employee training records, and because maintaining employee training records is a requirement for FDA-regulated organizations, the learning management system is fully validated.

In this case, the nonvalidated SaaS human capital management system transfers employee data to the learning management system through an interface that must be validated to ensure data integrity. This can be

SaaS validation approach / FIGURE 2


• User requirements
• Vendor evaluation
• Vendor report
• Vendor documentation
• cGMP assessment
• 21 CFR Part 11 assessment and report
SOP creation and system training
Ongoing vendor management

cGMP = current good manufacturing practices
SOP = standard operating procedure

SaaS applications **are here to stay.** Their presence in the marketplace will grow as more organizations **leverage the applications' advantages.**

accomplished in a similar fashion as for conventional software systems.

It's all too easy to overlook the validation of interfaces, particularly when the SaaS system being deployed is classified as nonregulated but still interfaces with validated systems.

The validation approach for SaaS is similar to that for a conventional software system (see Figure 2, p. 29). An assessment of applicability of FDA regulations to the system—known as a current good manufacturing practices assessment—is performed to confirm that the system falls under the regulation and requires formal validation.[3] User requirements are defined and used as criteria for choosing the software.

The vendor audit becomes more significant because it will be leveraged for ongoing management of the vendor. Most, if not all, of the typical validation deliverables—such as installation, operational and performance qualifications—may take on a different format because testing will be handled by the SaaS provider.

An exception is interfaces, which the organization must address. Management tools specific to the organization, such as a quality agreement, would be included in the ongoing vendor management, as is typical for managing outsourced activities.

The introduction of a new validated system requires introducing supporting standard operating procedures and providing training for the users. Ongoing monitoring of the SaaS supplier's quality systems and periodic audits also are part of the process.

Adapting for the future

SaaS applications are here to stay. Their presence in the marketplace will continue to grow as more companies leverage the applications' advantages. This means SaaS providers interested in marketing their applications to companies in FDA-regulated industries will need to understand regulatory requirements and take the proper steps to ensure compliance.

In addition, regulated organizations must expand their computer systems integration and validation perspectives beyond conventional applications to include management of SaaS applications vendors.

To put it simply, organizations must manage SaaS providers to ensure the delivery of reliable and secure services just as they would manage other third-party services, such as raw-material procurement, contract manufacturing or product distribution.

These new relationships will require some understanding and education by the SaaS suppliers and the firms purchasing their services. The upside is that the technologies for compliant software systems already exist, as do the validation methods to support them. It's just a matter of the suppliers and the purchasers adapting them to the SaaS model. QP

REFERENCES

1. PR Newswire, "New InformationWeek Analytics Research Finds 60% of Companies Using Applications in the Cloud," April 19, 2011, www.prnewswire.com/news-releases/new-informationweek-analytics-research-finds-60-of-companies-using-applications-in-the-cloud-120196859.html.
2. U.S. Food and Drug Administration, "Code of Federal Regulations Title 21," www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=11.
3. International Society for Pharmaceutical Engineering, *The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture*, version 5, January 2008.

BIBLIOGRAPHY

U.S. Food and Drug Administration, "General Principles of Software Validation; Final Guidance for Industry and FDA Staff," Jan. 11, 2002, www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm085371.pdf.

JIM DOUGHERTY is a director at Clarkston Consulting in Durham, NC. He earned an MBA from the University of North Carolina-Greensboro. A senior member of ASQ, Dougherty is an ASQ-certified quality engineer.

WYLENE LENGEL is a director at Clarkston Consulting. She earned an MBA from Wichita State University in Kansas. Lengel is a senior member of ASQ and an ASQ-certified quality auditor and engineer.