Considerations for validating SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System per the GAMP 5 guide

This white paper describes requirements that should be considered in order to validate Applied Biosystems™ Sequence Detection System (SDS) Enterprise Edition Software v2.x for the computerized Applied Biosystems™ 7900HT Fast Real-Time PCR System in accordance with the Good Automated Manufacturing Practice (GAMP™) 5 Guide for Validation of Automated Systems in Pharmaceutical Manufacture. The principles and approach outlined in the GAMP 5 guide were developed by the International Society for Pharmaceutical Engineering (ISPE) based on input from pharmaceutical industry professionals in an effort "to narrow interpretation of regulatory standards for improved compliance and quality, efficiency, and cost reductions" [1].

What is computer system validation?

Validation of computer systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records is a critical requirement of electronic record compliance, as described in the FDA 21 CFR Part 11 and EMA Annex 11, Section 4 [2,3].

Recommendations on how SDS Enterprise Software v2.x can be implemented for compliance with 21 CFR Part 11 are shown in Table 2 at the end of this document. Computer system validation (CSV) is distinct from hardware qualification (such as Installation Qualification (IQ)/ Operational Qualification (OQ)/Instrument Performance Verification (IPV)) [4].

Confirmation of conformity to user needs ("intended use") is obtained by comparing actual system performance to predetermined requirements. This is accomplished by executing test procedures and collecting objective evidence (computer-screen captures, printed reports, data files, etc.). The point is not to produce a mountain of documentation, but to demonstrate that validation activities were properly planned, and that the tests were executed according to the plan.

Computer system validation is distinct from assay validation or method validation. To help ensure that you understand your system's limitations and your operational readiness, it is advisable to complete your hardware qualification and CSV prior to validating your assay(s). Changes to a system in response to CSV could impact assay validation.

Who is responsible for validation?

Under the (European) Organisation for Economic Co-operation and Development (OECD) regulations, validation is the responsibility of the "test site management". In good laboratory practice (GLP), validation is the responsibility of the "system owner" or "business process owner" [5]—often this is the laboratory manager. While the laboratory manager may have ultimate responsibility for validation, the validation team should include representatives from all stakeholders. The quality assurance team certainly has a role to play in validation, ensuring thorough review to help verify that all company policies are met. Upper management also plays a key role, because they provide the impetus and resources for validation. They will also have ultimate responsibility if validation efforts prove to be inadequate.

Organizations can enlist third parties to design and perform system validation, but responsibility for the validation, compliance, and maintenance of a compliant validated state cannot be delegated and remains with the system owner.

To validate or not?

The most important update in the GAMP 5 guide over previous versions is the focus on risk management [6]. GAMP 5 requires "validation if there could be an impact on … product quality, or data integrity" [7]. Therefore, the decision to validate, what to validate, and how to validate is largely an exercise in risk management.

In other words, risk should be assessed based on critical functionality. For example, in SDS Enterprise Edition software, acquisition of sample data would be more critical than formatting reports. Therefore, more in-depth validation testing would be needed for sample data acquisition.

The GAMP 5 guide also recognizes that higher system complexity increases the likelihood of risk [4]. For example, a system configured to use SDS Enterprise Edition software in conjunction with a remote Oracle™ database for centralized security and file management would be more complex than a stand-alone system using a local PC. Therefore, additional tests would be required to validate the system with the remote server.

Validation throughout a system's lifecycle: prospective vs. retrospective

Ideally, the validation process should begin at the earliest stages of system procurement. Since one of the main goals of CSV is to document that the system fulfills "user needs" and that the requirements of the software "can be consistently fulfilled," outlining the precise requirements of the system is an essential first step. Basing procurement decisions on an explicit understanding of the needs of stakeholders and validation requirements helps to ensure that a new system is an appropriate choice for the lab—and simultaneously helps to fulfill CSV requirements.

In practice, however, validation is sometimes needed for existing systems. Whether this is required due to system changes or is the initial validation of a preexisting system, it is essential to capture system requirements and verify that those requirements are met.

A final consideration is that planning for the ultimate retirement of the system, and the data it generates, is also part of the validation process.

The cost of compliance vs. noncompliance

Deciding to forego validation when it is required could mean that an organization accepts the risk of noncompliance with applicable requirements. Companies are sometimes reluctant to invest in validation efforts that may cost several thousand dollars. This has proven to be a short-sighted strategy in many cases. A brief review of recent judgments against pharmaceutical companies and independent/contract labs reveals that the cost of noncompliance can be millions of dollars along with lost revenue and productivity, possible process rework, and damaged investor and customer confidence and goodwill.

Balancing risk and validation cost

Compliance could be accomplished by validating critical subsystems thoroughly while minimizing the validation effort for less critical functions. This approach does not eliminate risk but could reduce it to manageable levels, controlling validation effort and expense. In contrast, fully validating all components of a system further minimizes risk, but with a higher cost that is not necessarily commensurate with the level of risk reduction.

Building blocks for compliance controls

Technical and procedural controls

Consider design and placement of appropriate system controls for compliance. Controls can be classified as either technical or procedural. Technical controls are enforced through hardware and software. They reduce human effort through automation, thereby reducing the incidence of human error. Procedural controls are processes that are documented, approved, and enforced—typically in a standard operating procedure (SOP).

An example of a system component with both technical and procedural controls is a lab door with an electronic lock. Procedurally, the lab should have an SOP describing the assignment, distribution, and maintenance of identification (ID) devices such as pass codes, ID cards (or badges), or biometric identification equipment. The devices themselves are considered technical controls because the door lock uses hardware and software to allow or deny entry to the lab.

A procedural control could instruct users to "identify" themselves with a pass code or ID card to the lock in order to open the door. It could further specify that pass codes or ID cards should remain in the sole possession of the employees to whom they were assigned. If an employee were to loan an ID device to another employee, who then used it to access a restricted area, the procedural control would be compromised.

This example illustrates why it is important to put both technical and procedural controls in place.

SOPs

Since some requirements, such as training, cannot be met using technical controls, but should be satisfied through procedural controls, SOPs are an important part of system controls. Examples of important SOPs include the following:

- Issuance and control of usernames and passwords
- System access assignment and revocation
- Training procedures
- Change control procedures
- Documentation maintenance procedures
- Backup and restoration of data
- Archiving and retrieving of data

It is also advisable to document your company's computer system validation procedures and electronic signature policies (if applicable) in SOPs.

Change control

Validation efforts for the SDS Enterprise v2.x system should encompass the entire system lifecycle, from inception to retirement. Yet, change is inherent in any computerized system. As new requirements are identified, errors are found, and procedures are revised, changes to the system could become necessary. It is essential to carefully control any changes to a validated system through documentation, analysis, and testing. Furthermore, since changes to one subsystem might affect other, seemingly unrelated parts of the system, change analysis should include assessment of impacts to the entire system. It is not adequate to test only the change; testing should also include any potentially impacted functionality. The most important tool for maintaining a system in its validated state is the change control procedure. At a minimum, changes should be requested in writing via a change request. These should be analyzed and approved by the technical personnel and key stakeholders involved. In addition, the risk assessment for the system may need to be updated. Finally, change requests should be approved by the quality assurance unit and the system owner or equivalent, and the change control process should be documented in an SOP. By carefully following a predefined plan for evaluating and approving changes to the system, the physical environment, and the procedural environment, a system can be maintained in a validated state over time.

Failure to properly control and document system changes could result in a system that is no longer validated, exposing the business to noncompliance risk.

Important updates in the GAMP 5 guide

GAMP 5 software categories

Previous versions of the GAMP™ Good Practice Guide: Validation of Laboratory Computerized Systems classified computer software in five categories [7]. There were some changes to categorization of software introduced in the GAMP 5 guide and category 2 was discontinued, but the remaining categories were not renumbered. Therefore, SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System remains in category 4: configurable commercial off-the-shelf (configurable COTS) software [8].

SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System is classified as configurable because it accommodates the storage and persistence of usernames, passwords, customized audit trails, and instrument configuration. The effort required to validate a configurable system such as SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System is greater than that required to validate operating systems, firmware, and standard software functions such as simple arithmetic in Microsoft™ Excel™ software.

SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System provides an application programming interface (API) in Java™, which can be used to customize the application. Custom or bespoke software (GAMP 5 category 5) requires an even greater validation effort.

GAMP 5 guide increases supplier quality awareness for configurable and networked systems

The GAMP 5 guide recognizes that most computerized systems are now based on configurable packages that utilize computer networks (Figure 1). Therefore, it recommends that software-validation testing should focus on the specific configuration of the software program rather than on its core operational characteristics, especially when the system supplier can demonstrate that its core operational functionality was tested [9]. Because of these revisions, supplier audit programs have more importance in the GAMP 5 guide; increasingly, system-supplier certificates are accepted in lieu of actual supplier audits.

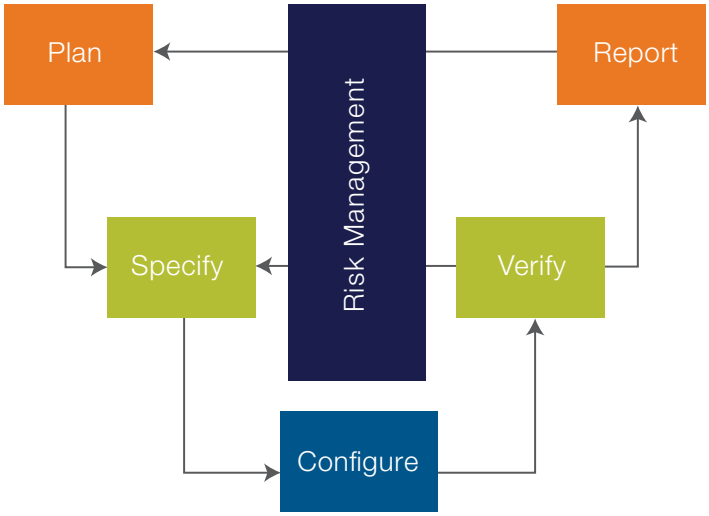

Figure 1. GAMP 5 validation lifecycle [1]. Because the GAMP 5 guide recognizes that most systems are configurable software, it suggests a simplified "V" validation lifecycle as shown here.

Important validation documents

At a minimum, the validation documentation set should contain documents 01 through 08, 10, and 12 described in Table 1. We provide documents 09 and 11 for CSV of SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System. Table 1 also includes a mapping of these documents to the GAMP 5 validation lifecycle.

Table 1. Software validation document descriptions and their relation to the GAMP 5 validation lifecycle.

Validation document	GAMP 5 guide lifecycle category	Description
01. Validation Plan (VP)	Plan	The VP is a key strategic planning document [9] that describes the entire validation effort and covers the system lifecycle from inception to retirement. The VP is the key to controlling the validation project. At a minimum, the VP should describe the scope of the validation project, the work to be done, the order of activities, and the individuals responsible for planning, execution, testing, and approval. Additionally, instructions for testing including protocol execution and collection of objective evidence, as well as post-validation activities, deliverables, and instructions for identifying and documenting exceptions, may be included in the VP or the test plan depending upon the needs of the system owner.
02. Validation Risk Assessment (VRA)	Plan and Risk Management	The VRA documents system operation risks and their impact in accordance with GAMP 5 guidelines and includes prescribed mitigations for each risk.
03. User Requirements Specification (URS)	Specify	The URS objectively states the system requirements. It should address technical controls, procedural controls, capacities, accuracy, security, fault tolerance, physical environment, and training requirements, among others, for SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System. It is critical that the URS be a complete statement of the needs and objectives of the acquiring organization. A typical URS may contain up to several hundred unique requirements.
04. System Configuration Specification (SCS)	Specify and Configure	Because SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System is configurable, it is adaptable to variations in instrument and peripheral equipment setup, security, and data processing. Therefore, it is necessary to describe the intended configuration in an SCS. Some examples of features of the SDS Enterprise Software v2.x for the 7900HT Fast Real-Time PCR System that are addressed in the SCS are: security and user roles, audit trail settings, equipment configuration, and quantitation settings. Because SDS Enterprise Edition Software v2.x is a configurable COTS system, as the vendor we document the design and development of the software. The SCS replaces the more "traditional" functional and design specifications used in validation of a GAMP 5 category 5 system.

Validation document	GAMP 5 guide lifecycle category	Description
05. Test Plan	Plan	The test plan is designed to address all testable user requirements. At a minimum, it serves as a forward-pointing traceability matrix showing the relationship of the tests to the user requirements. The test plan may also include general instructions for test execution, documentation, and the gathering of objective evidence. It may also define the data types and environments necessary to perform testing.
06. Installation Qualification (IQ)	Configure and Verify	The qualification of SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System can be separated into four phases: Design Qualification (DQ), Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ). Since it is not always clear in which phase a particular requirement or test belongs, the following guidance may be helpful.
07. Operational Qualification (OQ)	Verify	
08. Performance Qualification (PQ)	Verify	Since SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System is GAMP 5 category 4 software, as the vendor we perform the DQ. This can be verified by performing a vendor audit or accepting vendor certifications. We provide a standard postal audit that addresses the common elements of a vendor audit. It identifies the development and verification methodologies and the quality standards, such as ISO 9001 implemented by us. IQ, OQ, and PQ testing involves the execution of a defined set of tests using test scripts that contain the instructions, expected result, and acceptance criteria. They also include a section for the person conducting the test to record whether the system passed or failed. Ideally, test scripts reference each applicable requirement outlined in the test plan specifically. Several requirements may be addressed by a single test script, and conversely, some requirements may require more than one test. Normally, test scripts address a specific range of functionality, such as security or data acquisition. Test scripts should be logically designed, and should include both positive and negative tests. For example, a test for password acceptance will include procedures to verify the result of entering a valid password, as well as the result of entering an invalid password. If a test step fails, then additional documentation is required (usually in the form of deviation or exception logs and reports). The documentation should identify the nature of the exception, the test script or procedure where the exception occurred, proposed corrective action, and responsibility for implementation, verification, and acceptance.
09. 21 CFR Part 11	Configure and Verify	SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System has features that could be configured to help meet the requirements of US FDA 21 CFR Part 11: Electronic Records and Electronic Signatures. Part 11 regulates the security, reliability, and integrity of laboratory data, and the security and integrity of electronic signatures. The predicate rules contain relatively few signature requirements. Where signatures are required, such as in a data audit trail, Part 11 defines how an electronic signature should be derived and the meaning of the electronic signature. Many Part 11 requirements will be met with a combination of technical and procedural controls. The Part 11 Assessment (Table 2) contains a checklist that assists with compliance with Part 11 through system functionality and procedural control. Note: SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System assists with compliance with Part 11 once the software has been configured correctly and appropriate SOPs are in place.
10. Traceability Matrix (TM)	Plan, Verify, and Report	The TM shows the relationship between each user requirement and a corresponding test script (in the case of technical controls) or SOP (for procedural controls). The TM makes it possible to confirm that each user requirement has been addressed and satisfied by the validation process.

Validation document	GAMP 5 guide lifecycle category	Description
11. Quality Assurance Unit (QAU) Review	Verify and Report	The customer's quality assurance (QA) or quality control (QC) department should be actively engaged in the validation effort. Management approval of validation generally depends on the recommendation of the QAU. Fortunately, the GAMP 5 guide simplified the document approval process. The QAU should ensure that documents meet applicable regulations, but technical experts are now empowered to approve technical documentation. For example, the QAU should review a URS for compliance with the applicable regulations, but the URS technical review is the responsibility of technical subject matter experts. Thus, the QAU no longer needs to sign a configuration specification because they can rely upon technical subject matter experts. For example, the QAU should verify that configuration specifications are being produced for projects (i.e., verify that processes are being followed) but the QAU does not need to sign every document in a project [1]. After a final review for completeness, the QAU should submit recommendations to management regarding the release of the system for use. Consider including the QAU in the validation effort throughout the lifecycle to help ensure that the QAU can recommend the release of the system. The QAU review document provides a checklist to help ensure that the requirements have been completed and test criteria have been met. It also requires signatures denoting the pass/fail status of all validation documents. Note that in some GMP environments, the QAU will have final approval responsibility in addition to simple review and recommend responsibility.
12. Validation Summary Report (VSR)	Report	The VSR contains the results of the software validation project, including a summary of the plan execution and the decision as to whether the system passed or failed. The VSR is often the starting point for regulatory auditors.

It is important for the validation document set to be well organized. This can be accomplished by numbering the documents in a clear, easy-to-read manner. For example, each document is numbered 01–12 as shown above. Each document also has a code corresponding to the company, document, and version, such as CMPY-SCS-01 in the example shown in Figure 2, which is the typical introduction section in the document set for SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System. This type of cross-referencing makes the CSV document set easy to use and modular, and can assist any auditor in finding information quickly.

1. Introduction

Terms used in this document:

VENDOR	Thermo Fisher Scientific
COMPANY	Company name (CMPY)
TEAM	SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System Validation Project Team defined in the Software Validation Plan CMPY-SVP-01
SYSTEM	Defined in the System Configuration Specification CMPY-SCS-01
IQ	SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System Installation Qualification created by the TEAM in accordance with the Software Validation Plan CMPY-SVP-01

Figure 2. Example of a typical introduction section in the document set of SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System.

Replicated system validation

When more than one instrument is being installed in a laboratory at the same time, it would be redundant and costly to perform a complete software validation on each system. The following are guidelines for tailoring the software validation for replicated systems.

First, the VP should describe that several instruments are being validated at the same time. The strategy is to test all requirements on one system called "first in family," then test a subset of requirements on the replicated systems.

The test plan should denote tests to be performed on the first in family and tests to be performed on replicated systems. Tests to be performed on replicated systems include security, audit trail configuration, and acquisition settings. Thus, testing is limited to confirming that the configuration is correct. Additionally, a small number of samples should be run on each instrument to ensure the instrument is acquiring data properly. Quantitation validation would not be necessary, nor would testing reporting, because these functions have been tested on the first in family.

There should be two sets of IQ/OQ/PQ protocols, one for the first in family and one for replicated systems. The validation TM should trace both the first in family and the replicated systems. More than one trace table may be required. The VSR should list the validation status of each system and any anomalies encountered for each system.

Conclusion

Validation of SDS Enterprise Edition Software v2.x for the 7900HT Fast Real-Time PCR System need not be an onerous undertaking. By adopting the best practices prescribed by the GAMP 5 guide and other regulatory bodies and professional societies, validation can be performed efficiently. The GAMP 5 guide introduced some changes to software validation. These include:

- Validation based on risk management, with more testing required for functionality that could impact product quality or data integrity
- Increased awareness of configurable and networked systems
- Changes to the "V" validation lifecycle using risk management
- Simplified document approval process

In addition to regulatory compliance, the processes and business objectives of the organization could be enhanced by proper validation, and much of the overall risk to a business and its processes could be mitigated.

Contact us

Contact your sales representative or email our compliance services at **compliancesales@thermofisher.com** for information on services available to assist you with your SDS Enterprise Edition Software v2.x validation. SDS Enterprise Edition Software v2.x validation support is only available for the 7900HT Fast Real-Time PCR System, which is indicated For Research Use Only.

References

1. International Society for Pharmaceutical Engineering. http://www.ispe.org/gamp-5. Accessed August 25, 2016.
2. *GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems.* (2008) International Society for Pharmaceutical Engineering. 356 pp.
3. *IEEE 1012-2016, IEEE Approved Draft Standard for System, Software and Hardware Verification and Validation.* (2016) The Institute of Electrical and Electronic Engineers. 118 pp.
4. *GAMP Good Process Guide: Validation of Laboratory Computerized Systems.* (2005) International Society for Pharmaceutical Engineering. 96 pp.
5. Organisation for Economic Co-operation and Development. http://www.oecd.org. Accessed August 25, 2016.
6. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff.* (2002) U.S. Department of Health and Human Services, Food and Drug Administration.
7. *GAMP 4 to GAMP 5 Summary.* (2008) International Society for Pharmaceutical Engineering. 10 pp.
8. *Holistic Approach to Science-based Risk Management.* 13 March 2008. GAMP 5 Newsletter.
9. Martin KC, Perez A (2008) GAMP 5 Quality Risk Management Approach. *Pharmaceutical Engineering* 28(3).

Appendix

Table 2. Recommendations on how SDS Enterprise Edition Software v2.x can be implemented to support compliance with FDA 21 CFR Part 11.

21 CFR Part 11 section reference	21 CFR Part 11 requirement	Technical and procedural controls
§11.10 Controls for Closed Systems		
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include:		
11.10(a)	• Validation of the system to ensure accuracy, reliability, and consistent intended performance	This could be demonstrated through the entire process of validation including IQ, OQ, and PQ testing.
	• Validation of the system with the ability to discern invalid or altered records	SDS Enterprise Edition Software v2.x maintains checksums on the data. The checksums are designed to prevent unauthorized records from opening.
11.10(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by agency.	If configured correctly, reporting functionality could satisfy this requirement.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	This could be satisfied through customer SOPs for record backup and data archiving.
11.10(d)	System access limited to authorized individuals.	The software includes user authentication and access permission functionality that could be configured to limit system access.
11.10(e)	Audit trails shall be used that:	SDS Enterprise Edition Software v2.x includes this audit trail functionality.
	• Are secure, computer generated, and time stamped	
	• Independently record the date and time of operator entries and actions that:	
	– Create electronic records	
	– Modify electronic records	
	– Delete electronic records	
	• Ensure that record changes do not obscure previously recorded information	
	• Audit trail documentation is retained for a period at least as long as that required for the subject electronic records and is available for agency review and copying.	This could be satisfied through customer SOPs for record backup and data archiving. Audit trail information is stored by the software in the same manner as actual data.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	This could be demonstrated through the functionality of the software itself. It has built-in checks to ensure that steps are carried out in sequence. Steps and events that occur outside the software should be defined in SOPs and protocols.
11.10(g)	Use of authority checks to ensure that only authorized individuals can:	User authentication and access permissions within the software provide this functionality.
	• Use the system and access the operation or computer system input or output device	
	• Electronically sign a record	
	• Alter a record	
	• Perform the operation at hand	
11.10(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	The software has built-in checks designed to ensure that there cannot be incorrect inputs.
11.10(i)	Determination that the following persons have the education, training, and experience to perform their assigned tasks:	
	• Developers of the system	Software release certificates from the vendor showing compliance with ISO standards could satisfy this requirement.
	• Maintainers of the system	Maintenance contract with vendors or trained staff and SOPs could satisfy this requirement.
	• Users of the system	Customer training SOPs and training records should be maintained.

21 CFR Part 11 section reference	21 CFR Part 11 requirement	Technical and procedural controls
11.10(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Customer SOPs could satisfy this requirement.
11.10(k)	Use of appropriate controls over systems documentation, including:	
11.10(k)[1]	• Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance	Customer SOPs could satisfy this requirement.
	• Adequate controls over the access to documentation such as directions for modifying security features	Customer SOPs could satisfy this requirement.
11.10(k)[2]	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Customer SOPs could satisfy this requirement. Vendor is ISO certified and maintains revision control of published documentation.
§11.30 Controls for Open Systems		
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.		
11.30	Controls in place to protect open systems as effectively as closed systems.	Not applicable. SDS Enterprise Edition Software v2.x is a closed system.
§11.50 Signature Manifestations		
Signed electronic records shall contain information associated with the signing that clearly indicates the following:		
11.50(a)[1–3]	• The signer's printed name • The date and time when the signature was executed • The meaning (such as review, approval, responsibility, or authorship) associated with the signature	If configured correctly, reporting functionality in SDS Enterprise Edition Software v2.x could meet this requirement.
§11.70 Signature/Record Linking		
Electronic signatures are linked:		
11.70	To their respective electronic records to ensure that the signatures cannot be excised, copied, or transferred to falsify an electronic record by ordinary means.	The records and electronic signatures are relationally linked to each other through tables using keys and unique identifiers in a relational database management system. Due to the design of the scheme as well as security controls, the signatures cannot be decoupled from their respective electronic records.
§11.100 General Requirements		
11.100(a)	Each electronic signature is unique to one individual and is not to be reused by, or reassigned to, anyone else.	This is done in the software itself and can also be mandated by customer SOPs.
11.100(b)	The organization verifies the identity of the individual before the organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature.	This is a responsibility of the customer and should be defined in a customer's SOP.
11.100(c)[1–2]	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	This is a responsibility of the customer and is independent of the system.
§11.200 Electronic Signature Components and Controls		
Electronic signatures that are not based upon biometrics:		
11.200(a)[1]	Employ at least two distinct identification components (e.g., ID code and password).	Electronic signature functionality requires both username and password.

21 CFR Part 11 section reference	21 CFR Part 11 requirement	Technical and procedural controls
11.200(a)[1i]	• When an individual executes a series of signings during a single continuous period of controlled system access, the first signing is executed using all electronic signature components; subsequent signings are executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	Electronic signature functionality requires both username and password for initial signing and, at minimum, the password for subsequent signings in a session.
11.200(a)[1ii]	• When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing is executed using all of the electronic signature components.	Initial electronic signature functionality requires both username and password.
11.200(a)[2]	Are used only by their genuine owners.	This is a responsibility of the customer and should be defined in an SOP concerning logical security.
11.200(a)[3]	Are administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	System requires username and password. Password control is a responsibility of the customer and should be defined in a customer's SOP concerning logical security and electronic signature usage.
11.200(b)	Electronic signatures based upon biometrics are designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable. System does not employ biometrics.
§11.300 Controls for Identification Codes/Passwords		
Persons who use electronic signatures based upon the use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall:		
11.300(a)	Maintain uniqueness of each combined ID code and password pair such that no two individuals have the same combination of ID code and password.	Software will not allow identical usernames to be created more than once.
11.300(b)	Ensure ID code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Password aging is an SDS Enterprise Edition Software v2.x function. Use of aging and all other aspects of this requirement are the responsibility of the customer and should be defined in customer's SOPs.
11.300(c)	Provide that loss management procedures exist to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate ID code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Not applicable. Token access is not used by the system.
11.300(d)	Provide that transaction safeguards exist to prevent unauthorized use of passwords and/or ID codes, and to detect and report any attempts at their unauthorized use to the administrator and as appropriate, to management.	Users are locked out for a configurable period of time if incorrect passwords are entered consecutively. In addition, administrators can be notified or actively monitor the system for failed access attempts.
11.300(e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information, to ensure that they function properly and have not been altered in an unauthorized manner.	Not applicable. Token access is not used by the system.

Find out more at **thermofisher.com/complianceservices**