Services and support

Considerations for validating instrument software per the GAMP 5 guide

This white paper describes requirements that should be considered in order to validate the Applied Biosystems™, Invitrogen™, and Ion Torrent™ instrument software 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?

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

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.) to demonstrate that validation activities were properly planned, and that the tests were executed according to the plan.

Computer system validation (CSV) is distinct from assay validation or method validation. It is also distinct from instrument hardware qualification (such as installation qualification (IQ)/operational qualification (OQ)/instrument performance verification (IPV)/ performance qualification (PQ)) [4]. To help ensure understanding of system limitations and operational readiness, it is advisable to complete instrument hardware qualification and CSV prior to validating assay(s). Changes to a system in response to CSV could impact assay validation.

Recommendations on how the instrument software can be implemented for compliance with 21 CFR Part 11 are shown in the Appendix (Table 2) at the end of this document.

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. 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]. The GAMP 5 guide 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 an exercise in risk management.

Risk should be assessed based on critical functionality. For example, in the Applied Biosystems™ 3500 Series Data Collection Software System, acquisition of sample data would be more critical than formatting reports. Therefore, more in-depth validation testing would need to be defined and created for sample data acquisition, and prioritized over report formatting.

The GAMP 5 guide recognizes that higher system complexity increases the potential for risk and the need to mitigate it [4]. For example, a system configured to transfer data to secondary analysis software would be more complex than a stand-alone system. Therefore, additional tests would be required to validate the system.

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

Validation should begin with the process 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-intended use—and simultaneously helps to fulfill CSV requirements.

However, validation is sometimes also needed for installed systems. Whether this is required due to changes in the system or is the initial validation of a preexisting system, it is essential to capture system requirements and verify that those requirements are met. For example, transferring a system from R&D to a preclinical environment would require a CSV.

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, and issues such as data and method transfer should be considered.

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

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. Compliance can 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.

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 an instrument 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 could present risk. A change analysis should be performed including risk 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. Typically, changes would 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, Applied Biosystems, Invitrogen, and Ion Torrent instrument software remain in category 4: configurable commercial off-the-shelf (COTS) software [8].

The instruments are classified as configurable because they accommodate the storage and persistence of usernames, passwords, customized audit trails, and instrument configuration. The effort required to validate a configurable system such as the 3500 Series Data Collection Software System is greater than that required to validate operating systems, firmware, and standard software functions such as simple arithmetic in Microsoft™ Excel™ software.

The 3500 Series Data Collection Software System provides command-line interface (CLI) utilities that allow automation or semi-automation of certain tasks. These utilities can be used to customize the application. Custom 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.

Important validation documents

The validation documentation set contains documents 01 through 08, 10, and 12 described in Table 1. We provide documents 09 and 11 for CSV of the applicable instrument software. Table 1 also includes a mapping of these documents to the GAMP 5 validation lifecycle.

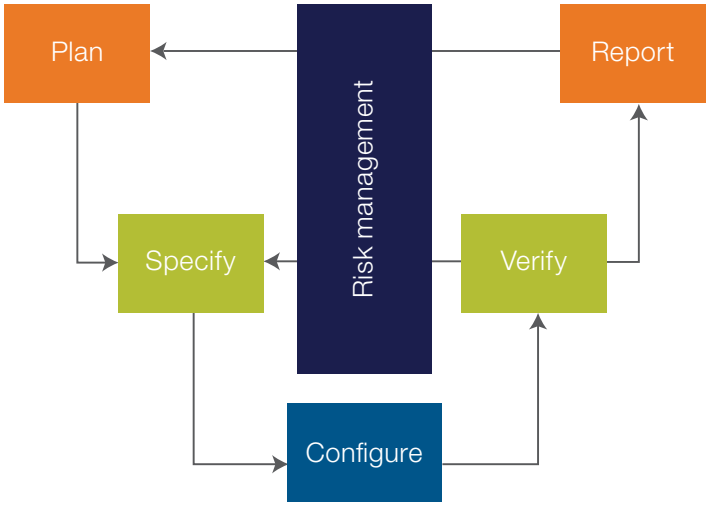

Figure 1. GAMP 5 validation lifecycle [1]. Because the GAMP 5 guide recognizes that most systems are configurable software, it suggests a simplified "V" validation lifecycle as shown here.

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 document that is essential to the success of the validation project. The VP defines the scope of the validation effort and key documentation deliverables. The VP will describe components such as the system lifecycle from inception to retirement, system application, scope of work, order of activity, and responsible individuals, as well as any relevant details for testing, including collection of objective evidence, and exceptions.
02. Validation risk assessment (VRA)	Plan and risk management	The VRA documents identified operation risks of the system, impacts, and prescribed mitigations in accordance with GAMP 5 guidelines.
03. User requirements specification (URS)	Specify	The URS objectively states the system requirements. The URS includes details such as technical controls, procedural controls, capacities, accuracy, security, fault tolerance, and physical environment, among others defined. It is critical to the validation success that the URS be a complete statement of the needs and objectives of the acquiring organization.
04. System configuration specification (SCS)	Specify and configure	The SCS objectively describes the organization's intended configuration, including any variations in the instrument, peripheral equipment, security, and data processing. As the vendor, we will provide documentation for the design and development of software for a COTS system. This document replaces a functional and design specification document in a traditional validation of a GAMP 5 category 5 system.

Validation document	GAMP 5 guide lifecycle category	Description
05. Test plan	Plan	The test plan describes all testable user requirements identified. The test plan and its objective results are linked to the traceability matrix for closure. The test plan supplements the validation plan with details for test execution, collection of objective evidence, and documentation.
06. Installation qualification (IQ)	Configure and verify	The IQ, OQ, and PQ are three phases of testing that involve the execution of a defined set of tests referenced in the test plan, using specific scripts, instructions, results, and acceptance criteria.
07. Operational qualification (OQ)	Verify	Tests in an IQ include verification that the system, including the software, was correctly installed.
08. Performance qualification (PQ)	Verify	Tests in an OQ include verification that the system is performing as configured in the SCS. There may be separate tests for secondary analysis software identified for use as part of the SCS. Tests in a PQ include performing an application run, and generating reports in both primary and secondary analysis software if applicable.
09. 21 CFR Part 11	Configure and verify	US FDA 21 CFR Part 11 provides guidance to industry on the security, reliability, and integrity of laboratory data as it relates to use of electronic records and electronic signatures. When software developed with essential 21 CFR Part 11 features are configured correctly and SOPs are in place, this assists with laboratory compliance. The Part 11 Assessment (Table 2) contains a checklist that assists with compliance through system functionality and procedural control.
10. Traceability matrix (TM)	Plan, verify, and report	The TM makes it possible to confirm that each identified testable user requirement has been executed and documented in accordance with the validation plan.
11. Quality assurance unit (QAU) review	Verify and report	QAU review is essential to the success of the validation project. A customer's quality department's engagement in the development, review, and approvals of the validation steps and documentation determines the effectiveness of validation for use of applicable features and functions in the defined environment.
12. Validation summary report (VSR)	Report	The VSR contains an executive summary of results for the software validation. The executive summary includes high-level plan execution and decision recommendations for pass, fail, and exceptions noted. 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. 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 The 3500 Series Data Collection Software System Validation Project Team defined in the Software Validation Plan CMPY-SVP-01

System Defined in the System Configuration Specification CMPY-SCS-01

IQ The 3500 Series Data Collection Software 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 the 3500 Series Data Collection Software 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 can 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 can 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 replicate 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 instrument software containing 21 CFR Part 11 features and functionality 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 a consulting services specialist at **thermofisher.com/csv** for information on services available to assist you with your computer system validation needs. 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 the 3500 Series Data Collection Software System 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 • Validation of the system with the ability to discern invalid or altered records	This is demonstrated through the entire process of validation including IQ, OQ, and PQ testing. The 3500 Series Data Collection Software System programmatically prevents alteration of records outside the system. The data are not accessible. In addition, security, audit trails, and electronic signature functionality prevent the unauthorized alteration of records from within the application. Each file has a checksum built in, and if the file is changed outside the application, it will fail to open the file and inform the user that the file has been modified outside the application.
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.	When configured correctly, reporting functionality can satisfy this requirement.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	This can 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: • 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.	The 3500 Series Data Collection Software System includes this audit trail functionality. 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: • 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	User authentication and access permissions within the software provide this functionality.

21 CFR Part 11 section reference	21 CFR Part 11 requirement	Technical and procedural controls
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.
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. If installed and configured properly, the 3500 Series Data Collection Software System 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 the 3500 Series Data Collection Software System 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 linked to each other through the data files. Records as well as electronic signatures are recorded in the same file, so electronic signatures are linked directly to the respective records. Due to the design of the system as well as security controls, the signatures cannot be decoupled from their respective electronic records.

21 CFR Part 11 section reference	21 CFR Part 11 requirement	Technical and procedural controls
§ 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.
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.
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 a function of the 3500 Series Data Collection Software System. Use of aging and all other aspects of this requirement are the responsibility of the customer and should be defined in customer's SOPs.

21 CFR Part 11 section reference	21 CFR Part 11 requirement	Technical and procedural controls
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.

Learn more about computer system validation at
thermofisher.com/csv