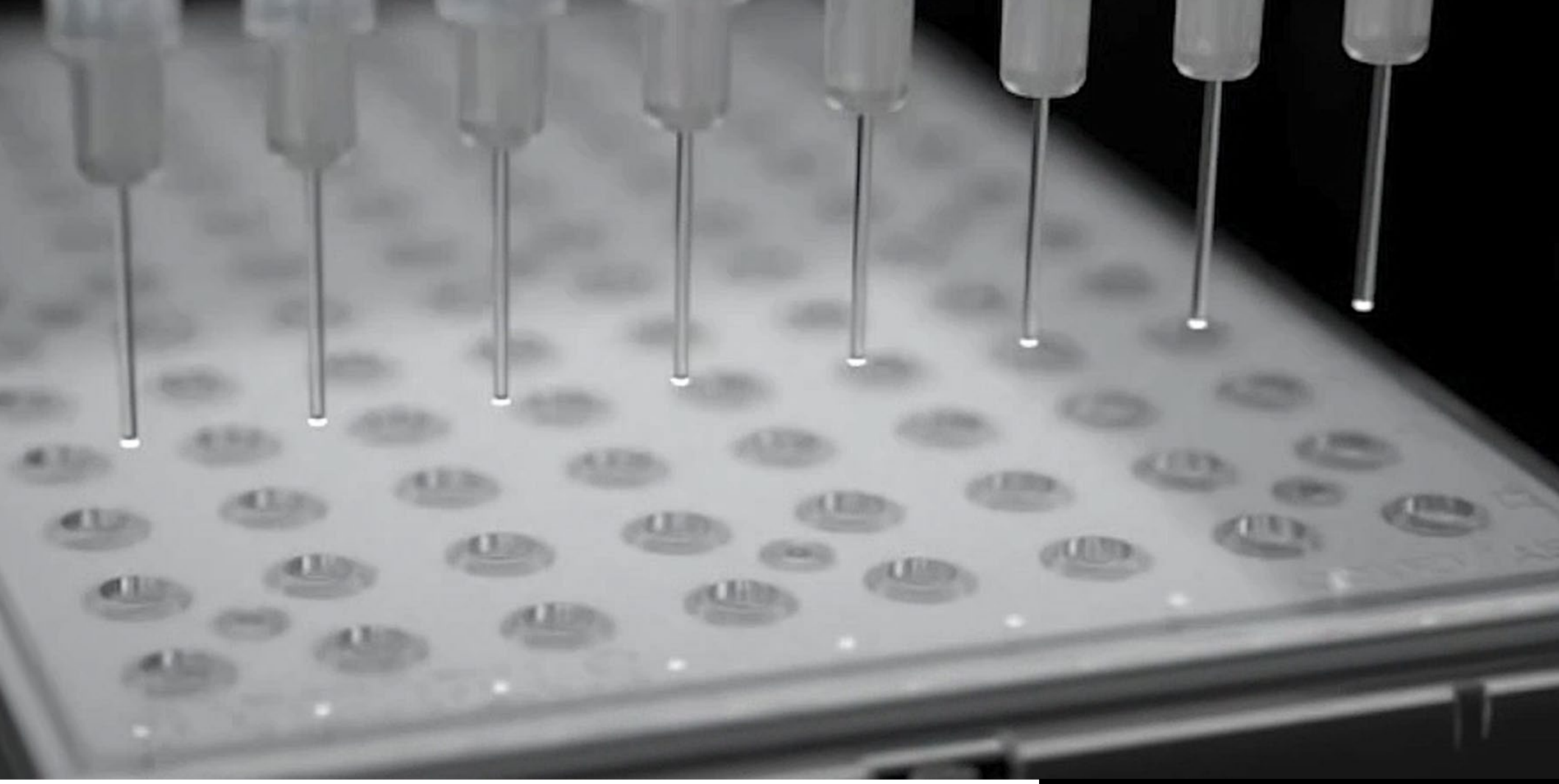

Octet® BLI Compliance Suite Checklist

Simplifying Progress

SARTORIUS

Octet® BLI Compliance Suite Checklist

This compliance checklist is intended to be used as a reference for version 14 of the Octet® BLI Compliance Suite. Compliance Suite software is intended to enable users to comply with 21 CFR Part 11 of the FDA guidelines.

Overview	Yes/No/N.A.
Is the system a Closed System, where system access is controlled by the persons who are responsible for the content of the electronic records that are on the system?	Yes
Is the system an Open System, where system access is not controlled by the persons who are responsible for the content of the electronic records that are on the system? (e.g. a service provider controls and maintains access of the contents of the system, etc.).	No
Does the system use an ID/ password combination?	Yes
Does the system use tokens?	No
Does the system use biometrics?	No

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart B – Electronic Records | 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 the following:					
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.					
1.	11.10 (a)	Is the application validated?	Yes	A Software validation package is available to validate software performance against industry standard software modules.	The customer must purchase the Octet® Compliance Suite software package with the Octet® BLI system. The Octet® software validation package is provided upon purchase of Octet® R8, Octet® R8e, and Octet ® RH16 GxP packages.
2.	11.10 (a)	Does the validation documentation show that Part 11 requirements have been met and are functioning correctly?	Yes	The Octet® BLI software allows customers to be compliant with 21 CFR Part 11, but compliance can only occur if the applications user management, and electronic signature and audit trail are used. Validation documentation can be available for examination during an audit of the Sartorius quality system.	The customer must purchase the Octet® Compliance Suite software package with the Octet® BLI system.
3.	11.10 (a)	Is it possible to discern invalid or altered records?	Yes	Modifications to system settings are limited to user roles with appropriate rights. System settings also include the user management and password settings. All modifications are recorded in the system audit trail. Octet® BLI methods and data files are digitally signed to ensure authenticity. Attempts to alter Octet® BLI files will invalidate the digital signature. File integrity is automatically verified any time an Octet® application opens a file.	Limit the access to the settings menu to selected users (by default only the administrator has access to the settings menu).

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
(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 the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.					
4.	11.10 (b)	Is it possible to view the entire contents of electronic records?	Yes	Settings and modification of settings are recorded in the audit trail and can be viewed. Users with the Administrator or Review Audit Trail privilege can view events associated with all users, otherwise only events associated with the currently logged in user are shown. Audit trails are recorded in the database managed by the Octet® Compliance Hub software. Each experiment has a unique identifier and all data-specific audit trails are logged with the experiment identifier. Audit trails can be filtered by experiment, user, machine, project or date for viewing and printing.	
5.	11.10 (b)	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?	Yes		Each organization must develop controlled, documented procedures for compliance with this requirement.
6.	11.10 (b)	Is the system capable of producing accurate and complete copies of electronic records on paper?	Yes	It is possible to print the audit trail and/or export it to a file in a readable format. Copies of electronic records generated by the system, on paper or in electronic format, must be accurate and contain all required data and metadata necessary to review the records as if they were the original record displayed by the system.	Each organization must develop controlled, documented procedures for compliance with this requirement. It is the customer's responsibility to set print profiles for tasks.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.					
7.	11.10 (c)	Are records protected against intentional or accidental modification or deletion? Can all the archived data be accurately retrieved after system upgrades?	Yes	System audit trails are protected from modification or deletion by any access level. Any modification or tampering outside of the Octet® Compliance Suite software environment invalidates the digital signature. After an upgrade to a newer version of Octet® Compliance Suite software, the existing audit trail database upgrades to the latest schema.	Each organization must develop controlled, documented procedures for compliance with this requirement. It is the customer's responsibility to set print profiles for tasks. It is recommended to use time-controlled actions to automatically export and backup data and the audit trail at set intervals.
8.	11.10 (c)	Does the system provide a time stamped audit trail for tracking events, data creation, modifications and deletions?	Yes	All data acquired using Octet® BLI Compliance Suite software is time stamped and traceable to the user who initiated data acquisition.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
9.	11.10 (c)	Are the records readily retrievable throughout their retention period?	Yes	System audit trails are protected from modification or deletion by any access level. Experimental data can be printed on paper or stored in electronic form.	The customer should specify the retention period (in accordance with the auditor) and responsibilities for ensuring data is retained securely for those periods. By setting the print profiles and time-controlled actions properly the customer can archive all necessary data for audits as printout and/or electronic records. It is the customer's responsibility to print and archive experimental data.
10.	11.10 (c)	Are data records reports, and audit trail data saved automatically to pre-defined external folder in the Octet® Compliance Hub?	Yes	The audit trail is saved in the Octet® Compliance Hub automatically and user decides where to save the data files on the local machine prior to transfer to a network drive for backup.	
(d) Limiting system access to authorized individuals.					
11.	11.10 (d)	Is the system access limited to authorized individuals?	Yes	The Octet® Compliance Suite software restricts the use of all features that can be used to acquire, modify, and analyze data, including exporting and saving the results as files. A user with no explicit privileges cannot access the software. The user management is part of the system settings and the access is limited to user roles with appropriate rights. In the user management user roles and rights, local password rules and password settings are configured.	For locally administrated users the customer needs to organize the users and the user rights.
12.	11.10 (d)	Are successful and failed logins logged by the system?	Yes	Successful and failed logins are recorded into the audit trail. The system administrator can set the maximum number of failed login attempts. If the user tries to log in with the incorrect information for the set number of tries, the account is locked, and this action is logged into the audit trail. The administrator can unlock the user and reset the user password. If a user leaves the group or company, the system administrator can inactivate the user, to help prevent unauthorized use of the software. User accounts can be inactivated, not deleted.	By setting a time controlled action the audit trail is automatically exported at set intervals. Furthermore the audit trail can be exported at any time to a connected USB drive.
13.	11.10 (d)	Does the system lock the user out after a set number of failed login attempts?	Yes	The system locks the user account after a minimum of three failed login attempts. The system administrator can set the maximum number of failed login attempts. If the user tries to log in with the wrong password and reaches the set number of tries, their account locks and this action logs into the audit trail. The administrator can unlock the user and reset the user password.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
14.	11.10 (d)	Does the system ensure that only authorized individuals can log into the system?	Yes	The Octet® Compliance Hub Administrator creates users and assigns permissions according to the user type. The Administrator assigns these user properties: ▪ Unique User Identifier (ID) ▪ Password	
15.	11.10 (d)	Does the system mask the user's password during password entry?	Yes	Passwords are displayed as bullets during entry.	
16.	11.10 (d)	Is it possible to create a user account with an existing username?	No	The Octet® Compliance Hub Administrator creates users and assigns permissions according to the user type. The Administrator assigns these user properties: ▪ Unique User Identifier (ID) ▪ Password If a user leaves the group or company, the system administrator can inactivate the user, to help prevent unauthorized use of the software. User accounts can be inactivated, not deleted.	
17.	11.10 (d)	Is it possible to delete a user account?	No	User accounts can be inactivated, not deleted. If a user leaves the group or company, the system administrator can inactivate the user, to help prevent unauthorized use of the software. The creation/inactivation of users and assigned role settings are recorded in the audit trail.	
18.	11.10 (d)	Do administrative accounts have operator privileges?	No	Default setting for the administrator do not confer privileges for creating and editing methods or running experiments. Where desired, user account settings can be personalized. Operator permissions can be defined based on assigned on projects.	
19.	11.10 (d)	Are there more account permission levels available than just User and Administrator accounts?	Yes	The following default group selections are available: ▪ Administrators — can manage Users and Group settings including add, delete, edit and view all events. ▪ Project Owner — can review data and events. ▪ Scientist — can create, run, save and export data. ▪ Technician — can run experiments and analyze data. ▪ Viewer — can only view a project . Additional groups with bespoke setting may be created by the administrator.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.					
20.	11.10 (e)	Is there a secure, computer generated, time stamp audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?	Yes	Octet® Compliance Suite software automatically generates time-stamped Audit Trails that record transactions that create, delete, or modify electronic records. In each instance, the Audit Trail records the date and time of the transaction, the computer and project name, the user ID of the person who was logged on, and information on the action performed. Additional information such as old and new values are also added for some Audit Trails that log changes in method file modifications and analysis settings. System function/operation (i.e. log mechanical movements, log alarms/error messages, etc.) are not recorded in the Audit Trail. Audit trails are recorded in the database managed by the Octet® Compliance Hub software. Each experiment has a unique identifier, and all data-specific audit trails are logged with the experiment identifier. Audit trails can be filtered by experiment, user, machine, project, or date for viewing and printing. Users can also add comments to an audit trail. Once logged, the audit trail cannot be deleted.	
21.	11.10 (e)	Is data generated attributed to a user or process and time stamped?	Yes	The integrity of raw data is a primary design consideration of Octet® Compliance Suite software. All data acquired using Octet® BLI Discovery Compliance Suite software is time stamped and traceable to the user who initiated data acquisition. All method files, acquired data files, and analysis settings files are digitally signed to ensure data integrity.	
22.	11.10 (e)	Are electronic Records (raw data and audit trail data) captured and saved automatically in real-time?	Yes		
23.	11.10 (e)	Does the audit trail require a comment/ reason for change upon data modification?	Yes	Octet® Analysis Studio in the Octet® Compliance Suite software also has an option to require users to enter comments or notes for each audit trail event. This option can be enabled and disabled using the Set Commenting Requirement permission. Users can also add comments to an audit trail. Once logged, the audit trail cannot be deleted.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
24.	11.10 (e)	Upon making a change to an electronic record, is previously recorded information still available?	No	Assay data files are treated as write once and are not modified when using Octet® BLI Discovery software as part of the Octet® Compliance Suite software with Octet® Compliance Hub. Data analysis using Octet® Analysis Studio with Compliance Hub is treated independently and is overwritten when analysis settings are modified. Previous versions of the analysis settings are not retained but the audit trail records any variables that have changed. Modification of files outside the Octet® BLI software environment will cause the data integrity checks to fail.	
25.	11.10 (e)	Is an electronic record's audit trail retrievable throughout the record's retention period?	Yes	The Octet® Compliance Hub is a key part of keeping records compliance. Strictly control the access to the computer hosting the Octet® Compliance Hub software. Any Windows accounts that are Administrators on the server can directly access the user and audit trail databases to backup work.	Place the server under the control of a department separate from the day-to-day users of the Octet® system, for example local IT, or the Quality department. Control the Octet® Compliance Hub installation media to prevent the setup of "rogue" Compliance Hub instances.
26.	11.10 (e)	Is the audit trail available for review and copying by the FDA?	Yes	The audit trail can be exported in PDF format to a USB drive at anytime. The PDF file can be printed using a standard office printer.	
27.	11.10 (e)	Can selected portions of the audit trial be viewed and printed or saved by inspectors?	Yes	The audit trail can be filtered by project, machine, and users. Searches can also to limited to a specific period of time. categories and sorted by ID, timestamp, or user. List of records are exported as PDF files using the selected categories and used filters and can be printed using a normal office printer.	
28.	11.10 (e)	Is the audit trail stored locally within the system/instrument?	No	The Octet® Compliance Hub software manages the user database and stores audit trail data. The Octet® Compliance Hub should be installed on a dedicated administrator computer. This can be a dedicated physical server workstation, or a virtual machine.	
29.	11.10 (e)	Can the audit trail be temporarily turned off during normal operation?	No	An audit trail of all activities performed in any Octet® Compliance Suite application is stored in the Octet® Compliance Hub database. It is not possible to turn off or pause the audit trail.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
30.	11.10 (e)	Is it possible to configure what types of events will be captured in the audit trail?	No	The audit trail records the date and time of the transaction, the computer and project name, the user ID of the person who was logged on, and information on the action performed. Additional information such as old and new values are also added for some audit trails that log changes in method file modifications and analysis settings.	
31.	11.10 (e)	Can general users access (read-only) the audit trail?	Yes	By default, only events associated with the currently logged in user show. Users with the Administrator or Review Audit Trail privilege can view events associated with all users. It is not possible to access the Octet® Compliance Suite software without an assigned User ID and Password combination.	
32.	11.10 (e)	Are audit trails FIFO and/or is there a retention time limit for any audit trail events?	No	Previously recorded information is not obscured by subsequent record changes. The audit trail does not have an enforced limit size but the practical limit is the space available on the computer hard drive.	
33.	11.10 (e)	Does the audit trail size continuously grow or is the size limited to the experiment timeslot?	Yes	There are no enforced limits. The practical limit is the space available on the computer hard drive.	
34.	11.10 (e)	Does the system/instrument consider windows event logs or SQL transaction logs as part of the audit trail?	No		
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.					
35.	11.10 (f)	If the sequence of system steps or events is important, is this enforced by the system (e.g. as would be the case in a process control system)?	N. A.		

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.					
36.	11.10 (g)	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?	Yes	The Administrator is responsible for configuring user accounts, managing user IDs, user passwords and all aspects of 21 CFR part 11, electronic signatures and audit trails. A user with no explicit privileges cannot access the software. In the settings menu the local password rules (minimum length, complexity, validity period, automatic logout time after inactivity, maximum retries of password entries and action after maximum failed password entries) can be defined. By the unique combination of user profile and password the access is limited to authorized personnel and restricted to granted role rights. To sign electronic records the user must enter their password.	If the access is administrated locally the customer needs to define user profiles and educate administrative staff in the usage and configuration of user profiles.
37.	11.10 (g)	Does the system require the user to change the password when first logging in?	Yes	New user account creation by the Administrator includes the option “User must change password at next login”. This forces the new user to personalize their password before using the system.	
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.					
38.	11.10 (h)	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals) does the system check the validity of the source of any data or instructions received?	N. A.		
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.					
39.	11.10 (i)	Is there documental training, including on the job training for users, developers, IT support staff?	Yes	Sartorius offers the installation and IQ/OQ and PQ for Octet® BLI systems. In the IQ/OQ protocol the list of trained personnel is documented and signed by the customer. Sartorius also offer a dedicated global technical support network for Octet® BLI that comprises of experienced field service engineers and field application scientists, that can answer customer questions and provide additional Octet® BLI training.	Each organization must develop controlled, documented procedures for compliance with this requirement. It is the customer’s responsibility to train users and support staff in the operation and administration of the Octet® BLI system.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
(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.					
40.	11.10 (j)	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signature?	N. A.		The customer is responsible for a written policy concerning the correct usage of electronic signatures.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.					
41.	11.10 (k)	Is the distribution of, access to, and use of systems operations and maintenance documentation controlled?	N. A.	If the Octet® BLI system is covered by a current service contract, then Sartorius can enter/maintain data on maintenances and device qualification (contact details, maintenance contract, next maintenance, warning date, maintenance cycle, device qualification).	Each organization must develop controlled, documented procedures for compliance with this requirement. It is the customer's responsibility to administrate these documents.
42.	11.10 (k)	Is access to "sensitive" systems documentation restricted e.g., net security documentation, system access documentation?	N. A.		Each organization must develop controlled, documented procedures for compliance with this requirement. It is the customer's responsibility to administrate these documents.
43.	11.10 (k)	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail for those changes made by Sartorius?	N. A.	Sartorius tracks the version number of software elements and operating instructions. Each change at the Octet® BLI system is recorded in the audit trail. Version control is an important part of the IQ/OQ documentation. Every change made to the system must be documented in the IQ/OQ documentation.	Each organization must develop controlled, documented procedures for compliance with this requirement. It is the customer's responsibility to define a change control procedure for the Octet® BLI configuration and documentation.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart B – Electronic Records | 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.					
44.	11.30	What controls ensure record authenticity, integrity, and confidentially?	N.A.	The Octet® BLI is a closed system	The Octet® BLI Compliance Suite with Compliance Hub software validation package is provided upon purchase.
45.	11.30	Is data encrypted?	N.A.	The Octet® BLI is a closed system	The customer must purchase the Octet® Compliance Suite with Compliance Hub software package with the Octet® BLI system.
46.	11.30	Are digital signatures used?	N.A.	The Octet® BLI is a closed system	Limit the access to the settings menu to selected users (by default only the administrator has access to the settings menu).

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart B – Electronic Records | 11.50 Signature Manifestations					
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).					
47.	11.50	Do signed electronic records contain the following related information? ▪ The printed name of the signer ▪ The date and time of signing ▪ The meaning of the signing (such as create, approval, review, responsibility)	Yes	Each electronic statement contains: ▪ User who signed the document ▪ Workstation or machine information ▪ Octet® Compliance Hub module information ▪ Project information ▪ Date and time ▪ Statement note In the electronic record the user name, date and time of signing are saved. Electronic statements are created and signed by the user who is logged in.	Sartorius assumes that the audit trail is not reviewed at the instrument but the audit trail is exported and externally reviewed and approved. It is the customer's responsibility to perform audit trail review and approval in an appropriate way.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
48.	11.50	Is the identity of an individual verified prior to issuance of the electronic signature?	Yes	Application of an electronic signature requires the user to input their password.	
49.	11.50	Is the above information shown on displayed and printed copies of the electronic record?	Yes		
50.	11.50	Are date and time stamps applied automatically (vs. being keyed in by the user)	N. A.	Date and time are automatically added to electronic records.	The default is to use the Windows OS system clock which is synchronized to a Microsoft NTP server. By connecting the Octet® BLI system to an NTP server the system automatically receives the correct time and date settings at set intervals.
51.	11.50	Are date and time stamps derived in a consistent way in order to be able to reconstruct the sequence of events?	Yes	Date and time stamps are the local date and time at the location where the signature was executed. The local time recorded in the audit trail is traceable to UTC time.	The default is to use the Windows OS system clock which is synchronized to a Microsoft NTP server. By connecting the Octet® BLI system to an NTP server the system automatically receives the correct time and date settings at set intervals.
52.	11.50	Are changes to electronic signatures included in the audit trail?	N. A.	Electronic signatures cannot be changed.	
53.	11.50	Do the printed name, date, time and electronic signature meaning appear in every human readable form of the electronic record?	Yes		

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart B – Electronic Records | 11.70 Signature/Record Linking					
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.					
54.	11.70	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied or otherwise transferred by ordinary means for the purpose of falsification?	Yes	Octet® BLI methods and data files are digitally signed to ensure authenticity. Attempts to alter Octet® BLI files will invalidate the digital signature. File integrity is automatically verified any time an Octet® application opens a file.	
55.	11.70	If handwritten signatures are executed to electronic records, are the handwritten signatures linked to the electronic record?	N. A.	In electronic records no handwritten signatures can be executed.	
56.	11.70	If the electronic record is changed, is the signer prompted to re-sign (via either manual procedures (SOP) or technical means)?	N.A.	Electronic records cannot be changed.	
57.	11.70	Are the electronic signatures linked (via technology, not procedures) to their corresponding electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?	Yes	Electronic signatures are part of electronic reports and create an entry in the audit trail.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart C – Electronic Signatures | 11.100 General Requirements					
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.					
1.	11.100 (a)	Are electronic signatures unique to an individual?	Yes	Electronic signatures are signed with the user name an application of an electronic signature requires the user to input their password. The Octet® Compliance Suite software package does not allow the creation of user accounts with identical names.	It is the customers' responsibility to ensure that users do not make password available to other internal or external individuals.
2	11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else?	Yes	The user name is unique and cannot be assigned to anyone else.	Each organization must develop controlled, documented procedures for compliance with this requirement. If a user leaves the group or company, the system administrator can inactivate the user, thereby preventing any unauthorized use of the software.
3.	11.100 (a)	Are E-Signs only possible with local accounts?	Yes		
4.	11.100 (a)	Does the system/instrument utilize active directory (AD) to authenticate E-Signs?	No		
5.	11.100 (a)	Is there a second, verifying E-Sign required or able to be enabled for system processes?	Yes	After the first signature is performed, the data locks out additional analysis settings modifications. A second user can counter-sign the experiment.	
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.					
6.	11.100 (b)	Is the identity of an individual verified before an electronic signature is allocated?	Yes	Before the electronic signature is assigned to an electronic record the user must enter their password to authorize the signing process.	
7.	11.100 (b)	Is there a procedure for reissuing forgotten passwords that verifies the requestor's identity?	N.A.		Each organization must develop controlled, documented procedures for compliance with this requirement.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
(c) 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.					
(1) The certification shall be signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement.					
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.					
8.	11.100 (c) (1)	Has certification of the intent to use electronic signatures been submitted to the agency in paper form with a traditional handwritten signature?	N.A.		Each organization must develop controlled, documented procedures for compliance with this requirement.
9.	11.100 (c) (2)	Can additional certification or testimony be supplied to show that an electronic signature is the legally binding equivalent of the signer's handwritten signature?	N.A.		Each organization must submit their written intent to comply with this requirement.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart C – Electronic Signatures | 11.200 Electronic Signature Components and Controls					
(a) Electronic signatures that are not based upon biometrics shall:					
(1) Employ at least two distinct identification components such as an identification code and password.					
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.					
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.					
10.	11.200 (a) (1) (i)	Is the electronic signature made up of at least two components, such as an identification code and password, or an ID card and password?	Yes	An electronic signature comprises of a unique user name and a password. The user has to log on with password to start tasks and must enter the password again to sign electronic reports.	The user management and electronic signature must be licensed and activated. Furthermore, the user must have set a password to sign reports.
11.	11.200 (a) (1) (ii)	When several signings are made during a continuous session, is the password executed at each signing (Note: Both components must be executed at the first signing of a session)?	Yes	Electronic signatures must be added to an analysis workspace to prevent further modification within the Octet® Compliance Suite software-environment. An audit trail of all activities performed in any Octet® Compliance Suite application is stored in the Octet® Compliance Hub database. After the first signature is performed, the data locks out additional analysis settings modifications.	
12.	11.200 (a) (1) (ii)	If signings are not made in a continuous session, are both components of the electronic signature executed with each signing?	N.A.	An automatic log off after a selected time of inactivity can be configured. By the automatic log off the current session is closed and is not continued if user logs in again.	It is the customer's responsibility to correctly configure the automatic log off function to avoid endless sessions. The time of inactivity until automatic log off must be selected.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
(2) Be used only by their genuine owners					
13.	11.200 (a) (2)	Are non-biometric signatures only used by their genuine owners (e.g. by procedures or training reinforcing that non-biometric electronic signatures are not "loaned" to co-workers or supervisors for overrides)?	N.A.		Each organization must develop controlled, documented procedures for compliance with this requirement.
(3) Be 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.					
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.					
14.	11.200 (a) (3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	Yes		Each organization must develop controlled, documented procedures for compliance with this requirement.
15.	11.200 (a) (3) (b)	Are biometric electronic signatures designed to ensure that they can be used only their genuine owners?	N.A.	The Octet® BLI system does not use biometric electronic signatures.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart C – Electronic Signatures | 11.300 Controls for Identification Codes/Passwords					
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:					
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.					
16.	11.300 (a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	Yes	If a new user account is created the Octet® Compliance Suite software checks if the user name is already in use. It is not possible to create a user account with identical names therefore, user name and password combinations are unique.	The customer must define procedures for the definition of unique user names or password reuse.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).					
17.	11.300 (b)	Are procedures in place to ensure that the validity of identification codes are periodically checked?	N.A.		Each organization must develop controlled, documented procedures for compliance with this requirement.
18.	11.300 (b)	Do passwords periodically expire and need to be revised?	Yes	The system administrator can set user passwords to expire after a period of time. If the system administrator activates the password expiration, the users must change their passwords at designated intervals. After a password expires, the software prompts the user to reset it at the next login.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
19.	11.300 (b)	Is there a procedure for recalling identifications codes and passwords if a person leaves or is transferred?	N.A.	Users can be inactivated/reactivated by the administrator.	Each organization must develop controlled, documented procedures for compliance with this requirement.
20.	11.300 (b)	Is there a procedure for electronically disabling an identification code or a password if it potentially comprised or lost?	Yes	Users can be inactivated/reactivated by the administrator. In the local password settings, the validity period of password can be set. The user password can be modified at any time if necessary.	Each organization must develop controlled, documented procedures for compliance with this requirement.
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.					
21.	11.300 (c)	Is an SOP in place directing action to be taken to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices used to carry or generate electronic signature components?	N.A.		Each organization must develop controlled, documented procedures for compliance with this requirement.
22.	11.300 (c)	Does this SOP contain procedures for managing and controlling temporary or permanent token/card replacements?	N.A.	The Octet® BLI system does not accept tokens/cards.	
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.					
23.	11.300 (d)	Is there a procedure for detecting attempts of unauthorized use and for informing security?	Yes	After an invalid login attempt an immediate message is displayed. If the user tries to log in with the incorrect information for the set number of tries, the account is locked, and this action is logged into the audit trail.	It is the customer's responsibility to set the access management rules appropriately and to control if e.g. user accounts have been inactivated after the maximum number of allowed login attempts were exceeded.
(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.					
24	11.300 (e)	Are there procedures covering the initial and periodic testing of devices, such as tokens or cards that bear or generate identification code or password information?	N.A.	The Octet® BLI system does not accept tokens/cards.	
25	11.300 (e)	Does the testing include checks for proper functioning, performance degradation, and possible unauthorized alterations?	N.A.	The Octet® BLI system does not accept tokens/cards.	

Germany
Sartorius Lab Instruments GmbH & Co. KG
Otto-Brenner-Strasse 20
37079 Goettingen
Phone +49 551 308 0

USA
Sartorius Corporation
3874 Research Park Dr.
Ann Arbor, MI 48108
Phone +1 734 769 1600

For further information, visit
www.sartorius.com

Version: 04 | 2026 Octet-BLI-21-CFR-Checklist-eBook-en-Sartorius Marketing Code: C202