Cubis® II MCA 21 CFR Part 11 Compliance Checklist

Simplifying Progress

SARTORIUS

Cubis® II MCA 21 CFR Part 11 Compliance Checklist

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					
1.	11.10 (a)	Is the application validated?	Yes	Sartorius has structurally validated the Cubis II MCA software (firmware and QApp packages).	
2.	11.10 (a)	Does the validation documentation show that Part 11 requirements have been met and are functioning correctly?	Yes	The Cubis II MCA software allows customers to be compliant with 21 CFR Part 11, but compliance can only occur if the QApp package pharma (QP1) is licensed and the applications user management, electronic signature and audit trail are used. Validation documentation is available for examination during an audit of the Sartorius quality system for product development.	The customer must buy the pharma software package QP 1 with the balance.
3.	11.10 (a)	Is it possible to discern invalid or altered records?	Yes	To avoid invalid entries the software displays a guidance to the user how to enter values and the range of allowed values (depending upon the weighing module), checks if entries are within permissible limits and if mandatory entries are complete. 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. Electronic records are stored with MD5 checksum. The system will detect manipulations by deviations in the MD5 sum.	Limit the access to the settings menu to selected users (by default only the administrator has access to the settings menu).
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. The audit trail can be filtered and sorted for review. System information, messages and warnings are recorded in the Status Center message archive. Weighing results are documented in the alibi memory. The alibi memory can be filtered by date or ID.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
5.	11.10 (b)	Is the system capable of producing accurate and complete copies of electronic records on paper?	Yes	Measured weight values and if applicable calculated and statistical values are collected in a print queue and can be printed using a laboratory printer or a standard network printer. Task settings, alibi memory and audit trail as complementary records can be exported to e.g. USB and printed on a standard printer. It's in the customer's responsibility to set print profiles for tasks. For each weighing task two print profiles can be set.	Each organization must develop controlled, documented procedures for compliance with this requirement. It's the customer's responsibility to set print profiles for tasks. For each weighing task two print profiles can be set.
6.	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	Measured weight values and if applicable calculated and statistical values are collected in a print queue and can be stored as pdf, csv or Excel files to a USB drive or an FTP/FTPS/SMB server. Task settings, alibi memory and audit trail as complementary records can be exported as pdf file to a USB drive or an FTP/FTPS/SMB server.	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's recommended to use time controlled actions to automatically export the alibi memory and audit trail at set intervals.
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	Measured weight values and if applicable calculated and statistical values are collected in a print queue and can be stored as pdf, csv or Excel files to a USB drive or an FTP/FTPS/SMB server. Task settings, alibi memory and audit trail as complementary records can be exported as pdf file to a USB drive or an FTP/FTPS/SMB server.	Each organization must develop controlled, documented procedures for compliance with this requirement. It's in the customer's responsibility to set print profiles for tasks. It's recommended to use time controlled actions to automatically export the alibi memory and audit trail at set intervals.
8.	11.10 (c)	Are the records readily retrievable throughput their retention period?	Yes	The audit trail and alibi memory cannot be modified or deleted by the customer. The audit trail and the alibi memory are organized in ring buffers. Before data is overwritten the customer gets a message and is advised to create a backup. Experimental data can be printed on paper or stored in electronic form. Before a weighing task is shut down and unsaved data collected in the print queue is deleted the user gets a safety query.	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's in the customer's responsibility to print and archive experimental data.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
9.	11.10 (d)	Is the system access limited to authorized individuals?	No	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. Alternatively the balance can be connected to a local LDAP server. User roles, rights and passwords are then administrated by the LDAP system. The creation/inactivation of users and assigned role settings are recorded in the audit trail. Failed login attempts are recorded in the audit trail and depending upon the system settings after the maximum number of failed attempts is reached the next login attempt is blocked for a set time or the user is inactivated.	For locally administrated users the customer needs to organize the users and the user rights. For balances connected to an LDAP server users and user rights are administrated by the IT department of the company/institute.
10.	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	All actions and entries that create electronic records are tracked with username, date & time stamp traceable to UTC and for some actions with reason entered by the user in the audit trail. The created records are grouped into categories depending upon which function is affected. E.g. the modification of system- and task settings, the installation of tasks and the uninstallation of tasks is tracked. The audit trail function cannot be switched off and the system doesn't allow to modify or delete records. Accidently acquired weight values can be set to invalid by the user and a reason be entered. The invalidation and reason are recorded in the audit trail. It's not possible for users to delete acquired weight values.	
11.	11.10 (e)	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?	N.A.	The system doesn't allow to modify electronic records. All electronic records are exported with MD5 checksum to prevent data corruption.	
12.	11.10 (e)	Is an electronic record's audit trail retrievable throughout the record's retention period?	Yes	The audit trail is organized in a ring buffer and cannot be modified or deleted by any user. Before the maximum storage capacity is reached and records are overwritten the user gets a message.	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 (e)	Is the audit trail available for review and copying by the FDA?	Yes	The audit trail can be exported in PDF format to USB at any time. The PDF file can be printed using a standard office printer.	
14.	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 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.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
15.	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)?	Yes	The balance offers to create tasks for different weighing applications. The users without the permission to create or modify tasks are not allowed to modify the basic settings of weighing tasks and can only execute the process. In the weighing task the user is guided by instructive texts and icons through the workflow.	If a weight value is acquired accidently the user can mark the value as invalid and enter a reason for the invalidation.
16.	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	In the user management user profiles and role rights are configured. The role rights are a list of functions a user is allowed to perform with the system. Furthermore in the settings menu the local password rules (length, minimum length, validity period, reuse, automatic logout time after inactivity, maximum retries of password entries and action after maximum failed password entries) are 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 his password. Failed attempts to sign electronics records are recorded in the audit trail.	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. Alternatively the balance can be connected to the company's/institute's LDAP server. Then the customer needs to work with the IT department for the configuration of user profiles.
17.	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.	The Cubis II MCA balance is a stand-alone system and don't need external input. If the balance is connected to external systems or databases the integrity of exchanged files is checked using MD5 checksum files. Connected devices must be configured and enabled in the balance system settings.	
18.	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 for Cubis II MCA balances. In the IQ/OQ protocol the list of trained personnel is document and signed by the customer.	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 Cubis II MCA balance.
19.	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.
20.	11.10 (k)	Is the distribution of, access to, and use of systems operations and maintenance documentation controlled?	N.A.	The Sartorius Service can enter data on maintenances and device qualification (contact details, maintenance contract, next maintenance, warning date, maintenance cycle, device qualification) at the balance.	Each organization must develop controlled, documented procedures for compliance with this requirement. It is the customer's responsibility to administrate these documents.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
21.	11.10 (k)	Is access to "sensitive" systems documentation restricted e.g., net security documentation, system access documentation?	N.A.	On the balance only users with the right to access the settings menu can view, sort or export the alibi memory or audit trail.	Each organization must develop controlled, documented procedures for compliance with this requirement.
22.	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 the pharmaceutical organization?	N.A.	Sartorius tracks the version number of software elements and operating instructions. Each change at the balance 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, e.g. firmware and QApp Center updates.	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 Cubis II MCA configuration and documentation.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart B – Electronic Records | 11.30 Controls for Open Systems					
23.	11.30	What controls ensure record authenticity, integrity, and confidentially?	N.A.	The Cubis II MCA balance is a closed system	
24.	11.30	Is data encrypted?	N.A.	The Cubis II MCA balance is a closed system	
25.	11.30	Are digital signatures used?	N.A.	The Cubis II MCA balance is a closed system	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart B – Electronic Records | 11.50 Signature Manifestations					
26.	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	In the electronic record the user name, date and time of signing are saved. Electronic records are created and signed by the user who started the weighing task.	Sartorius assumes that the audit trail is not reviewed at the instrument but the audit trail and alibi memory data is exported and externally reviewed and approved. It is the customer's responsibility to perform audit trail review and approval in an appropriate way.
27.	11.50	Is the above information shown on displayed and printed copies of the electronic record?	Yes	The electronic signature is displayed and printed with user name, date and time of signing in reports.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
28.	11.50	Are date and time stamps applied automatically (vs. being keyed in by the user)	Yes	Date and time are automatically added to electronic records.	By connecting the balance to an NTP server the balance automatically receives the correct time and date settings at set intervals.
29.	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.	By connecting the balance to an NTP server the balance automatically receives the correct time and date settings at set intervals.
30.	11.50	Is the above information subject to the same controls as electronic records? (Audit trail, access control, etc.)	Yes	The user must have licensed the audit trail function. Then the system creates electronic records for events as listed above.	Each organization must develop controlled, documented procedures for compliance with this requirement.
31.	11.70	Are changes to electronic signatures included in the audit trail?	N.A.	Electronic signatures cannot be changed.	
32.	11.70	Do the printed name, date, time and electronic signature meaning appear in every human readable form of the electronic record) (e.g. all screens and printed reports).	Yes	The user name, date, time and meaning are displayed and printed in human readable form which each electronic signature (the Cubis MCA II only allows to create records.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart B – Electronic Records | 11.70 Signature/Record Linking					
33.	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	Each electronic signature is linked to a specific record and the record is saved with MD5 checksum. If electronic signatures are changed, deleted or transferred the manipulation will be detected by a mismatch in the MD5 checksum.	
34.	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. Handwritten signatures may be executed to a printed report and such a report by its metadata is traceable to the original electronic record.	The Cubis II MCA balance offers different print formats for reports. In principle any report can be signed by handwritten signatures but to print a complete dataset incl. metadata the GLP print incl. all data is the best option.
35.	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.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
36.	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. The Cubis II MCA balance doesn't allow to modify electronic records or the audit trail.	

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
Subpart C – Electronic Signatures | 11.100 General Requirements					
37.	11.100 (a)	Are electronic signatures unique to an individual?	Yes	Electronic signatures are signed with the user name. The Cubis II MCA balance does not allow to create user accounts with identical names.	If the user accounts at the Cubis II MCA balance are controlled by a local LDAP system it's in the customer's responsibility not to allow group accounts (accounts used from more than one individual to access network or local resources). Furthermore it must be regulated that users do not make password available to other internal or external individuals.
38.	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 users leave the lab the system administrator can inactivate the user.
39.	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 his password to authorize the signing process.	
40.	11.100 (b)	Is there a procedure for reissuing forgotten passwords that verifies the requestor's identity?	N.A.		
41.	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.
42.	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					
43.	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 if a unique user name and a password. The user has to log on with password to start tasks and 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.
44.	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	The user has to select their unique user name and to log on to the balance with his password. For each signing process the user must enter his password again.	
45.	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.
46.	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.
47.	11.200 (a) (3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	N.A.	For LDAP the functionality to rest the passcode require at least the resetter and witness to ensure that the reset is trustworthy. This rest mechanism must be implemented in the customer directory service.	Each organization must develop controlled, documented procedures for compliance with this requirement.
48.	11.200 (b)	Are biometric electronic signatures designed to ensure that they can be used only their genuine-owners?	N.A.	The Cubis II MCA 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					
49.	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 new user account are created the Cubis II MCA checks if the user name is already in use. It is not possible to create a user accounts with identical names. In the local password settings the rules for the reuse of passwords can be set.	If using LDAP it's the customer's responsibility to ensure that user accounts are unique and to prevent the reuse of user names if a user leaves the company. The customer must define procedures for the definition of unique user names or password reuse.

Ref.		Question	Yes/No/N.A.	Comments	Recommended Customer Actions
50.	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.
51.	11.300 (b)	Do passwords periodically expire and need to be revised?	Yes	In the local password settings the validity period of password can be set.	If using LDAP it's the customer's responsibility to ensure that passwords have a limited period of validity.
52.	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.
53.	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.
54.	11.300 (c)	Is a 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.
55.	11.300 (c)	Does this SOP contain procedures for managing and controlling temporary or permanent token/card replacements?	N.A.	The Cubis II MCA balance does not accept tokens/cards.	
56.	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 and a record is created in the audit trail. The number of maximum retries and the action if the maximum number of allowed failed login attempts is reached can be configured at the Cubis II MCA balance in access management rule management menu. The Cubis II MCA balance does not inform the system administrator but instead the system administrator defines the action of the software if the maximum number of login attempts is exceeded.	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. If using LDAP it is the customer's responsibility to define the action of the system at attempts of unauthorized use and the information procedure.
57.	11.300 (a)	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 Cubis II MCA balance does not accept tokens/cards.	
58.	11.300 (b)	Does the testing include checks for proper functioning, performance degradation, and possible unauthorized alterations?	N.A.	The Cubis II MCA balance does not accept tokens/cards.	