System Assessment Report

Relating to Electronic Records and Electronic Signatures;

21 CFR Part 11

System: Mira Cal Software
(Software version 3.1)

1 Procedures and Controls for Closed Systems

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.1	11.10 (a)	Validation, IQ, OQ	Is the system validated?	O		The operator is solely responsible for the validation of the system. The responsibility of the supplier lies in supplying systems which are capable of being validated. This is supported by the internal Metrohm quality management system which can be audited on request. In this respect Metrohm offers a range of validation services: conformity certificates, prepared documentation for IQ and OQ, support for performing IQ and OQ at the operator's premises. Standard methods for system validation (i.e. system suitability tests) are stored in the system.
1.2	11.10 (a)	Audit Trail, Change	Is it possible to discern invalid or altered records?	X		All relevant operator entries are recorded in an automatically generated audit trail: the date, time with difference to UTC (Coordinated Universal Time) and the user ID of the respective operators. The audit trail is stored internally and can be copied via export function. The audit trail can be examined within the software. For libraries and training set modifications, all former versions are saved in the database and data modifications require a comment to be entered. Operating procedures are subject to a version control. This means that modified data of an operating procedure leads to a new entry (version) in the database.
1.3	11.10 (b)	Report, Printout, Electronic Record	Is the system capable of producing accurate and complete copies of electronic records on paper?	X		Reports can be printed out for results, operating procedures, samples and the audit trail. Reports for libraries and training sets are not available, but reports of each containing sample can be created. Reports are created in PDF[1] format. Each printout is accompanied by a time stamp giving information about the time with difference to UTC (Coordinated Universal Time).

[1] PDF: Portable document format

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.4	11.10 (b)	Report, Electronic Record, FDA	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?	**X**		All data can be stored as an encrypted file and can be evaluated by means of the Mira Cal software. Via the report generator all reports can be provided in PDF format. Sample reports can exported in CSV[2] format
1.5	11.10 (c)	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	**X/O**		The operator is solely responsible for record storage/archiving. The system stores the data permanently either in the Mira Cal software database. Copies of the operational data can be made locally or on a network drive via the system backup function, just as copies on paper via the regular print-out. The data on the storage device is encrypted and provided with a checksum. This way it is protected against accidental and improper modification. Modifications are recognized by the system. The content can be read by the Mira Cal software at any time. The method used for archiving data together with the definition which data to be archived must be defined by the operator. Interfaces for archiving are present in the system. System setting can be made to enforce that archiving is allowed for the administrator role only.
1.6	11.10 (d)	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals?	**X**		The system provides a login system with three internal access levels (System Administrator, Lab Manager and Instrument User). The person responsible for the system (administrator) must ensure that access rights are granted to authorized persons only. All changes of access rights are recorded in the audit trail.

[2] CSV: Comma separated values

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.7	11.10 (e)	Audit Trail, Electronic Record, Operator Entries	Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records? Does the audit trail (mandatorily) collect the reason for a record change or deletion?	X		The audit trail documents all user entries and actions on electronic records with date, time with difference to UTC and user. Additionally, all modifications of security settings (e.g. invalid access attempts, change of the password policy), user administration or configuration data are recorded in the audit trail. Mira Cal software offers a feature for commenting each action. This feature can be set as required. When the compliance setting is enabled, Mira Cal Software requests the user to enter a comment after a user entry.
1.8	11.10 (e)	Electronic Record, Overwriting data, Change	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?	X		A new version is automatically created, if objects or determination data are changed and saved. An old version can be restored (via 'revert object' function which restores the old record set as the current version). Note: If printouts exist of the electronic records, organizational safeguards have to be implemented to ensure that, after the alteration, printouts of the respective methods and determinations can be: - identified unambiguously - referred to the correct methods and determinations.
1.9	11.10 (e)	Audit Trail, Retention Period	Is the audit trail of an electronic record retrievable throughout the retention period of the respective record?	X/O		As long as the audit trail has not been archived, it is kept within the software. The disk space is the limiting factor here. The audit trail can only be deleted after it has been archived beforehand. The operator is solely responsible for the safe storage of the archived audit trail. The software provides a setting which limits archiving functionality to the administrator role only.
1.10	11.10 (e)	Audit Trail, FDA, Inspection	Is the audit trail available for review and copying by the FDA?	X		The audit trail can be exported from Mira Cal software. The available format is protected PDF, CSV and XLSX. Thus, it is available in electronic form and on paper.
1.11	11.10 (f)	Control over sequence of steps, Plausibility Check, Devices	If the sequence of system steps or events is important, is this enforced by the system (e.g., as it would be the case in a process control system)?	X		Sequences are defined by design of the software. The user is guided through the steps. The operator is solely responsible for enforcing the steps. The system provides a setting to limit the synchronization of Operating Procedures to signed Operation Procedures only.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.12	11.10 (g)	Login, Access Protection, Authorization, User, Administrator	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?	**X**		The system gives access to the computer and the instrument for valid user accounts only. The person responsible for the system (system administrator) must ensure that access rights are granted to authorized persons only. The administrator function can be clearly separated from user roles, see also 11.10 (d), No. 1.6. Objects and determinations can be signed electronically. There are two signature levels. The system demands that the reviewing and the releasing person is not the same.
1.13	11.10 (h)	Balance, Connection, Terminals, Input data, Devices	Does the system control validity of the connected devices? *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? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).*	**X**		Metrohm RAMAN instruments are recognized, their validity is being checked automatically (e.g. firmware version checked and the serial number is recorded). No other devices are needed and are therefore not supported. Qualification of the connected instruments is carried out as part of the system validation (see also 11.10 (a), No. 1.1) which is part of the operator's responsibility.
1.14	11.10 (i)	Training, Support, User, Administrator	Is there documented training, including on the job training for system users, developers, IT support staff?	**X/O**		The operator is responsible for user training and the supporting staff. Metrohm offers standard training courses for all application fields. Individual training courses can be arranged separately. Metrohm's product developers and service personnel receive further training on regular intervals.
1.15	11.10 (j)	Policy, Responsibility, Electronic Signature	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	**O**		If an electronic signature is used the operator must have a policy in place in which the equality of handwritten and electronic signatures is made clear.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.16	11.10 (k)	Documentation, Distribution of Documentation, Access to Documentation, System Documentation, Logbook, Manuals	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	**O**		Paper-based documentation is delivered together with the system and is additionally available as PDF on Metrohm's website. Distribution of documentation to users is in the responsibility of the operator.
1.17	11.10 (k)	SOP, Documentation, Manuals, System Documentation, Audit Trail , Logbook	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail (= version history) for creation and modification?	**X/O**		The system documentation is unambiguously assigned to a particular system and software version. Release notes which are published with each software version, describe the changes compared to the predecessor version. However, the operator must maintain records about documentation and system changes which are supplied by Metrohm.

2 Additional Procedures and Controls for Open Systems

Run no.	Ref.	Topic	Question	Yes	No	Comments
2.1	11.30	Data, Encryption, Data Transfer	Can methods and determinations be sent securely to another system? Is data encrypted?	**N/A**		Access to Mira Cal software via the Internet is not provided.
2.2	11.30	Electronic Signature	Are digital signatures used to authenticate involved parties?	**N/A**		Access to Mira Cal software via the Internet is not provided.

3 Signed Electronic Records

Run no.	Ref.	Topic	Question	Yes	No	Comments
3.1	11.50	Electronic Signature	Do signed electronic records contain the following related information: - The printed name of signer, - The date and time of signing, - The meaning of the signing (such as approval, review, responsibility)?	X		All signatures contain the full name of the signer (displayed in the audit trail), date and time of the signature and the meaning (out of a list box) for signing. In addition, a comment can be added to the signature, which is saved together with the electronic signature.
3.2	11.50	Electronic Signature	Is the above information shown on displayed and printed copies of the electronic record?	X		User ID, timestamp (date and time) and meaning of the signature is displayed on screen and on the reports. Additionally the full name is displayed in the audit trail and user management of Mira Cal software.
3.3	11.70	Electronic Signature	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?	X		The signature is securely linked to the respective configuration or sample. Signature elements cannot be cut, copied or transferred by ordinary means.

4 Electronic Signature (General)

Run no.	Ref.	Topic	Question	Yes	No	Comments
4.1	11.100 (a)	Electronic Signature	Are electronic signatures unique to an individual?	**X/O**		Each user gets a unique user ID. It must operationally be ensured, that user IDs are assigned to a single person instead of a user group (i.e. group account). The system monitors the unambiguousness of the user ID.
4.2	11.100 (a)	Electronic Signature	Are electronic signatures ever reused by, or reassigned to, anyone else?	**O**		The user ID is assigned to one person. It must operationally be ensured, that this user ID is not re-assigned to another person. User accounts can be disabled but not deleted.
4.3	11.100 (a)	Electronic Signature, Representative	Does the system allow the transfer of the authorization for electronic signatures (to representatives)?	**O**		Secure and traceable user rights management is in the responsibility of the operator. The assignment of representatives is part of the regular user management and has to be carried out by the administrator. A procedure has to be in place for this.
4.4	11.100 (b)	Electronic Signature	Is the identity of an individual verified before an electronic signature is assigned?	**O**		With the initial assignment of signing rights to a user, the identity of the respective person has to be verified.

5 Electronic Signatures (Non-biometric)

Run no.	Ref.	Topic	Question	Yes	No	Comments
5.1	11.200 (a) (1)(i)	Electronic Signature	Is the signature made up of at least two components, such as an identification code and password, or an ID card and password?	X		The signing function is carried out with user ID and password.
5.2	11.200 (a) (1)(ii)	Electronic Signature	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).	X		The user ID and password has to be entered with each signature.[3]
5.3	11.200 (a) (1)(iii)	Electronic Signature	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	X		The user ID and the password have to be entered with each signature.
5.4	11.200 (a) (2)	Electronic Signature	Are non-biometric signatures only used by their genuine owners?	O		The operator has to ensure that a user uses his/her signature credentials only.
5.5	11.200 (a) (3)	Electronic Signature, Falsify Electronic Signature	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	X		Nobody has access to the electronic signature data by ordinary means.

[3] There is no function like “Signing in a continuous session”

6 Electronic Signatures (biometric)

Run no.	Ref.	Topic	Question	Yes	No	Comments
6.1	11.200 (b)	Electronic Signature, Biometric Electronic Signature	Has it been shown that biometric electronic signatures can be used by their genuine owner only?	**N/A**		Electronic signature is not based on biometric means.

7 Controls for Identification Codes and Passwords

Run no.	Ref.	Topic	Question	Yes	No	Comments
7.1	11.300 (a)	Identification Code, Uniqueness, Password, Identification, Login, Access Protection	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?	X		The system ensures that each user ID is used only once within the system and therefore each combination of identification code and password can exist only once. Alterations of names must be managed by the operator. It is recommended that unambiguous identification codes (e.g. personnel number or initials) are used for all systems across the whole organization. In general it is recommended that guidelines are drawn up for the whole organization in which the creation of user accounts and the requirements for password complexity (length, period of validity...) are defined.
7.2	11.300 (b)	Identification Code, Password, Validity, Identification, Login, Access Protection	Are procedures in place to ensure that the validity of identification code is periodically checked?	O		The operator is responsible for checking the identification codes periodically. The system supports the operator with a password expiration function.
7.3	11.300 (b)	Password, Validity, Password Expiry, Identification, Login, Access Protection	Do passwords periodically expire and need to be revised?	X		The validity period of the password can be defined by the administrator. After this period is expired, the user is forced to change his/her password. The system maintains the password history and prevents the user from re-using one of the last 5 passwords.
7.4	11.300 (b)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	O		The procedure has to be set up by the operator. The corresponding user account can be disabled in the system by the administrator, but remains saved in the system without any access rights.
7.5	11.300 (c)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection, Loss of ID card	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	O		The procedure has to be set up by the operator. The corresponding user account can be disabled in the system by the administrator, but remains saved in the system without any access rights.

Run no.	Ref.	Topic	Question	Yes	No	Comments
7.6	11.300 (c)	Loss of / compromised ID card, Electronically Disabling ID card	Is there a procedure for electronically disabling a device if it is lost, or stolen, or potentially compromised?	**N/A**		There is no hardware token or device for user identification.
7.7	11.300 (c)	ID card, Replacement	Are there controls over the temporary or permanent replacement of a device?	**N/A**		There is no hardware token or device for user identification.
7.8	11.300 (d)	Unauthorized Use, Log-in, Access Protection	Are there security safeguards in place to prevent and/or detect attempts of unauthorized use of user identification or password?	**X/O**		After *n* incorrect attempts (number can be defined by the administrator) a message is displayed, saying that the maximum number of unsuccessful login attempts has been reached and the user account is disabled. This is logged in the audit trail.
7.9	11.300 (d)	Unauthorized Use, Log-in, Access Protection, Inform management	Is there a procedure in place to inform the responsible management about unauthorized use of user identification or password?	**O**		The procedure to inform the security manager has to be implemented by the operator.
7.10	11.300 (e)	Testing of ID cards, ID card, Access Protection	Is there initial and periodic testing of tokens and cards?	**N/A**		There is no hardware token or device for user identification.
7.11	11.300 (e)	Modification of ID cards, ID card, Unauthorized Use, Access Protection	Does this testing check that there have been no unauthorized alterations?	**N/A**		There is no hardware token or device for user identification.

O = Implementation is in the operator's responsibility
N/A = Not Applicable to the system

This 21 CFR Part 11 assessment is based on an on-site audit performed January, 12th 2017. Subject of this audit was the software version 3.0 with all compliance features enabled. According to Metrohm AG management (development and QA) all implemented changes in the following version are not relevant with regard to 21 CFR Part 11 or 21 CFR Part 11 compliant (see Release Notes 8.105.8023EN). Therefore, this update does not require an on-site re-audit.

8 Indices

Reference to the page number:

Reference to the run number of the entry: