System Assessment Report

Relating to Electronic Records and Electronic Signatures;

21 CFR Part 11

System: MagIC Net
(Software Version 3.3)

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 control system which can be audited at any time. In this respect Metrohm offers a range of validation services: conformity certificates, prepared documentation for IQ and OQ, carrying out IQ and OQ at the operator's premises. Standard methods for system validation 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 together with date, time with difference to UTC Coordinated Universal Time) and user. This time is taken from the client's system time, which means that the administrator has to take care of the system time to be reliable (e. g. by synchronizing all clients connected with a time server). In the report generator, the report can be defined in order to indicate any modified results data (results). For method modifications all former versions are saved in the database and a comment has to be entered. Methods are subject to a version control. This means that modified data of a method leads to a new entry (version) in the database. If the results data are changed (recalculation), all former versions are saved in the database and a comment has to be entered. A version check is implemented for determinations. This means that modified data leads to a new entry in the database. Invalid results can be recognized if limit values have been defined. In case of exceeding this limits it can be defined in the system whether a message is displayed on the screen or on the report or whether an e-mail is sent. Additionally it can be defined whether the determination has to be canceled.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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		Configurable reports can be printed out for determinations (results data). Alterations to the report configuration can be disabled for routine users. The automatic printout at the end of an analysis can be triggered by settings in the method. In this way it can be ensured that the operator of the system can reliably track any alteration, overwriting or deletion of the data of a determination. Each printout is accompanied by a time stamp giving information about the time with difference to UTC (Universal Time, Coordinated).
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 encrypted XML file and can be evaluated by *MagIC Net*. Data can be exported to XML, CSV and SLK format. Via the report generator all reports can be provided in PDF format. The automatic data export at the end of an analysis can be triggered by settings in the method. In this way it can be ensured, that the operator of the system can reliably track any alteration, overwriting or deletion of the data of a determination.
1.5	11.10 (c)	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	O		The operator is solely responsible for storage/archiving. *MagIC Net* can be installed as local server or client version. The system can permanently store the data either in the *MagIC Net* database or on the computer or on a network drive by using an archiving system or via print-out on paper. The database has an automatic backup function. The data on the storage device is encrypted and provided with a checksum. In this way it is protected against accidental and improper alteration. Alterations are recognized by the system. The content can be read by the *MagIC Net* software at any time. The method used for archiving data and which data are to be archived must be defined by the operator. Interfaces for archiving (XML files) are available in the system.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.6	11.10 (d)	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals?	X		The system is provided with a login system with an unlimited number of profiles (access rights / user groups). The access rights for the single user groups can be arbitrarily defined by the administrator.
						The person responsible for the system (administrator) must ensure that access rights are assigned to authorized persons only.
						All changes of access rights are recorded in the audit trail.
1.7	11.10 (e)	Audit Trail, Electronic Record, Operator Entries, Reason for Change/Deletion	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?	X		The audit trail records all relevant user entries and actions on electronic records with user name, date, time with difference to UTC; changes to methods, determinations or sample data (only live modifications) require the entry of a comment by the user.
			Does the audit trail (mandatorily) collect the reason for a record change or deletion?			Additionally, all modifications of security settings, user administration or configuration data are recorded in the audit trail.
1.8	11.10 (e)	Electronic Record, Over-writing 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 methods or determination data are changed and saved.
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		All audit trail data are stored and kept in the configuration database as long as the audit trail has not been deleted. The disk space is the limiting factor here. The audit trail can only be deleted after it has been archived before. The audit trail is being archived as a text file with a checksum.
						The operator is solely responsible for the safe storage of the archived audit trail.
						The log named "audit trail" which records all changes to methods, determinations and configuration data (devices, global tables, GLP, user management, etc.) is clearly separated from the normal logging of system actions (data communication, device actions, errors, etc.).
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 to a text file with a checksum and is therefore available in electronic form and on paper. Via the checksum, the integrity of the Audit Tail can be verified.
						Additionally, a read-only PDF file of the audit trail can be created and printed.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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		Plausibility checks are carried out by the system when a determination is started. For example, a check is made whether all necessary devices are present. The sequence of the determination is programmed in the method and must be strictly followed. Following of the sequence is supported by using of the sample assignment table or automatic sample data request. Only those functions are enabled which are able to be executed.
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 user can be identified by the login function. The person responsible for the system (= administrator) must ensure that access rights are assigned to authorized persons only. The administrator function can be clearly separated from user roles, see also 11.10 (d), No. 1.6. Methods and determinations can be signed and with that released 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/O		During the IQ all the devices connected are entered into the list of instruments and are subsequently checked. Metrohm instruments are recognized, their validity is being checked and they are automatically entered into the list of devices. Validation 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 training the users 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 training on regular intervals.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 then the operator must have a policy in which the equality of handwritten and electronic signatures is made clear.
1.16	11.10 (k)	Documentation, Distribution of Documentation, Access to Documentation, System Documentation, Change Control, Logbook, Manuals	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	O		The system has a comprehensive online help system that supports the user and the service personnel. Distribution of paper-based system documentation (e. g. system manual) is in the responsibility of the operator.
1.17	11.10 (k)	SOP, Documentation, Manuals, System Documentation, Ver3sion 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 system and a software version. Release notes are kept with each software version. However, the operator must maintain records about documentation and system changes – e. g. in the device logbook. Templates of these documents 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		*MagIC Net* is not designed to be accessed via the Internet. The data are stored as a file, encrypted and provided with a checksum. This protects the data against unauthorized modification. In case of a modification the data become useless. Even if corrupted data are transferred to another system this is recognized.
2.2	11.30	Electronic Signature	Are digital signatures used to authenticate the involved parties?	N/A		*MagIC Net* is not designed to be accessed via the Internet. Methods and determinations can be signed and with that released electronically. There are two signature levels. The data are stored as a file, encrypted and provided with a checksum. This protects the data against unauthorized modification. In case of a modification the data become useless. Even if corrupted data are transferred to another system this is recognized.

07.2019-V1

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		In case of methods and determinations all signatures contain the full name of the signer, date and time of the signature and the meaning (out of a list box) for signing. Additionally, a comment on a signature can be entered, 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		Full signature data are shown on the display and on printouts.
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 method or determination. Signature elements cannot be cut, copied or transferred by ordinary means. User information is completely integrated in the signature. When displaying the signature, this information is always readable in plain text.

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		Each user gets a unique login name; The system checks the unambiguousness of the login name. It must be ensured operationally, that a user name is assigned to one person only.
4.2	11.100 (a)	Electronic Signature	Are electronic signatures ever reused by, or reassigned to, anyone else?	O		A login name used is assigned to one person. It must operationally be ensured, that this login name is not assigned to another person. A reactivation is not affected by this.

Run no.	Ref.	Topic	Question	Yes	No	Comments
4.3	11.100 (a)	Electronic Signature, Representative	Does the system allow the transfer of the authorization for electronic signatures (representatives)?	O		The secure and traceable user rights management is in the responsibility of the user. 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 signing rights assignment to a user, the identity of the respective person has to be verified against the user rights request.

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 login name 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 password has to be entered with each signature.
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 login name 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 only uses his/her own signature
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		The data of the database are encoded in a format non-readable for humans.

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**		No electronic signature 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 identification code (user name) is used only once within the system and therefore each combination of identification code and password can also exist only once. Alterations of names must be managed by the operator. The system can be run as client server system. This ensures that all identification codes are identical on all clients. It is recommended to use unambiguous identification codes (e. g. personnel number or initials) covering the entire organization. In general it is recommended that guidelines are drawn up for the whole organization in which the creation of user accounts and the use of passwords (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.
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 saves the password history and prevents re-use of passwords.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 administrator can disable the respective user in the system, but the account remains saved in the system as part of the group "removed users" 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 administrator can disable the respective user in the system, but the account remains saved in the system as part of the group "removed users" without any access rights.
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 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 device for user identification.
7.8	11.300 (d)	Unauthorized Use, Login, 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 is disabled. A corresponding message can be sent to the management by e-mail.
7.9	11.300 (d)	Unauthorized Use, Login, 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 device for user identification.
7.11	11.300 (e)	Modification of ID cards, ID card, Unauthorized Use, Access Protection	Does the token or card verification includes a check that there have been no unauthorized alterations?	**N/A**		There is no hardware device for user identification.

Legend

X   Applies to the system
O   Implementation in the operator's responsibility
N/A   Not applicable to the system

This 21 CFR Part 11 assessment is based on a physical audit performed January the 13th 2009. Subject of this audit was the platform commonly used by MagIC Net 2.x and tiamo 2.x. This platform provides the functionality for electronic record and signature processing. According to Metrohm AG management (development and QA) all implemented changes in the following versions – including the current version – are not relevant with regard to 21 CFR Part 11 or 21 CFR Part 11 compliant (see Release Notes 8.102.8016EN, 8.102.8024EN, 8.102.8033EN, 8.102.8039EN, 81028048, 8.102.8060EN, 8.102.8072EN, 8.102.8082EN). Therefore, this update does not require an on-site re-audit.

8 Indices

References to the page number:

References to the run number of the entry: