

System Assessment Report
Relating to Electronic Records and Electronic Signatures;
21 CFR Part 11

System: Vision Air Software
(Software version 2.0)

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		<p>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.</p> <p>In this respect Metrohm offers a range of validation services: conformity certificates, prepared documentation for IQ and OQ, performing IQ and OQ at the operator's premises.</p> <p>Standard methods for system validation (i. e. diagnostics tests) are stored in the system.</p>
1.2	11.10 (a)	Audit Trail, Change	Is it possible to discern invalid or altered records?	X		<p>All relevant operator entries affecting measurement (e. g. operating procedures, parameter profiles, prediction models, signatures, instrument details, diagnostics tests) are recorded in an automatically generated audit trail: the date, time with difference to UTC (Coordinated Universal Time) and the user ID of the different operators. The audit trail is stored internally and can be copied via export function. The audit trail can be examined within the software.</p> <p>In the report, any altered configurations are indicated. Old and new values are displayed.</p> <p>During the signing process, every change can be commented by the operator who signs the configuration (Level 1 and Level 2).</p> <p>Invalid results can be recognized if limits have been defined. If these are infringed, the result will be highlighted and a message will be displayed.</p> <p>A configuration change can never be deleted, a cancelled configuration change will always be displayed as such.</p>

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		<p>Configurable, customized reports can be printed for results, instrument configurations and operating procedures.</p> <p>The automatic printout at the end of an analysis can be forced by system settings. Therefore it can be ensured that the operator of the system can reliably track every alteration, overwriting or deletion of determination data.</p> <p>Each printout is accompanied by a time stamp giving information about the time respective to UTC (Coordinated Universal Time).</p>
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		<p>Data can be provided in formatted CSV, XLS, NIR or CAL-format. Formatted CSV and XLS include result data but spectrum data can be added. Automatic report creation can be forced. The automatically generated report can be saved in different formats (PDF, DOC, CSV...).</p> <p>The automatic printout at the end of an analysis can be forced by system settings. Therefore it can be ensured that the operator of the system can reliably track every alteration, overwriting or deletion of determination data.</p>
1.5	11.10 (c)	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	X/O		<p>The operator is solely responsible for record storage/archiving.</p> <p>No records can be deleted or edited by the user except of sample number. Once a sample is signed, it is no longer possible to edit it (to avoid the use of the sample number, the operator can use user defined fields instead).</p> <p>The data on the data carrier is encrypted and provided with a checksum, thus it is protected against accidental and improper alteration. Alterations are recognized by the system.</p> <p>The method used for archiving data, together with the definition which data to be archived, must be defined by the operator.</p>
1.6	11.10 (d)	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals?	X		<p>The system provides a login system with four internal access levels (System Administrator, Network/Group Manager and Instrument User). The person responsible for the system (administrator) must ensure that access rights are granted to authorized persons only.</p>

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.7	11.10 (e)	Audit Trail, Electronic Record, Operator Entries	<p>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?</p> <p>Does the audit trail (mandatorily) collect the reason for a record change or deletion?</p>	X		<p>All relevant operator entries affecting measurement (e. g. operating procedures, parameter profiles, prediction models, signatures, instrument details, diagnostics tests) are recorded in an automatically generated audit trail. The configuration changes which will be uploaded to the instrument have to be signed (two level signing process) and will display the date, time with difference to UTC (Coordinated Universal Time) and the user IDs of the different operators. The audit trail is stored internally and can be exported via export function. The audit trail can be examined within the software. The display of records can be filtered for ease of use.</p> <p>No records can be deleted or edited by the user except of sample number. Once a sample is signed, it is not possible to edit it anymore. In addition the use of the sample number can be circumvented by using user defined fields instead.</p> <p>The system provides a function to comment data alteration of configuration and signatures.</p> <p>A system time modification is monitored in Vision Air (PC system) and requires syncing of the modified time setting. Change of the system time will be logged.</p>
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		<p>If a configuration is altered, a new version will be created automatically. The previously recorded information is displayed in the audit trail and on the stored reports (with one exception: sample number changes are traceable not before the sample is signed; workaround: use user defined fields instead of the sample number).</p> <p>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:</p> <ul style="list-style-type: none"> - 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		The audit trail is stored internally and can be archived via backup function. The audit trail can be reported in PDF format. The operator is solely responsible for storage/archiving after export.

Run no.	Ref.	Topic	Question	Yes	No	Comments
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 as PDF file using Vision Air Manager. Thus, the audit trail 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. Additionally Vision Air is divided in program part Vision Air Routine and Vision Air Manager which gives different user interfaces to routine use (i. e. limited function set) and configuration use.
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 is identified by the login function. (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 other user roles, see also 11.10 (d), No. 1.6. There are two signature levels. The system demands that the same person cannot sign on both levels.
1.13	11.10 (h)	Balance, Connection, Terminals, Input data, Devices	Does the system control validity of the connected devices? <i>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).</i>	X		Metrohm NIR instruments are recognized, their validity is being checked. 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 training of 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 further 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?	<input type="radio"/>		If an electronic signature is used then the operator must have a policy in place 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, Logbook, Manuals	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	<input type="radio"/>		The system has a comprehensive online help system that supports the user and the service personnel. Distribution of paper-based documentation 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?	<input checked="" type="radio"/>		The system documentation is unambiguously assigned to a particular system and software version. Release notes are kept with each software version, document changes can be derived from the entries there. 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		Access to Vision Air 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 Vision Air 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? <ul style="list-style-type: none"> - 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 configuration changes, samples and diagnostic tests, all signatures contain the full name of the signer, date and time of the signature and the meaning (out of a list box) of the signature. 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 is 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 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		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 An existing user account cannot be deleted, only disabled.
4.2	11.100 (a)	Electronic Signature	Are electronic signatures ever reused by, or reassigned to, anyone else?	O		A user ID used is assigned to one person only. It must operationally be ensured, that this user ID is not re-assigned to another person.
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 password has to be entered for each signing process.
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 for each signing process.
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 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.

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		<p>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.</p> <p>It is recommended that unambiguous identification codes (e. g. personnel number or initials) are used for all systems across the whole organization.</p> <p>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.</p>
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		<p>The operator is responsible for checking the identification codes periodically (user accounts are locked if there password expires).</p> <p>The system supports the operator with a password expiration function.</p>
7.3	11.300 (b)	Password, Validity, Password Expiry, Identification, Login, Access Protection	Do passwords periodically expire and need to be revised?	X		<p>The validity period of the password can be defined by the administrator. After this period expires, the user is locked and the system administrator has to unlock the account. The system saves the password history and prevents the user from re-using a password. The size of this password history (i. e. number of password which are not allowed to be reused) can be configured.</p>
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		<p>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 as part of the group "disabled" without any access rights or permissions.</p>
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		<p>The procedure has to be set up by the operator. The administrator can disable the corresponding user account in the system.</p>

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, 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 <i>n</i> incorrect attempts (<i>n</i> is the 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. The information is logged in the event log.
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		Vision Air Manager is capable of sending an e-mail automatically to inform the system administrator about a locked account. Dealing with this information is in the responsibility of 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 on January the 13th 2017. Subject of this audit was the software version 2.0 with all compliance features enabled.

8 Indices

Reference to the page number:

A			
Access Protection.....	3, 5, 12, 13		
Access to Documentation.....	6		
Administrator.....	3, 5		
Archiving.....	3		
Audit Trail.....	2, 4, 5, 6		
Authorization.....	3, 5		
B			
Balance.....	5		
Biometric Electronic Signature.....	11		
C			
Change.....	2, 4		
Compromised ID card.....	13		
Connection.....	5		
D			
Data.....	7		
Data Transfer.....	7		
Devices.....	5		
Disable User Access.....	12		
Distribution of Documentation.....	6		
Documentation.....	6		
E			
Electronic Record.....	3, 4		
Electronic Signature.....	6, 7, 8, 9, 10, 11		
Electronically Disabling ID card.....	13		
Encryption.....	7		
F			
Falsify Electronic Signature.....	10		
FDA.....	3, 5		
I			
ID card.....	13		
Identification.....	12		
Identification Code.....	12		
Inform management.....	13		
Input data.....	5		
Inspection.....	5		
IQ2			
L			
Logbook.....	6		
Login.....	3, 5, 12, 13		
Loss of ID card.....	12, 13		
M			
Manuals.....	6		
Modification of ID cards.....	13		
O			
Operator Entries.....	4		
OQ.....	2		
Overwriting data.....	4		
P			
Password.....	12		
Password Expiry.....	12		
Plausibility check.....	5		
Policy.....	6		
Printout.....	3		
R			
Replacement.....	13		
Report.....	3		
Representative.....	9		
Responsibility.....	6		
Retention Period.....	3, 4		
S			
Sequence.....	5		
Sequence of steps.....	5		
SOP.....	6		
Support.....	5		
System Documentation.....	6		
T			
Terminals.....	5		
Testing of ID cards.....	13		
Training.....	5		
U			
Unauthorized Use.....	13		
Uniqueness.....	12		
User.....	3, 5		
V			
Validation.....	2		
Validity.....	12		

Reference to the run number of the entry:

A	Encryption..... 2.1	Plausibility Check1.11
Access Protection..... 7.11, 7.10, 7.9, 7.8, 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6	F	Policy1.15
Access to Documentation..... 1.16	Falsify Electronic Signature 5.5	Printout1.3
Administrator 1.14, 1.12, 1.6	FDA..... 1.10, 1.4	R
Archiving 1.5	I	Replacement7.7
Audit Trail..... 1.17, 1.10, 1.9, 1.7, 1.2	ID card 7.11, 7.10, 7.7	Report.....1.4, 1.3
Authorization 1.12, 1.6	Identification..... 7.5, 7.4, 7.3, 7.2, 7.1	Representative4.3
B	Identification Code 7.5, 7.4, 7.2, 7.1	Responsibility1.15
Balance 1.13	Inform management..... 7.9	Retention Period.....1.9, 1.5
Biometric Electronic Signature 6.1	Input data..... 1.13	S
C	Inspection 1.10	Sequence1.11
Change..... 1.8, 1.2	IQ1.1	SOP1.17
Compromised ID card 7.6	L	Support.....1.14
Connection 1.13	Logbook..... 1.17, 1.16	System Documentation.....1.17, 1.16
Control over sequence of steps..... 1.11	Login.....7.9, 7.8, 7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6	T
D	Loss of ID card..... 7.6, 7.5	Terminals.....1.13
Data.....2.1	M	Testing of ID cards7.10
Data Transfer2.1	Manuals 1.17, 1.16	Training.....1.14
Devices 1.13, 1.11	Modification of ID cards 7.11	U
Disable User Access 7.5, 7.4	O	Unauthorized Use7.11, 7.9, 7.8
Distribution of Documentation 1.16	Operator Entries..... 1.7	Uniqueness.....7.1
Documentation 1.17, 1.16	OQ 1.1	User.....1.14, 1.12, 1.6
E	Overwriting data..... 1.8	V
Electronic Record..... 1.8, 1.7, 1.5, 1.4, 1.3	P	Validation.....1.1
Electronic Signature6.1, 5.5, 5.4, 5.3, 5.2, 5.1, 4.4, 4.3, 4.2, 4.1, 3.3, 3.2, 3.1, 2.2, 1.15	Password 7.5, 7.4, 7.3, 7.2, 7.1	Validity7.5, 7.4, 7.3, 7.2
Electronically Disabling ID card..... 7.6	Password Expiry 7.3	