UNICORN 5.0
21 CFR Part 11 System Assessment checklist

Amersham Biosciences

Author(s) Stefan Simon	

edition	AA
page	Page 1 of 11
Date 2003-10-14	

1. Procedures and Control for Closed Systems

	Question	Yes	No	Comment
11.10 (a)	Is the system validated?	X		• UNICORN is present in a number of FDA approved processes. • The software comes with a Validation Support Package. • UNICORN is also supported by an Audit Report. This report is based upon an annual on site audit of the current UNICORN version, and of the developmental and support processes of Amersham Biosciences, by an outside independent expert auditor. Most recent audit report date: December 2003. • Amersham Biosciences *Fast Trak* business area offer validation services. • Actual system validation is the responsibility of the user organization.
11.10 (a)	Is it possible to discern invalid or altered records?	X		• All data interaction is performed using UNICORN. • The *Evaluation* log function provides an audit trail for operations performed on data • Data is stored in vendor specific format not recognized by common editors like Excel, Word etc. • Raw data cannot be changed; UNICORN uses checksum protection of files to detect unauthorized raw data manipulation. • To avoid unintentional loss of data limiting access to editors using the *Windows Policy Editor* is recommended.
11.10 (b)	Is the system capable of producing accurate and complete copies of electronic records on paper?	X		*Evaluation*, *Method Editor* and *UNICORN Manager* can produce printouts on paper.
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?	X		Export to several formats are available in: - *Evaluation:File:Export* - *Method Editor:File:Export.* - *UNICORN Manager:Administration:Audit Trail:File:Export*
		X		• File formats for methods and results are backward compatible.

11.10 (c)	Are the records readily retrievable throughout their retention period?			• It is the responsibility of the system user to define the retention period and to have a policy on data storage and migration.
11.10 (d)	Is the system access limited to authorized individuals?	X		• UNICORN uses password control to limit access. • User profiles and users are set-up in *UNICORN Manager:Administration:User Setup.* • Establishing appropriate user policies is the responsibility of the system user.
11.10 (e)	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 concept is supported by: - *UNICORN Manager:Administration:Audit Trail* containing global and system specific information - Resultfile *Logbook* containing all commands and events occurring during a method run. - Result file *Evaluation log* containing all data manipulation performed. Records are time stamped and identified by time zone. UNICORN uses checksum protection of files to detect unauthorized raw data manipulation.
11.10 (e)	Upon making a change to an electronic record, is previously recorded information still available (i.e., not obscured by the change)?	X		Raw data can never be deleted or overwritten. New, processed curves, are stored in new curve positions.
11.10 (e)	Is an electronic record's audit trail retrievable throughout the record's retention period?	X		• It is the responsibility of the system user to define the retention period and to have a policy on data storage and migration. • UNICORN is backward compatible with data from earlier releases.
11.10 (e)	Is the audit trail available for review and copying by the FDA?	X		The audit trail concept is supported by: - *UNICORN Manager:Administration:Audit Trail* containing global and system specific information - Resultfile *Logbook* containing all commands and events occurring during a method run. - Result file *Evaluation log* containing all data manipulation performed. Audit trails can be reviewed on screen. Audit trail files can be exported or printed.
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)?	X		• The sequence of events is defined in the *MethodEditor* the *Method Executor* then ensures that instructions are executed as set-up. • It is the responsibility of the system user to define the sequence of steps in a UNICORN *Method.*

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?	X		• UNICORN provides a set of functions and instructions to support in setting up a secure system. • Conditions are fulfilled when user organization operates the system in the manner prescribed in training and support documentation, which recommend that the user set up the system with an appropriate user structure, that the system is properly installed and that the Operative System is configured to meet requirements.
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? (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		• The instrument (pumps, monitors, valves) itself is closed and not distributed on a network. • Remote clients may access the instrument in a network configuration. These clients are identified and verified as strictly as a local user. If required the system can also be set up for a remote client to be in *View mode* only.
11.10 (i)	Is there documented training, including on the job training for system users, developers, IT support staff?	X		• Training records for UNICORN developers are kept for each individual. Planning of education is updated and followed up on a yearly basis. GMP awareness training is a priority of developers. • It is the responsibility of the user organization to demonstrate that their staff has the education, training and experience to performed their assigned tasks.
11.10 (j)	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	X		• UNICORN provides the possibility to make an electronic signature. • It is the concern of the user organization to establish a policy describing the significance of electronic signatures, in terms of individual responsibility, and the consequences of falsification both for the user organization and for the individual.
11.10 (k)	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	X		• UNICORN provides on-line help, User and administration manuals. • It is the concern of the user organization to establish procedures covering distribution of, access to, and use of operational and maintenance documentation once the system is in operational use.
11.10 (k)	Is there a formal change procedure for system documentation that maintains a time sequenced audit trail for those changes made by the pharmaceutical	N/A		The user organization must ensure adequate change control procedures for operational and maintenance documentation.

	organization?			

2. Additional Procedures and Controls for Open Systems

	Question	Yes	No	Comment
11.30	Is data encrypted?	***N/A***		UNICORN is designed to operate as a closed system.
11.30	Are digital signatures used?	***N/A***		UNICORN is designed to operate as a closed system.

3. Signed Electronic Records

	Question	Yes	No	Comment
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 approval, review, responsibility)	X		Electronic signature is available in - *Method Editor:File:Sign Method* - *System Control:Message* command (optional). - *Start Protocol: Authorized Questions* - *Evaluation File:Sign Result* YYYYMMDD dating is utilized; local time 24 hour clock is utilized
11.50	Is the above information shown on displayed and printed copies of the electronic record?	X		Signatures, including the information above, can be viewed on screen. For example: *Evaluation:File: Sign Result* Signatures can be included in custom printed report formats and in method editor printouts.
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 purpose of falsification?	X		Signatures are stored in the data that is signed. This ensures that the signature is always with the data.

4. Electronic Signatures (General)

	Question	Yes	No	Comment
11.100 (a)	Are electronic signatures unique to an individual?	X		• UNICORN supports definition of Users and Access Groups (*UNICORN Manager:Administration:User Setup*). The software prevents User names from being re-issued. • The system user needs to set up a user structure and to establish SOPs that ensures that Users ids and signatures are unique.
11.100 (a)	Are electronic signatures ever refused by, or reassigned to, anyone else?		X	• UNICORN supports definition of Users and Access Groups (*UNICORN Manager:Administration:User Setup*). The software prevents User names from being re-issued. • The system user needs to set up a user structure and to establish SOPs that ensures that Users ids and signatures are unique.
11.100 (b)	Is the identity of an individual verified11.200 (a) before electronic signature is allocated?	X		• UNICORN verifies the signature given before it is entered in the document. • The user organization needs to verify the identity of individuals being granted access to the system.

5. Electronic Signatures (non-biometric)

	Question	Yes	No	Comment
11.200 (a) (1)(i)	Is the signature made up of at least two components, such as an identification code and password, or an id card and password?	X		UNICORN uses password-password identification.
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).	X		Both password components are executed at each signing.
11.200 (a) (1)(iii)	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	X		Both password components are executed at each signing.
11.200 (a) (2)	Are non-biometric signatures only used by their genuine owners?	N/A		The user organization must ensure that staff only use their own electronic signature, not anyone else’s even on their behalf, as that would be falsification.
11.200 (a) (3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	X		• The user organization needs procedure that users do not divulge their electronic signature. • Passwords are encoded and can not be accessed by other users.

6. Electronic Signatures (Biometric)

	Question	Yes	No	Comment
11.200 (b)	Has it been shown that biometric electronic signatures can be used only by their genuine owner?	N/A		Not applicable. UNICORN uses non-Biometric signatures.

7. Controls for Identification Codes and Passwords

	Question	Yes	No	Comment
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?	***X***		See 11.100 (a) above.
11.300 (b)	Are procedures in place to ensure that the validity of identification codes is periodically checked?	***X***		• The user organization needs procedures to cover: removal of system access from obsolete users; changing of profiles as user roles change; periodic checking of identification codes for inconsistencies with current users; periodic changing of passwords. • Having a password policy is the responsibility of the system user. • Password age, length etc can be set in UNICORN:*UNICORN Manager:Administration:User Setup*
11.300 (b)	Do passwords periodically expire and need to be revised?	***X***		• The user organization needs procedures to cover: removal of system access from obsolete users; changing of profiles as user roles change; periodic checking of identification codes for inconsistencies with current users; periodic changing of passwords. • Having a password policy is the responsibility of the system user. • Password age, length etc can be set in UNICORN:*UNICORN ManagerAdministration:User Setup*
11.300 (b)	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	***X***		• The user organization needs procedures to cover: removal of system access from obsolete users; changing of profiles as user roles change; periodic checking of identification codes for inconsistencies with current users; periodic changing of passwords. • Functionality for recalling the identification codes exist in UNICORN:*UNICORN Manager:Administration:User Setup*, either by deleting or by temporarily disabling the user.
11.300 (c)	Is there a procedure for electronically disabling an	***X***		• The user organization needs procedure for management of lost passwords. • The Administrator can temporarily disable a user or issue a new password.

	identification code or password if it is potentially compromised or lost?			• The user can be configured to be disabled automatically after failed login attempts.
11.300 (d)	Is there a procedure for detecting attempts at unauthorized use and for informing security?	***X***		• Failed attempts to log in are logged in the *UNICORNManager:Administration:Audit Trail*. • The user can also be configured to be disabled automatically after failed login attempts.
11.300(d)	Is there a procedure for reporting repeated or serious attempts at unauthorized use of management?	***N/A***		The user organization needs procedure to describe how response to attempted or actual unauthorized access is managed.

For tokens, cards, and other devices bearing or generating identification code or password information:

	Question	Yes	No	Comment
11.300 (c)	Is there a loss management procedure to be followed if a device is lost or stolen?	***N/A***		UNICORN does not require a token or a card for identification.
11.300 (c)	Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?	***N/A***		UNICORN does not require a token or a card for identification
11.300 (c)	Are there controls over the issuance of temporary and permanent replacements?	***N/A***		UNICORN does not require a token or a card for identification
11.300 (e)	Is there an initial and periodic testing of tokens and cards?	***N/A***		UNICORN does not require a token or a card for identification
11.300(e)	Does this testing check that there have been no unauthorized alterations?	***N/A***		UNICORN does not require a token or a card for identification