

## WinSOTAX Revision 2V

### Compliance of WinSOTAX regarding 21 CFR Part 11

#### Abstract

WinSOTAX is a modular and configurable software package to collect data from various laboratory instruments, to store this data in a database, to retrieve it for analysis, monitoring and report generation. From the beginning the package has been developed following the rules of GLP, GALP and the GAMP guidelines. It therefore matches the requirements of 21 CFR Part 11 with few exceptions by design.

#### Introduction

In the adjacent table the requirements defined in 21 CFR Part 11 are listed paragraph by paragraph and the appropriate feature of WinSOTAX is described, where applicable. The list follows the proposals and annotations as published in the draft GAMP guide to Part 11, as of Dec. 1999. The list starts with Subpart B, § 11.10, of 21 CFR Part 11.

#### 21 CFR Part 11 and WinSOTAX

§	Requirement / text of regulation	Approach of WinSOTAX	Eval. *)
11.10	<b>Controls for closed systems.</b> Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	-- (According to the GAMP interpretation of the legislation WinSOTAX is a "closed system". WinSOTAX does support the owner / user adequately in complying with FDA's requirements; see below)	n.a.
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	WinSOTAX does provide all necessary mechanisms to maintain an audit trail on the electronic records. In addition all user actions are logged in independent files for analysis. WinSOTAX is fully qualified following the GAMP3 and a validation support is available.	✓
11.10 (b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.  Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	WinSOTAX stores all data in a common, normalized and relational designed SQL database. Reports may be reproduced (as printed copies) at any time, including data about setup and configuration ("meta data").  In addition to above, WinSOTAX features an export function for data in electronic form.  The audit trail may be inspected on-screen for any selected method or data record.	✓  ✓  ✓

§	Requirement / text of regulation	Approach of WinSOTAX	Eval. *)
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	WinSOTAX will support file formats of previous versions through future updates (or supply a conversion utility, if applicable)	✓
11.10 (d)	Limiting system access to authorized individuals.	Access to the screens of WinSOTAX is only granted through a login procedure. The functionality of the procedure as well as the recorded user data may not be changed or removed and the user data is encrypted. (cf. also 11.10 (g))	✓
11.10 (e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	<p>In standard setup WinSOTAX does not allow any editing of automatically collected raw data (including creation time stamp). In case of the data import option all affected records are flagged and all reports marked with a corresponding header.</p> <p>The methods defined within WinSOTAX to collect and analyze data and to produce reports contain a full audit trail (generation of a copy including time stamps and operator identification).</p> <p>At times the hardware configuration is assumed fix and therefore not tracked. It is up to the owner of the system to keep records in case the hardware configuration should be changed.</p>	<p>✓</p> <p>✓</p> <p>✗</p>
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	WinSOTAX is driven by predefined and version controlled methods. The procedure to setup or update a method depends on the hardware configuration and is controlled by WinSOTAX.	✓
11.10 (g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<p>WinSOTAX defines some 20 access permissions that may be assigned to individual users or groups of users. There is a user management feature similar to the one of Windows NT.</p> <p>Access at runtime is controlled though the login procedures. Signing a record ("validating" a report or result record) requires individual login and specific access permission.</p>	✓
11.10 (h)	Use of device (e. g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	<p>The hardware configuration is stored within WinSOTAX and may only be changed by a "System Administrator". At runtime identification and setup of the data sources (analytical instruments used in the method) is automatically checked as far as applicable.</p> <p>Systems (instruments) that do not allow automated identification must be identified through manual procedures.</p>	<p>✓</p> <p>✓</p>

§	Requirement / text of regulation	Approach of WinSOTAX	Eval. *)
11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	SOTAX keeps record of the professional qualification of the developers of WinSOTAX.	✓
11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	-- (not a supplier issue)	n.a.
11.10 (k)	Use of appropriate controls over systems documentation including:  (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.  (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Documentation to WinSOTAX is compiled in electronic form as Windows Help File. The file is not accessible for edit by the user. Each release of WinSOTAX contains a release specific version of this file. SOTAX tracks change control through the release control of WinSOTAX.	✓
11.30	Controls for open systems. ...	-- (WinSOTAX is a "closed system")	n.a.
11.50	Signature manifestations.  (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:  (1) The printed name of the signer;  (2) The date and time when the signature was executed; and  (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.  (b) The items identified in paragraphs (a)( 1), (a)( 2), and  (a)( 3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Information about the users is stored in a separate, encrypted section of the database of WinSOTAX.  A signed ("validated") record contains a link to the users record in the user database as well as an appropriate timestamp.  Records in the user database contain full name, identifier, password and access profile of the user and may not be changed (except password and profile) or removed by ordinary means.  The meaning of an access profile (such as "supervisor", "QC person", etc.) must be defined and controlled by the owner. It is good practice to use this identifiers as names of access profiles.  Whenever a validated report is printed the validation information (full name, timestamp) is part of the printout.	✓  ✓  ✓  ✓  ✓
11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	See 11.10 (g) and 11.50 for detailed explanations.  The electronic signing of reports is an optional feature of WinSOTAX. The owner may choose to stay with handwritten signature on original printouts.	✓

§	Requirement / text of regulation	Approach of WinSOTAX	Eval. *)
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The user database of WinSOTAX in itself is unique for it does not allow for multiple entries using same name or identifier. Once created, name or identifier in the record may not be changed any more.	✓
11.100 (b), (c)	.... (not cited)	-- (not a supplier issue)	n.a.
11.200 (a)	<p>Electronic signatures that are not based upon biometrics shall:</p> <p>(1) Employ at least two distinct identification components such as an identification code and password.</p> <p>(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.</p> <p>(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.</p> <p>(2) Be used only by their genuine owners; and</p> <p>(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</p>	<p>WinSOTAX does not use biometrics.</p> <p>The login for signing a record consists of entering an identifier and the corresponding password.</p> <p>For each record to be signed a full login procedure is needed.</p> <p>For each record to be signed a full login procedure is needed.</p> <p>-- (not a supplier issue)</p> <p>The user data in WinSOTAX is encrypted and may not be accessed unless through proper login as "system administrator".</p>	<p>✓</p> <p>✓</p> <p>✓</p> <p>n.a.</p> <p>✓</p>
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	-- (WinSOTAX does not support user identification upon biometrics)	n.a.
11.300 (a)	<p>Controls for identification codes/ passwords.</p> <p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</p> <p>(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.</p>	See 11.100 (a).	✓

§	Requirement / text of regulation	Approach of WinSOTAX	Eval. *)
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e. g., to cover such events as password aging).	WinSOTAX require that users periodically change their passwords	✓
11.300 (c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	The "system administrator" may define or change passwords in WinSOTAX. Users are able to change their passwords	✓
11.300 (d)	Use of transaction safeguards to prevent unauthorized use of passwords and/ or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	WinSOTAX does log any attempt of login in an independent log file. After 3 unsuccessful attempts of id/password combinations WinSOTAX will halt and shut down automatically.	✓
11.300 (e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	WinSOTAX expects login input through the keyboard interface. If other input devices are installed within this interface it is up to the owner to setup testing procedures.	n.a.

\*) Evaluation of compliance:

- n.a. .... not applicable;
- ✓ ..... in full compliance;
- ✗ ..... in partial compliance (does need owner action);
- ↘ ..... compliance problem will be addressed in a future update;
- † ..... there is no solution within WinSOTAX.