Sparta Systems Stratas Solution

21 CFR Part 11 and Annex 11 Assessment

October 2017

Introduction

The purpose of this document is to outline the roles and responsibilities for compliance with the FDA's 21 CFR Part 11 and the European Union's Annex 11 as they apply to Sparta System's Stratas product. The regulations require organizations to have administrative, procedural and technical controls in place. While it is not possible for Sparta to offer a turnkey 21 CFR Part 11 or EU Annex 11 compliant system, the recommendations in this document will assist using organizations in achieving compliance.

Both regulations cover the same topic, the use of computerized systems in regulatory environments. However, the approach of 21 CFR Part 11 is to clarify the requirements to be met with an emphasis on activities and reporting. EU Annex 11 points to risk assessment as the start of compliance activities. In addition, Part 11 differentiates security for open and closed systems, with security for open systems but without reference to risk and criticalities. The aggregate of these differences is represented with the comparison matrix shown below.

High-level Comparison of EU Annex 11 and FDA 21 CFR Part 11

	Part 11	Annex 11
Scope/Principle	Electronic records and electronic signatures as used for all FDA regulated activities.	Computerized systems as part of GMP regulated activities. Application should be validated. IT infrastructure should be qualified.
Focus	Using electronic records and signatures in open and closed computer systems.	Risk- based quality management of computerized systems.
Objective	Electronic records and signatures should be as trustworthy and reliable as paper records and handwritten signatures.	Using a computerized system should ensure the same product quality and quality assurance as manual systems with no increase in the overall risk.

Procedures and Controls for Closed Systems

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.10(a) Is the system validated?	4.1 Do validation documents and reports cover the relevant steps of the life cycle? 4.2 Do validation documents include change control records (if applicable) and reports on deviations observed during the validation process?	User	Validation is the overall responsibility of the using organization. Sparta validates all products following an established procedure. The validation includes modules pertaining to security, audit trails and data integrity. Sparta provides validation documentation, including a set of Performance Qualifications that help ensure that the operating version of the software in the installed configuration conforms to prepackaged validation tests.
11.10(a) Is it possible to discern invalid or altered records?		Sparta	Stratas offers a full audit trail where relevant changes are logged. The audit trail includes user ID, old and new value and time stamp. Unauthorized changes are prevented by the access security controls. Multiple checks, such as unique identifiers of files, are used to help detect unauthorized data manipulation.
11.10(b) Is the system capable of producing accurate and complete copies of electronic records on paper?	8.1 Is the system capable of producing clear printed copies of electronically stored data?	Sparta	Products provide the ability to print record and audit trail data.
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?		Sparta	Records can be exported for viewing and printing.

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.10(c) Are the records readily retrievable throughout their retention period?	17 Is data archived? If data is archived is it checked for accessibility, readability and integrity? When changes are made to the system, is the ability to retrieve archived data ensured and tested?	User & Sparta	Records are available while subscriptions are current. Local copies of data can be maintained locally post-subscription. *Note: For Supplier Collaboration, Supplier's only have access to data during period defined by the customer. All system of record data is available in TrackWise.*
11.10(d) Is system access limited to authorized individuals?	7.1 How is data secured by both physical and electronic means against damage? How is data accessible throughout the retention period? 12.2 The extent of security controls depends on the criticality of the system.	User & Sparta	A unique user ID and password is required for each user session. The using organization is responsible for defining authorized access to the system.
11.10(e) Is there a secure, computer generated, time stamped audit trail that records the date and time of entries and actions that create, modify, or delete electronic records?	9 Is an audit trail available to document the creation, change or deletion of data? 12.4 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time?	Sparta	Stratas records the user identification, time stamp and action each time a record is created, modified or deleted. The audit trail is secure within Stratas and cannot be modified by a user.
11.10(e) Upon making a change to an electronic record, is the previously recorded information still available (e.g. not obscured by the change)?		Sparta	The Stratas Audit Trail records previous values. Audit Trail entries cannot be deleted.

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.10(e) Is an electronic record's audit trail retrievable throughout the record's retention period?		Sparta	The audit trail is available during the entire retention period.
11.10(e) Is the audit trail available for review and copying by the FDA?		Sparta	The audit trail is available during the entire retention period and can be printed.
11.10(f) If the sequence of system steps or events is important, is this enforced by the system?		User & Sparta	Stratas EQMS allows for fully configurable workflow management, thus the user can define the sequence of steps and events and ensure the proper process must be followed. *Note: For Supplier Collaboration, workflows are fixed and cannot be adjusted by the customer.*
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?	12.1 Are physical and/or logical controls in place to restrict access to the system?	User & Sparta	Stratas is a role based system that enforces consistent behaviors across the application including electronic signature and electronic record controls.
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	4.8 When data is transferred to another data format or system, does the system check the validity to confirm data was not altered in value and/or meaning during migration.	Sparta	Stratas EQMS authenticates all user access using standard HTTP session management with a two-factor credential. This is standard across all browser-oriented devices accessing the system. All data in transit is encrypted using SSL between the input terminal and the central server.

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.10(i) Is there documented training, including on the job training for system users, developers, IT support staff?	2 Is there close cooperation between all relevant personnel such as process owner, system owner, qualified persons and IT? Do all personnel have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties?	User & Sparta	Within Sparta, employees are formally trained on policies, SOPs and work instructions. Employees also receive on the job training appropriate to their responsibilities. These SOPs outline how relevant personnel work together to complete their tasks and areas of responsibility. It is the using organization's responsibility to demonstrate that their staff has the education, training and experience to perform their assigned tasks.
11.10(j) Is there a written policy that makes individuals fully responsible for actions initiated under their electronic signatures?		User	It is the responsibility of the customer to establish a policy describing the significance of electronic signatures in terms of individual responsibility and the consequences of falsification both for the using organization and for the individual. Users are unable to complete registration in Stratas without first confirming that they agree to an electronic signature certification.
11.10(k) Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?		User	Sparta restricts distribution of system operation and maintenance documentation to contracted customers. It is the responsibility of the using organization to establish procedures covering the distribution of, access to, and use of documentation once the system is in use.
11.10(k) Is there a formal change procedure for system documentation that maintains a time sequenced audit trail of changes?		User & Sparta	It is the responsibility of the customer to ensure adequate change control procedures for documentation. Sparta controls this for contents of the Stratas validation package.

Additional Procedures & Controls for Open Systems

21 CFR Part 11	Annex 11	Responsible Party	Stratas

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.30 Is data encrypted?	5. Data What built-in checks are in place to confirm the correct and secure entry and processing of data?		Not Applicable. Closed System.
11.30 Are digital signatures used?			Not Applicable. Closed System

Signed Electronic Records

21 CFR Part 11	Annex 11	Responsible Party	Stratas
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)	14 (c) Do electronic signatures include the time and date applied?	Sparta	Yes.
11.50 Is the above information shown on displayed and printed copies of the electronic record?		User & Sparta	Electronic signature information can be viewed on the record and record history in Stratas. *Note: For Supplier Collaboration, data is available in the audit trail.*
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 the purpose of falsification?	14(b) Are electronic signatures permanently linked to their respective record	Sparta	Yes

Electronic Signatures – General

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.100(a) Are electronic signatures unique to an individual?	Not covered	User & Sparta	Yes. Users log-in via email which is unique.
11.100(a) Are electronic signatures ever reused by, or reassigned to, anyone else?	Not covered	User & Sparta	It is the responsibility of the using organization to ensure user IDs are not reassigned to another user.
11.100(b) Is the identity of an individual verified before an electronic signature is allocated?	Not covered	User	It is the using organization's responsibility to verify the identity of individuals assigned to an electronic record.
11.100(c) Can the user certify that the electronic signatures in their system are the legally binding equivalent to traditional handwritten signatures?	14 (a) Do electronic signatures have the same impact as hand-written signatures within the boundaries of the company?	User	It is entirely the responsibility of the customer to manage this certification to the agency. In Stratas, users are unable to complete registration without first confirming that they agree to an electronic signature certification.

Electronic Signatures – Non-Biometric

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.200(a) (1) Is the signature made up of at least two components, such as an identification code and password?		Sparta	Signatures in Stratas consist of a User ID and Password.
11.200(a) (1) (i) 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 the session.		Sparta	The User ID and Password are entered at each signing.
11.200(a) (1) (ii) If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?		Sparta	The User ID and Password are entered at each signing.
11.200(a) (2) Are non-biometric signatures only used by their genuine owners?		User	It is the responsibility of the using organization to ensure employees only use their own electronic signature.
11.200(a) (3) Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?		User	Using organizations need procedures that users do not divulge their electronic signature (e.g. password).

Electronic Signatures – Biometric

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.200(b) Has it been shown that biometric electronic signatures can be used only by their genuine owner?			Not Applicable.

Controls for Identification Codes and Passwords

21 CFR Part 11	Annex 11	Responsible Party	Stratas
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?		User & Sparta	Yes. Users log-in via email which is unique.
11.300(b) Are procedures in place to ensure that the validity of identification codes is periodically checked?	11 Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. Every significant modification should be validated.	User	The management of change for a fully validated and deployed system is the sole responsibility of the customer. Sparta Systems may be contracted to assist in the deployment and validation of an approved change, but the customer is responsible for maintaining the Change Control process.

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.300(b) Do passwords periodically expire and need to be revised?		User & Sparta	Stratas detects expired passwords and prompts the user to create a new password every 90 days.
11.300(b) Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	12.3 Is the creation, change and cancellation of access authorisations recorded?	User & Sparta	It is the customer's responsibility to provide procedures that address the removal of system access.
11.300(c) Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	12.3 Is the creation, change and cancellation of access authorisations recorded?	User & Sparta	It is the responsibility of the using organization to establish procedures for disabling an identification code and/or password.
11.300(d) Is there a procedure for detecting attempts at unauthorized use and for informing security?		User & Sparta	After the fifth, failed consecutive login or electronic signature attempt, a user's account will be inactivated in Stratas.
11.300(d) Is there a procedure for reporting repeated attempts at unauthorized use of the system to management?		User & Sparta	It is the responsibility of the customer to provide a procedure for reporting repeated or serious attempts at unauthorized use.

Controls for Identification Codes and Passwords – For tokens, cards, and other devices bearing or generating identification code or password information

21 CFR Part 11	Annex 11	Responsible Party	Stratas
11.300(c) Is there a loss management procedure to be followed if a device is lost or stolen?			Not applicable.
11.300(c) Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?			Not applicable.
11.300(c) Are there controls over the issuance of temporary and permanent replacements?			Not applicable.
11.300(e) Is there an initial and periodic testing of tokens and cards?	11 Periodic Evaluation		Not applicable.
11.300(e) Does this testing check that there have been no unauthorized alterations?			Not applicable.

EU Annex 11 Control for which there is no Part 11 Equivalent

Annex 11	Responsible Party	Stratas
1 Risk Management Are decisions on the extent of validation and data integrity controls based on a justified and documented risk assessment?	User & Sparta	Using organizations are responsible for decisions regarding validation and data integrity controls.
3.1 When third parties are used to provide, install, configure, integrate, validate, maintain, modify or retain the system, do formal agreements exist?	User & Sparta	See Subscription agreement.
3.1 Do agreements with third parties clearly define the responsibilities of the third party?	User & Sparta	See Subscription agreement.
3.2 Are third parties audited?	User & Sparta	Using organizations are responsible for auditing any third parties they utilize. Sparta periodically audits all critical vendors.
3.3 Is documentation from commercial off-the-shelf products reviewed to check that user requirements are fulfilled?		Not applicable.
3.4 Is quality system and audit information relating to third party suppliers or developers of software & implemented systems available to inspectors on request?		Not applicable.
4.3 Is an up to date listing of relevant systems and their GMP functionality available? For critical systems, an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, hardware and software pre-requisites and security measures is available.	User & Sparta	Sparta maintains application architecture diagrams, security details, system requirements and specifications and a detailed integration architecture.
4.4 Do user requirement specifications describe the required functions of the system? Is URS based on documented risk assessment and GMP impact. Are User requirements traceable throughout the life-cycle?	Sparta	User requirement specifications drive system design and a traceability matrix is provided. User requirements are the responsibility of the using organization.
4.5	Sparta	Sparta Systems is ISO 9001:2008

Annex 11	Responsible Party	Stratas
Was the system developed in accordance with an appropriate quality management system?		certified.
4.6 For customized systems, what process is in place to ensure the formal assessment and reporting of quality and performance measures for the life-cycle stages of the system.		Not applicable. Stratas is not customized.
4.7 What evidence of test methods and scenarios are available? Were parameter limits, data limits and error handling considered? How are automated testing tools and test environments assessed for adequacy?	Sparta	A validation package is available for each release. Parameter limits, data limits and error handling are considered during validation. Testing tools and environments use industry-leading tools whenever possible, and are otherwise reviewed for adequacy
6 Accuracy Checks What accuracy checks are in place for critical data entered manually?	User	Workflow based controls are in place to ensure manual review of data before record completion.
7.2 Are regular back-ups of relevant data done? How is the integrity and accuracy of data and the ability to restore data checked during validation and monitored periodically?	User	See Sparta backup and restore policy.
8.2 For records supporting batch release, are printouts available to indicate if any data was changed since original entry?		Not applicable.
10 Are system changes made in a controlled manner in accordance with a defined procedure?	User	Using organizations are responsible for defining a procedure for system changes.
13 Are all incidents reported and assessed? Is the root cause of critical incidents identified? Does the identified root cause form the basis of corrective and preventive actions?	User and Sparta	All product related incidents are brought to a weekly meeting where they are prioritized, severity noted and effort is decided. All high severity incidents are investigated, root cause analysis completed, and if applicable, a corrective action is identified.
15 Does the system allow only qualified persons to certify the release of batches and clearly identify and record the person releasing or certifying the batches?		Not Applicable.

Annex 11	Responsible Party	Stratas
16 What provisions are made to ensure continuity of support for critical processes in the event of a system breakdown? Is the time required to bring alternative arrangements into use based on risk and appropriate for the system and business process it supports? Are these arrangements adequately documented and tested?		Sparta leverages AWS redundancy for system fail-over. See the Stratas Whitepaper.

DocuSigned by:
335DA50EBA2C4C3...

October 30, 2017 | 11:06 AM EDT