cytiva

FDA 21 CFR Part 11 System Assessment Checklist

Biacore T200 GxP Software

Table of contents

Introduction

This is a 21 CFR Part 11 System Assessment Checklist. The intention of the document is to give a brief description of the technical functionalities implemented in the Biacore T200 GxP Software version 3.2.1 for the regulated company to comply with requirements in the FDA's 21 CFR Part 11 regulation, ref [1].

Biacore T200 GxP Software (henceforth the Software) consists of these programs:

- Biacore T200 Control Software
- Biacore T200 Evaluation Software
- Biacore T200 GxP Package

Table content

The text in the Question field of the table starts with the original text from *FDA 21 CFR part 11 -- ELECTRONIC RECORDS; ELECTRONIC SIGNATURES*, ref [1]. The text in the Question field of the table ends with Cytiva's interpretation of the section. In the Comment field, the answer of the question is written for the product described.

References

[1] Code of Federal Regulations title 21 part 11 Electronic Records and Signatures https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11
[2] Biacore T200 GxP Handbook, 28976881, Cytiva
[3] Biacore T200 Recommended configuration of operating system for 21 CFR Part 11 compliance, 28981329, Cytiva

Revision history

Revision	Approved by	Description
AA	Thomas Sjöström Quality Management	Original version
AB	Thomas Sjöström QA Sr Site Leader	Updated for version 2.0 of Biacore T200 GxP Software.
AC	Thomas Sjöström QA Sr Site Leader	Updated for version 3.0 of Biacore T200 GxP Software.
AD	Thomas Sjöström QA Sr Site Leader	Updated for version 3.1 of Biacore T200 GxP Software: • Control software 2.0.2 • Evaluation software 3.1 • GxP package 2.0.3
AE	Pär Säfsten Product Manager	Updated for version 3.2 of Biacore T200 GxP Software. Approval aligned to Work Instruction for Software Validation Support File, DOC1098458.
AF	Pär Säfsten Product Manager	Updated for version 3.2.1 of Biacore T200 GxP Software.

Procedures and Controls for Closed Systems

	Question	Yes	No	N/A	Comment
CFR part 11.10	*Controls for closed systems.* *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:*				
11.10 (a)	*CFR part 11.10 (a): Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.* Is the system checked to ensure accuracy, reliability and consistent intended performance?	x			• Development and verification have been performed according to our Quality Management System that is certified according to ISO 9001. • Cytiva Fast Trak Validation offers validation services. • Final validation of the system in target environment is a responsibility of the regulated company.
11.10 (a)	*CFR part 11.10 (a): See above* Is it possible to discern invalid or altered records?	x			• Any changes made to a run or evaluation file will need to be saved with a new file name annotated with an audit trail. • File accessibility should be restricted via the operative system or network settings, see ref [2] and [3].
11.10 (b)	*CFR part 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.* Is the system capable of generating accurate and complete copies of records in human readable form, electronic form, and as printouts suitable for inspection, review, and copying by the agency?	x			• All GxP relevant data within the system can be printed. • An automatic backup of files to a customer specified folder is a feature in the Software. • All electronic records are saved in a proprietary format and require dedicated software to inspect and review.
11.10 (c)	*CFR part 11.10 (c): Protection of records to enable their accurate and ready retrieval throughout the records retention period.* Are the records readily retrievable throughout their retention period?	x			• Electronic records are stored as files and can thus be stored accordingly on a suitable media. • Dedicated software is required to open and view the files. • Procedures to define the retention period and suitable storage policy of maintained records.
11.10 (d)	*CFR part 11.10 (d): Limiting system access to authorized individuals.* Has the system access control?	x			• System is designed to limit access to authorized individuals by using Windows access control system. Only users that belong to any of the Biacore specific user groups will have access to the Software. • Procedures to handle the documentation and maintenance of users and access rights.

	Question	Yes	No	N/A	Comment
11.10 (e)	*CFR part 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.* 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? Upon making a change to an electronic record, is previously recorded information still available (i.e., not obscured by the change)? Is an electronic record's audit trail retrievable throughout the record's retention period? Is the audit trail available for review and copying by the FDA?	x			• Creation of and changes in GxP runs and evaluations are covered by a secure, computer generated, time stamped audit trail. • The audit trail information is stored together with the electronic record (same electronic file). • Deletion of electronic records can be disabled or granted to certain users only as required. • Any changes made to a run or evaluation file will be enforced by the system to be saved with a new file name, with a link back to the original file in the audit trail. The original file is left unchanged. • File creation, modification and deletion rights should be restricted via the operative system or network settings, see ref [2] and [3]. • Procedures to avoid branching of file versioning is recommended. • Procedures to define the retention period and suitable storage policy of maintained records. • The audit trail information can be printed. • The electronic files may be copied. Dedicated software is required to open and view the files.
11.10 (f)	*CFR part 11.10 (f): Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.* 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 Software forces the operator to perform all steps in correct order whenever applicable within a published run or evaluation. Suitable evaluation settings can be linked to each run method, by creating a Published Procedure, so that correct evaluation settings are automatically applied, and correct operation sequence is used. • It is the responsibility of the regulated company to define suitable settings when creating a Published Procedure. • It is the responsibility of the regulated company to establish procedures to ensure correct operational procedures between runs.
11.10 (g)	*CFR part 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.* 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			• System is designed to limit access to authorized individuals by using Windows access control system. Only users that belong to any of the Biacore specific user groups will have access. • System does not include functions for electronic signatures. • Procedures to handle the documentation and maintenance of access rights are recommended.

	Question	Yes	No	N/A	Comment
11.10 (h)	*CFR part 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.* 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			• Authorization of the connected Biacore instrument is performed before the connection is established. • The instrument itself is closed and not distributed on a network. • The Software stores together with each result operational statistics that includes serial number of the used Biacore instrument. • The serial number is available when inspecting results.
11.10 (i)	*CFR part 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.* Is there documented training, including on-the-job training for system users, developers, IT support staff?			x	• Training records for software developers are kept within Cytiva. • It is the responsibility of the regulated company to demonstrate that their personnel have the required education, training, and experience to perform their assigned tasks.
11.10 (j)	*CFR part 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.* Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?			x	• Electronic signatures are not implemented in the Software.
11.10 (k)	*CFR part 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.* Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	x			• Biacore system documentation, such as operating instructions and user manuals, is version controlled. • Procedures covering distribution of, access to, and use of operation and maintenance documentation are recommended. • It is the responsibility of the regulated company to ensure adequate change control procedures for operation and maintenance documentation.

Additional Procedures and Control for Open Systems

	Question	Yes	No	N/A	Comment
CFR Part 11.30	*Controls for open systems:* *Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.*				
11.30	*CFR part 11.30 Controls for open systems* Is data encrypted? Are digital signatures used?			x	• The Software is designed to operate as a closed system.

Signed Electronic Records

	Question	Yes	No	N/A	Comment
CFR Part 11.50	*Signature manifestations*				
11.50 (a)	*CFR part 11.50 (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.* Do signed electronic records contain the above information?			x	• The Software has no support for electronic signatures.
11.50 (b)	*CFR part 11.50 (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).* Is the above information shown on displayed and printed copies of the electronic record?			x	• The Software has no support for electronic signatures.
CFR Part 11.70	*Signature/record linking*				
11.70	*CFR part 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.* 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 Software has no support for electronic signatures.

Electronic Signatures (General)

	Question	Yes	No	N/A	Comment
CFR Part 11.100	*General requirements*				
11.100 (a)	*CFR part 11.100 (a): Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.* Are electronic signatures unique to an individual?			x	• The Software has no support for electronic signatures.
11.100 (b)	*CFR part 11.100 (*b*): Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.* Are electronic signatures ever reused by, or reassigned to, anyone else? Is the identity of an individual verified by the organization before electronic signature is allocated?			x	• The Software has no support for electronic signatures.
11.100 (c)	*CFR part 11.100 (c): Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.* *(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.* *(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.* Is the person using the electronic signature aware that their electronic signature is intended to be the legally binding equivalent to traditional handwritten signatures?			x	• The Software has no support for electronic signatures.
CFR Part 11.200	*Electronic signature components and controls*				

	Question	Yes	No	N/A	Comment
11.200 (a) (1) (i)	*CFR part 11:200 (a): Electronic signatures that are not based upon biometrics shall:* *(1) Employ at least two distinct* identification *components such as an identification code and password.* *(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.* 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 Software has no support for electronic signatures.
11.200 (a) (1) (ii)	*CFR part 11:200 (a): Electronic signatures that are not based upon biometrics shall:* *(1) Employ at least two distinct* identification *components such as an identification code and password.* *(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.* 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 Software has no support for electronic signatures.
11.200 (a) (2)	*CFR part 11:200 (a): Electronic signatures that are not based upon biometrics shall:* *(2) Be used only by their genuine owners* Are non-biometric signatures only used by their genuine owners?			x	• The Software has no support for electronic signatures.

	Question	Yes	No	N/A	Comment
11.200 (a) (3)	*CFR part 11:200 (a): Electronic signatures that are not based upon biometrics shall:* *(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.* Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?			x	• The Software has no support for electronic signatures.

Electronic Signatures (Biometric)

	Question	Yes	No	N/A	Comment
CFR Part 11.200	*Electronic signature components and controls*				
11.200 (b)	*CFR part 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.* Has it been shown that biometric electronic signatures can be used only by their genuine owner?			x	• The Software has no support for electronic signatures.

Controls for Identification Codes and Passwords

	Question	Yes	No	N/A	Comment
11.300	*Controls for identification codes/ passwords.* *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:*				
11.300 (a)	*CFR part 11.300 (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.* 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 Software does not have any built-in user account management but is using Windows access control system for user authentication. • Consequently, procedures for identification codes and passwords is a responsibility of the regulated company.
11.300 (b)	*CFR part 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).* Are procedures in place to ensure that the validity of identification codes is periodically checked? Do passwords periodically expire and need to be revised? Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?			x	• The Software does not have any built-in user account management but is using Windows access control system for user authentication. • Consequently, procedures for identification codes and passwords is a responsibility of the regulated company.
11.300 (c)	*CFR part 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.* Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?			x	• The Software does not have any built-in user account management but is using Windows access control system for user authentication. • Consequently, procedures for identification codes and passwords is a responsibility of the regulated company.

	Question	Yes	No	N/A	Comment
11.300 (d)	*CFR part 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.* Is there a procedure for detecting attempts at unauthorized use and for informing security? Is there a procedure for reporting repeated or serious attempts at unauthorized use of management?			x	• The Software does not have any built-in user account management but is using Windows access control system for user authentication. • Consequently, procedures for identification codes and passwords is a responsibility of the regulated company.

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

	Question	Yes	No	N/A	Comment
11.300	*Controls for identification codes/ passwords.* *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:*				
11.300 (e)	*CFR part 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.* Is there a loss management procedure to be followed if a device is lost or stolen? Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised? Are there controls over the issuance of temporary and permanent replacements? Is there an initial and periodic testing of tokens and cards? Does this testing check that there have been no unauthorized alterations?			x	• The Software does not have any built-in user account management but is using Windows access control system for user authentication. • Consequently, procedures for identification codes and passwords is a responsibility of the regulated company.

cytiva.com/biacore