

Empower 2 Software

EU Annex 11 COMPLIANCE ASSESSMENT

Note: Information presented in this document assumes that the appropriate Empower 2 System Policies have been configured for Electronic Record (ER) and Electronic Signature (ES) support.

Overview	Yes/No/NA
Is the system a Closed System, where system access is controlled by the persons who are responsible for the content of the electronic records that are on the system?	Yes
Does the system use an ID/ password combination?	Yes
Does the system use tokens?	No
Does the system use biometrics?	No

Ref.		Yes/No/NA	Explanation
EU Annex 11			
1.	Annex 11.2 Validation	NA	Each organization must develop a controlled, documented procedure for managing system testing and validation based on acceptable industry standards.
2.	Annex 11.2 Validation	Yes	Empower 2 software allows users to be compliant with Annex 11, but complete compliance can only occur within a validated electronic records environment. Validation documentation is available for examination during an audit of the Waters quality system for data products development.
3.	Annex 11.3 System	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.

Ref.			Yes/No/NA	Explanation
4.	Annex 11.4 System	A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures.	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
5.	Annex 11.5 System	The software is a critical component of a computerized system. The user of such software should take all reasonable steps to ensure that it has been produced in accordance with a system of Quality Assurance.	Yes	Waters Corporation has structurally validated Empower 2 software and supplies a certificate of structural validation with the Empower 2 software. Validation documentation is available for examination during an audit of the Waters quality system for data products development.

Ref.	Ref.	Yes/No/NA	Explanation
6.	Annex 11. 6 System	The system should include, where appropriate, built-in checks of the correct entry and processing of data.	<p>Yes</p> <p>Empower 2 designates appropriate input based on user authentication, and not device authentication. Raw data may only come from a device on which Empower 2 acquisition software has been configured. Other instructions may only come from devices on which Empower 2 database access has been configured and enabled.</p> <p>Empower 2 software allows the use of Wizards to ensure proper processing as well as built in restrictions related to the order of processing data. In order to access the Empower 2 system, individuals must have a user account. This account will define the capabilities that user will have on the system. Without an account, no access to the system is allowed.</p> <p>Raw data may only come from a device on which Empower 2 acquisition software has been configured. Other instructions may only come from devices on which Empower 2 database access has been configured and enabled.</p>
7.	Annex 11. 7 System	Before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results. If a manual system is being replaced, the two should be run in parallel for a time, as a part of this testing and validation.	<p>NA</p> <p>Each organization must develop a controlled, documented procedure for managing system testing and validation based on acceptable industry standards.</p>

Ref.	Ref.	Yes/No/NA	Explanation
8.	Annex 11. 8 System	Data should only be entered or amended by persons authorized to do so.	<p>Yes</p> <p>In order to access the Empower 2 system, individuals must have a user account. This account will define the capabilities that user will have on the system. Without an account, no access to the system is allowed.</p> <p>User access is based on the concept of “User Types”. A user type defines a specific level of access based on allowed activities/responsibilities. Changes to user types are documented in the system audit trail. The ability to create, modify or delete user types are discrete privileges that may be assigned to specific individuals.</p> <p>User access levels are set and approved during the process of creating a user. Only an individual who has explicitly been given the privilege to create or alter a user account can change the access level for a particular user.</p>
9.	Annex 11. 8 System	Suitable methods of deterring unauthorized entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals.	<p>Yes</p> <p>User access levels are set and approved during the process of creating a user. Only an individual who has explicitly been given the privilege to create or alter a user account can change the access level for a particular user.</p> <p>User creation, modification and deletion are controlled through application security and are only accessible to appropriately privileged users. In addition, Empower 2 System Policies can be used to predefine specific aspects of the user creation process to ensure compliance with Annex 11.</p>

Ref.			Yes/No/NA	Explanation
10.	Annex 11.8 System	There should be a defined procedure for the issue, cancellation, and alteration of authorization to enter and amend data, including the changing of personal passwords.	NA	Each organization must develop controlled, documented procedures for compliance with this requirement. Empower 2 allows a user account to be removed from active use while retaining it for complete records. Each organization must develop controlled, documented procedures to ensure proper notification of user status changes.
11.	Annex 11.8 System	Consideration should be given to systems allowing for recording of attempts to access by unauthorized persons.	Yes	When an invalid login attempt is made, an immediate notification is displayed on the consoles of all system administrators currently logged into the system. In addition, all system administrators not currently logged in will be informed when they next access the Empower 2 system. This information is also stored in the software message log and System Audit Trail.
12.	Annex 11.9 System	When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.	NA	Each organization must develop controlled, documented procedures for compliance with this requirement. Data fields may also have upper and lower limits defined.

Ref.			Yes/No/NA	Explanation
13.	Annex 11.10 System	The system should record the identity of operators entering or confirming critical data.	Yes	<p>In order to access the Empower 2 system, individuals must have a user account. This account will define the capabilities that user will have on the system. Without an account, no access to the system is allowed.</p> <p>User access is based on the concept of "User Types". A user type defines a specific level of access based on allowed activities/responsibilities. Changes to user types are documented in the system audit trail. The ability to create, modify or delete user types are discrete privileges that may be assigned to specific individuals.</p> <p>Every electronic record or meta data relating to a record, which is created, modified or deleted by a user is monitored and recorded along with the identity of the operator.</p>
14.	Annex 11.10 System	<p>Authority to amend entered data should be restricted to nominated persons.</p> <p>Any alteration to an entry of critical data should be authorized and recorded with the reason for the change.</p>	Yes	<p>The abilities to modify or delete data within the Empower 2 software application are specifically assigned privileges. All actions involving a creation, deletion or modification of data is audit trailed and requires user confirmation before changes are committed to the database.</p> <p>All previous values are stored in the embedded database. When data is changed, new values are added to the database, and previous information is not overwritten or obscured. The privileges to change or delete data may be assigned only to specific users.</p> <p>In addition, Audit Trails can be configured to require the input of a text string (free text or predefined texts) indicating the reason for change.</p>

Ref.	Ref.	Yes/No/NA	Explanation
15.	<p>Annex 11.10 System</p>	<p>Consideration should be given to building into the system the creation of a complete record of all entries and amendments (an "audit trail").</p>	<p>Yes</p> <p>A designated system administrator may configure audit trail settings on a per project basis, no other users will have control over audit trails. All activities for all users in projects with full audit trail turned on will be audit trailed, with no user types or activities treated differently.</p> <p>The system audit trail cannot be disabled. Empower 2 data is stored in Projects and it is impossible to disable or modify audit trail settings for a project after its creation. A designated system administrator may configure audit trail settings.</p> <p>Project audit trails cannot be modified or deleted. The system audit trail can be archived and removed – and requires the active collaboration of 2 system administrators to sign off on this archival and removal before the process can begin.</p> <p>Audit trails are maintained either as part of project archives and database backups. In addition, the system audit trail may be specifically archived in either ASCII or binary format. A binary archived system audit trail can be retrieved into the Empower 2 "Offline System Audit Trail" view for review and analysis. ASCII archives may used for paper or electronic review outside Empower 2.</p> <p>Full searching and filtering capabilities are available with the Empower 2 audit trails.</p>

Ref.			Yes/No/NA	Explanation
16.	Annex 11.11 System	<p>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.</p> <p>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.</p>	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
17.	Annex 11.12 System	For quality auditing purposes, it should be possible to obtain clear printed copies of electronically stored data.	Yes	<p>It is possible to view and print the entire contents of electronic records from within Empower 2.</p> <p>It is also possible to generate all the records electronically in a format that can be put on a portable medium (e.g. diskette or CD) or transferred electronically.</p>
18.	Annex 11.13 System	Data should be secured by physical means against willful or accidental damage, in accordance with item 4.9 of the Guide.	NA	Each organization must develop a controlled, documented procedure for managing system security and protection.

Ref.			Yes/No/NA	Explanation
19.	Annex 11.13 System	Data should be secured by electronic means against willful or accidental damage, in accordance with item 4.9 of the Guide.	Yes	<p>If a user attempts to modify the raw data in any way, it is marked as altered and can no longer be used or viewed in Empower 2.</p> <p>Even if Full Audit Trail has been turned off, audit trails are available in the database. Alteration of information creates new values that are stored in the database. Records are never overwritten and full audit trails are available to document changes. Access to these hidden Audit Trails will require calling Waters and help from the Waters development team.</p>
20.	Annex 11.13 System	Stored data should be checked for accessibility, durability and accuracy. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used.	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
21.	Annex 11.14 System	Data should be protected by backing-up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.

Ref.			Yes/No/NA	Explanation
22.	Annex 11.15 System	<p>There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them.</p> <p>For example, information required to effect a recall must be available at short notice.</p>	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
23.	Annex 11.16 System	The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded.	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
24.	Annex 11.17 System	A procedure should be established to record and analyze errors and to enable corrective action to be taken.	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
25.	Annex 11.18 System	When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of the responsibilities of that outside agency (see Chapter 7).	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.

Ref.	Ref.	Yes/No/NA	Explanation
26.	Annex 11.19 System	When the release of batches for sale or supply is carried out using a computerized system, the system should allow for only a Qualified Person to release the batches and it should clearly identify and record the person releasing the batches.	<p>Yes</p> <p>In order to access the Empower 2 system, individuals must have a user account. This account will define the capabilities that user will have on the system. Without an account, no access to the system is allowed.</p> <p>The audit trail records the operator name, date, time, and indication of record (or file) being approved for release (if electronic signature is used), and if configured by the administrator in the System Policies will also require a comment for the audit trail.</p> <p>There are two levels of electronic signature available and the ability to make the final approval signature can be limited to a specific group of individuals.</p>