DIFFRAC.SUITE

User Manual

EU Annex 11 Policy - White Paper

Original Instructions

Innovation with Integrity

XRD

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections are included in subsequent editions. Suggestions for improvement are welcome.

All configurations and specifications are subject to change without notice.

Order no. DOC-M88-EXX249 V1 September 03, 2019.

Printed in the Federal Republic of Germany.

Bruker AXS GmbH
Östliche Rheinbrückenstr. 49
76187 Karlsruhe, Germany
Tel. +49 721 50997-0
Fax +49 721 50997-5654
info.baxs@bruker.com
www.bruker.com

Table of Contents

Table of Contents

1 Purpose

This document outlines Bruker AXS's interpretation of EU Annex 11 requirements and implementation into Bruker AXS XRD systems (hard- and software).

For Bruker AXS's interpretation of 21 CFR Part 11 requirements and implementation please refer to the document "Bruker AXS 21 CFR Part11 Policy - White Paper", order number DOC-M88-EXX241.

2 General

Bruker AXS XRD systems (hard- and software) are being developed by applying a formal design process and product development life cycle according to Bruker AXS's ISO9001 and 14001 certified product development procedures, based on US cGAMP and EudraLex Volume 4 Annex 15 requirements. Written standards exist such as coding standards, configuration management, programmer qualifications, software version control, maintenance, formal testing of software/hardware, incident reporting and tracking, and disaster recovery.

DIFFRAC.SUITE Part11 is the software package used for X-ray powder diffraction data acquisition and evaluation using Bruker AXS XRD systems.

DIFFRAC.SUITE Part11 supports 21 CFR Part 11 / EU Annex 11 compliance in regulated environments by offering several tools to provide and guarantee authenticity, integrity and confidentiality of electronic records and electronic signatures including

- Secure system log-ins
- Automatic audit trail generation
- Electronic signatures with reports and data
- Network security with Windows
- Tamper proof data files with the ability to discern invalid or altered records
- Data storage and archiving

Bruker AXS also offers tools and expertise to help meeting the requirements of equipment qualification EQ (including design qualification DQ, installation qualification IQ, operation qualification OQ, and performance qualification PQ) for system validation (21 CFR Part 11, §B11.10a), which is the ultimate responsibility of the system owner.

3 DIFFRAC.SUITE Part11

DIFFRAC.SUITE Part11 is compliant to the requirements for a closed system as defined by 21 CFR Part 11, section 11.3,

“an environment in which the system access is controlled by persons who are responsible for the content of electronic records that are on the system”,

and section 11.10,

“Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure authenticity, integrity, and when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as genuine”.

The following sections outline, how system safety, audit trailing, electronic records, electronic signatures, data storage, and archiving are implemented in DIFFRAC.SUITE Part11 to support 21 CFR Part11 as well as EU Annex 11 requirements.

3.1 System Safety

Operation of DIFFRAC.SUITE Part11 is possible using a local PC, PCs within a LAN or via Internet. Security is ensured due to a two-stage security system, that is the mandatory and independent Windows and DIFFRAC.SUITE Part11 secure logons. Logon can be restricted to any PCs using their unique IP address.

An administrator has to configure Windows secure logons for controlling access to the system and should also install and configure suited backup and disaster recovery procedures.

Successful login to the Windows system is required to launch and logon to DIFFRAC.SUITE Part11, each login attempt is added to the system audit trail (see section *Audit Trails [▶ 6]*).

To prevent unauthorized access to the system, the maximum number of unsuccessful login attempts to a user account is limited and can be configured by the administrator. If the maximum number of unsuccessful login attempts is exceeded, the DIFFRAC.SUITE Part11 user account is disabled and must be reactivated by the administrator before it can be used again. If an account is deactivated a message is displayed informing about deactivation. The deactivation message is also added to the system audit trail (see section *Audit Trails [▶ 6]*). If there are repeated failed logons the time between again opening the logon dialog will be increased considerably to prevent password guessing.

The combination of username and password is enforced to be unique by the system. Usernames cannot be reused, reassigned or deleted. The administrator can disable user accounts and set a new password, but cannot read any passwords of any user. He can also define the minimum length, expiration date or expiry period and configure a user login timeout.

DIFFRAC.SUITE Part11 defines a set of predefined user account levels configured with default rights: **IT Administrator**, **Lab Manager**, **Engineer** and **Operator**. An **IT Administrator** can only modify the user rights, whereas a **Lab Manager** is the highest customer level. A **Lab Manager** can modify the rights and additionally change the instrument configuration and start and watch experiments. An **Engineer** can start signed experiments and watch the experiment results, an **Operator** can only start experiments.

The group rights of every group can be configured by the customer according to his company regulations.

3.2 Audit Trails

DIFFRAC.SUITE Part11 uses a database to store the user data, the experiments, results and audit trails.

- The system **Audit trail** automatically documents who has accessed the computer system and what operations he or she has performed during a given period of time such as logins, logouts, any configuration changes of user accounts or the instrument by the **LabManager**.
- New experiments, results and evaluations are stored in the database as **electronic records**. Those can be signed, and the signer, date/time is also written into the database and the audit trail.

The database is inaccessible by the customer and protected by user name and password.

Auditing trailing is always enabled; it cannot be disabled, nor can it be bypassed. Audit trails always record the event type, the username of the person causing the event, the date/time of the event, and all operator entries. Audit trails are stored into the database, and can be read by DIFFRAC.SUITE.

3.3 Electronic Records

In DIFFRAC.SUITE Part11 electronic records comprise instrument configuration files, experiments, measurement (raw) data files and files containing evaluation results created by application software. For each file an electronic record audit trail is automatically created and stored into the database.

For data evaluation all evaluation steps performed within application software are recorded in an electronic record audit trail which is automatically associated with result files written by this software package. Whenever the user decides to save new evaluation results as a results file, this file can be electronically signed (section *Electronic Signatures [▶ 7]*) and will be added to the database as a new revision. The related electronic record audit trail allows to unambiguously link these different revisions with the respective evaluation steps performed.

All electronic records are protected from both modification and deletion by the database. The database itself is inaccessible by the user and protected by username and password.

The readability of all file formats is guaranteed by the respective application software throughout a minimum retention period at least as long as that required for the subject electronic records. Archiving and restoring of the database is possible from DIFFRAC.SUITE.

3.4 Electronic Signatures

In DIFFRAC.SUITE Part11 non-biometric electronic signatures are implemented and include both the user name and the full printed name of the signer, the date and time when signed. The identity of the user is verified at login to DIFFRAC.SUITE Part11 (section *System Safety [▶ 6]*).

All sessions are treated as non-continuous sessions, signing always requires username and password. Each electronic signing is logged into both the system audit trail and the respective electronic record audit trail (section *Audit Trails [▶ 6]*).

An electronic signature is stored in the database in the same electronic record that is signed and therefore directly linked to the electronic record. The database is inaccessible by the user and protected by username and password.

As an alternative to electronic signatures DIFFRAC.SUITE Part11 also allows to print and manually sign paper records, which are tamper protected and linked to the respective electronic record by a unique database id of the electronic record printed on each page of the paper record.

3.5 Data Storage and Archiving

DIFFRAC.SUITE Part11 uses a PostgreSQL database to store electronic records comprising user data, experiment details, evaluation results, and audit trails.

The software provides database upgrades, ensuring a retention period at least as long as is required for the electronic records in question, as well as backup and recovery capabilities for regular data backup.

4 Checklist

Section	Requirement	Implementation
1. Risk management		
	Risk management should be applied throughout the life cycle of the computerized system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized system.	Bruker AXS XRD systems (hard- and software) are being developed by applying a formal design process and product development life cycle according to Bruker AXS's ISO9001 and 14001 certified product development procedures, based on US cGAMP and EudraLex Volume 4 Annex 15 requirements. Bruker AXS trains its personnel according to its quality procedure, Q521. Training includes GxP and 21 CFR Part 11 requirements, where applicable. Bruker AXS is ISO 9001 certified and follows these guidelines when developing all products.
2. Personnel		
	There should be close cooperation between all relevant personnel such as process owner, system owner, qualified persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Bruker AXS provides a comprehensive selection of training classes for system owner's service personnel and end-users.
3. Suppliers and service providers		
3.1	When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT departments should be considered analogous.	Bruker AXS requires formal agreements for installation, configuration, integration, validation, and maintenance of its XRD systems. Both written and onsite audits are welcome. Bruker AXS offers full support before (Design Qualification, DQ) and at any time after instrument purchase. Relevant documentation will be made available on request.
3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	
3.3	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	

Section	Requirement	Implementation
3.4	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	
4. Validation		
4.1	The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	Bruker AXS offers products and services to support system validation including Design Qualification (DQ), Installation Qualification (IQ), Operation Qualification (OQ), and Performance Qualification (PQ). System specifications, standards, acceptance criteria, and validation procedures are published and part of the system documentation. Bruker AXS offers full support before (Design Qualification) and after instrument purchase in matching actual instrument specifications with user requirements. Both written and onsite audits are welcome. Data format changes are not supported by by the DIFFRAC.SUITE. The software and its database can be transferred to another PC system. Electronic records are protected against corruption, modification and deletion.
4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	
4.3	An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be 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, any hardware and software pre-requisites, and security measures should be available.	
4.4	User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life cycle.	
4.5	The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.	
4.6	For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life cycle stages of the system.	

Section	Requirement	Implementation
4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	
4.8	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	
5. Data		
	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	Data exchange is limited between instrument and measurement PC and is protected by TCP/IP transport layer security. Electronic records are protected against corruption, modification and deletion.
6. Accuracy checks		
	For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	For all manually entered data, the software can be configured to enforce the 4-eye principle. This is achieved by activating mandatory electronic signatures by a supervisor.
7. Data storage		
7.1	Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.	Archiving and restoring of the database is possible from DIFFRAC.SUITE. The database is protected against unauthorized access. The readability of all file formats is guaranteed by the respective application software throughout a minimum retention period at least as long as that required for the subject electronic records.
7.2	Regular backups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	

Section	Requirement	Implementation
8. Printouts		
8.1	It should be possible to obtain clear printed copies of electronically stored data.	Supported by DIFFRAC.SUITE Part11 (printing, audit trailing).
8.2	For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	
9. Audit trails		
	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated “audit trail”). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	DIFFRAC.SUITE Part11 offers full audit trailing support as detailed in section *Audit Trails [▶ 6]*.
10. Change and configuration management		
	Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Bruker AXS offers Operation Qualification (OQ) products and services to support changes made to it's XRD systems.
11. Periodic evaluation		
	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Bruker AXS offers products and services to support Performance Qualification (PQ).
12. Security		
12.1	Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	DIFFRAC.SUITE Part11 offers a comprehensive set of features to guarantee system data security as detailed in section *DIFFRAC.SUITE Part11 [▶ 5]*.
12.2	The extent of security controls depends on the criticality of the computerized system.	
12.3	Creation, change, and cancellation of access authorizations should be recorded.	

Section	Requirement	Implementation
12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	
13. Incident management		
	All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	All relevant events including system failures are recorded in a system log and the audit trail, as applicable. The system log can be inspected.
14. Electronic signature		
	Electronic records may be signed electronically. Electronic signatures are expected to: 1. have the same impact as hand-written signatures within the boundaries of the company, 2. be permanently linked to their respective record, 3. include the time and date that they were applied.	DIFFRAC.SUITE Part11 offers a comprehensive set of features to support electronic signatures as detailed in section *Electronic Signatures [▶ 7]*.
15. Batch release		
	When a computerized system is used for recording certification and batch release, the system should allow only qualified persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	DIFFRAC.SUITE Part11 offers a comprehensive set of features to support electronic signatures as detailed in section *Electronic Signatures [▶ 7]*.
16. Business continuity		
	For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Bruker AXS provides a comprehensive selection of service contract levels which can be tailored to the needs.

Section	Requirement	Implementation
17. Archiving		
	Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	Archiving and restoring of the database is possible from DIFFRAC.SUITE. The database is protected against unauthorized access. The database protects electronic records against voluntary and involuntary change.

5 Glossary

Application:

Software installed on a defined platform/hardware providing specific functionality.

Bespoke/Customized computerised system:

A computerised system individually designed to suit a specific business process.

Commercial of the shelf software:

Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users.

IT Infrastructure:

The hardware and software such as networking software and operation systems, which makes it possible for the application to function.

Life cycle:

All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.

Process owner:

The person responsible for the business process.

System owner:

The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.

Third Party:

Parties not directly managed by the holder of the manufacturing and/or import authorisation.

This page is intentionally left blank.

This page is intentionally left blank.

Bruker Corporation

info.baxs@bruker.com
www.bruker.com

Order No: DOC-M88-EXX249 V1 - 09.2019