Luminex®
complexity simplified.

xMAP INTELLIFLEX® Compliance Matrix – EU Annex 11

Technical Support
Telephone: 512-381-4397
North America Toll Free: 1-877-785-2323
International Toll Free: + 800-2939-4959
Email: *support@luminexcorp.com*
www.luminexcorp.com

RUO For Research Use Only.
Not for use in diagnostic procedures
89-30000-01-001
04/2023

Luminex Corporation
12212 Technology Blvd.
Austin, Texas 78727
U.S.A

Table of Contents

Introduction

The Regulatory Compliance Matrix is intended to describe how the xMAP INTELLIFLEX® system software enables the regulated customer to comply with the EU Annex 11, Computerised Systems.

The xMAP INTELLIFLEX® system equipment is designed to facilitate compliance with EU Annex 11. Under the EU Annex 11, xMAP INTELLIFLEX® system equipment is designed to be used as a closed system. A closed system is controlled by a user responsible for the content of the electronic records generated on the system. In addition to the system technical controls, EU Annex 11 requires that user facilities have established procedural and administrative controls. These include defined and documented lab policies, standard operating procedures, personnel training, and notification and management controls.

Definitions

Understanding the following terms are essential for the successful implementation of the regulations in EU Annex 11. These definitions will be the starting point for xMAP INTELLIFLEX® software compliance with the regulation.

- **Application:** Software installed on a defined platform/hardware providing specific functionality.
- **Digital signature (DS)**—An electronic signature using a Certificate Authority based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
- **Electronic record—**Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
- **Electronic signature**— A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
- **Bespoke/Customized computerized system**: A computerized 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 computerized 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 authorization.
- **Regulated Customer:** A company that must demonstrate that its drug or biological product is safe and effective for the intended use, and that it can manufacture the product to federal quality standards.

Software Features

xMAP INTELLIFLEX® software adheres to quality guidelines covering all aspects of development. The following features are included in the INTELLIFLEX software to facilitate adherence to EU Annex 11 regulations.

- **Audit Trail**

  The system automatically generates audit trail information, located in the system log. Changes to the configuration are logged. Once the audit log record is written, it cannot be modified by normal means. The audit log will include user comments for actions. Software provides human-readable and digitally signed reports of the results log. The system provides access to this audit trail information in the System Logs area, this information can also be exported to an Excel file for a specific individual date or a date range. The audit trail provides the read-only log of data file creation and modification activities.

- **Curated Workflow**

  When successive operations, events, and/or data entry are required, the system ensures the steps are followed in the correct sequence and logs each step in the Audit Trail. The software can be configured to require electronic signatures to perform specific actions. Input data is validated when appropriate.

- **Detailed Reports**

  Reports and output files are available in human-readable CSV, and XLS format. Raw, per-well fluorescence data is not exported and is not available in human-readable format as this data is not considered a required portion of the result output. Acquisition data may be manually or automatically exported from the instrument as human-readable CSV files. XLS files contains both acquisition data and configuration/logging data associated with the acquisition. The xMAP INTELLIFLEX system allows the creation of a report of the system’s calibration, verification, and fluidics history, system log report, and plate configuration. Each report is a multi-page XLS file with summary and detail pages, and includes lot numbers, timestamps, and run information. In addition to providing summary and detail result information Luminex® technical support uses this information to aid in troubleshooting failures; this information can also be helpful for your internal Quality Control (QC) purposes.

- **Digital Signatures**

  Files exported in Excel format are digitally signed using the Excel digital signature process that can be used to verify the content of the file has not changed since export. Files exported in the xMAP INTELLIFLEX CSV format can be configured to include a proprietary digital signature that can be used to verify the content of the file has not changed since export.

- **Electronic Signature**

  The system logs separate computer system sign in events and application events which require an electronic signature. Electronic signatures are attached to the relevant records. The electronic signature includes:

  - Username of the signer
  - Computer generated date and time
  - User comment (default comments are provided)

  Electronic signatures are user configurable and can be applied for the following actions:

  Maintenance:

  - Running a Calibration, Verification or Fluidics Verification
  - Importing/Saving a Calibration or Verification Kit

  Results:

  - Exporting Result Data
  - Changing the Column Formatting of the xMAP INTELLIFLEX format
  - Archiving Result Data
  - Running a Plate
  - Ignoring Laser Warm-up when Running a Plate
  - Running Without Valid Calibration/Verification
  - Running a Plate with Reacquired Wells
  - Editing a Plate

  Saving/Deleting Configuration Items:

  - Saving/Deleting a Protocol
  - Saving/Deleting a Panel
  - Saving/Deleting Acquisition Settings
  - Saving/Deleting a Plate Layout
  - Saving/Deleting a Plate

  Admin Settings

  - Changing Administrator Settings

- **Secure Record Retention**

  The user may encrypt the hard drive using BitLocker. Data acquired on the instrument is retained in various formats:

  - Secured SQL Server Database
  - Raw fluorescence data is stored on the file system as FCS compatible files.
  - Acquisition data may be manually or automatically exported from the instrument as human-readable CSV files and XLS files. XLS files contain both acquisition data and configuration/logging data associated with the acquisition.

  Records are retained until an authorized user explicitly removes them through a process that exports them to an external device.

- **Secure Login**

  Windows users accounts are used to control access and prohibit access by unauthorized users. The administrator via User Management can set the attempt threshold, define a lockout period, and manually unlock the account. Unsuccessful sign in attempts are recorded in the system log. There are two (2) components required for access and are always required for user account access:

  - User account
  - Password

The xMAP INTELLIFLEX system supports the requirement to input user account and password required on startup. The system defines user access by assigning roles. The administrator does not have the ability to customize what each role has access to. The different roles are:

- Administrator
- Lab Lead
- Operator
- Field Technician

For unattended devices, the administrator can set the inactivity log-out/time-out. The user will have to sign in to re-access the application.

- **User Management**

Secure Login and User Management for the xMAP INTELLIFLEX System both support multiple user accounts that can be set up locally on the system or a network. The xMAP INTELLIFLEX user permissions are managed in four pre-defined Windows groups:

- Administrators: grants Administrator-level access to both Windows and the xMAP INTELLIFLEX Software interface.
- Luminex Lab Leads: grants Lab Lead-level access to the xMAP INTELLIFLEX Software interface.
- Users: grants Operator-level access to the xMAP INTELLIFLEX Software interface.
- Luminex Field Technicians: grants User-level access to Windows and access to the Service sections of the xMAP INTELLIFLEX interface software.

EU Annex 11 Compliance Statements

The software application uses the following to facilitate compliance with EU Annex 11.

General

§1.0 Risk Management

> *Risk management should be applied throughout the lifecycle of the Computerized system considering 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.*

The xMAP INTELLIFLEX is developed to ISO 13485 standards.

§2.0 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.*

1) Windows users accounts are used to control access and prohibit access by unauthorized users.
2) The system is capable of defining system access and security levels for authorized individuals. The different roles are:
    - Administrator
    - Lab Lead
    - Operator
    - Field Technician

§3.0 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.*

EU Annex 11 (§3.1) is not applicable to the xMAP INTELLIFLEX system.

§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.*

EU Annex 11 (§3.2) is not applicable to the xMAP INTELLIFLEX system.

§3.3

Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

xMAP INTELLIFLEX is supplied with a user manual and administrator guide to fulfill the requirements of §3.3.

§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.

EU Annex 11 (§3.4) is not applicable to the xMAP INTELLIFLEX system.

Project Phase

§4.0 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.

EU Annex 11 (§4.1) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

§4.2

Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

EU Annex 11 (§4.2) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

§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.

EU Annex 11 (§4.3) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

§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.

EU Annex 11 (§4.4) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

§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.

EU Annex 11 (§4.5) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

§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.

EU Annex 11 (§4.6) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

§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.

EU Annex 11 (§4.7) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

§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.

EU Annex 11 (§4.8) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to all validations.

Operational Phase

§5.0 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, to minimize the risks.

Users are able to export these records in a variety of **Detailed Reports**. Data exports can be secured with a **Digital Signatures** that can be used to verify data has not been altered after it has left the instrument.

§6.0 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.

The xMAP INTELLIFLEX system utilizes **Curated Workflow** to comply with EU Annex 11 §6.0 Accuracy Checks and to cover risk management.

§7.0 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.

The xMAP INTELLIFLEX system utilizes **Secure Record Retention** to comply with EU Annex 11 §7.1. Records are maintained as part of a **Secure Record Retention** repository on the system. These records may be exported from the system in a variety of **Detailed Reports** that can be verified with **Digital Signatures.** The regulated company may use these records to meet their own retention procedure and is responsible for configuring record retention procedure.

§7.2

Regular back-ups 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.

The xMAP INTELLIFLEX enables full backup and restore to comply with §7.2. Full back up and restore is referenced in the administrator guide provided to the end user.

§8.0 Printouts

§8.1

It should be possible to obtain clear printed copies of electronically stored data.

All **Detailed Reports** are able to be exported to end user media and can be formatted for print.

§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.

For a full plate, XLS format exports full history of changes to the plate as part of the report.

§9.0 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.

The system automatically generates **Audit Trail** information, located in the system log. The **Audit Trail** is configurable to allow for actions to be automatically generated. It is not automatically generated if disabled by the customer and changes to the configuration are logged. Once the audit log record is written, it cannot be modified by normal means and will include user descriptions/explanations for actions. The software provides human-readable and digitally signed reports of the results log. The **Audit Trail** will provide the read-only log of data file creation and modification activities.

§10.0 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.

The system configuration changes require elevated access, requires an administrator, and changes can be required to add digital signatures.

§11.0 Periodic Evaluation

> *Computerised 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.*

Periodic evaluation is supported by the system log or the calibration and verification reports. Verification is required daily on xMAP INTELLIFLEX as default, but the frequency is configured by the administrator.

§12.0 Security

§12.1

> *Physical and/or logical controls should be in place to restrict access to computerized system 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.*

Windows users accounts are used to control access and prohibit access by unauthorized users. Administrator can set the attempt threshold, define a lockout period and manually unlock the account. Unsuccessful attempts are recorded in the system log. There are two (2) components required for access and are always required for user account access:

- Username
- Password

The system user accounts are intended for use by a single user. The xMAP INTELLIFLEX system supports session time-out and is the same as the Windows time-out; the user will have to log in and log out of Windows user account to re-access the application.

The system is capable of defining system access and security levels for authorized individuals. The different roles are:

- Administrator
- Lab Lead
- Operator
- Field Technician

§12.2

> *The extent of security controls depends on the criticality of the Computerized system.*

Security Controls such as Digital Signature Requirements, Lockout Periods, etc. are configurable via the administrator settings.

§12.3

> *Creation, change, and cancellation of access authorizations should be recorded.*

The xMAP INTELLIFLEX auto-log system records the creation, modification, and removal of a local user.

§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.

The xMAP INTELLIFLEX auto-log system is designed to record the identity of operators entering, changing, confirming, or deleting data including date and time.

§13.0 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.

The software records all incidents. The customer is able to forward a record of the incident to Luminex® for evaluation and is responsible for keeping records of incidents. The instrument logs abnormal incidents such as low bead counts and pressure abnormalities. These incidents are included with the result reports

§14.0 Electronic Signature

Electronic records may be signed electronically. Electronic signatures are expected to:

a) *have the same impact as hand-written signatures within the boundaries of the company,*

b) *be permanently linked to the respective record*

c) *include the time and date that they were applied*

The xMAP INELLIFLEX **Electronic Signature** includes all the required information to comply with EU Annex 11 §14.0.

§15.0 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.

EU Annex 11 (§15.0) is not applicable to the xMAP INTELLIFLEX system. It is the responsibility of the regulated customer to adhere to certify batch releases.

§16.0 Business Continuity

For the availability of computerized 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.

A Backup & Restore feature is available on the xMAP INTELLIFLEX system for disaster recovery and business continuity.

§17.0 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.

Archived data is automatically exported to the customer’s media. If relevant changes are made to the data storage system, the customer is responsible for the transfer and retrieval of data.