



**Agaram**  
TECHNOLOGIES

# How Logilab SDMS helps Laboratories to enable Eudralex Annex 11 Compliance

White Paper

**Part 3**

**V. Raghavan**

Agaram Technologies Private Limited

---

28 – Dec - 2020

## TABLE OF CONTENTS

|                                                                         |                                     |
|-------------------------------------------------------------------------|-------------------------------------|
| Logilab SDMS solution for Eudralex Annex 11 Compliance requirements.... | 3                                   |
| <b>Principle</b> .....                                                  | 3                                   |
| <b>General</b> .....                                                    | 4                                   |
| 1. Risk Management .....                                                | 4                                   |
| 2. Personnel .....                                                      | 4                                   |
| 3. Suppliers and Service Providers .....                                | 5                                   |
| <b>Project Phase</b> .....                                              | 6                                   |
| 4. Validation.....                                                      | 6                                   |
| <b>Operational Phase</b> .....                                          | <b>Error! Bookmark not defined.</b> |
| 5. Data.....                                                            | 9                                   |
| 6. Accuracy Checks.....                                                 | 10                                  |
| 7. Data Storage .....                                                   | 11                                  |
| 8. Printouts .....                                                      | 12                                  |
| 9. Audit Trail .....                                                    | 12                                  |
| 10. Change and Configuration Management .....                           | 13                                  |
| 11. Periodic Evaluation.....                                            | 13                                  |
| 12. Security .....                                                      | 14                                  |
| 13. Incident Management.....                                            | 15                                  |
| 14. Electronic Signature .....                                          | 15                                  |
| 15. Batch Release .....                                                 | 16                                  |
| 16. Business Continuity.....                                            | 16                                  |
| 17. Archiving.....                                                      | 17                                  |

# Logilab SDMS solution for Eudralex Annex 11 Compliance requirements

## Principle

### Requirement

*This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.*

*The application should be validated; IT infrastructure should be qualified.*

*Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process*

### Logilab SDMS Approach

Logilab SDMS is the computerized system which has been developed with the required functionalities. It is a generic software application designed to handle scientific instrument data from any analytical instrument and can facilitate data management with access control. Logilab SDMS will perform scheduled data capture, cataloguing, archival and facilitate restoring data and has capabilities to extract data of interest from instrument output to be pushed to external systems like Electronic Note Book (ELN), Laboratory Information Management System (LIMS) and Enterprise Resources Planning (ERP). It is intended to improve the product and service quality and reduce the overall risk.

## General

### 1. Risk Management

#### Requirement

*Risk management should be applied throughout the lifecycle of the computerised 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 computerised system*

#### Logilab SDMS Approach

While implementing Logilab SDMS, necessary care will be taken to assess and document the risk elements and their impact on various laboratory and manufacturing parameters including data integrity and quality. The validation process and data integrity controls will be based on the assessed risks that are predicted.

### 2. Personnel

#### Requirement

*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.*

#### Logilab SDMS Approach

Normally it is the organization implementing the computerized systems must identify, qualify and recruit personnel based on qualification and experience for positions such as Process Owner, System Owner and IT Admin, etc. Logilab SDMS has the full-fledged user management functionality to configure the users and assign them roles to have access to the relevant functionalities within the system.

### 3. Suppliers and Service Providers

#### Requirement

*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 computerised 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.*

*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.*

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

*Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.*

#### Logilab SDMS Approach

Agaram Technologies, who developed Logilab SDMS, will be engaged by the manufacturer or laboratories to install, configure, validate, maintain, modify the system and will ensure that formal agreements, Purchase Order and Project Plan which will have the details of responsibilities of customer and supplier (Agaram). IT department of the customer will also be involved. Agaram Technologies has a vast experience in implementation of Logilab SDMS for several of its customers successfully and it is also an ISO 9001:2015 certified organization, which means it is a reliable and competent supplier of the laboratory information software products.

Agaram also provides documentation namely Qualification documents, Validation documents, User guides, etc which can be verified and signed-off by the customer. The

customers are free to visit Agaram and contact by mail for inspecting any process documentation.

## Project Phase

### 4. Validation

#### Requirement

- 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.*
- 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 computerised 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 customised computerised 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.*

- 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.*

## **Logilab SDMS Approach**

4.1 Logilab SDMS has been designed and demonstrated to be fit for purpose in a GLP environment and introduced in a pre-planned manner. The system's operational validation process during its original product development as well as any project implementation stage includes requirement specification, design documentation, industry coding standards, unit and system testing processes with test documents and reports. Typically, Installation Qualification (IQ) and Operational Qualification (OQ) documents are prepared by implementation Project Team. While carrying out validation process the complexity and intended use of a system with adequate risk management are considered.

4.2 Change control is the formal approval and documentation of any change to the computerized system during the operational life of the system. It is needed when a change may affect the computerized system's validation status. Change control procedures must be effective during the project implementation phase as well as after system go-live.

The requirement of proper Support mechanism to be in place is being carefully considered to ensure that the Logilab SDMS has been used correctly by the end users. The implementation team as well as Agaram's Quality Assurance (QA) team work in collaboration with Product Development to resolve any issues encountered during implementation stage. The implemented changes are system tested by QA team and testing procedure as well as results are documented in test cases.

4.3 Relevant Information with respect to system pre-requisites, its availability, technical architectures, security requirements are documented in Installation Guide and they are validated during the installation. They are documented in Installation qualification document.

4.4 User requirement specifications are of paramount importance for all validation activities and should be generated for all Eudralex Annex11-relevant computerized systems. Hence Agaram 's Logilab SDMS Development team considered all aspects of Laboratory best business processes and the detailed functional requirements during the software design and development. Customer specific functional requirements are also considered during the Project implementation. An initial validation risk assessment is based upon an understanding of the business processes, user requirement specifications and regulatory requirements.

User requirement specifications is documented covering all GLP-relevant functions of a system and is be used in the risk assessment to identify critical functions and appropriate testing activities. This requirement specification and functional design in conjunction play a vital role in software design, development, configuration and testing.

4.5 In Agaram Product Development, Project Implementation team works with Quality Assurance team during the validation process. This as per Agaram' s Software Development as well as Implementation Process developed for ISO 9001: 2015 Quality Management System for which Agaram is certified by TUV.

4.6 Logilab SDMS can be implemented by the Laboratories without any customization in the functionalities. It is fully configurable by the Administration Users of Laboratories. However, during the implementation stage, any custom reports or workflows or any laboratory-specific or customer-specific custom extensions are developed, it goes through software development life cycle with adequate processes like requirements gathering, functional design documentation, Technical Design documentation, Test case documents during QA testing and UAT acceptance.



4.7 In Agaram, testing activities related to Logilab SDMS (e.g. installation testing, System Integration Testing and user acceptance testing) are carried out to ensure that a system meets predefined requirements. Test documents are prepared by QA team describing how tests are conducted and the test results are recorded. The project Implementation team also prepares Installation Qualification (IQ) and Operational Qualification (OQ) documents with screenshots as evidences.

When testing leads to system changes in codes or configuration or any custom extension, these should be managed via change control.

4.8 Data migration may be required during the project implementation. This data may be configuration data, meta data or transactional data. Where electronic data are transferred from one system to another, the details including what data needs to be migrated, the reason for migration (for example, new application implementation, upgrade from one version to another, etc.), migration technical details (namely database tables, codes, procedure, to which format, etc.) are documented in Technical Design Document. Necessary precautions and efforts are taken so that migrated data should remain usable and should retain its content and meaning. The value and/or meaning of and links between a system audit trail and electronic signatures are also ensured in a migration process.

## Operational Phase

### 5. Data

#### Requirement

*Computerised 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.*

#### Logilab SDMS Approach

Logilab SDMS has Data Scheduler as the core functionality which carries out the following:

- ✓ Fully automated & error-free capture of data without human intervention
- ✓ Options of time-based scheduling and live-capture
- ✓ Stores Instrument data in FTP file server in secured manner
- ✓ The original folder structure can be replicated in the file server (easy files organization)
- ✓ Option to setup Deletion of files in clients
- ✓ Version control of Files updated in the source
- ✓ File type watcher to look for specific file type to be stored (file filters)
- ✓ Server duplicate file delete policy

SDMS has built-in parsing tools to setup how to extract specific pieces of data from the instrument output.

- ✓ There is no complex coding or scripting involved
- ✓ Users can use easy to use interface to create parsing logic
- ✓ The parsed data can be used for further integration of data from Logilab SDMS to external systems.
- ✓ Improved accuracy, automation in data processing and reduced errors due to reduced human tasks

## 6. Accuracy Checks

### Requirement

*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.*

### Logilab SDMS Approach

Logilab SDMS ensures that users can verify the data that is captured from the instruments can go through a workflow process. Using the workflow tool users will be guided to follow the review and approval processes so that data errors can be avoided.

Logilab SDMS also supports electronic signature. Authorised users can place electronic signatures on appropriate records with the username, password and the reason with a date

and time stamp is recorded. This will ensure that users can be fixed with the responsibility to carry out necessary checks during the data transaction process.

Scheduling certain type of files generated in Lab process using file type watcher. This will ensure filtering out of unwanted data or files.

Users can identify or provide additional metadata for instrument generated data by entering batch numbers, sample types, projects, sample ids. Whatever metadata that is suitable for the instrument data, it can be tagged in meaningful names. This improves the accuracy of the data. The instrument data can be searched easily using the specific tag name.

## 7. Data Storage

### Requirement

- 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.*
- 7.2 *Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.*

### Logilab SDMS Approach

The core functionality of Logilab SDMS is Scheduler. The Scheduler can capture data generated by instruments automatically. It can be configured with respect to time. Live-capture module is used as and when data is generated being used by any other software.

All the data is being stored in a secured FTP server which is the backbone for the entire system for file storage. The changes made to the files in the source will be captured with proper version control. Automated removal of files from local clients can be configured based on file deletion policy.

It is very easy to search (wider search criteria), view (using preview facility), retrieve and navigate the data (including all the versions) inside the SDMS Explorer which is similar Windows Explorer. SDMS Explorer is easily accessible by authorised personnel using role-

based access control. Also, data can be logically separated by creating multiple FTP storage systems.

## 8. Printouts

### Requirement

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

### Logilab SDMS Approach

Logilab SDMS supports easy readability of data in PDF format and printing. Just like Eudralex Annex 11, human Readable data is also a mandatory process for US FDA's 21 CFR Part 11.

Whenever there is a report generated by an instrument software, users can store this report in a human readable format. Logilab SDMS provides a virtual PDF printer. Once the users have finalised the data inside the instrument software, Logilab virtual PDF printer can be used to generate a human readable PDF format of the report and then send to printer for printing on a paper if required.

Version control is also maintained which means files can be queried based on version and can be printed any version of the file.

## 9. Audit Trail

### Requirement

*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.*

## Logilab SDMS Approach

Audit trails module records each and every user & system action namely uploads, downloads Logins, Logoffs, failed logins, password policy, etc. Audit Trail has features to filter data based on user-based or module-based, time-based, type of audit trails. The audit trail settings are carried out only by Administrator users. Auditors can review specific audit trails and record/mark them. Audit trails can be exported such that Auditors can take them away as part of their audits.

The Audit Trail module records data with Time stamp, who did what and when and why at any point in time. Any communication failures that happen with respect to instrument are also audit-trailed inside the system.

## 10. Change and Configuration Management

### Requirement

*Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.*

### Logilab SDMS Approach

Agaram follows Support Agreement (SLA) with Laboratory customers with all necessary precautions and information is prepared in collaboration with them so that business continuity, reliability and responsiveness are ensured. Agaram's helpdesk support will ensure that issues encountered after go-live are properly recorded, segregated as issue or change, responded and resolved in collaboration with Agaram's Quality Assurance and Product Development team. The changes or bug-fixes or patch/upgrades are deployed in the production after Testing by QA and then by Users' signoff.

## 11. Periodic Evaluation

### Requirement

*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.*

## **Logilab SDMS Approach**

Agaram' s support team as well as Marketing team periodically takes customer inputs and feedback for the software product performance in terms of functionalities, issues/bugs, reliability and security. The market information as well as regulatory compliance requirements are also considered during the periodic review by Product Development to incorporate new changes, fixes, patches and upgrades of the product.

## **12. Security**

### **Requirement**

- 12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised 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.*
- 12.2 The extent of security controls depends on the criticality of the computerised system.*
- 12.3 Creation, change, and cancellation of access authorisations should be recorded.*
- 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*

## **Logilab SDMS Approach**

Logilab SDMS has the functionality to configure Users, their access rights restrictions and password policies.

Logilab SDMS has got its own built-in security module where Admin Users will be able to create users, groups and provide rights for users to access various parts of the applications, functionalities of the application or only view the data.

Also, password policies, which correspond to 21 CFR Part 11 and Eudralex Annex 11 can be setup inside the Logilab Security module with full control over the access to functionalities and data. This will ensure different operations will be performed based on the restrictions/privileges setup on the individual users as per company policies.

### **13. Incident Management**

#### **Requirement**

*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.*

#### **Logilab SDMS Approach**

Logilab SDMS has an audit trail module which records each and every user & system action namely uploads, downloads Logins, Logoffs, failed logins, password policy, etc. The Audit Trail module records data with Time stamp, who did what and when and why at any point in time. Any communication failures that happen with respect to instrument are also audit-trailed inside the system. This helps easy trouble-shooting of any issues encountered.

### **14. Electronic Signature**

#### **Requirement**

*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 their respective record,*
- c. include the time and date that they were applied.*

## Logilab SDMS Approach

Logilab SDMS has the functionality to incorporate electronic signature for the changes of system parameters. The users who make the changes must enter username, password and reasons for the changes along with date and time stamp. They are recorded in the audit trail module of the application which ensures the permanent link. There is also a workflow to configure who is the reviewer and who is the approver of the electronic data generated. Electronic signature is also recorded during review and approval process along with date and time stamp.

## 15. Batch Release

### Requirement

*When a computerised 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.*

## Logilab SDMS Approach

Only authorized and qualified personnel can perform electronic signatures and it could be part of batch release documents. Logilab SDMS has a workflow using which reviewer and approvers can be configured. The corresponding users can either review or approve the instrument generated data and metadata (using electronic signature) which helps to validate and improve accuracy and accountability

## 16. Business Continuity

### Requirement

*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.*

## **Logilab SDMS Approach**

Agaram recommends to the customer to provision proper load balancing and backup servers to take care of the system failures. Automatic switching to the backup server is highly recommended. Logilab SDMS fully supports high availability feature.

## **17. Archiving**

### **Requirement**

*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.*

### **Logilab SDMS Approach**

Using Logilab SDMS Scheduler, the archive policy can be implemented by scheduling the archival of data (i.e., file move) to the desired location. The retention period setting up (i.e., retaining the files to a specified period and removing them after that) can be setup by configuring the File delete options in the Scheduler.

In **Part 1**, we have understood the fundamental concepts of Eudralex Annex 11 and its principles as applicable to Computerized systems

In **Part 2**, we have understood the overview of Logilab SDMS and its importance in Eudralex Annex 11 as applicable to Computerized systems

In **Part 3**, we looked into how Logilab SDMS fulfils the requirements of Eudralex Annex 11.

(Concluded)