EU GMP Annex 11

Compliance checklist

This checklist is a nexus of EU GMP Annex 11's clauses and Scilife expertise. As a leading SaaS platform, Scilife's QMS harmonizes seamlessly with these mandates, guiding your digital transformation path. This matrix unveils alignment and synergy, where regulations find their match in Scilife's functionalities.

EU GMP Annex 11 is a guidance document that supplements the EU's GMP rules and provides guidelines for computerized systems used in GMP-regulated activities in the Life Sciences.

Scilife Supporting science. Improving life.

ITEM # & TITLE		REQUIREMENT / DESCRIPTION	APPLICABLE YES/NO	EXPLANATION
Validation				
1	Risk Management	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.	No	As part of the qualification, testing is done against Functional Specifications, as per defined validation procedure and individual validation plans developed for modules, to minimize the risks.
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.	Yes	Internal policies for acceptable use, data integrity and access control are established. Training management isdone as per defined procedure.

ITEM # & TITLE		REQUIREMENT / DESCRIPTION	APPLICABLE YES/NO	EXPLANATION
3	Suppliers and Service Providers	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. 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.	Yes	Supplier management is followed as per defined procedure. Suppliers assessments, change management,and agreements are performed and available.
4	Validation	The validation documentation and reports should cover the relevant steps of the life cycle.	Yes	Validation documentation is prepared according to Scilife's procedure and individual validation plans for each module.

ITEM # & TITLE		REQUIREMENT / DESCRIPTION	APPLICABLE YES/NO	EXPLANATION
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.	No	No data is exchanged by the system
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.	Yes	System requires unique User IDs and mandatory passwords for each active user. System requires authentication for any deletion and modification in the system.
7	Data Storage	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.	Yes	Records are maintained till retention period. Only authorized users can have access to records, using user ID and password. Additionally MFA authentication can be configured.
8	Data Storage	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.	Yes	Back-ups, integrity and accuracy checks are done as per defined procedure.

ITEM # & TITLE		REQUIREMENT / DESCRIPTION	APPLICABLE YES/NO	EXPLANATION
9	Printouts	It should be possible to obtain clear printed copies of electronically stored data.	Yes	Audit trails available in viewable and printable in human-readable form. System allows the user to view and print entire contents of records. When electronic records are displayed, printed, or copied, their meaning and content are preserved.
10	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.	Yes	Audit trail is available in the application which records all operator entries with user name, date, time and action performed. All records changes in the application are version controlled and audit trail is view only. Audit trail are retained and are available for review and copy.
11	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	Yes	Changes are made as per predefined procedure

ITEM # & TITLE		REQUIREMENT / DESCRIPTION	APPLICABLE YES/NO	EXPLANATION
12	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.	Yes	Periodic evaluation is made as per predefined procedure
13	Security	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. The extent of security controls depends on the criticality of the computerized system. Creation, change, and cancellation of access authorizations should be recorded. 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.	Yes	Access is restricted to authorized users. System requires unique User IDs and mandatory passwords for each active user. System asks for electronic signature for creation, modification or confirmation of records as per module configurations. Each executed electronic signature contains printed name of the signer, date and time of signature and meaning of the signature.

ITEM # & TITLE		REQUIREMENT / DESCRIPTION	APPLICABLE YES/NO	EXPLANATION
14	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.	Yes	Incidents are reported and assessed as per defined procedure
15	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 compan b. be permanently linked to their respective record c. include the time and date that they were applied.	Yes	System asks for electronic signature for creation, modification or confirmation of records as per module configurations. Each executed electronic signature contains printed name of the signer, date and time of signature and meaning of the signature.
16	Batch release	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.	Yes	System enforces electronic signature authentication with name of the signer, date and time of signature & meaning of the signature.

ITEM # & TITLE		REQUIREMENT / DESCRIPTION	APPLICABLE YES/NO	EXPLANATION
17	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.	Yes	Defined procedures are established to handle events and incidents, requiring proper management and disaster recovery plan.
18	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.	Yes	As per defined procedures