21 CFR Part 11 Whitepaper

LANEXO® Lab Inventory, Safety and Compliance Management System

Disclaimer

We provide information and advice to our customers on regulatory matters to the best of our knowledge and ability, but without obligation or liability. Existing applicable laws and regulations are to be observed in all cases by our customers. Our information and advice do not relieve our customers of their own responsibility for compliance with applicable regulations and checking the suitability of our products for their envisaged purposes.

We make no warranties of any kind or nature, express or implied, including any implied warranty of merchantability or fitness for any particular purpose, with respect to any technical assistance or information that we provide. Any suggestions regarding use, selection, application or suitability of our products shall not be construed as an express or implied warranty unless specifically designated as such in a writing signed by an officer or other authorized representative of our company.

We shall not in any event be liable for incidental, consequential, indirect, exemplary or special damages of any kind resulting from any use or failure of the products or services. The rights and responsibilities of the parties are set forth either in the applicable agreement in place between the parties or, if there are no such agreements, our standard Terms and Conditions of Sale.

TABLE OF CONTENTS

1. Introduction

The United States Food and Drug Administration (FDA) has a legal responsibility to ensure that drugs are safe and effective. Therefore, in FDA-regulated industries, quality and accountability standards are much higher. One of the ways the FDA assures quality in the industry is to require that records concerning important aspects of the manufacturing process be kept.

The objective of 21 CFR Part 11 is to allow industry to take advantage of electronic recordkeeping while making sure that electronic records and signatures are equivalent to paper records and signatures. The regulation defines what the FDA requires to ensure that electronic records are reliable, trustworthy, and authentic and that they can be considered equivalent to paper records and handwritten signatures for FDA purposes. This rule does not mandate the use of electronic records; however, if electronic records are used to keep FDA-required information, then the electronic records must comply with 21 CFR Part 11.

Similar to the FDA's 21 CFR Part 11, the European Union (EU)'s Annex 11 provides guidance for the use of computerized systems within Good Manufacturing Practice (GMP)–regulated activities in EU directives. The objective of Annex 11 is to ensure that when a computerized system is used, the same product quality and quality assurance can be achieved as with manual systems, with no increase in overall risk. Although Annex 11 is not a regulation, it is a guideline and is key to compliance with GMP principles in EU directives covering human and veterinary medicinal products.

This white paper illustrates how the LANEXO® System provides technology to support requirements for electronic records. The body of the white paper provides detailed "rule-by-rule" analyses of 21 CFR Part 11 and Annex 11 in tabular form in the next section. The Customer / end user organization is responsible for determining 21 CFR Part 11 / Annex 11 requirements based on their intended use of the LANEXO® System in the regulatory environment and for ensuring requirements are met, tested, and verified. This document is provided as guidance information for Customers. Wherever "supplier" is referenced in this document, it will refer to Merck, and "customer/end user" will refer to Merck's Customer.

Whenever the implementation column starts with the keyword remark, then this is additional information for that specific control to be considered and evaluated further by the Customer.

2. 21 CFR Part 11 and Annex 11 Controls

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
21 CFR Part 11, 11.10 (a)	Controls for closed systems: Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes	Both	Both	All data generated by Customers are kept confidential by encrypting them at rest in the database, and they are only ever transmitted over external networks in encrypted form. The LANEXO® System is hosted on a qualified cloud-based infrastructure with a dedicated qualification owner following Merck processes. The Customer / end user is responsible for validating the LANEXO® System and qualifying any associated mobile devices, computers/notebooks, and other IT infrastructure–related items. Such validation/qualification is based on the Customer's / end user's intended use in the regulatory area to meet GxP and Part 11 requirements.
21 CFR Part 11, 11.10 (b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for	Yes	Both	Both	Default LANEXO® System reports such as: a) Consumable report b) Experiment report

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
	inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.				are available in human-readable and electronic form. The customer / end user is responsible for ensuring that the required records meet applicable requirements based on their intended use of the records.
21 CFR Part 11, 11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Yes	Both	Both	The LANEXO® System will enable the accurate and ready retrieval of relevant data. Archiving the exported data is the responsibility of the Customer. The Customer / end user must define their record retention periods as per their record retention policies and ensure for implementation of the relevant processes.
21 CFR Part 11, 11.10 (d)	Limiting system access to authorized individuals.	Yes	Both	Both	LANEXO® administrator access is compliant with Merck internal guidelines and allows only certain authorized employees to access the system as administrators. System access for the Customer is controlled by personal username and password, personal access card, and Customer-registered device. The customer is responsible for ensuring that access control of authorized individuals by their admins / users is in place in accordance with the configuration and required procedural controls.
21 CFR Part 11, 11.10 (e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Yes	Both	Both	The LANEXO® System uses event sourcing as a key architectural principle. Any relevant action that the user performs will generate secure, immutable, and time-stamped events that cause changes to the data. The audit trail is a detailed projection of an event. An audit entry is created for each modified property in the event, containing also old values for these modified properties. Exporting and archiving audit trail data (e.g., for experiments, consumables, locations, users) is the responsibility of the Customer.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
					Customers should verify periodically that the date and time on the system are correct during the validation/qualification step or according to a defined standard operating procedure.
21 CFR Part 11, 11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	No	N/A	N/A	Remark: The LANEXO® System is a solution that is distributed over multiple computer systems and involves many different operating systems and services provided by the IaaS provider. The LANEXO® System makes extensive use of these operating systems and services to enforce permitted sequences of steps and events. These events are not directly applicable to the system's operational steps.
21 CFR Part 11, 11.10 (g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Yes	Both	Both	The LANEXO® System provides the technical means to perform security checks, but it is the responsibility of the Customer / end user to establish a procedure that enforces security controls. The audit trail contains the details of the user who performed each action.
21 CFR Part 11, 11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Yes	Both	Both	The end user interacts with a Mobile application and a Web application wherein the source of data (e.g., consumables) input or operational instructions (e.g., experiments) is clearly stated as part of the Customer audit trail. The Customer must verify their audit trail as part of their validation based on their implementation.
21 CFR Part 11, 11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Yes	Both	Procedural	The Customer is responsible for ensuring that administrators and users are qualified in accordance with the Customer's qualification process. Merck is responsible for ensuring that its developers and support personnel are qualified in accordance with its own qualification process.
21 CFR Part 11, 11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter	Yes	Customer	Procedural	It is the Customer's / end user's responsibility to implement these policies per their procedure.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
	record and signature falsification.				
21 CFR Part 11, 11.10 (k) (1)	Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Yes	Both	Procedural	Merck maintains system operations–related documentation in its document control system with required access control. The Customer is responsible for maintaining their validation and other operating documentation per their procedure.
21 CFR Part 11, 11.10 (k) (2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Yes	Merck	Procedural	Merck maintains system documentation through a change control process and version control. The Customer is responsible for maintaining their operating and validation documents in accordance with their established change control process.
21 CFR Part 11, 11.30	Controls for open systems: Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	No	N/A	N/A	Remark: Section 11.30's requirement for open systems does not apply to a closed system such as the LANEXO® System.
21 CFR Part 11, 11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	No	N/A	N/A	Remark: The LANEXO® System has technical features that provide this information. However, the Customer is responsible for determining electronic signatures of record based on the intended use of such signatures, as well as for verifying and validating the relevant requirements.
21 CFR Part 11, 11.50 (b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as	No	N/A	N/A	Remark: The LANEXO® System has technical features that provide this information. However, the Customer is

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
	for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).				responsible for determining the need for such usage of these records and the information they contain, based on this information's intended use, and for verifying and validating the relevant requirements.
21 CFR Part 11, 11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Yes	Both	Technical	All electronic records are hashed. The checksum of all electronic records are calculated and stored in the audit trail.
21 CFR Part 11, 11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Yes	Both	Both	It is the responsibility of the Customer to provide each individual user with a personal access card and to ensure that it is not reused by, or reassigned to, anyone else. The Customer is responsible for determining the use of this system for electronic signature of records based on the Customer's intended use.
21 CFR Part 11, 11.100 (b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Yes	Customer	Procedural	Customer responsibility.
21 CFR Part 11, 11.100 (c) (1)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	Yes	Customer	Procedural	Customer responsibility.
21 CFR Part 11, 11.100 (c) (2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of	Yes	Customer	Procedural	Customer responsibility.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
	the signer's handwritten signature.				
21 CFR Part 11, 11.200 (a) (1)	Electronic signatures that are not based upon biometrics shall: Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	No	N/A	N/A	While we assume that the LANEXO® system will not hold electronic records, as stipulated by predicate rules or in accordance with a wider interpretation of its purpose, the system provides features to allow electronic and even digital signatures in the sense of 21 CFR § 11.3 (5) and (7): all electronic records are hashed. The checksum of all electronic records are calculated and stored in the audit trail. The system must not be used for batch release and is not meant to replace LIMS, Lab Journal, MES, or similar systems. If the system is used for any of the above activities, the Customer must take precautions to fulfill all predicate rules.
21 CFR Part 11, 11.200 (a) (2)	Be used only by their genuine owners.	Yes	Both	Procedural	Merck is responsible for assigning access cards to the correct Customer account. The Customer is responsible for assigning the access cards to the correct users and controlling user access implementation.
21 CFR Part 11, 11.200 (a) (3)	Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	No	N/A	N/A	Remark: The Customer is responsible for implementing this control. The customer is responsible for determining the use of this system for electronic signatures for records based on these signatures' intended use.
21 CFR Part 11, 11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	No	N/A	N/A	Remark: The system does not provide electronic signatures based on biometrics.
21 CFR Part 11, 11.300 (a)	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same	Yes	Both	Both	The "identification codes" are generated by the Android app and the cloud backend. They are ephemeral and unique to the logged-in user. The Customer must ensure that no two individuals are given the same combinations (LANEXO® Access Card and password).

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
	combination of identification code and password.				The Customer is responsible for implementing this requirement based on their intended use.
21 CFR Part 11, 11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	No	N/A	N/A	Remark: The Customer is responsible for implementing this requirement. The Customer is responsible for determining electronic signatures for records based on the password policy's intended use.
21 CFR Part 11, 11.300 (c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Yes	Customer	Procedural	The Customer is responsible for implementing this requirement. Merck provides LANEXO® Access Cards for access to the system. The LANEXO® System enables the Customer to manage their own users, to include blocking compromised accounts and assigning access cards to users.
21 CFR Part 11, 11.300 (d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Yes	Both	Both	Merck provides LANEXO® Access Cards with unique identifications at the user level. The Customer is responsible for implementing the following: - Issue of LANEXO® Access Cards within the customer organization - Password management - Prevention of unauthorized use of access cards and/or passwords - Checking the user audit trail for unauthorized access - Detection process to identify unauthorized use of LANEXO® Access Cards and/or passwords and to take action against such unauthorized use The above is not a complete list; the Customer must identify any additional implementation needed to meet these requirements.
21 CFR Part 11, 11.300 (e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Yes	Customer	Procedural	Merck provides LANEXO® Access Card with unique identifications at the user level. The Customer is responsible for validating end user devices. Merck is responsible for recommending LANEXO® System–compatible mobile devices to the Customer. Merck will also ensure that operational change management is followed and maintained.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
					The Customer is responsible in determining and implementing the verification process.
EU Annex 11, Principle	The application should be validated; IT infrastructure should be qualified.	Yes	Both	Procedural	Merck ensures that the cloud infrastructure is qualified and maintained. Good Engineering Practices in development and operational change management are followed and maintained. The Customer has overall accountability for ensuring that the system is validated for their intended use and that infrastructure qualification, including of infrastructure accessories, is in place.
EU Annex 11, 1	Risk management should be applied throughout the lifecycle 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	Yes	Both	Procedural	Merck follows its risk management principles in development and testing. The Customer has overall accountability for applying risk management based on their implementation of the system.
EU Annex 11, 2	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	Both	Procedural	The Customer is responsible for ensuring their staff are trained on predicate rules, operating instructions, and the user manual and for creating appropriate training records. Merck is responsible for ensuring that its developers and support personnel are qualified.
EU Annex 11, 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.	Yes	Both	Procedural	When buying a LANEXO® System license, the Customer has a formal agreement with clear responsibilities regarding the management and maintenance of the system and its infrastructure by their supplier. In addition, the Customer is responsible for managing their agreements with such third parties. Merck is responsible for managing their suppliers in accordance with their supplier management process.
EU Annex 11, 3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for	Yes	Both	Procedural	Merck has selected a cloud service provider in accordance with its internal vendor qualification process.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
	an audit should be based on a risk assessment.				The Customer is responsible for determining the need to audit their supplier based on a risk assessment.
EU Annex 11, 3.3	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Yes	Customer	Procedural	If the Customer requests specific features or extensions to the LANEXO® System, they are responsible for checking the user requirements to ensure that these features or extensions are fit to their intended use. This process should be within the scope of the final validation performed by the Customer. The Customer should verify that their requirements have been fulfilled.
EU Annex 11, 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.	Yes	Customer	Procedural	The Customer is responsible for determining the need for regulatory inspection of the software supplier quality system and audit information. The required agreement with the supplier will be the Customer's responsibility.
EU Annex 11, 4.1	The validation documentation and reports should cover the relevant steps of the lifecycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	Yes	Both	Procedural	LANEXO® System development, testing, and maintenance follow Merck's internal Quality Management Systems (QMS) and ensure that the defined requirements are fulfilled. The Customer is accountable for installing and, where required, validating the LANEXO® System and verifying that their supplier documents meet all requirements based on the Customer's intended use of the system.
EU Annex 11, 4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	Yes	Both	Procedural	Merck maintains LANEXO® System development, testing, and change control documentation, including documentation related to infrastructure qualification. The Customer is accountable for validation of the system and change control documents for their installation.
EU Annex 11, 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	Yes	Both	Procedural	The Customer is responsible for maintaining an inventory of GMP systems, including validation documents and implemented system documentation. Merck maintains documentation related to development, testing, and maintenance per their internal QMS.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
	software pre-requisites, and security measures should be available.				
EU Annex 11, 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 lifecycle.	Yes	Both	Procedural	The Customer is responsible for documenting their user requirements, performing a risk assessment, and ensuring that in their validation process the requirements are traced throughout the Customer's implementation lifecycle. Merck's development, testing, and maintenance of systems, including traceability and risk assessment of the LANEXO® System, are based on potential user requirements derived from the voice of the Customer.
EU Annex 11, 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.	Yes	Customer	Procedural	Primarily a Customer responsibility; per their policies, support from their supplier may be required.
EU Annex 11, 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.	No	N/A	N/A	Remark: The LANEXO® System is not a unique, specific bespoke system based on the Customer's process. The Customer is accountable for determining and ensuring that this process is in place to meet this requirement.
EU Annex 11, 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.	Yes	Both	Procedural	The Customer is accountable for verifying these requirements as part of their validation. Merck has applied appropriate test methods and test scenarios in their development lifecycle testing, and a process is in place for the operational phase.
EU Annex 11, 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.	No	N/A	N/A	Merck offers APIs allowing integration of LANEXO® to customer's network. The use of such integration is optional, and its access authentication is configured by the Customer. The APIs are passive to send data out of LANEXO actively. If the Customer intends to use such electronic output for data migration into their system, it will be their responsibility.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
EU Annex 11, 5	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	N/A	N/A	Remark: The LANEXO® System can pull information from external APIs based on Customer user searches for pertinent information. This information is not Customer data. The Customer is responsible for using this pulled information to ensure that the LANEXO® System is fit for their purpose.
EU Annex 11, 6	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	Customer	Procedural	Customer responsibility.
EU Annex 11, 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.	Yes	Both	Both	Physically securing the data against damage is the responsibility of the IaaS provider (the cloud provider). Electronically securing data is done primarily by keeping data redundantly and distributing them into different availability zones. The Customer is accountable for determining the accessibility, readability, and accuracy of their data. Access to data should be ensured throughout the retention period and is the Customer's responsibility. The LANEXO® System has the technical capability to export plain-text backup of data. The Customer must determine the use of this capability for storage and retention per their policy.
EU Annex 11, 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.	Yes	Both	Both	For regular backups, Merck follows an established procedure that includes monitoring by a cloud service provider under a service level agreement (SLA). The integrity and accuracy of the backup are continuously verified. The distributed and redundant data storage is managed by the cloud service provider. Application events in the event log are used to drive the application itself, and a fault in the event log would break the entire application. No event log or backup errors are detected during our tests.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
					The Customer is accountable for having a process and /or agreement with their supplier in place for their data backup.
EU Annex 11, 8.1	It should be possible to obtain clear printed copies of electronically stored data.	Yes	Customer	Both	Relevant data generated by Customers can be exported in both human-readable and machine-readable formats. The Customer is responsible for determining the need for such copies based on their intended use, as well as verifying and validating this requirement.
EU Annex 11, 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.	No	N/A	N/A	Remark: The LANEXO® System does not support batch release.
EU Annex 11, 9	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	Customer	Both	The LANEXO® System uses event sourcing as a key architectural principle. Any relevant action that the user performs will generate secure, immutable, and time-stamped events that cause the changes to the data. The customer audit trail is an aggregate of these events. Exporting and archiving audit trail data is the responsibility of the Customer. The Customer should verify periodically that the date and time on the system are correct during the validation/qualification step or according to a defined standard operating procedure. Review of the audit trail is a procedural control that is the responsibility of the Customer.
EU Annex 11, 10	Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Yes	Both	Procedural	Addressed by the Customer and by Merck Change Management processes. The cloud-based service and software may be changed. Security patches that do not affect functionality may be applied as hot fixes. Feature releases will be announced with a grace period to allow for validation activities. The Customer is responsible for managing changes per their procedure.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
EU Annex 11, 11	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	Both	Procedural	Merck Periodic Review process. The Customer will determine and follow the periodic review process per their policy.
EU Annex 11, 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.	Yes	Both	Both	Merck ensures access control into the equipment area through an SLA with the cloud service provider. LANEXO® administrator access is compliant with Merck internal guidelines. System access by the Customer is controlled by personal usernames and passwords, personal access cards, and Customer-registered devices. The Customer is responsible for ensuring that access control by authorized individuals for their admin / users is in place in accordance with the configuration and required procedural controls.
EU Annex 11, 12.2	The extent of security controls depends on the criticality of the computerized system.	Yes	Both	Both	The LANEXO® System is a service offered by Merck to its customers and is therefore considered critical and held to high security standards. There are many layers of security controls in place, which are thoroughly tested by separate and dedicated teams for, e.g., penetration tests, security assessments, and security consulting. LANEXO® administrator access is compliant with Merck internal guidelines. System access control and security by the Customer is their responsibility.
EU Annex 11, 12.3	Creation, change, and cancellation of access authorizations should be recorded.	Yes	Merck	Technical	Any creation, changes and cancellations of user access authorization is logged in the audit-trail. All electronic records are hashed. The checksum of all electronic records is calculated and stored in the audit trail.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
EU Annex 11, 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.	Yes	Merck	Technical	The LANEXO® System uses event sourcing as a key architectural principle. Any relevant action that the user performs will generate secure, immutable and time-stamped events that cause changes to the data. The customer audit trail is a collection of these events. Exporting and archiving audit trail data is the responsibility of the Customer. Customers should verify periodically that the date and time on the system are correct during the validation/qualification step or according to a defined standard operating procedure. Deletion of data is not possible by end users or Customers.
EU Annex 11, 13	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	Both	Procedural	Addressed by the Merck Incident Management process for handling Customer report incidents. The Customer is accountable for reporting incidents related to the LANEXO® System to Merck.
EU Annex 11, 14	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.	No	N/A	N/A	Remark: All critical events must be explicitly confirmed by the user. While we assume that the system does not hold electronic records, as stipulated by predicate rules or in accordance with a wider interpretation of its purpose, the ® system provides features to allow electronic and even digital signatures in the sense of 21 CFR § 11.3 (5) and (7): Electronic signature: Critical actions/events can be confirmed using a dialog, expressing the user's will to execute and log the given event. All electronic records are hashed. The checksums of all electronic records are calculated and stored in the audit trail. The system must not be used for batch release and is not meant to replace LIMS, Lab Journal, MES, or similar systems.

Source	Control	Applicable	Customer/Merck Responsibility	Procedural/ Technical	Implementation
					If the system is used for any of the above activities, the Customer must take precautions to fulfill all predicate rules.
EU Annex 11, 15	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.	No	N/A	N/A	Remark: The LANEXO® System does not support batch release.
EU Annex 11, 16	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 Used 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	Both	Procedural	It is the Customer's responsibility to manage their manual backup plan in accordance with their business continuity policy. The manual/alternative system must be adequately documented and tested. Merck maintains its business continuity procedures.
EU Annex 11,17	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.	No	N/A	N/A	Remark: Merck does not guarantee compliance with predicate rules in the Customer's region, e.g., for retention times. Archiving is the responsibility of the Customer. The system does store data for a limited time, as long as the subscription is active. After termination of a subscription, the Merck Archival Service may extract, transform, and make available all information stored for the Customer.

3. Summary

The LANEXO® System simplifies and aids Customers' efforts to comply with the FDA's 21 CFR Part 11 and the EU's Annex 11 in the laboratory.

Life Science customers have overall accountability for ensuring that their systems are validated based on the systems' intended use. Ultimately, compliance with 21 CFR Part 11 and Annex 11 are the Customer's responsibility based on their intended use of the LANEXO® System.

From the Customer's perspective, the LANEXO® System is a GAMP 5 Software Category 4–Configured Product. It is recommended that the Customer base their validation process on the GAMP 5 approach.

In addition, the Customer must establish and implement documented operational processes covering areas such as archiving or business continuity planning.

Merck KGaA
Frankfurter Strasse 250
64293 Darmstadt
Germany

ManGo No. 20474386
11/2022
MK_WP12078EN