Millipore®
Preparation, Separation,
Filtration & Monitoring Products

White Paper

Facilitating 21 CFR Part 11 Compliance with Bio4C™ Orchestrator

21 CFR Part 11

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 high. 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 regulations is to allow industry to take advantage of electronic record keeping 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's EudraLex Volume 4 Annex 11 ("Annex 11") provides guidance for the use of computerized systems within 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 manual systems with no increase in the 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 Bio4C™ Orchestrator Software provides technology to support requirements for electronic records. The body of this white paper provides a detailed "rule-by-rule" analysis for 21 CFR Part 11 and Annex 11 in tabular form.

The customer organization is responsible to determine the 21 CFR Part 11/Annex 11 requirements based upon their intended use of Bio4C™ Orchestrator Software in the regulatory environment and ensure requirements are met, tested, verified. This document is provided as guidance information for customers.

Wherever "supplier" is referenced in this document it refers to Merck and "customer" refers to the Merck customer.

In the table below, where the Implementation column content begins with the keyword "Remark", this is additional information for that specific control to be considered and evaluated further by the customer.

MERCK

21 CFR Part 11 and EudraLex Volume 4 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: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes	Both	Both	Bio4C™ Orchestrator has been internally validated for intended use in accordance with Merck validation procedures. Part of this requirement is the responsibility of the customer who deploys the Bio4C™ Orchestrator software. Validation for intended use must be part of the deployment in their environment. The validation and qualification are based on customer's intended use to meet GxP and 21 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 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.	Yes	Both	Both	Bio4C™ Orchestrator's reports such as: a. Run Summary Report b. Consolidated Report c. Custom Report Audit Trail Report - are available in human readable and electronic form Customer is responsible to ensure the required records met the requirements based on their intended use of 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	Bio4C™ Orchestrator retrieves data without modification from connected CCP® Systems and stores it with access protection in Wonderware and SQL databases on the Bio4C™ Orchestrator server. Archiving these database files is the responsibility of the customer. The customer must define their record retention periods as per their record retention policies and ensure their implementation. The customer is responsible for ensuring that access to these databases is granted only to authorized individuals.
21 CFR Part 11, 11.10 (d)	Limiting system access to authorized individuals.	Yes	Both	Both	Bio4C™ Orchestrator provides access control to systems through defined roles and predefined access privileges assigned to each role. System access is controlled by unique usernames and passwords. The customer is responsible for ensuring access control. Using procedural controls, the customer's system administrator assigns an account with a unique login and password. The user's identity and role are combined to determine whether access and privileges are permitted or denied.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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	Bio4C™ Orchestrator provides an audit trail of all the relevant actions that users perform which cause changes to data and generates a secure, immutable, and time-stamped record of events. Bio4C™ Orchestrator's functionality does not permit deletion of any electronic records. User can generate an Audit Trail Report of user activity through Bio4C™ Orchestrator. Exporting and archiving the audit trail data is the responsibility of the customer. Customers should verify periodically that the date and time on the system are correct during validation or qualification steps 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	Bio4C™ Orchestrator checks to enforce permitted sequences of steps and events through functionalities such as Report Template Approval or Recipe Import and Dispatch.
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	Bio4C™ Orchestrator provides the technical means to perform security checks but it is the responsibility of the customer to establish procedural controls that enforce it. Customer is responsible to determine the electronic signature of record based on their intended use and ensure authorization.
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	Bio4C™ Orchestrator is designed to be accessed only through the customer's internal network using a web browser. The user's laptop/desktop needs to be connected to the customer's intranet directly or through a VPN provided by the customer. Customer should verify the devices connected to theirinternal network for source of data input. The validity of that input should be assured by procedural controls/SOPs.
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	Customer	Procedural	Supplier maintains the developer and support personnel's qualification as per internal process. Customer is responsible for ensuring that administrators and users are qualified in accordance with their 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 record and signature falsification.	Yes	Customer	Procedural	Customer responsibility to implement as per their procedural controls/SOPs.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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	Customer	Procedural	Merck maintains the systems related development documentation in the document control system with required access control. Customer is responsible to maintain their validation and other operating documentation per their procedures.
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	Customer	Procedural	Merck maintains the system documentation through change a control process and version control. Customer is responsible for maintaining their operating documents and validation documents with an 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 requirement for open systems does not apply to a closed system such as Bio4C™ Orchestrator.
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.	Yes	Both	Both	Bio4C™ Orchestrator has technical features for this information which captures all the relevant information for signed electronic records. Customer is responsible to determine the use of an electronic signature of the record based on their intended use. Customer is responsible to verify and validate these requirements
21 CFR Part 11, 11.50 (b)	4. The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Yes	Both	Both	Bio4C™ Orchestrator has technical features for this information. Customer is responsible to determine the use of an electronic signature of the record based on their intended use. Customer is responsible to verify and validate these 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	The encrypted signature is calculated for the content of each event; this makes it practically impossible to excise, copy or otherwise transfer the signature by ordinary means. Customer is responsible to determine the use of this system for electronic signature of record based on intended use.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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	Unique username and password combination is required for the electronic signatures. It is the responsibility of the customer to provide each individual user with a unique username to ensure that it is not reused by, or reassigned to, anyone else. Customer is responsible to determine the use of this system for electronic signature for record based on their 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 the signer's handwritten signature.	Yes	Customer	Procedural	Customer responsibility.
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	Yes	Merck	Technical	Bio4C™ Orchestrator has technical features for this. For each the executions of an electronic signature, the username is prepopulated for the logged in user and non-editable. The user need only enter the correct password each time – whether it is first execution of the e-signature or a consequent execution in the same user session.
21 CFR Part 11, 11.200 (a) (2)	Be used only by their genuine owners.	Yes	Customer	Procedural	The customer is responsible to assign access to the correct users and control the user access implementation. Customer is responsible to determine the use of an electronic signature for the record based on their intended use. Customer is responsible to verify and validate these requirements.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	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.	Yes	Customer	Procedural	Remark: The customer is responsible to implement this control. Customer is responsible to determine the use of an electronic signature for the record based on their intended use. Customer is responsible to verify and validate those requirements.
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: Electronic signature based on biometrics is not provided by the system.
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 combination of identification code and password.	Yes	Both	Both	The “identification codes” are usernames in Bio4C™ Orchestrator and are unique to the logged in user. Customer to ensure that no two individuals are given the same combinations (username and password). Customer is responsible to determine the electronic signature for records 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: Customer is responsible to implement and configure the password aging or password expiry in Windows Password Policy. Bio4C™ Orchestrator authenticates user via Windows Password Policy.
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.	No	Customer	Both	Bio4C™ Orchestrator enables the customer to administer their own users including disabling users. No tokens, cards, or other devices are provided as part of the system. Customer is responsible to implement this requirement based on the intended use.
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	Customer	Procedural	Customer is responsible to implement the following: (this is not complete list, customer to identify any additional implementation needed to meet this requirement) • Password management • Prevention of unauthorized use of password • Review user audit trail for unauthorized access • Establish process to identify unauthorized use of password and take action • Implement and configure the unsuccessful login threshold in windows Password Policy.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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.	No	Customer	Procedural	Customer is responsible to validate end-user devices. Customer is responsible to. Implement and configure the unsuccessful login threshold in Windows Password Policy. Bio4C™ Orchestrator authenticates user via Windows Password Policy. No tokens, cards or other devices are provided as part of the system.
EU Annex 11, Principle	The application should be validated; IT infrastructure should be qualified.	Yes	Both	Procedural	Merck ensures the application is validated in a qualified environment and follows good engineering practices in development, operational change management, and maintenance. Customer has overall accountability for ensuring that system is validated for their intended use and the infrastructure qualification including qualification 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 followed risk management principles in development and testing of Bio4C™ Orchestrator. Customer has overall accountability to apply 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 developers and support personnel involved in Bio4C™ Orchestrator development, testing, and maintenance are qualified and trained as per internal procedures. Customer is responsible for ensuring their staff is trained on predicate rules, operating instructions, and the user manual and also for creating appropriate training records.
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	Buying a Bio4C™ Orchestrator license, the customer has a formal agreement with clear responsibilities regarding the management and maintenance of Bio4C™ Orchestrator. In addition, customer is responsible to manage their agreements with their third parties. Merck is responsible for managing their parties 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 an audit should be based on a risk assessment	Yes	Both	Procedural	Merck selects suppliers in accordance with its internal vendor qualification process. Customer is responsible to determine the audit needs of their supplier based on 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	Customer specific extensions and fit to intended use of Bio4C™ Orchestrator should be in scope of the final validation done by customer. Customer should verify their requirements are fulfilled.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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	Customer is responsible to determine the need of the supplier quality system and audit information for regulatory inspection. Required agreement with 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	Bio4C™ Orchestrator's development, testing, and maintenance follows Merck's internal QMS (Quality Management Systems) and ensures that the defined requirements are fulfilled. Customer is accountable to install and, where required, validate Bio4C™ Orchestrator and verify their supplier documents meet the need based on the intend 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 Bio4C™ Orchestrator system development, testing, and change control documentation including infrastructure qualification related documentation. Customer is accountable for the 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 software pre-requisites, and security measures should be available.	Yes	Both	Procedural	Merck maintains development, testing, and maintenance related documentations per their internal QMS. Customer is responsible for maintaining an inventory of GMP systems, including validation documents and implemented system documentation.
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	Merck development, testing, and maintenance of systems including traceability, risk assessment of Bio4C™ Orchestrator is based on potential user requirements derived from voice of customers. Customer is responsible to document their user requirements, risk assessment, and ensure in their validation process the requirements are traced throughout their implementation life cycle.
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 as 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: Bio4C™ Orchestrator is not customized to customer's specific process or bespoke system. Customer is accountable to determine and ensure process is in place to meet this requirement.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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	Merck applied appropriate test methods and test scenarios in their development life cycle testing and a process is in place for an operational phase. Customer is accountable to verify this requirement as part of their validation.
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	Bio4C™ Orchestrator only provides export of recipes to user's system which has a signature file attached to each recipe file. Any changes done in the recipe file invalidates the signature. If the customer intend to use electronic output for migrating into their system, it will be the customer's responsibility.
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: Bio4C™ Orchestrator exchanges data with the below Millipore CCP® systems. The data is exchanged through secured protocols. 1. CoPrime® Biochromatography Systems. CCP® version 2.00.00.01 2. Mobius® FlexReady Solution with Smart Flexware® Assemblies for Chromatography and TFF. CCP® version 3.00.00.00 3. Mobius® Single-use Bioreactors. CCP® version 2.00.00.02
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. For data entries on Bio4C™ Orchestrator, there is a data entry check, e.g. while creating a user, edit user, back-up, settings, template name etc. Process data/recipe related data is entered at CCP® level. It is customer's responsibility to do the check at entry point.
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	Data is stored in Wonderware and SQL databases and on designated hard disk locations on the Bio4C™ Orchestrator Server. Physically securing this server against damage is the customer's responsibility. Electronically securing data is done through Wonderware and SQL internal mechanism. Customer should control the access to these databases and hard disk locations of the Bio4C™ Orchestrator server. The customer is responsible to determine that their data is accessible, readable and accurate. Access to data should be ensured throughout the retention period and is the customer's responsibility.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
					Bio4C™ Orchestrator has the technical capability to backup of the data; customer to determine the use of this capability for storage and retention per their policies.
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	Bio4C™ Orchestrator has the technical capability to backup and restore the data used in the application and to run integrity checks while restoring the data. Customer is accountable to have a process in place for back-up, restoration testing and periodic monitoring.
EU Annex 11, 8.1	It should be possible to obtain clear printed copies of electronically stored data.	Yes	Customer	Both	Bio4C™ Orchestrator provides report generation in PDF formats which can be printed using a configured printer. Customer is responsible to determine based on their intended use and verify and validate the requirements.
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: Customer can generate an audit trail report from Bio4C™ Orchestrator for the connected systems. The use of this audit trail report for supporting the batch release is customer's responsibility.
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	Bio4C™ Orchestrator provides an audit trail of all the relevant actions that the user performs which causes a change in data and generates a secure, immutable, and time-stamped events. User can generate an audit trail report of these events though Bio4C™ Orchestrator. Exporting and archiving the audit trail data is the responsibility of the customer. Customers should verify periodically that the date and time on the system are correct during validation and qualification steps 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	Customer	Procedural	Customer is responsible to manage the changes per their procedures.
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	Customer	Procedural	Customer to determine and follow the periodic review process per their policy.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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	Bio4C™ Orchestrator is designed to be only accessed through internal network using web browser. The user's laptop/desktop needs to be connected to intranet directly or through VPN provided by customer to access the Bio4C™ Orchestrator application. System access by customer is controlled by unique username and password, customer registered device. The customer is responsible for ensuring access control. Using procedural controls, the customer's system administrator assigns an account with a unique login and password. The user's identity and role are combined to determine whether access and privileges are permitted or denied.
EU Annex 11, 12.2	The extent of security controls depends on the criticality of the computerized system.	Yes	Both	Both	Bio4C™ Orchestrator server will be deployed on a Virtual Machine provided/managed by Customer and it is designed to be only accessed through internal network using web browser. The user's device accessing the Bio4C™ Orchestrator application needs to be connected to intranet directly or through VPN provided by customer. System access control and security control is customer's responsibility.
EU Annex 11, 12.3	Creation, change, and cancellation of access authorizations should be recorded.	Yes	Both	Technical	Any creation, changes and cancellations of user access authorization is logged in the audit-trail. Customer to validate the audit trail functionality as part of their validation.
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	Bio4C™ Orchestrator provides an audit trail of all the relevant actions that the user performs which causes a change in the data and generates a secure, immutable and time-stamped events. User can generate an audit trail report of these events though Bio4C™ Orchestrator. Exporting and archiving the audit trail data is the responsibility of the customer. Customers should verify periodically that the date and time, on the system are correct during validation and qualification steps or according to a defined standard operating procedure. Deletion of data is not possible by end users or customers.

21 CFR Part 11 and EudraLex Volume 4 Annex 11 Controls (continued)

Source	Control	Applicable	Customer/ Merck responsibility	Procedural/ Technical	Implementation
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	Customer is responsible for managing all types of incidents per their internal procedure. As needed customer may contact the supplier for any issue that may need vendor support. For this purpose, customer may have service level agreement with the supplier
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	Yes	Both	Both	Bio4C™ Orchestrator provided technical capability for electronic signatures which are permanently linked to their respective electronic records which include time and date that they were applied. Customer is responsible to determine the use of this system for electronic signature of record based on intended use and verify, validate the requirements.
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: Customer can generate a batch report from Bio4C™ Orchestrator for the connected systems. The use of this batch report for the batch release is customer's responsibility. Customer is responsible for access control and qualification of users to generate and or sign batch report in Bio4C™ Orchestrator.
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	Customer	Procedural	It is customer's responsibility that a business continuity plan is in place. Per customer policy required manual back-up plan. The manual/alternative system is adequately documented and tested.
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	Customer	N/A	Archiving is the responsibility of the customer as per their procedures.

Summary

Bio4C™ Orchestrator simplifies and aids customer's compliance efforts for the FDA's 21 CFR Part 11 and EU's Annex 11 in their plant.

Merck customers have overall accountability for ensuring that their system is validated based on their intended use. Final compliance with 21 CFR Part 11 and Annex 11 based on their intended use are the customer's responsibility.

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

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.

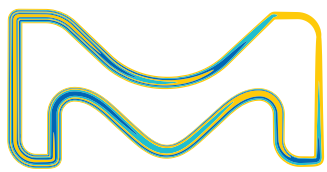
To place an order or receive technical assistance

Please visit: **MerckMillipore.com/contactPS** or
email **OrchestratorSupport@MerckGroup.com**

For additional information, please visit:
MerckMillipore.com/Bio4COrchestrator

MerckMillipore.com

Merck KGaA
Frankfurter Strasse 250
64293 Darmstadt, Germany



MK_WP7689EN Ver. 1.0
35555
05/2021