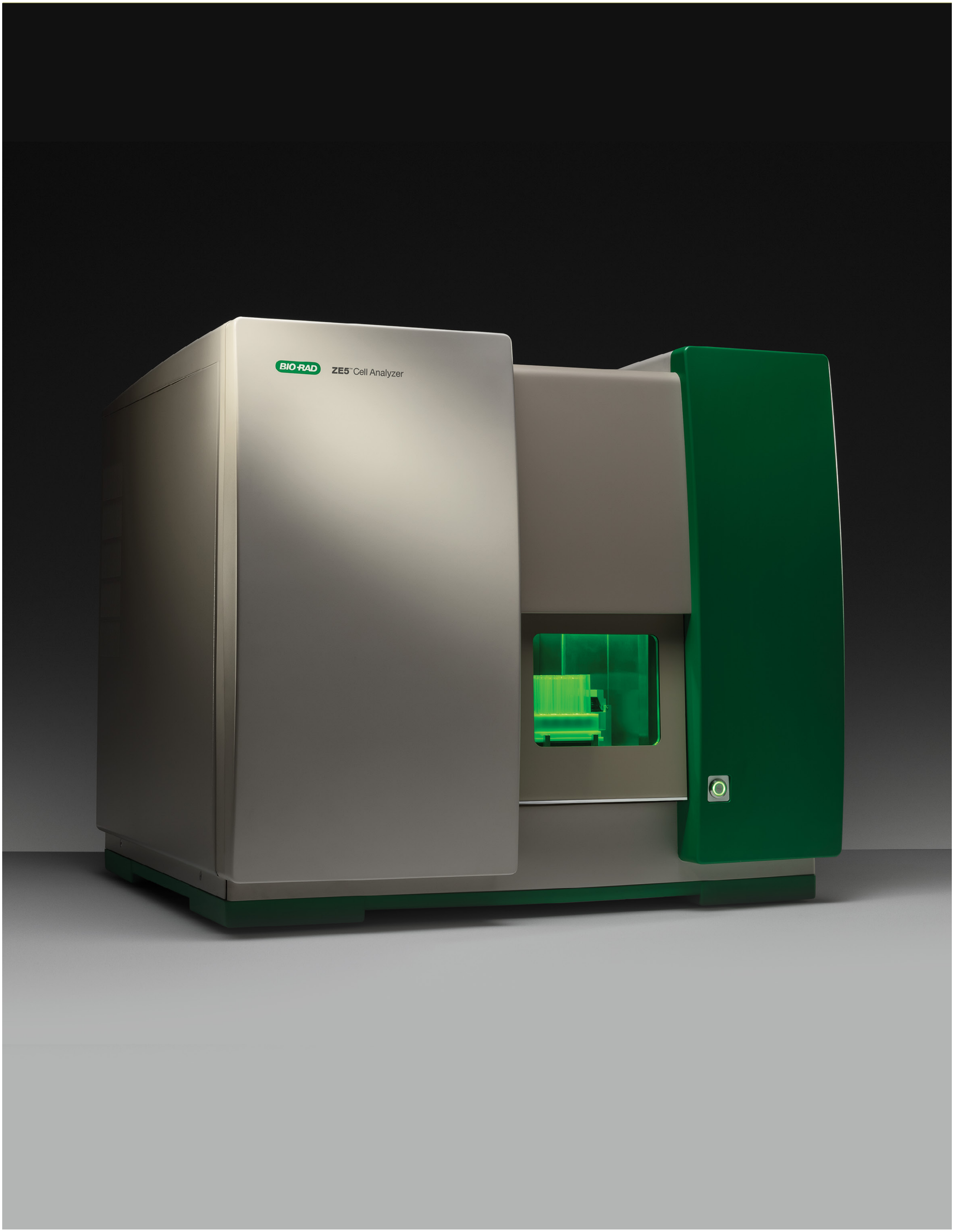
Flow Cytometry

Xybion Compliance Builder Software for ZE5 Cell Analyzer Users

Visit bio-rad.com/ZE5-compliance for more information.


BIO-RAD
ZE5™ Cell Analyzer

To enable the use of the ZE5 Cell Analyzer and Everest Software in regulated environments that require U.S. FDA 21 CFR Part 11 compliance, Bio-Rad™ Laboratories, Inc. has partnered with Xybion Digital Inc. The Xybion CQRM XD Compliance Builder (CQRM XD) is a unique software that helps companies enable U.S. FDA 21 CFR Part 11 compliance and ensure data integrity with real-time monitoring.

Now the benefit of fast, reliable, automation-ready flow cytometry can be combined with features including:

- Audit trail
- Electronic signatures
- Dashboards
- Email notifications and alerts
- Revision history
- Controlled user access
- Audit schema structure
- Multidomain support

Find out more about how Everest and Xybion CQRM XD Compliance Builder Software provide comprehensive support for U.S. FDA 21 CFR Part 11 compliance.

Everest Software with Xybion CQRM XD Compliance Builder Software provides extensive tools and features that support compliance with U.S. FDA 21 CFR Part 11: Electronic records and electronic signatures.

Subpart B — Electronic Records

11.10 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.

Section	Rule	Rule Summary	Everest Software	Xybion CQRM XD Software
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	System validation	IQ and OQ procedures available	Optional: Xybion Consulting provides this service. CQRM XD Software can help automate
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	Record generation for inspection	Provides both electronic and human readable formats for records such as QC trending reports, user login histories, etc.	Optional: Xybion CQRM XD Software Quality Management System (QMS) and Document Management System (DMS) provide documentation, change control, and document retention solutions
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period	Record protection	Data are saved in FCS file format. This format can be opened only with a specialized program. No data are overwritten. Any new data for the same experiment/sample are saved to a different, unique folder location	Audit trail records are maintained in a secure database and are available for viewing in a report for the life of the system. Data file revisions may be maintained as well and are available for download at any time
11.10(d)	Limiting system access to authorized individuals	System access limitation	Everest Software provides for unique user names and passwords. Different levels of privileges for authorized users limits access. User-tracking logs are available	All access to system administrative functions, reporting, etc. is controlled by user groups and requires a sign-in. High-level access is controlled with a workstation lock and application execution security
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	Audit trails	Logs are created with record date, time, operator, actions, D drive folder names, etc.	Critical data folders in Windows that may contain Everest Software data or any other data are monitored. Any actions that occur will be automatically audited with time stamp and Windows ID
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate	Operational checks	Restricts usage based on privilege assigned to user roles	N/A
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	Authority checks	Ensures proper authority based on user type. Tracking logs monitor the system. Only an administrator user can access tracking data. Date, time, user name, and experiment are on the top of each page of a generated PDF report	System interaction is controlled by permissions; only assigned users can log in, run audit trail reports, or electronically sign audit trail events
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	Data/operation validity checks	Changed data cannot be reimported to Everest Software. The files need to be associated with an experiment folder with specific files enclosed	Records of any change to Everest Software data files. The organization may use this information to determine the validity of any of their data files

11.10 Controls for closed systems continued.

Section	Rule	Rule Summary	Everest Software	Xybion CQRM XD Software
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	User training	N/A	Xybion provides Compliance Builder user and system administrator training. Xybion Consulting offers more generic U.S. FDA 21 CFR Part 11 training
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	User accountability	Organization's responsibility	Organization's responsibility Xybion Consulting offers organizational quality management/standard operating procedure (SOP) design services
11.10(k)	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation	System documentation control	Organization's responsibility	Organization's responsibility Xybion Consulting offers organizational quality management/SOP design services

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 section 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.

11.50 Signature manifestations.

Section	Rule	Rule Summary	Everest Software	Xybion CQRM XD Software
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer (2) The date and time when the signature was executed (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature	Enforces the requirement that every signed electronic record must have certain information associated with the signature	Experiment report in Publish tab includes time, date, and signed-in name of active user. Organization is responsible for tracking user names to actual users and their legal names	Records an electronic signature and meaning for any events captured in the monitored Everest Software folders. This information will be available in the File Audit Trail report, clearly showing the name of the signer, the time stamp, and the meaning that was entered
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 for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)			File Audit Trail report provides all the required electronic signature information

11.70 Signature/record linking.

Section	Rule	Rule Summary	Everest Software	Xybion CQRM XD Software
	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		Experiment report in Publish tab includes signed-in user name and date and time stamp	All electronic signatures are linked permanently to files and any file revision for the life of the system. Electronic signatures cannot be changed or deleted once accepted by the system

Subpart C — Electronic Signatures

11.100 General requirements.

Section	Rule	Rule Summary	Everest Software	Xybion CQRM XD Software
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	Signatures must be unique to the individual	N/A	Any user providing their electronic signature must have their own unique individual account in the system. User accounts can be disabled when someone leaves the organization
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	Verify the identity of the user	Organization's responsibility	Organization's responsibility
11.100(c)	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 (1) 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 (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	Electronic signatures must be unique when they are assigned, and they can never be reassigned to anyone else. The signer must certify in writing ownership of the signature and that it is the legal equivalent of a binding signature	Organization's responsibility	Organization's responsibility Each electronic signature is linked to a unique user account and is only attributable to that user. It can never be reassigned and can no longer be used when the user account is deactivated

11.200 Electronic signature components and controls.

Section	Rule	Rule Summary	Everest Software	Xybion CQRM XD Software
11.200(a)	Electronic signatures that are not based upon biometrics shall:	Guidelines for electronic signature		
	(1) Employ at least two distinct identification components such as an identification code and password	Employ at least two distinct identification components	Allows for assignment of unique name and password for Everest Software login	Each electronic signature requires entry of user ID 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	User should log into the user's own account at the beginning of a data entry session, input information (including changes) on the electronic record, and log out at the completion of the data entry session	Organization's responsibility	Organization's responsibility
	(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	Login must be required for every period of controlled system access	Organization's responsibility	Each electronic signature will require the entry of user ID and password, regardless of continuous session duration
	(2) Be used only by their genuine owner	User should work only under the user's own login	Organization's responsibility	Organization's responsibility
	(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals		Organization's responsibility	Organization's responsibility to ensure user accounts are properly administered with no generic logins that are shared
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		N/A	N/A

11.300 Controls for identification codes/passwords. Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity.

Section	Rule	Rule Summary	Everest Software	Xybion CQRM XD Software
11.300(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password	Unique user name and password combinations for all users	Everest Software allows for assignment of unique name and password	Allows operators to log in with their organization's credentials, thus falling under the organization's rules for such. Or allows for internal user accounts with assignment of unique name and password for all users
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)	Forced periodic password resets	Everest Software allows an administrator to force the change of passwords	Follows organization's rules for domain accounts. For internal accounts, passwords forced to reset after a configurable number of days
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	Loss management capabilities to deactivate compromised accounts and issue temporary access	Everest Software administrator can manage user profiles and deactivate accounts if no longer needed	System administrator can quickly deactivate accounts and provide access as needed
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	Transaction and security safeguards to detect and prevent unauthorized system access	Organization's responsibility	Organization's responsibility
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	Scheduled testing of safety devices	Organization's responsibility	Organization's responsibility

Visit bio-rad.com/ZE5-compliance for more information.

***Bio-Rad
Laboratories, Inc.***

*Life Science
Group*

***Website** bio-rad.com **USA** 1 800 424 6723 **Australia** 61 2 9914 2800 **Austria** 00 800 00 24 67 23 **Belgium** 00 800 00 24 67 23 **Brazil** 4003 0399
Canada 1 905 364 3435 **China** 86 21 6169 8500 **Czech Republic** 00 800 00 24 67 23 **Denmark** 00 800 00 24 67 23 **Finland** 00 800 00 24 67 23
France 00 800 00 24 67 23 **Germany** 00 800 00 24 67 23 **Hong Kong** 852 2789 3300 **Hungary** 00 800 00 24 67 23 **India** 91 124 4029300 **Israel** 0 3 9636050
Italy 00 800 00 24 67 23 **Japan** 81 3 6361 7000 **Korea** 82 080 007 7373 **Luxembourg** 00 800 00 24 67 23 **Mexico** 52 555 488 7670
The Netherlands 00 800 00 24 67 23 **New Zealand** 64 9 415 2280 **Norway** 00 800 00 24 67 23 **Poland** 00 800 00 24 67 23 **Portugal** 00 800 00 24 67 23
Russian Federation 00 800 00 24 67 23 **Singapore** 65 6415 3188 **South Africa** 00 800 00 24 67 23 **Spain** 00 800 00 24 67 23 **Sweden** 00 800 00 24 67 23
Switzerland 00 800 00 24 67 23 **Taiwan** 886 2 2578 7189 **Thailand** 66 2 651 8311 **United Arab Emirates** 36 1 459 6150 **United Kingdom** 00 800 00 24 67 23*