VAISALA

Application Note

www.vaisala.com

Annex 11 compliance for environmental monitoring systems: Beyond electronic records and signatures

A broader guidance

Annex 11 is often thought of as the European version of the US FDA's 21 CFR Part 11. This is far from the truth. The full title "Annex 11: Computerized Systems" immediately tell us that Annex 11 has a broader scope than Part 11. A greater scope of compliance entails a different approach than used in addressing a more focused regulation, such as 21 CFR Part 11. Annex 11 pertains to more than electronic records and takes a more holistic system life cycle perspective with a focus on risk assessment as a tool for ensuring product safety and efficacy.

Annex 11 is a short document; only five pages. The first page includes titles and legal preludes.

As a part of European Good Manufacturing Practice guidelines, Annex 11 outlines the proper use of computerized systems used in GxP-regulated industries. Annex 11 is published by the executive branch of the European Union, known as the European Commission (EC). The EC proposes legislation, upholds EU treaties, and oversees trade that can benefit from regulatory oversight. Good manufacturing practice falls under the last function of the EC.

Much like the FDA's 21 CFR Part 11, Annex 11 defines the criteria by which electronic records and electronic signatures can be considered equivalent to paper documents. Unlike 21 CFR Part 11, Annex 11 is not a regulation; it is a guideline. Annex 11 outlines basic compliance standards for GxP principles in the EU directives, which are the actual regulations contained in EudraLex.

Comprising 10 volumes, Eudralex Volume 1 and Volume 5 outline the regulations that are enforceable under law. The other 8 volumes contain guidelines. Eudralex Volume 4 contains 19 annexes, including Annex 11. Annex 11 refers to the use of computerized systems in GxP-regulated applications. In 1991, the Pharmaceutical Inspection Co-operation Scheme (PIC/S) published non-binding requirements for computer systems. In 2011, these would be re-released as Annex 11 and thereafter part of the EU's GxP guidelines.

The section titled "Principle" states:

"Annex 11 applies to GMP computerized systems, including both software and hardware. The application should be validated and IT infrastructure should be qualified. Using a computerized system should not cause any increase in quality, control, or risk."

This means that Annex 11 applies to automated environmental monitoring systems. Validation, IT controls, and risk assessment are key topics in Annex 11 guidance.

Annex 11 controls

Technically, there are 17 controls listed in Annex 11. The first three controls come under the heading of "General" and should be regarded as a prelude to guide compliance with Annex 11. The first three areas of controls are:

1 RISK MANAGEMENT:

Use a documented risk management process that focuses on patient safety, data integrity, and product quality.

2 PERSONNEL:

Ensure close cooperation between *all* relevant personnel (including IT specifically) and verify that the people involved are qualified and supported by the organization.

3 SUPPLIER AND SERVICE PROVIDERS:

Leverage third parties where possible. Use formal agreements to define responsibilities. Annex 11 refers to suppliers of third-party software having quality systems in place.

The wording of Annex 11 makes it clear that compliance activities are resource intensive and recommends a focus on critical functions through risk assessment. The risk-based approach is cross-functional, that is, inclusive of quality, end users, IT, and third-party providers. If Annex 11 ended there, it would already have provided a lot of value in considering the cost of compliance and different levels of risk in different applications.

The instruction to leverage third parties is important, especially with the growing need for automation, increasing complexity in computerized systems, and new technologies. In terms of automated monitoring systems, the system vendor can aid in compliance efforts by providing a product that was developed for quality systems in regulated environments; for example, by providing validation protocols.

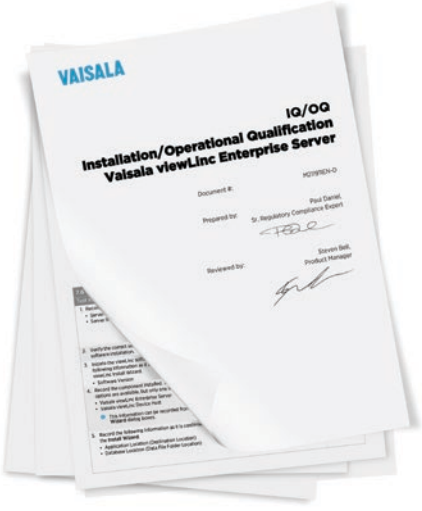
Of the 14 specific controls remaining in Annex 11, we can categorize them as validation plus 13 ongoing controls. Supporting this perspective is the fact that the validation section of Annex 11 makes up more than 25% of the remainder of the document. In addition, the validation section is given the heading "Project Phase", separate from the remaining controls that occur under the heading "Operational Phase". This reflects the guidance's focus on the life cycle of a system and it tells us that validation will be the foundation for ongoing compliance with Annex 11.

Project Phase – Validation

In Annex 11, validation is an ongoing activity that occurs through the entire life cycle of a system, from implementation to retirement, including change control as updates are made to the system. Annex 11 recommends an inventory to document all GMP computerized systems and critical systems. This inventory should include: detailed system descriptions, flow charts, and interfaces with other systems. These guidelines set the expectation that validation is a recursive activity, ongoing at your facility rather than a single effort directed at qualifying a single system.

Annex 11 outlines the validation process, starting with traceable User Requirements, which aligns with the GAMP® approach published by the International Society for Pharmaceutical Engineering (ISPE). We hear echoes of the GAMP philosophy of leveraging supplier involvement; Annex 11 recommends selecting systems developed in accordance with a modern quality management system from an audited or assessed supplier. Validation testing is expected to be appropriate to the criticality of the application, which is another way of referencing risk assessment. And if data is transferred between systems, a focus on data integrity is expected.

Annex 11 outlines a validation approach that entails vendor cooperation by way of the vendor's quality management system. A system vendor can meet customer needs with robust quality policies and supporting documentation. For example, Vaisala offers a comprehensive GxP Documentation Package for its viewLinc Continuous Monitoring System. The package includes a template User Requirements document that is directly related to the system's Installation Qualification/Operational Qualification (IQOQ) validation protocol through a Traceability Matrix, also contained in the package. Further, a vendor can offer an accompanying Risk Assessment document, as Vaisala does, to demonstrate that the critical system features are tested.



Operation Phase – Use of computerized systems

After creating the foundation for compliance of computerized systems with validation, Annex 11 moves on to the Operation Phase, which details 13 controls. The first two controls address data entering the system.

1 DATA:

Where data is exchanged with other systems, built-in checks are needed to ensure correct and secure transfer.

2 ACCURACY CHECKS:

Manually entered critical data must be double checked. A monitoring system collects raw data from a network of hardware that is distributed throughout a facility. Ideally, the system relies primarily on proprietary sensors so that data is only allowed into the system from devices that have been previously verified. Furthermore, manual entry or revision of raw data is not allowed. These features ensure that data enters the monitoring system database with integrity and accuracy.

Data integrity

The next three controls focus on data access and protections that ensure data integrity.

1 DATA STORAGE:

Data must be secure against damage, yet remain accessible, readable, and accurate throughout the retention period. Regular backups are expected and should be verified and monitored.

2 PRINTOUTS:

Clear printed copies of electronically stored data should be easily available. Any changes to data should be indicated.

3 AUDIT TRAILS:

Audit trails track all instances of record creation, modification, and deletion, including the system user, the reason for the change, and a timestamp.

Monitoring system software needs specific data protections that provide these controls. For example, in viewLinc, raw data is stored in an encrypted database within viewLinc's server, and cannot be changed by any user, much like a protected archive. Unlike an archive, the data is immediately available for inclusion to trends and reports for analysis and printing.

Backups can be managed with a copy of the database files, or by imaging the entire viewLinc server. For changes to system parameters and recording other system events, viewLinc provides an audit trail (Event Log) that can be filtered, searched, and printed as needed.

System security

The security of computerized systems is also addressed in Annex 11.

1 SECURITY:

Systems must have physical and logical controls that restrict access to authorized personnel only. Audit trails must include access authorizations.

Any monitoring system used in a GxP application requires software with advanced security functions to limit access to and within the software. For example, in viewLinc users can opt to use Windows Authentication. Alternatively, viewLinc features native security features with complex passwords, password aging, and lockout after multiple failed login attempts. Regardless of the security method chosen, all login attempts are recorded in viewLinc's audit trail.

Quality management controls

Annex 11 includes guidance on: Change and Configuration Management, Periodic Evaluation, Incident Management, and Business Continuity. Together these controls ensure that a system has ongoing support to ensure continued operation in a validated and controlled state.

1 CHANGE & CONFIGURATION MANAGEMENT:

Any changes made to a computerized system need to be made in a controlled manner following a defined procedure.

2 PERIODIC EVALUATION:

Periodic evaluation to verify a validated state and continued GMP compliance, including a review of incidents, deviations, and other major events.

3 INCIDENT MANAGEMENT:

All incidents must be reported and assessed. Critical events are investigated to determine root causes and corrective and preventive actions are taken.

4 BUSINESS CONTINUITY:

System uptime or return-to-use is ensured in case of disruption. This should be based on application risk and criticality.

These Annex 11 controls are a fundamental part of an organization's internal Quality Management System. A monitoring system vendor can provide support with system function design and value-added services. For example, viewLinc includes a report that compares system parameters before and after system changes. In addition, periodic software updates are available to keep viewLinc in alignment with changing technology and regulations. As a service Vaisala provides expert technical support to assist in investigations, or for emergency support to ensure business continuity.

Electronic signature, batch release & archiving

These features may or may not be included in a monitoring system. Some systems still produce paper documents for manual signatures. For example, viewLinc does not currently support electronic signatures for data review and approval because all current signature methods require that signed documents be stored in the system where they were signed. The viewLinc system was not designed for document storage. The functions of document storage and electronic signatures are effectively assigned to a centralized system for document control.

Batch Release and certification is also not a function of a monitoring system. This function is typically found in a Quality Assurance Release System, or in an Enterprise Resource Planning (ERP) system. Archiving, which protects data from changes, is another control that doesn't apply to viewLinc. Rather than storing reports, viewLinc stores all raw data in a way that it is indelible and uneditable, but is readily accessible and readable.

Risk-based and quality focused

Although concise, Annex 11 addresses risk management, quality systems, third-party vendors, periodic reviews, and operational guidance for ensuring the efficacy of computerized systems. In a global manufacturing and distribution landscape, it is a partner guidance to 21 CFR Part 11. While Part 11 is focused on electronic records and signatures, Annex 11 addresses computerized systems as a whole. Annex 11 takes into account how systems fit with modern validation expectations and IT infrastructure. Further, it allows a risk-based approach that can help with resource allocation.

Like Part 11, the important controls in Annex 11 are not performed by any single system feature. Although system features can simplify compliance efforts with audit trails and access controls, the crucial elements of the controls contained in Annex 11 depend on the quality management system of your organization.

VAISALA

Please contact us at
www.vaisala.com/contactus

www.vaisala.com

Scan the code for more information