WHITE PAPER

ON

Annex 11 Compliance for Continuous Temperature Mapping (cTM)

This white paper evaluates the compliance of xLM's AI-powered Industrial Internet of Things (IIoT) solution, cTM, with EU Annex 11 requirements.

www.continuousintelligence.ai

1. Overview of cTM

Continuous Temperature Mapping (cTM) is an AI-enabled IIoT platform that automates real-time temperature and environmental monitoring for manufacturing, storage, and distribution. It replaces manual spot checks with intelligent, 24/7 monitoring—improving data integrity, enabling proactive interventions, and supporting continuous compliance.

The system integrates sensor data, audit trails, workflow controls, and electronic signatures into a unified platform validated according to xLM's Quality Management System (QMS) and Software Development Life Cycle (SDLC) procedures.

2. Annex 11 Clause-by-Clause Assessment

Annex 11 Section	Title	cTM Compliance Summary
1	Risk Management	cTM supports real-time anomaly detection and proactive alerts, aiding in risk-based decision-making. It complements organizational risk assessment practices with continuous monitoring insights.
2	Personnel	Role-based access control is supported with user authentication.
3	Suppliers and Service Providers	xLM delivers cTM as a validated platform. Calibration and validation of IIoT devices are maintained.
4	Lifecycle Documentation	Full traceability of data acquisition, record handling, audit trail logging, and system updates. Documented evidence of validation lifecycle and system performance.

Annex 11 Section	Title	cTM Compliance Summary
5	Validation	The cTM platform itself is validated and used to monitor qualified GxP environments. Device calibration, automated validation reporting, and inspection readiness are included.
6	Data	Temperature data is stored in secure, tamper-evident formats with ALCOA+ principles enforced. Timestamped audit trails support data accuracy.
7	Accuracy Checks	Real-time data validation through sensor calibration and comparison workflows. Alerts highlight deviations immediately.
8	Data Storage	Configurable retention policies for long-term data archiving and retrieval. Records remain secure and exportable throughout lifecycle.
9	Printouts	cTM provides encrypted, exportable reports that preserve metadata such as timestamps and user identity. Available in formats suitable for inspections.
10	Audit Trails	All data, changes, and approvals are logged in immutable, timestamped audit trails. Accessible for audits and system forensics.
11	Change and Configuration Management	Change tracking and automated configuration management are built into the system, with audit-ready logs.
12	Electronic Signatures	cTM supports e-signatures per Annex 11: timestamps and unique hash markers for tamper detection. Signature responsibility remains with client organization.

Annex 11 Section	Title	cTM Compliance Summary
13	Batch Release	cTM is not a batch release system, but provides validated environmental records that can be used as part of batch release documentation.
14	Business Continuity	Cloud deployment with redundancy, encrypted backups, and disaster recovery protocols ensure continuous availability.
15	Archiving	Version-controlled, read-only archives are maintained with role-based access controls and export capability. Searchable and inspection-ready.

3. Summary of cTM Alignment with Annex 11

Validated System

cTM is developed under a validated SDLC and QMS framework with calibration records for all IIoT devices.

End-to-End Lifecycle Support

The system logs and manages all events and records across the monitoring and validation lifecycle, with full auditability.

Audit and Traceability

Secure, computer-generated audit trails ensure every data point and user interaction is recorded and uneditable.

Electronic Records and Signatures

E-signatures include user identity, timestamps, and integrity verification using cryptographic hashes.

Risk and Change Management

Built-in alerts and change logs ensure controlled, risk-based actions throughout the monitoring process.

User and Access Control

Role-based access and strong authentication mechanisms protect sensitive records and restrict system access.

Business Continuity and Data Integrity

Data is continuously collected, stored redundantly, and monitored to ensure regulatory-grade reliability and availability.

4. Conclusion

Regulatory agencies, including the EMA, promote digital transformation in life sciences—as long as systems maintain integrity, auditability, and human accountability. The cTM platform fulfills these expectations by embedding compliance into its architecture.

It combines validated device integration, automated audit trails, and secure e-signatures with real-time analytics to deliver a modern, inspection-ready system. While compliance responsibilities also lie with the client organization (e.g., SOPs, training), cTM provides the technological backbone to uphold Annex 11 mandates.

By adopting cTM, life sciences companies can improve temperature control, reduce manual effort, and maintain continuous compliance in regulated environments.

5. References

This document is based on the System assessment Checklist from the Good Manufacturing Practice Medicinal Products for Human and Veterinary Use document, issued jointly by EUROPEAN COMMISSION HEALTH AND CONSUMERS DIRECTORATE-GENERAL version 4 dated 2010, “EudraLex The Rules Governing Medicinal Products in the European Union”