How does Qtegra ISDS Software for gas IRMS support 21 CFR Part 11 compliant environment?

The analysis of isotope ratios using gas Isotope Ratio Mass Spectrometry (IRMS) is a powerful tool in assessment of the authenticity and origin of samples covering a range of applications from forensics to food.

Compliance to regulatory guidelines for data acquisition, data storage and integrity are key requirements for many laboratories. One of the most mentioned guidelines to assure data integrity and quality is Part 11 of Title 21 of the “Code of Federal Regulations; Electronic Records; Electronic Signatures” (21 CFR Part 11), governing federal guidelines for storage and protection of electronically stored data and the application of electronic signatures in the United States. Other regulations are applicable in other geocenters for example through ICH guideline 7.5.43, EU Annex 11 or local regulations.

This document examines all sections of 21 CFR Part 11 and describes how the Thermo Scientific™ Qtegra™ Intelligent Scientific Data Solution (ISDS) Software supports compliant environments. The Qtegra ISDS Software is an instrument agnostic software platform employed across a range of instruments in the Thermo Scientific portfolio from Gas IRMS to ICP-MS. With the same workflow, functionality and look and feel across multiple instruments, analysts are empowered and can flexibly switch between different techniques eliminating any barrier from learning a completely new software package.

The Qtegra ISDS Software platform provides a wide range of features, which enable laboratories to operate within total compliance, not only with respect to 21 CFR Part 11, but also other compliance guidelines applicable in different regions. Key elements to operate in compliance with 21 CFR Part 11 and others are for example:

- Audit Trails to establish traceability of all actions taken to obtain a particular result from a sample. This includes general system configuration, analysis procedure and data manipulation steps (e.g. mathematical operations to convert raw data to results).
- Access authorization to assure that only specific individuals (for example with necessary qualification) are able to operate the system and generate results.
- Checks and controls for analytical procedures to avoid the use of instrumentation or procedures that could lead to obtaining potentially erroneous data.
- Accurate copies and secure retention and retrieval of records, including procedures for secure data storage and back up.
- Electronic signatures for full control for data generation, review and approval.

In order to operate an analytical system in compliance with regulatory guidelines such as 21 CFR Part 11, it is key to understand that this cannot be achieved through functionality and checks available in software (or hardware) alone, but only in conjunction with procedural, administrative and technical controls established in the organization operating a particular instrument.

Development and validation of Qtegra ISDS

Qtegra ISDS Software is developed in accordance with the ISO 9001 certification of the Thermo Fisher Scientific Center of Excellence for Mass Spectrometry in Bremen, Germany. This certification assures that appropriate procedures are established to assure hardware and software development is accomplished according to relevant requirements, is performed by qualified (and regularly trained) individuals and internally documented.

Qtegra ISDS Software Qualification

Qtegra ISDS Software includes an extensive toolset for the performance of software IQ. An Installation Qualification (IQ) is executed when the Qtegra ISDS Software is initially installed. During the IQ process, the tool verifies that all files are installed in the correct locations, and their integrity is verified via comparison of checksums. The IQ process can be performed whenever it is required (for example after updates to the computer system, such as an operating system change) to meet established company SOPs.

Table 1. Requirements as per 21 CFR Part 11 and implementation in Qtegra ISDS Software

Point no.	21 CFR Part 11 requirement	Availability in Qtegra ISDS (Y/N)	Additional information
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:			
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Y	Qtegra ISDS Software is developed using the latest industry standard software development tools. All Qtegra ISDS Software files (executable program, libraries etc.) are encrypted and cannot be accessed outside of the software development environment at the manufacturer's facility. Each time Qtegra ISDS Software is opened, a complete scan of all system files is performed to ensure the validity of all software components and procedures. A series of systems and procedures within Qtegra ISDS Software allow the user to identify invalid or altered data.
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.	Y	Qtegra ISDS Software stores all electronic records in a proprietary, encrypted data container called a LabBook that can only be accessed through the Qtegra ISDS Software. All electronic records, including instrument calibrations, performance tests, analytical data, metadata, analytical reports, log files and audit trails can be stored as human readable files and be made available for inspection by an auditor.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Y	Qtegra ISDS Software provides all the necessary functionality to provide safe and secure storage of records throughout the retention period. The entire electronic data, including audit trails, can be backed up to a centralized storage server and retrieved at any point of time for review on a Qtegra ISDS Software equipped data station. All electronic records, including instrument calibrations, performance tests, analytical data, metadata, analytical reports, log files and audit trails can be stored as human readable files for review without requiring access to Qtegra ISDS Software.
11.10 (d)	Limiting system access to authorized individuals	Y	User access to Qtegra ISDS Software is controlled through user management tools provided by the Microsoft Windows® 10 Operating System. Both local and Active Directory based accounts are supported. Specific user groups are automatically created during software installation. Membership of these groups is assigned to specific users by a separate System Administrator who is not able to perform data acquisition.
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.	Y	No electronic records are deleted in Qtegra ISDS Software. A complete audit trail of any changes in records are automatically captured and permanently retained within the LabBook data container. Changes are captured with full details on: 1. The user account making the change 2. The change made 3. The date/time stamp of the change 4. The reason for the change. Qtegra ISDS Software therefore provides full who/what/when/why information for all changes made. Differences between stored versions of records can be compared at any time and reported in a human readable format for review. The audit trail is an integral part of the analytical data and does not need to be separately stored or archived, improving data clarity and traceability. In addition, all deletions, amendments or moving of the LabBook data container are documented. Complete trails can be inspected and exported for auditor review as required.

Point no.	21 CFR Part 11 requirement	Availability in Qtegra ISDS (Y/N)	Additional information
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Y	Qtegra ISDS Software follows a structured, logical sequence that guides the analyst through the workflow. System checks with visual indicators highlight gaps that must be addressed before data acquisition can be performed. Laboratory managers can establish method specific templates that define the analytical method used. In combination with automated quality control checks and data highlighting tools, users are alerted to potentially suspect analytical data as it is generated. For EA-IRMS Qtegra ISDS Software can automatically dilute samples that do not meet method defined analytical criteria minimizing the need for secondary analysis.
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.	Y	All Qtegra ISDS Software users must be members of specific User Groups and can only log in to the system after a successful two-stage identity check. The System Administrator defines User Group membership as well as the program and operational access rights and privileges for each user group to meet existing company standard operating procedures (SOP). After login, the user can only perform the activities (electronic signing etc.) as defined by the System Administrator.
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.	Y	Instrument performance is assessed in Qtegra ISDS Software through an automated 'Get Ready' process. This automated workflow takes the system through a series of predefined (customer modifiable) performance checks and any required appropriate system optimization or calibration routines, before performing a subsequent performance check. A comprehensive series of quality control (QC) checks are available that can be used to verify method and instrument performance during analytical runs. Human readable reports of the results from performance or QC checks can be generated for export or print. The instrument serial number and control PC identifier can be displayed in both software and reports.
11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems has the education, training and experience to perform their assigned tasks.	Y	Powerful and flexible user access tools in Qtegra ISDS Software are used to allow authorized users access to individual applications, granular functional actions as well as electronic (e-)signatures. While suggested defaults are provided, the appropriate definition and ongoing control of access rights is the responsibility of the user and should be controlled by appropriate procedures and documentation. Full audit trailing of access rights provides traceability.
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.	Y	Qtegra ISDS Software provides a comprehensive feature set to support the use of e-signatures. E-signatures are completely integrated within the LabBook and cannot be extracted or externally modified. E-signatures are unique to each user and require a two-stage identity check before application. E-signatures records include the printed name of the signee, the date/time stamp as well as meaning. Additional actions such as addition and revoking of signatures, multiple level signing, support of the 'four eyes' principle are supported. Changes in the LabBook record by e-signatures are captured in the audit trail. A dedicated e-signature workflow editor allows organizations to extend their own e-signature workflow within Qtegra ISDS Software. Individual signature actions can be renamed, added/deleted and reordered to meet customer SOP requirements. Changes in the e-signature workflow are captured in the audit trail for complete traceability. Any e-signature applied during the data set lifecycle can be added to human readable reports. While suggested defaults are provided, the appropriate definition and ongoing control of e-signatures is the responsibility of the user and should be controlled by appropriate procedures and documentation.

Point no.	21 CFR Part 11 requirement	Availability in Qtegra ISDS (Y/N)	Additional information
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.	N/A	This is the responsibility of the organization.
Controls for open systems			
11.3	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.	N/A	Qtegra ISDS Software is not designed to operate as an open system.
Signature manifestations			
11.50 (a)	Signed electronic records shall contain information associated 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.	Y	Qtegra ISDS Software offers a workflow adaptive feature set for application of e-signatures. E-signatures include the printed name of the signee, the date/time stamp as well as meaning of the signature.
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).	Y	Any usage of e-signatures is captured in the same audit trail as the electronic record. Complete version control of e-signatures is also provided. Electronic signatures can be included in any human readable form of electronic recording displayed either on screen or in print to show the printed name of the signee, the date/time stamp as well as meaning of the signature.
Signature/record linking			
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.	Y	Electronic signatures are applied to electronic records in Qtegra ISDS Software and are inextricably embedded in the encrypted LabBook record. Any change in the use of e-signatures is captured in the audit trail. Handwritten signatures are not recognized within Qtegra ISDS Software.
General requirements			
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Y	In principle, e-signatures are validated with digital certificates. The organization can build its own infrastructure for assigning digital certificates or purchase them from commercial vendors. Signatures are linked to unique system user accounts and a two-stage identity check must be passed before an e-signature can be applied.
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.	N/A	This is the responsibility of the organization.

Point no.	21 CFR Part 11 requirement	Availability in Qtegra ISDS (Y/N)	Additional information
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.	N/A	This is the responsibility of the organization.
Electronic signature components and controls			
11.200 (a)	Electronic signatures that are not based upon biometrics shall: 1. 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.	Y	A combined user ID and password is required each time an e-signature is applied to the LabBook data container.
	(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.	Y	A combined user ID and password is required each time an individual log in to the system. A combined user ID and password is required each time an e-signature is applied to the LabBook data container.
	2. Be used only by their genuine owners; and	Y	The user ID and password must be kept confidential by the user.
	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.	Y	The user ID must be unique with only one user of each ID allowed on the domain, as per Windows authentication and the system administrator settings. Users are instructed to change their password to one that is known only to them.
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	Qtegra ISDS Software does not support biometric signatures.
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. Such controls shall include:			
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.	Y	The combination of user ID and password must be unique. This is ensured by Microsoft Windows® and should be controlled by the organization's system administrator.
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).	Y	Qtegra ISDS Software uses the Windows domain controller for password control that allows for control of these events. It is the responsibility of the organization's network administrator to ensure that these criteria are met.

Point no.	21 CFR Part 11 requirement	Availability in Qtegra ISDS (Y/N)	Additional information
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.	N/A	Qtegra ISDS Software does not support the use of tokens, cards or other such devices.
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.	Y	All log in and log off attempts are detected and fully documented whether they are successful or unsuccessful. Any such events can be sorted (by event, user account or time period) and exported and reported in a human readable format.
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.	N/A	Qtegra ISDS Software does not support the use of tokens, cards or other such devices.

In addition to the detailed requirements as per 21 CFR part 11, Table 2 contains more information about additional features, related to questions frequently asked by customers/operators.

Table 2. Additional frequently asked questions on compliance features implemented in Qtegra ISDS Software.

General information on Qtegra ISDS Software	
Question	**Answer**
Where is the Qtegra ISDS Software developed?	All programming for Qtegra ISDS Software is performed at the manufacturer's facility in Bremen, Germany
Where is the Qtegra ISDS Software source code archived?	The Qtegra ISDS Software source code is archived at a secure, offsite, access limited, specialized data facility.
Who performs the software testing?	All formal regression and functional testing of Qtegra ISDS Software is defined and performed at the manufacturer's facility in Bremen, Germany, by a separate, independent, Product Evaluation team.
Are employees sufficiently trained?	Yes. All employees are appropriately trained for their respective roles.
Are development documents available for inspection?	Yes. All documentation can be viewed at the manufacturer's facility after signing of non-disclosure agreement (NDA).
If relevant changes are made to the system (computer equipment or programs) is the ability to retrieve the data ensured and tested?	Before release of any software version it is thoroughly tested through a combination of automated and manual regression tests. The data generated from previous versions are validated to be retrievable using the latest version.
User access control functions	
Is system access password policy configurable?	Yes. Controls on password length, complexity, history, duration of validity, etc. are provided.
How many types of user access control level are provided, and can these be user modified?	A maximum of seven user groups are available. These can be removed or renamed by the customer to fit with existing SOPs.
Is there provision to capture changes in user access and/or management	Yes. Any changes in user access management are captured in the system. Activities such as user log on, log off, granting or denying of access etc. are captured in the audit trail. A comprehensive report of changes can be displayed on screen in Qtegra ISDS Software or exported in a human readable form for independent review.
Are controls available to restrict data access to avoid accidental or willful changes of records?	Yes. Qtegra ISDS Software includes powerful tools to restrict user access to records. Access to records can be restricted per folder or even individual LabBook data containers in accordance with user SOPs.

General information on Qtegra ISDS Software	
Question	**Answer**
Workflow	
Can I verify that my instrument is meeting the required performance?	Yes. The Get Ready process confirms performance to defined criteria as well as triggering corrective actions (e.g. autotune). Get Ready must be completed before any analytical measurement can be started. Flexible templates in the Sample List allow the user to verify system performance through the analysis of quality checks during routine analysis. Data can be compared to previously defined criteria, allowing electronic or paper format reports to be generated with specific formats to flag values outside of specification.
Do I have to manually start the system?	No. The Get Ready routine automatically starts the system.
Do I have to stop the analysis to allow for changes in user, for example caused by shift changes or supervisor/manager access?	No. Data acquisition in Qtegra ISDS Software is performed independent of any user account using a dedicated Windows service. This allows for rapid, documented and secure switching between users, for example to allow for batch release by electronic signature. All user changes are tracked in a protected, unmodifiable audit trail.
Are there any additional checks on the accuracy of the data?	Yes. A comprehensive set of quality control functions are included as standard in Qtegra ISDS Software. Additional checks allow for the flagged display of data (either on-screen or in human readable reports) outside of customer defined limits.
Do I have to export data into Excel to perform simple mathematical tests?	No. The Qtegra ISDS Software provides a series of simple calculation tools. such as STDEV calculations or data evaluation according to external reference material.
Data integrity and security	
How can I ensure that data files can no longer be modified?	LabBook datafiles can be locked using e-signatures to disable any further data manipulation.
How can I ensure that intermediate records cannot be exported or reported to ensure agreement between human readable and electronic records?	LabBook datafiles can be locked using e-signatures to disable data export or reporting.
Are there controls to ensure data backup, retrieving and maintenance process is carried out with due diligence?	Yes. All Qtegra ISDS Software related data files can be backed up using standard Windows compatible backup applications. Definition of the backup process and schedule is the responsibility of the user. Qtegra ISDS Software provides an additional, optional facility to automatically backup the complete LabBook data container to guard against sudden PC hardware failure.
Can the system generate printouts indicating if any of the e-records has been changed since the original entry?	Yes. Any changes in the e-record (the LabBook) are captured in the audit trial. With every change in the record, new data version is generated with date & time, user identification, reason of change etc. Version to version changes can be compared and captured in human readable reports for review.
Audit trail	
Are changes in method parameters captured in the audit trail?	Yes. The audit trail captures every change made to the method and any effect on the analytical data.
Can the reason for a modification be captured?	Yes. Before implementing any changes to the record, changes must be saved. A comment must be entered for any change to be made.
Can the audit trail functionality be switched OFF?	No. Audit trail functionality in Qtegra ISDS Software is always ON. It cannot be disabled.
What information is captured when a change to the record is made?	Full who/what/when/why information is captured in the audit trail when a change to a record is made.
Electronic signatures	
Are controls available to restrict users from e-signing one record with more than one role, e.g. a user signs first as an Analyst and then as a Reviewer?	Yes. Qtegra ISDS Software does not allow individual users from performing multiple e-signatures on a single record.

Find out more at **thermofisher.com/QtegraIRMS**

ThermoFisher SCIENTIFIC