QN1-OQ-007 21 CFR PART 11 SOFTWARE REGULATION GUIDELINES

IZON

www.izon.com

CONTENTS

1 / SCOPE

This document details the tests and acceptance criteria required in order to verify that Izon Science Ltd.'s Control Suite Software (CSS) has been developed in accordance with and complies to the 21 CFR Part 11 guidelines. It outlines which guidelines are relevant to Izon's CSS and links the guidelines to each specific test.

This SOP should be executed each time CFR compliance verification is required.

2 / 21 CFR PART 11 GUIDELINES

21 CFR PART 11 SUBPART A / DEFINITIONS

The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. The following definitions of terms also apply to this part:

Term	Definition
Act	The Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).
Agency	The Food and Drug Administration.
Biometrics	A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
Closed System	An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Digital Signature	An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
Electronic Record	Any combination of text, graphics, data, and audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
Electronic Signature	A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
Handwritten Signature	The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate writing in a permanent form. The act of signing with a writing or marking instruments such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
Open System	An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Under these definition guidelines, Izon's Control Suite Software is considered a closed system and will follow the 21 CFR Part 11 closed system guidelines.

21 CFR PART 11 SUBPART B

21 CFR Part 11, Section 11.10 / Controls for Closed System

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:

Note: Test IDs denoted by T#. "P" denotes where access has been provided or an on-site training date has been scheduled.

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.				
11.10 (a)	Life cycle doc IAW, Section 9.53 of GAMP4	NA	Izon instruments do not use automated processes.	NA
	Operation and Maintenance manuals	Y	VPM manual provided. Instructions on use of software features are available within software (see Instructions panels and Help files)	P
	User Training Program	Y	On-site user training provided. Online user training modules available.	P
	Maintainers Training Program	Y	Company policy is that CSS upgrades, provided to a company Administrator, will follow a CSS Upgrade SOP.	P
	System needs to provide an automated means to ensure the ability to discern invalid or altered records.	Y	NA	T9
The ability to generate accurate complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.				
11.10 (b)	System needs to be able to produce a hard copy (paper) of individual and/or the entire relevant e-record(s) for inspection	Y	NA	T12
	E-records need to be produced in an electronic format (e.g., portable document format, CD, electronic transportable format, Excel spreadsheet, .txt file)	Y	NA	T13

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
System allows for protection of records to enable their accurate and ready retrieval throughout the records retention period.				
11.10 (c)	Records may not be over-written	Y	NA	T8
	Record ID cannot be duplicated	Y	NA	T7
	A unique Record ID must be unique	Y	NA	T7
System access is limited to authorized individuals.				
11.10 (d)	A unique User ID and password must be used to access the system	Y	NA	T2
	The system has an automatic lockout after a specified period of inactivity	Y	NA	T6
System uses 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.				
11.10 (e)	Secure time stamped Audit Trail that records Date, Time (local), User ID, Action, State Change, Related Data Record (where relevant) is automatically generated	Y	NA	T15
	Audit Trail records login, lockout, logout and security violation events	Y	NA	T16
	Audit Trail records data record creation, modification, export and deletion	Y	NA	T17
	Entries cannot be deleted from the Audit Trail	Y	NA	T19
	Audit Trail can be exported, backed up, and printed	Y	NA	T20
11.10 (f)	System uses operational system checks to enforce permitted sequencing of steps and events, as appropriate.	NA	CSS does not sequence steps or events	NA
System uses authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer input or output device, alter a record, or perform the operation at hand.				

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
11.10 (g)	System requires user login for access	Y	NA	T2
	System provides three levels of security to ensure that only suitably authorized users can perform system tasks	Y	NA	T14
System uses device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.				
11.10 (h)	System can only use an Izon instrument as a data input device	Y	NA	T1

21 CFR Part 11, Section 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.

Per 21 CFR Part 11's definition of an open system (see section 2.1.9), Izon's Control Suite Software does not fall under the "open system" guidelines and thus does not need to meet Section 11.30 requirements.

21 CFR Part 11, Section 11.50 / Signature Manifestations

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:				
11.50 (a)	The printed name of the signer.	Y	NA	T11
	The date and time when the signature was executed.	Y	NA	T11
	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Y	NA	T11
The items identified in 11.50(a) (1) (2) (3) 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).				

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
11.50 (b)	E-signatures are included in the system-Audit Trail	Y	NA	T18
	E-signatures can only be executed by authorized users	Y	NA	T10
	E-signatures are included as part of any human readable form of the electronic record.	Y	NA	T11
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.	NA	Requires company policy	NA

21 CFR PART 11 SUBPART C

21 CFR Part 11, Section 11.100 / Signature/Record Linking

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
11.100 (a)	Each electronic signature must be unique to one individual and must not be reused by, or reassigned to, anyone else.	NA	Requires company policy	NA
11.100 (b)	The identity of the individual must be verified prior to the organization establishing, assigning, certifying, or otherwise sanctioning that individual's name identified	NA	Requires company policy	NA
11.100 (c)	Persons using electronic signatures must, prior or at the time of use, certify to the FDA that the electric signature used in the computerized system after August 20, 1997 are intended to be legally binding equivalent of traditional handwritten signatures.	NA	Requires company policy	NA
11.100 (d)	The certificate must be submitted [in paper form and signed with a traditional handwritten signature] to the appropriate FDA Office specified in the regulation.	NA	Requires company policy	NA

21 CFR Part 11, Section 11.200 / Electronic Signature Components and Controls

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
Electronic signatures that are not based on biometrics shall:				
11.200 (a)	Employ at least two distinct identification components such as an identification code and password.	Y	NA	T10
	When an individual executes a series of signings during a single continuous period of controlled system access, the first signing must be executed using all electronic signature components. Subsequent signings must be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	Y	NA	T10
	When an individual executes one or more signings not performed during a single continuous period of controlled access, each signing must be executed using all of the electronic signature components.	Y	NA	T10
	Be used only by their genuine owners.	Y	Requires company policy	NA
	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.	Y	NA	T5
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owner.	NA	The software does not use biometrics for electronic signatures.	NA

21 CFR Part 11, Section 11.300 / Controls for identification codes/passwords

Part 11 Req't #	Requirements	Conforms (Y/N/NA)	Remarks (required if Assessment is NA)	Met by
Persons who use electronic signatures based on identification codes in combination with passwords shall employ controls to ensure their security and integrity, including:				
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	NA	T4
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	NA	T5
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.	NA	Tokens/cards/other devices are not compatible with CSS	NA
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	NA	T3
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.	NA	Tokens/cards/other devices are not compatible with CSS	NA

21 CFR PART 11 USER CASE SCENARIOS

Izon's Control Suite Software will include three different user access levels as described below:

User

The access level for a "User" is described below:

- User logs into the system using a unique User ID and password
- Users can sign data records
- User operates system with the following exceptions:
  - If the system is inactive (no mouse or key board actions) for longer than the system timeout then the user needs to log back in
  - Users actions are recorded in a system Audit Trail and a Data Record Audit Trail – this is transparent to the User in operation
  - User cannot edit nor change a signed and sealed data record
- Occasionally Users will need to change their password in accordance with the system administrator's management plan
- Users will need to keep and secure their password in accordance with the organisation's management policy

Manager

As per User except able to manage the Data repository and perform following functions:

- Exporting and archiving/deleting data records from system as required
- Performing backups of the data repository and system Audit Trail
- Running and checking audit reports

Admin

As per Manager except for performing the following system administration tasks as specified in the system management plan:

- Adding, deleting and editing User
- Implementing and maintaining system management plan
- Unable to sign data records or delete data signatures

3 / TESTING OVERVIEW

ACCEPTANCE CRITERIA

The system must conform to the requirements detailed in 21 CFR Part 11 regulations.

TEST PROCEDURE

Before beginning the CFR verification protocols, the CSS must be successfully installed on an appropriate computer; a base Instrument must also be installed and the functionality verified.

Test files 1 and 2 from Sections 5 and 6 of QN1-OQ-002 will be required to complete certain tests in this test procedure.

For each CFR verification protocol, complete the procedure as described. Examine the records generated (along with any comments) during the execution of the protocol. Compare the test results/comments to the acceptance criteria to determine whether the 21 CFR Part 11 requirements have been fully satisfied. For each verification protocol, complete the accompanying sign off box.

VERIFICATION DETAILS

Test Date (DD/MM/YY)		
Verification Test Executor	Name	
	Position	
	Signature	
Verification Test Reviewer	Name	
	Position	
	Signature	
CSS Version Number		
Base Instrument Serial Number		

Computer Description	
Computer ID	
Location	
Serial Number	
Operating System	

4 / VERIFICATION PROTOCOLS

TEST 1

21 CFR Part 11 Requirement:

11.10 (h) System can only use an Izon TRPS instrument as a data input device

Solution:

The CSS will only recognise and accept data input from an Izon TRPS Instrument

Testing Protocol:

1. Connect a TRPS instrument to AC power using the power cable. Use the USB cable to plug a TRPS instrument into the computer. Confirm that the CSS correctly recognises and registers an IZON TRPS device, shown by the classic capture tab becoming active, and the power plug icon (bottom left on welcome screen) becoming connected.
2. Plug other USB devices into the computer (i.e. mp3 player, DVD player, etc.). Confirm that other USB devices are not recognized registered by the CSS.

Acceptance Criteria (Mark the Check Box if passed):

1. TRPS instrument is recognized by the CSS. ☐
2. Other USB devices are not recognized by the CSS. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 2

21 CFR Part 11 Requirement:

11.10 (d, g) A unique User ID and Password must be used to access the system. System requires user login for access

Solution:

In order to log into the CSS, users must use both a unique user ID and a password. For this system to be effective there must be internal user/password protocols established in order to ensure users do not share log-in information.

Testing Protocol:

1. Attempt to use the system without logging in, confirm that this is not possible.
2. Attempt to login using an invalid User ID and/or Password combination, confirm that access is denied.
3. Attempt to login using a valid User ID and Password, confirm that access is granted. Logout.

Acceptance Criteria (Mark the Check Box if passed):

1. It is not possible to use the system. ☐
2. System access is denied. ☐
3. System access is granted. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 3

21 CFR Part 11 Requirement:

11.300 (d) Persons who use electronic signatures based on identification codes in combinations with passwords shall employ controls to ensure their security and integrity including 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 organisational management.

Solution:

The CSS shuts the system down after 4 failed login attempts and records this security lockout in the Audit Trail along with each failed login attempt. Reporting to Organizational Management is dependent upon the Audit Trail reporting processes employed by the organization.

Testing Protocol:

1. Try to log-in to the system by typing an incorrect Password 4 times in a row. Confirm that the CSS shuts the system down after 4 failed login attempts.
2. Correctly log in and access the audit trail to confirm failed attempts have been logged

Acceptance Criteria (Mark the Check Box if passed):

1. The system shuts down. ☐
2. Failed attempts correctly recorded in audit trail. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 4

21 CFR Part 11 Requirement:

11.300 (a) Persons who use electronic signatures based on identification codes in combinations with passwords shall employ controls to ensure their security and integrity including maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

Solution:

The CSS does not allow User IDs to be re-used. This means that any given combination of User ID and Password is unique to the original assigned User.

Testing Protocol:

1. Login as Admin and create a dummy User and record the User ID.
2. Attempt to create a new dummy User with the same User ID; confirm that the system prohibits this.
3. Delete the dummy User created in Step 1 and then try to create a new dummy User with the original User ID; confirm that the system prohibits this

Acceptance Criteria (Mark the Check Box if passed):

1. Login proceeds without error. ☐
2. Cannot create a second User with same User ID. ☐
3. Cannot create a second User with same User ID. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 5

21 CFR Part 11 Requirement:

11.200 (a3) Electronic signatures that are not based on biometrics shall 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.

11.300 (b) Persons who use electronic signatures based on identification codes in combinations with passwords shall employ controls to ensure their security and integrity including ensuring the Identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Solution:

The CSS requires that Users log in using a unique User ID and a private Password. In order for anyone other than the genuine owner to use a signature it requires that the other party either acquires or is given the owners Password and User ID. If the owner gives another party their User ID and Password this would presumably be in breach of the organization's security protocols and would constitute the collaboration of two or more individuals. To avoid the acquisition of a User's Password from the system, User Passwords are inaccessible to any other User including the Administrator once the Password has been set by the User.

In the case that the Administrator has to reset a User Password (for example in the case of a genuine loss of Password), then the User will be required to change the Password on first logon.

Every 90 days the system requires Users to revise their Password. When the administrator sets a new user password the user password is automatically aged, and the user is required to change the password on next login.

Testing Protocol:

1. Log in as Administrator, create a new User and confirm that it is impossible to recover the Password that has been set for a User.
2. Reset the User Password and confirm that the system requires the User to reset their Password as soon as they first login after the Administrator Password reset.

Acceptance Criteria (Mark the Check Box if passed):

1. Cannot recover a Password set by a User. ☐
2. User must reset their Password at first login. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 6

21 CFR Part 11 Requirement:

11.10 (d) The system has an automatic lockout after a specified period of inactivity.

Solution:

The CSS has an automatic lockout after a period of inactivity that can be set by the system administrator. It is important that the organization has a documented policy on how long a lockout period should be applied, and effectively manages this aspect of the system.

Testing Protocol:

1. Login to the CSS and then leave the system idle for the specified lockout period (the default time is 5 minutes). Confirm that the User is locked out of the CSS after the specified system idle time.
2. Verify that the system returns to an active state when the User correctly logs back in.

Acceptance Criteria (Mark the Check Box if passed):

1. The User is locked out of the software after specified time. ☐
2. System becomes active. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 7

21 CFR Part 11 Requirement:

11.10 (c) A unique Record ID must be unique and cannot be duplicated.

Solution:

All Izon Data Records are labelled with a GUID (Globally Unique Identifier). This will guarantee that all records generated on a single system will have unique IDs. The GUID, in conjunction with device ID tagging, virtually guarantees that all Izon Data Records will be globally unique. The User cannot set nor edit Record IDs in any manner.

Testing Protocol:

1. Capture a series (e.g.: 3 files) of successive Data Records. Process the files and note the Record IDs (Record IDs can be viewed by expanding the width of the Data Files window). Confirm that they are unique, non-sequential GUIDs.
2. Confirm that the Record IDs cannot be edited.
3. Save these files in a group called Test File 3 (for later use).

Acceptance Criteria (Mark the Check Box if passed):

1. The Record IDs are unique, non-sequential GUIDs. ☐
2. The Record IDs cannot be edited. ☐
3. Saving proceeds without error. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 8

21 CFR Part 11 Requirement:

11.10 (c) Records may not be over-written.

Solution:

Izon's software automatically generates filenames using the Sample ID name. Izon Data Records cannot be saved over-top of existing files. Where filenames are automatically generated, the system ensures that the filename does not exist on the system. Where User- selected filenames are used, the system locks out attempts to save over the top of existing files.

Testing Protocol:

1. Collect and save a data file.
2. Record the Sample ID.
3. Collect a second data file and save with identical Sample ID details.
4. Process both files and confirm that the second data-file has had a number post fixed to the filename and that both files still exist. The filename is viewed by expanding the width of the Data Files window.
5. Create a new group using files collected in Step 1 and attempt to save to an existing filename (e.g.: Test File 3). Confirm that the system raises an error and will not allow this.

Acceptance Criteria (Mark the Check Box if passed):

1. Proceeds without error. ☐
2. Proceeds without error. ☐
3. Proceeds without error. ☐
4. The second data file has had a number post-fixed to the filename and both files still exist. ☐
5. Confirm that the system raises an error and does not allow saving to an existing filename. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 9

21 CFR Part 11 Requirement:

11.10(a) System needs to provide an automated means to ensure the ability to discern invalid or altered records.

Solution:

E-records are saved in a propriety format that cannot be edited with other applications. Any attempt to edit the E-record outside of the application will result in an invalid Data Record that will not be opened by the application. In the case that the data format is hacked the record is stamped with a SHA512 hash that is also logged to the Audit Trail any change to the Data Record will invalidate this hash.

Testing Protocol:

1. Edit a test file:
   - Record a 5 second data file "Test File T9". Ignore the 30 second warning message.
   - Process the file and save this into a Group.
   - Export the file and then close the Data Record (requires Manager or Admin).
   - Open Test File T9 in a 3rd party application i.e. opens in Notepad.
   - Edit a simple part of the data (e.g. change a 1 to a 2) and save the file.
   - Attempt to open the modified Data Record in the CSS.
   - Confirm that the Record is identified as corrupted and does not open.
2. Revert edits:
   - Open the edited Record in Notepad (or similar) and revert the edit in Step 1(e). Save the file.
   - Try to open in the CSS. Confirm that the Record is identified as corrupted.

Acceptance Criteria (Mark the Check Box if passed):

1. The Record is identified as corrupted. ☐
2. The Record is identified as corrupted. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 10

21 CFR Part 11 Requirement:

11.50 (b) E-signatures can only be executed by authorized users.

11.200 (a) Electronic signatures that are not based on biometrics employ at least two distinct identification components such as an identification code and password. When an individual executes a series of signings during a single continuous period of controlled system access, the first signing must be executed using all electronic signature components. Subsequent signings must be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. When an individual executes one or more signings not performed during a single continuous period of controlled access, each signing must be executed using all of the electronic signature components.

Solution:

Data Records can only be electronically signed from within the CSS thus can only be sanctioned by Users authorised to use the system. The CSS requires that both User ID and Password are provided at every signing. All Users/Managers are able to sign Data Records, but only Managers can delete signatures.

Testing Protocol:

1. Outside of the CSS, attempt to access Test File 2 and sign it. Confirm that Data Records cannot be signed outside of the CSS.
2. Log in at the User account level, open Test File 2. Perform multiple signings on Test File 2. Confirm that both User ID and Password are required at each signing. Confirm that the signatures cannot be deleted.
3. Log in at the Manager account level. Perform multiple signings on Test File 2. Confirm that both User ID and Password are required at each signing. Confirm that the signatures can be deleted.

Acceptance Criteria (Mark the Check Box if passed):

1. Data Records cannot be signed. ☐
2. User ID and Password required for e-signature. Signatures cannot be deleted. ☐
3. User ID and Password required for e-signature. Signatures can be deleted. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 11

21 CFR Part 11 Requirement:

11.50 (a) Signed electronic records shall contain the printed name of the signer. Signed electronic records shall contain the date and time when the signature was executed. Signed electronic records shall contain the meaning (such as review, approval, responsibility, or authorship) associated with the signature).

11.50 (b) E-signatures are included as part of any human readable form of the electronic record.

Solution:

The CSS produces a data archive of the relevant data sets and results for any given analysis. The Record details can be directly reported from the Izon Data Suite via standard Reports. As the raw data associated with an analysis on Izon's systems is very large (potentially many GB in size) these Reports do not contain the actual raw data but provides all of the data collection and analysis details.

Where a hard copy of raw data is explicitly required the raw Data Record can be output to an external CSV format and may be output in hard copy from that format. However, a typical analysis would require in the order of 500 thousand to 1.5 million A4 pages to output a hardcopy of the raw data.

Testing Protocol:

1. Sign Test File 2. Note signature details.
2. Open a report, view the signature and confirm that this correctly includes the full printed name of the signer, date and time for each signature and a purpose field that describes the meaning of the signature.

Acceptance Criteria (Mark the Check Box if passed):

1. Proceeds without error. ☐
2. Report correctly includes:
   - Full printed name of each signer. ☐
   - Date and Time each signature was executed. ☐
   - A type field describing the meaning of the signature. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 12

21 CFR Part 11 Requirement:

11.10 (b) System needs to be able to produce a hard copy (paper) of individual and/or the entire relevant e-record(s) for inspection.

Solution:

Electronic Signatures associated with Izon Data Records include the full printed name of the signer; date and time are which the signature was executed and a mandatory purpose field that describes the meaning of the executed signature. E-Signatures (where present) are included as part of the printed Data Record Report.

Testing Protocol:

1. Print a Record Report for Test File 2.
2. Check that the printed Report matches the data shown onscreen.

Acceptance Criteria (Mark the Check Box if passed):

1. Proceeds without error. ☐
2. The printed Record Report matches the data shown onscreen. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 13

21 CFR Part 11 Requirement:

11.10 (b) E-records needs to be produced in an electronic format (e.g., portable document format, CD, electronic transportable format, Excel spreadsheet, .txt file).

Solution:

Record Reports (see T12) can be output in PDF. Izon's analysis results are stored in individual data archives that can be copied and viewed on different systems.

Testing Protocol:

1. Save a Report for Test File 2 in PDF format (on the 1st computer) and open in a PDF viewer. Confirm that the PDF report matches the original Record Report.
2. Export a copy of Test File 2 and open the copy on a 2nd computer with the CFR21 Part 11 CSS installed (Export requires Manager or Admin privileges).
3. Confirm that exported details in the DATA VIEW are identical on both computers.

Acceptance Criteria (Mark the Check Box if passed):

1. The PDF report matches the original Record Report. ☐
2. Proceeds without error. ☐
3. Data records identical on both computers. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 14

21 CFR Part 11 Requirement:

21 CFR Part 11 Requirement: 11.10 (g) System provides three levels of security to ensure that only suitably authorized users can perform system tasks.

Solution:

The CSS provides three levels of Authorization and access control.

1. Administrator: There is only a single Administrator account and this account is the only account that can access and change security settings on the system (such as idle lockout times) and change User account details (add/remove Users, change Passwords etc.). Additionally, the Administrator account has access to all of the functionality available to Managers, with the exception of signing data files and deleting data signatures.
2. Manager: Manager accounts can access the Audit Trail in order to perform tasks such as Audit Trail backup and reporting. Additionally, the Manager accounts can export and archive/delete Data Records from the system and can remove signatures from signed Data Records. Additionally, the Manager account has access to all of the functionality available to Users.
3. User: User accounts are the standard operator accounts and have access to all data capture, data editing, data reporting functionality, plus are able to sign Data Records. Users do not have access to any security settings, the Audit Trail, nor can they remove signatures from signed Data Records or export/ archive/ delete Data Records from the system.

Table 1. Summary of all content and settings available to the three different user levels in the CSS.

	User	Manager	Administrator
Data record signing	✓	✓	✗
Security settings	✗	✗	✓
Audit trail	✗	✓	✓
Signature removal	✗	✓	✗
Export, archive/delete	✗	✓	✓
Manage users	✗	✗	✓

Testing Protocol:

1. Log in as a User and, using Test File 2, confirm access to data record signing.
2. Log in as a Manager and confirm access to all functionality available to users, audit trail, signature removal, export and archive/deletion of data records.
3. Log in as an Administrator and confirm access to all of the functionality available to Managers, with the exception of signing data files and deleting data signatures. Can also access security settings and manage users.

Acceptance Criteria (Mark the Check Box if passed):

1. As User: Only able to access data record signing. ☐
2. As Manager: Access granted to all applicable criteria in Table 1, access denied to all others. ☐
3. As Administrator: Access granted to all applicable criteria in Table 1, access denied to all others. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 15

21 CFR Part 11 Requirement:

11.10 (e) Secure time stamped Audit Trail that records Date, Time (local), User ID, Action, State Change, Related Data Record (where relevant) is automatically generated.

Solution:

The CSS automatically generates an Audit Trail that records: Date/Time, User ID, Action, State Change (where relevant), Data Record ID (where relevant).

Testing Protocol:

1. Open the Audit Trail Viewer (Manager or Administrator login required).
2. Confirm that the Audit Trail events record:
   - Date/Time
   - User ID
   - Action (Type column)
   - State Change (Description column)
   - Data Record ID (Data stamp column, where applicable)

Acceptance Criteria (Mark the Check Box if passed):

1. Proceeds without error. ☐
2. The Audit Trail events record:
   - Date/Time ☐
   - User ID ☐
   - Action ☐
   - State Change ☐
   - Data Record ID ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 16

21 CFR Part 11 Requirement:

11.10 (e) Audit Trail records login, lockout, logout and security violation events.

Solution:

All login, lockout, logout and security violation events are recorded along with all events that change security settings and all events that view and/or report the Audit Trail.

Testing Protocol:

#	Test	User ID used	Time	Access (D/G)
1	Attempt to log into the system using false credentials, note the time and attempted User ID. Confirm that access is denied.			
2	Log into the system using valid credentials; note the time and User ID. Confirm that access is granted.			
3	Manually lock the system, note the time and User ID. Confirm that the system is locked			
4	Attempt to log into the system using false credentials, note the time and attempted User ID. Confirm that access is denied.			
5	Unlock the system using valid credentials; note the time and User ID. Confirm that the system is unlocked.			
6	Leave the system idle until the idle lockout time has passed, and the system is locked. Confirm the system is locked. Note the User ID and time of lock out.			
7	Unlock the system the system using valid credentials; note the time and User ID. Confirm that the system is unlocked.			
8	Logout of the system, note the time and User ID.			
9	Log into the system using valid credentials for either the System Administration or a Manager level account; note the time and User ID. Confirm that access is granted.			
10	Open the Audit Trail viewer. Confirm that the Events associated with Steps 1-9 are correctly recorded in the Audit Trail.	N/A	N/A	N/A

Acceptance Criteria (Mark the Check Box if passed):

1. Access is denied ☐
2. Access is granted ☐
3. The system is locked ☐
4. Access is denied ☐
5. The system is unlocked ☐
6. The system is locked ☐
7. The system is unlocked ☐
8. System is logged out of ☐
9. Access is granted ☐
10. Events associated with Steps 1-10 are recorded in the Audit Trail ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 17

21 CFR Part 11 Requirement:

11.10 (e) Audit Trail records data record creation, modification, export and deletion.

Solution:

All data creation, modification, export and deletion events are automatically added to the Audit Trail by the system. In this system deletion is accomplished by archiving the data file.

Testing Protocol:

#	Test	User ID used	Time
1	Close all data files		
2	Capture two new records		
3	Process data records		
4	Close all data files		
5	Re-open the two data records from Step 2 and edit one of the data records		
6	Save the edited Data set		
7	Save the two files as a new group		
8	Export the group		
9	Archive the group		
10	View the audit trail. Confirm that the events related to Steps 2, 3 and 5-9 are correctly recorded in the audit trail.	N/A	N/A

Acceptance Criteria (Mark the Check Box if passed):

1. Steps 2, 3 are correctly recorded in the audit trail. ☐
2. 5-9 are correctly recorded in the audit trail. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 18

21 CFR Part 11 Requirement:

11.50 (b) E-signatures are included in the system Audit Trail.

Solution:

All signature events (Sign, Delete, and View) are recorded in the Audit Trail.

Testing Protocol:

#	Test	User ID used	Time
1	Open Test File 2		
2	Sign the Data File		
3	View the signature by opening the Data Signature window		
4	Delete the Signature.		
5	View the Audit Trail. Confirm that the events related to Steps 1-4 are correctly recorded in the Audit Trail.	N/A	N/A

Acceptance Criteria (Mark the Check Box if passed):

1. The events related to Steps 1-4 are correctly recorded in the Audit Trail. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 19

21 CFR Part 11 Requirement:

11.10 (e) Entries cannot be deleted from the Audit Trail.

Solution:

The Audit Trail entries are not User-editable.

Testing Protocol:

1. User login - Confirm that the audit trail cannot be accessed.
2. Manager login - Attempt to edit, delete, and disable an entry in the Audit Trail. Confirm that this is not possible.
3. Administrator login - Attempt to edit, delete, and disable an entry in the Audit Trail. Confirm that this is not possible.

Acceptance Criteria (Mark the Check Box if passed):

1. Audit Trail is not accessible (User). ☐
2. Audit Trail is not editable, delete-able, and cannot be disabled (Manager). ☐
3. Audit Trail is not editable, delete-able, and cannot be disabled (Administrator). ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

TEST 20

21 CFR Part 11 Requirement:

11.10 (e) Audit Trail can be exported, backed up, and printed.

Solution:

The Audit Trail can be exported, backed up and printed from the CSS. This facility is accessible to Manager and Administrator accounts only.

Testing Protocol:

1. Export the Audit Trail viewer. Confirm that this is correctly exported.
   - Click the export button in the audit trail viewer and save the audit trail to the desktop.
   - Open the exported audit trail in Excel (if available) or notepad.
2. Confirm that the exported file contains the same details as visible in CSS audit trail viewer.
3. Perform a manual backup. Confirm that this correctly produces a backup.
   - Click on backup audit trail and save to desktop
   - Confirm that the backup has been saved to desktop.
4. Print a copy of the Audit Trail. Confirm that this prints a correct copy of the Audit Trail.
   - Open the audit trail viewer.
   - Click on the Report button.
   - Save a copy of the audit trail.
   - Print a copy of the audit trail from the report viewer.
   - Check that the details on the printed copy match those on the displayed record.

Acceptance Criteria (Mark the Check Box if passed):

1. Audit Trail is exported. ☐
2. Exported file contains same details as visible in CSS audit trail. ☐
3. Audit Trail back-up is created. ☐
4. Printed copy matches the displayed records. ☐

Result satisfies AC? (Y/N)		Executor Initial:	Date:
		Reviewer Initial:	Date:

5 / VERIFICATION SIGN OFF

Fill in the following sign-off box and complete the box in Section 8 of QN1-OQ-002.

Task	Name	Signature	Initial	Date	Pass / Fail
Executed					
Reviewed					