Compass for iCE (V2.0) Title 21 Code of Federal Regulations (CFR) Part 11 Compliance Checklist

This document supports the use of Maurice® systems (Maurice, Maurice S., and Maurice C.) in a QC and GMP environment. All functionality is integrated in Compass for iCE software (V2.0) for compliance with 21 CFR Part 11. The information presented assumes that the appropriate system configuration parameters have been set.

Compass for iCE is a closed system where access is controlled by the person(s) responsible for electronic records content. Compass for iCE uses an ID/password combination and doesn't use any tokens or biometrics.

Part 11, Subpart B — Electronic records

If you use Compass for iCE to create, modify, maintain, or transmit electronic records, you'll need procedures and controls to ensure authenticity, integrity, and, when appropriate, the confidentiality of the electronic record. Procedures and controls should also ensure that signers can't easily deny the validity of signed records. The following is a breakdown of these procedures and controls.[1,2]

Section 11.10 — Controls for closed systems

SECTION 11.10(a)				
REGULATION	**YES**	**NO**	**N/A**	**IMPLEMENTATION AND APPLICATION**
Is Compass for iCE software validated?	✓			Compass for iCE software is validated and comes with a certificate of validation with software installation.
Does the validation documentation confirm Part 11 requirements have been met and are functioning correctly?	✓			Compass for iCE software lets you be compliant with 21 CFR Part 11 guidelines, but complete compliance can only occur within a validated electronic records environment. Applicable methods and corresponding records are available for review at our San Jose, California USA facility upon formal request by authorized governmental/regulatory agencies.
Are invalid records detected where applicable, like when there are invalid field entries, fields left blank that should contain data, or values outside of limits?	✓			Software utilities are in place to detect input errors/invalid data types, range checking for numeric entries, and marking of mandatory fields.

SECTION 11.10(b)				
REGULATION	**YES**	**NO**	**N/A**	**IMPLEMENTATION AND APPLICATION**
Can I view the entire contents of the records?	✓			
Can I print the entire contents of the records?	✓			
Can I generate all the records electronically in a format that can be put on a portable medium (e.g., diskette or CD) or transferred electronically?	✓			Batch and injection data, instrument and cartridge data can be viewed/printed as an electronic report in PDF format.

SECTION 11.10(c)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Are my records protected against intentional or accidental modification or deletion?	✓			The ability to modify data is a specifically assigned privilege. When you create or modify data, the action is logged to the audit trail and requires user confirmation before changes are saved. File management and keeping users from deleting data files is a customer responsibility.
Can my data be archived from the system? If so, is the meta data (including the audit trail) archived as well? Can all the archived data be accurately retrieved after system upgrades?	✓			Data is file-based, each organization is responsible for archiving data as applicable. Archived Maurice and Authorization Server data files include all information that is part of the electronic record, including audit trail information. Archived data can be retrieved after system upgrades as necessary.

SECTION 11.10(d)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Are there different levels of access based on user responsibilities (e.g., user, administrator)? Is this documented and controlled?	✓			
Are user access levels approved by management or the system owner before assignment to a user?	✓			
Is there is a controlled, documented process for granting access to a new user, for changing privileges for an existing user and for deleting user accounts?	✓			
Are there physical security and procedures to protect the server, database and system components from unauthorized access?			✓	

SECTION 11.10(e)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Can I automatically generate an electronic audit trail function all operator entries?	✓			When Access Control is enabled, all activities for all users in projects with full audit trail turned on will be audit trailed, with no user types or activities treated differently.
Is the audit trail completely outside the control and access of users (except for read-only access of the audit trail file)?	✓			
Is it impossible to disable the audit trail function?	✓			When Access Control is enabled, the audit trail can't be disabled.
Is Compass for iCE's date and time protected from unauthorized change?			✓	Date and time are taken from the local date and time for the Authorization server. The ability to change the system date and time is controlled through the computer operating system.
When my data is changed, are all previous values still electronically available?	✓			
Is the audit trail data protected from accidental or intentional modification or deletion?	✓			The audit trail can't be modified or deleted.
Are electronic audit trails maintained and retrievable for at least as long as its respective electronic records?	✓			Audit trails can be maintained and retrieved as part of a regular backup procedure. Each organization is responsible for Maurice and Authorization Server data file backup as applicable.

SECTION 11.10(e), *continued*

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Are electronic audit trails readily available for inspections and audits?	✓			Audit trail entries are available for inspection by authorized users via the Compass Authorization Server.
Can I select portions of the audit trail for inspectors to view and print?	✓			The audit trail is available for review by authorized users and can be printed via the Compass Authorization Server.
Can I select portions of the audit trail to extract in a transportable electronic format for regulatory agencies?	✓			The audit trail can be downloaded as a PDF file by authorized users via the Compass Authorization Server.
If no audit trail is available, can Compass for iCE detect that a record was altered since its last approval?	✓			Compass for iCE software uses the SHA1 hash algorithm to generate a 160 bit hash code that is unique for all files. All files saved are encrypted with a digital key. This key along with the hash codes guarantees the file history is correct and no other edits were made.
Is the operator name, date, time, and indication of record (or file) creation, modification or deletion recorded in audit trail?	✓			
If the predicate regulation requires it, is the reason for a change included in the audit trail?	✓			When signing files, the user is prompted to enter the meaning of the signature, which will be logged to the Audit trail.

SECTION 11.10(f)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
If Maurice requires sequenced steps, does it ensure that the actions are performed in the correct sequence?	✓			

SECTION 11.10(g)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Does Compass for iCE only let authorized individuals use Maurice?	✓			When Access Control is enabled, you must have a user account. This account will define the capabilities you'll have on Maurice. You won't have any access without an account.
Does Compass for iCE verify that an individual has the authority to electronically sign a record before allowing them to do so?	✓			The ability to sign-off is a specifically assigned privilege. If you haven't been assigned this privilege, you can't electronically sign a record.

SECTION 11.10(h)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Does Compass for iCE require that data input or instructions only come from specific instrument/ terminal? Does Compass for iCE check for this?	✓			Users connect to Maurice from the Compass for iCE software to submit operational instructions (batch).

SECTION 11.10(i)				
REGULATION	**YES**	**NO**	**N/A**	**IMPLEMENTATION AND APPLICATION**
Is there documentation to show that everyone who *develops* Compass for iCE has the education, training and experience to perform their assigned tasks?	✓			Full documentation is available as part of an audit of ProteinSimple quality and training processes.
Is there documentation to show that everyone who *maintains* or *uses* Compass for iCE has the education, training and experience to perform their assigned tasks?	✓			Each organization must develop their own controlled, documented procedures for compliance with this requirement.
Is there documentation to show that everyone who *uses* the system has the education, training and experience to perform their assigned tasks?	✓			Each organization must develop their own controlled, documented procedures for compliance with this requirement.

SECTION 11.10(j)				
REGULATION	**YES**	**NO**	**N/A**	**IMPLEMENTATION AND APPLICATION**
Is there a written policy in place and enforced that holds users fully accountable and responsible for actions initiated under their electronic signatures?			✓	Each organization must their own develop controlled, documented procedures for compliance with this requirement.

SECTION 11.10(k)(1)				
REGULATION	**YES**	**NO**	**N/A**	**IMPLEMENTATION AND APPLICATION**
Is the distribution of, access to, and use of Compass for iCE operation and maintenance documentation controlled?			✓	Each organization must develop their own controlled, documented procedures for compliance with this requirement.
Is access to "sensitive" Compass for iCE documentation restricted e.g., network security documentation, system access documentation?			✓	Each organization must develop their own controlled, documented procedures for compliance with this requirement.

SECTION 11.10(k)(2)				
REGULATION	**YES**	**NO**	**N/A**	**IMPLEMENTATION AND APPLICATION**
Is there a written policy in place and enforced that holds users fully accountable and responsible for actions initiated under their electronic signatures?			✓	Each organization must their own develop controlled, documented procedures for compliance with this requirement.

Section 11.30 — Controls for open systems

SECTION 11.30				
REGULATION	**YES**	**NO**	**N/A**	**IMPLEMENTATION AND APPLICATION**
Are there controls to ensure record authenticity, integrity, and confidentiality?			✓	Compass for iCE and Compass Authorization Server software is a closed system.
Is data encrypted?			✓	Compass for iCE and Compass Authorization Server software is a closed system.
Are digital signatures used?			✓	Compass for iCE and Compass Authorization Server software is a closed system.

Section 11.50 — Signature manifestations

SECTION 11.50(a)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Do all electronically signed records contain the full printed name of the signer?		✓		Electronically signed records show the user ID of the user that signed the record, not the full printed name of the signer.
Do all electronically signed records contain the date and time of signing?	✓			
Do all electronically signed records contain the meaning of the signature (e.g., review, approval)?		✓		You can provide the meaning of the electronically signed records in the 'Comments' field. This is a mandatory entry field you'll have to fill yourself.
Are the date and time stamps applied automatically and not keyed in by the user?	✓			
Are the date and time stamps presented in a consistent way that makes it simple to reconstruct the sequence of events?	✓			Date and time stamps are the local date and time at the location where the signature was executed.

SECTION 11.50(b)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Is the above information subject to the same controls as electronic records? (audit trail, access control, etc.)	✓			
Are changes to signatures included in the audit trail?	✓			Signatures may not be altered; new signatures may be added to a record and are fully audit-trailed.
Do the printed name, date, time, and signature meaning appear in printed reports of the electronic record?	✓			The electronic signature for a file will be persisted with the record and can be viewed in the file History.

Section 11.70 — Signature/record linking

SECTION 11.70				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
If handwritten signatures are executed to electronic records, are the handwritten signatures linked to the electronic records?			✓	Handwritten signatures are not executed to electronic records. Handwritten signatures may be executed to a printed report, and such a report may include information identifying (and providing a link to) the original electronic record.
If the electronic record is changed, is the signer prompted to re-sign (via either manual procedures (SOP) or technical means)?	✓			All changes to an electronic record are audit trailed.The audit trail includes information on the user making the change, the date and time of the change, what was changed and the reason for the change. If electronic record information is modified, the electronic record can be re-signed in the Compass for iCE software. Each organization must develop their own controlled, documented procedure to determine when a re-signing is required.
Are the E-signatures linked (via technology, not procedures) to their corresponding electronic records to ensure that the signature can't be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?	✓			

Part 11, subpart C— Electronic signatures

Section 11.100 — General requirements

SECTION 11.100(a)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Is each E-signature unique to one individual?	✓			
Are E-signatures ever reused by, or reassigned to, anyone other than the original owner?		✓		E-signature is based on User ID and Password. User IDs can be deleted and re-used on the Authorization Server by an Administrator.

SECTION 11.100(b)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Is the individual identified adequately verified prior to issuance of an electronic signature?			✓	Each organization must develop their own controlled, documented procedures for compliance with this requirement.
Is there a procedure for reissuing forgotten passwords that verifies the requestor's identity?			✓	Each organization must develop their own controlled, documented procedures for compliance with this requirement.

SECTION 11.100(c)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Has certification of the intent to use electronic signatures been submitted to the agency in paper form with a traditional handwritten signature?			✓	Each organization must submit their written intent for compliance with this requirement.
Can additional certification or testimony be supplied to show that an electronic signature is the legally binding equivalent of the signer's handwritten signature?			✓	Each organization must develop their own controlled, documented procedures for compliance with this requirement.

Section 11.200 — Electronic signature components and controls

SECTION 11.200(a)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Does the signature consist of at least two distinct identification components?	✓			A signature comprises a user name and a password.
If continuous signing sessions are used, are two (or more) E-signature components required for the initial signing?	✓			The user name and password are required for the initial signing.

SECTION 11.200(a), *continued*

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
If only one E-signature component is required for subsequent signings:				
• Is the private component, known to and only useable by its owner, used for each subsequent signing?	✓			The account password is the private component.
• Is the user required to stay in close proximity to the workstation for the entire session?			✓	You can launch the Compass for iCE lock screen at any time and re-enter the password to unlock the screen.
• Is there an automatic logoff, or password-protected screen saver that launches after a short period of inactivity (with the password known only by one user)?	✓			If there is no activity in Compass for iCE for 20 minutes, the software automatically locks. You must re-enter their passwords to perform any controlled actions.
If I leave the workstation, do procedures and/or automatic controls ensure that it's treated as a non-continuous session?	✓			You must re-enter passwords to have access to the software after leaving the workstation for a short period of time (due to inactivity), or after manually activating the password-protected lock screen.
Are two (or more) E-signature components required for each signing during a non- continuous signing session?	✓			The user name and password are required for each signature during a non-contiguous signing session.
Are non-biometric signatures only used by their genuine owners (e.g., by procedures or training reinforcing that non-biometric E-signatures are not "loaned" to co-workers or supervisors for overrides)?			✓	Each organization must develop their own controlled, documented procedures for compliance with this requirement.
Are non-biometric signatures administered and executed so that unauthorized use requires the collaboration of two or more individuals?			✓	Each organization must develop their own controlled, documented procedures for compliance with this requirement. Individual users can't view any information on other user accounts unless they are explicitly given the "Alter User" privilege. Under no circumstances is access to another user's password available to any user.

SECTION 11.200(b)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Are biometric E-signatures designed to ensure that they can be used only by their genuine owners?			✓	Compass for iCE software doesn't use biometric E-signatures.

Section 11.300 — Controls for identification codes/passwords

SECTION 11.300(a)

REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals can have the same combination of identification code and password?	✓			The Compass Authorization Server ensures that there must be unique combination of user names and passwords used on the system.
Are controls (procedural or technical) in place to prevent the re-use of identification codes?	✓			The Compass Authorization Server policies can be used to ensure that passwords may not be reused for individual user accounts, and that user names can't be reused for multiple users.

SECTION 11.300(b)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Is the issuance of identification codes and passwords periodically checked, recalled, or revised (e.g., to cover such events as password aging)?	✓			The Compass Authorization Server policies can be used to set password aging based on corporate policies. Additionally, when LDAP is enabled, this allows you to connect the Compass Authorization Server to your own network's domain controller, so users can log on with their existing network password. With LDAP, passwords are not maintained by the Compass Authorization Server, they are administered by the network administrator.
Do passwords periodically expire and need to be revised?	✓			The Compass Authorization Server policies can be used to set password aging based on corporate policies. Additionally, when LDAP is enabled, this allows you to connect the Compass Authorization Server to your own network's domain controller, so users can log on with their existing network password. With LDAP, passwords are not maintained by the Compass Authorization Server, they are administered by the network administrator.
Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	✓			The Compass Authorization Server allows a user account to be removed from active use. Each organization must develop controlled, documented procedures to ensure proper notification of user status changes.

SECTION 11.300(c)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Is an SOP in place directing action to be taken to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices used to carry or generate E-signature components?			✓	Compass for iCE doesn't use tokens, cards or other devices to carry E-signature components.
Does this SOP contain procedures for managing and controlling temporary or permanent token/ card replacements?			✓	Compass for iCE doesn't use tokens, cards or other devices to carry E-signature components.

SECTION 11.300(d)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Are any attempts to unauthorized use detected and reported immediately to the system "security unit" (e.g., a system administrator is notified automatically by console message or paper) and, as appropriate, to organizational management?		✓		The user account will be locked once the number of login attempts exceeds the password policy set in the Compass Authorization Server. Only the Administrator can unlock the account.

SECTION 11.300(e)				
REGULATION	YES	NO	N/A	IMPLEMENTATION AND APPLICATION
Are there procedures covering the initial and periodic testing of devices, such as tokens or cards that bear or generate identification code or password information?			✓	Compass for iCE doesn't use tokens, cards or other devices to carry E-signature components.
Does the testing include checks for proper functioning, performance degradation, and possible unauthorized alteration?			✓	Compass for iCE doesn't use tokens, cards or other devices to carry E-signature components.

Reference

1. FDA Regulation 21 CFR Part 11 — Electronic Records; Electronic Signatures (FDA, 1997)

2. Empower 2 — 21 CFR 11 Compliance Worksheet (Waters Corporation, 2005)

proteinsimple
a bio-techne brand

Toll-free: (888) 607-9692
Tel: (408) 510-5500
info@proteinsimple.com
proteinsimple.com