IQ Consortium Data Integrity Risk Assessment Tool

The tool is intended to assess data integrity risks associated with GxP use of non-enterprise computerized analytical data acquisition and processing software systems deployed in an R&D environment that generate electronic data stored in persistent storage.

Summary	Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
System control and access						
1.1	Is Access to the system via individual login credentials made up of a combination of a unique user id and user generated	☐	☐	☐	Use of generic passwords (when absolutely necessary) should be procedurally controlled.	Click here to enter text.
1.2	Are any non-person system accounts (generic accounts), such as those shipped with the system, or service accounts, disabled?	☐	☐	☐	Accounts should be turned off, disabled, or have access revoked if determined to be unnecessary for system operations. If such accounts should be used to run the application, then procedure should specify that activities performed under such account are traceable to the individual who performed the activities in an automated manner.	Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
1.3	If system is configured to use the Operating System's user credentials to login into software, are user groups defined in the software to ensure only authorized users are able to access the instrument/software?	☐	☐	☐	If there is no ability to prevent access to instrument/software then is access read-only or no ability to make changes/delete? Is user access tracked in audit trail?	Click here to enter text.
1.4	Is there a Procedure that requires maintaining a **list of system users and their access privileges**, as well as retention and continuous availability of historical information regarding system users and administrators, and their access level, according to an applicable retention schedule? Is there a Procedure to ensure records are maintained that demonstrate the current and historical access levels granted to individuals, including approvals?	☐	☐	☐	If historical information is not continuously available then can it be recovered and is there a process to review periodically?	Click here to enter text.
1.5	Is there a Procedure to **grant, record, approve, and deactivate system access** (users and administrators) based on specific individual role, responsibilities, qualification, and verified training? Is there a Procedure to ensure records are maintained that demonstrate the current and historical access levels granted to individuals, including approvals?	☐	☐	☐		Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
1.6	Are there standards for system password strength/complexity and expiry defined and documented?	☐	☐	☐		Click here to enter text.
1.7	Are the User and administrator roles and access levels defined and documented?	☐	☐	☐	Ensure that people have access only to functionality that is appropriate for their job role.	Click here to enter text.
1.8	Does the system lock users out after a defined period of time of user inactivity, via computer screensaver or application?	☐	☐	☐		Click here to enter text.
1.9	Is the system configured to minimize physical and logical access to ports used for remote diagnostic and configuration functions?	☐	☐	☐		Click here to enter text.
1.10	Is the system configured that ports not necessary for business operations which are capable of being disabled have been disabled or otherwise access controlled, based on risk?	☐	☐	☐	Port examples include USB drive, external device, etc. Remote access is acceptable but access should be controlled.	Click here to enter text.
1.11	Does the system lock out users after no more than a defined number of-consecutive unsuccessful login attempts?	☐	☐	☐	Once lockout is triggered, the system should not allow another login for a minimum of "x" minutes (appropriate time), or until an administrator enables the account	Click here to enter text.
1.12	Does the system maintain a history (log) of the changes to individual user accounts (e.g., when user account is created, when rights are modified, when access is removed)?	☐	☐	☐	May be in an administrative audit trail	Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
1.13	If a user locks themselves out of the system, does the system administrator have the ability to reset the user account?	☐	☐	☐		Click here to enter text.
1.14	Does the system obscure passwords during entry?	☐	☐	☐	If the system does not enforce this, a procedure may be put in place to instruct users to obscure display of their passwords.	Click here to enter text.
1.15	Does the system enforce users to change password upon first initial login?	☐	☐	☐	If the system does not enforce this, a procedure should be put in place that users update their password on initial log on. Passwords for accounts that do not grant access to Sensitive, Confidential or production data (i.e. test accounts) are exempt from this requirement.	Click here to enter text.
1.16	Does the system log capture user account activity in a manner that ensures such activity is traceable to a unique user?	☐	☐	☐		Click here to enter text.
1.17	Does the system encrypt or otherwise limit visibility of passwords when stored electronically?	☐	☐	☐		Click here to enter text.
1.18	Do procedures exist to define Administrator responsibilities and activities allowed to be performed by system administrator that do not require a formal change control process?	☐	☐	☐		Click here to enter text.
1.19	Does the system prevent an unauthorized user from generating data?	☐	☐	☐		Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
1.20	**Recommended.** Is the system set up where the lock screen does not reveal clues that could enable an unauthorized user gaining access the system	☐	☐	☐	Where technically feasible, the system should not display information about the system or application until successful login is complete.	Click here to enter text.
Data protection, controls and compliance						
2.1	Is what constitutes the complete primary GMP data record clearly defined for the system (e.g., raw data files, processed data files, audit logs, methods, etc.)?	☐	☐	☐	Provide a statement in the validation documentation.	Click here to enter text.
2.2	Is the source and location of all components of the **complete** primary GMP data record clearly defined for the system?	☐	☐	☐	Validation documentation to include mapping of the data flow (if appropriate) including meta data, audit trail, configuration flow	Click here to enter text.
2.3	When the primary data record consists of electronic data files: Does the system generate accurate and complete copies of the electronic record that preserve the content and meaning in human readable format?	☐	☐	☐		Click here to enter text.
2.4	Are there controls to prevent raw data deletion, modification or overwriting using the instrument/device software?	☐	☐	☐	Implement technical controls (system configuration) where possible. Procedural / process control maybe used to supplement remediation.	Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
2.5	Are all electronic records (raw data, metadata, audit trails) protected from deletion, modification, or being overwritten from outside the software application (e.g., using Windows Explorer) by non-administrators?	☐	☐	☐	Implement technical controls (i.e.; system configuration) where possible. Procedural / process control may be used to supplement remediation	Click here to enter text.
2.6	Does the system record including printouts indicate change(s) to GMP data since its original entry?	☐	☐	☐	Audit trail requirements should include old and new value. Procedural control may be used to supplement audit trail.	Click here to enter text.
2.7	Is each re-integration/re-processing of data tracked, reported by the system and managed via SOP or other means?	☐	☐	☐	Testing into compliance or orphan data is not allowed. There should be procedures / controls governing re-integration / re-processing.	Click here to enter text.
2.8	If manual data processing steps (e.g., manual integration) are permitted, are the actions driven via a procedure outlining justification and requirements?	☐	☐	☐	Testing into compliance is not allowed. There should be procedures / controls governing manual data processing steps (e.g., manual integration).	Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
2.9	Is a documented system in place for the data reviewer to review appropriate electronic and hardcopy data (including metadata, relevant audit trails, etc.) generated by the instrument/system? Includes hybrid equipment (those systems that require both electronic and hardcopy records to be a complete record) also.	☐	☐	☐	The data review procedure should have a requirement to review paper and electronic records, inclusive of applicable audit trails. a) The level of review for intermediate result sets (where reprocessing was needed) should be included and where less than the rigor required for final reported data supported by rationale. b) Where there are both paper and electronic records there should be appropriate linkage and coordination of changes between the paper and electronic records maintained.	Click here to enter text.
2.10	If true copies of original records are retained in place of the original record (e.g., scan of a paper record): Is the record a complete record (i.e., includes all raw data, metadata, relevant audit trails, result files, and all data processing parameters, including methods) and reviewed for completeness?	☐	☐	☐	If the process of generating a true copy is not validated, then there should be a procedure ensuring the true copy is reviewed for completeness. If the original data is dynamic, then a static copy should include all critical data needed to render the static version equivalent to a true dynamic copy based on risk.	
Audit trails, metadata, and data review						

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
3.1	Has the scope of the audit trail been identified and procedures exist for the review of audit trails/meta data before final approval of the record?	☐	☐	☐		Click here to enter text.
3.2	Is there a procedure that defines the elements of data integrity for this particular software control strategy and rigor of review required?	☐	☐	☐		Click here to enter text.
3.3	Is the audit trail function always enabled and can be accessed in human readable format (intelligible form) to support the review of electronic records?	☐	☐	☐		Click here to enter text.
3.4	Does the system prevent audit trails from being edited, disabled or deleted?	☐	☐	☐		Click here to enter text.
3.5	Does the audit trail include: User ID/identity of individual performing activity, Time / Date stamp, old and new value and reason for change?	☐	☐	☐		Click here to enter text.
3.6	Is the audit trail automatically generated at the time of the transaction?	☐	☐	☐		Click here to enter text.
3.7	Are audit trails retrievable and unaltered for the retention period of the record?	☐	☐	☐		Click here to enter text.
3.8	Does the audit trail provide for automatically applied time stamp which are locked and use an unambiguous format?	☐	☐	☐		Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
3.9	Does the data review procedure provide guidance as to what steps to take in the event an error or data integrity issue is detected (i.e. not reporting all data, testing into compliance)?	☐	☐	☐		Click here to enter text.
3.10	Is the data review documented, including audit trail? If so, describe how / where.	☐	☐	☐		Click here to enter text.
Archive, retrieval, back-up, disaster recovery/contingency plans						
4.1	Are complete electronic records backed up?	☐	☐	☐	Backup in a separate location from the original to ensure data is recoverable	Click here to enter text.
4.2	Do backups include Libraries (if applicable)?	☐	☐	☐	Clarification of libraries vs. data management system	Click here to enter text.
4.3	Is the original record including all configuration parameters, audit trails and the like available in the backup so as to preserve its original content and meaning to permit reconstruction of an activity?	☐	☐	☐		Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
4.4	Is completion of back-up verified and is a test performed periodically for restoration?	☐	☐	☐	NOTE: Manual backups should be proceduralized. All back-ups should be verified periodically to ensure continued backup of all associated electronic records	Click here to enter text.
4.5	Do you have a data backup SOP?	☐	☐	☐		Click here to enter text.
4.6	Do data backups or copies (true copies) have the same level of controls to prohibit unauthorized access to changes or deletions of data?	☐	☐	☐		Click here to enter text.
4.7	Is archived data checked periodically for readability?	☐	☐	☐		Click here to enter text.
4.8	Do you have an SOP on data archival?	☐	☐	☐		Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
4.9	Are processes or procedures in place for the disposal of data records that reach the end of their required retention period?	☐	☐	☐		Click here to enter text.
4.10	Are backed up and/or archived data stored in a separate physical location?	☐	☐	☐		Click here to enter text.
4.11	Is there a disaster recovery plan in place where all primary GMP data are secured and recoverable?	☐	☐	☐	Consideration should be given for paper and electronic data.	Click here to enter text.
Electronic signatures						
5.1	Does the system utilize electronic signatures, as configured?	☐	☐	☐	Indicate if the system is capable of electronic signature (or sign-off) and, if so, if they are being utilized. In the case electronic signatures are available but not used, this should be justified.	Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
5.2	Do electronic signatures prompt the user for a password (or biometric signature) when signing?	☐	☐	☐	Electronic signatures should prompt the user for at least a password when the signature is executed*. If this feature does not exist, it is not a true electronic signature system. Address any risk as appropriate. * When a series of signings are required during a single, continuous period of controlled system access, the first signing should include all electronic signature components; subsequent signings require at least one electronic signature component.	Click here to enter text.
5.3	Are signatures attributable to an individual?	☐	☐	☐	Electronic signatures should include the user ID, the name of the individual, the date, the time and the reason for the signature. If any of these elements are missing, then it is not a true electronic signature system. Address any risks as appropriate.	Click here to enter text.
5.4	Once a signature has been applied, is the data locked such that it cannot be modified?	☐	☐	☐	Measures should be put in place to secure approved/signed data from modification or deletion without having to be re-approved (and reason for change documented). Address any risks as appropriate.	Click here to enter text.

#	Questions	Responses				Comments, mitigation of risk
		Yes	No	N/A	Guidance	
5.5	Is the electronic signature linked and retained with the signed record?	☐	☐	☐	Electronic Signatures should be permanently linked and retained with the associated data record. Address any risks as appropriate	Click here to enter text.
5.6	Is the time/date of the signature recorded?	☐	☐	☐	See comment on 5.2. Address any risks as appropriate	Click here to enter text.
5.7	Do the signed records ensure attributability of the person signing?	☐	☐	☐	Consider adding capabilities to the system to visually label signed/approved records. Address any risks as appropriate	Click here to enter text.
5.8	If there are multiple levels of signature applied (e.g. analyst, reviewer, administrator), is the meaning of signature clearly recorded and visible?	☐	☐	☐	The signature meaning should be clearly visible (human readable) and/or documented via standard or procedure. Address any risks as appropriate.	Click here to enter text.
5.9	Are signatures protected from being modified, deleted or copied?	☐	☐	☐	Electronic signature should be protected from modification and deletions, nor shall the system allow signatures to be copied. The system should be capable of producing an audit trail associated to the electronic signature. Address any risks as appropriate	Click here to enter text.

This risk assessment tool was developed with the support of the International Consortium for Innovation and Quality in Pharmaceutical Development (IQ, www.iqconsortium.org). IQ is a not-for-profit organization of pharmaceutical and biotechnology companies with a mission of advancing science and technology to augment the capability of member companies to develop transformational solutions that benefit patients, regulators and the broader research and development community.