PERFORMING A DATA INTEGRITY REMEDIATION

Note: The below tables do not contain the complete set of items to be evaluated as part of Risk Assessment and serves as a guidance or example on how a Risk Assessment Template could be created. Based on the applicable local regulations, processes at your organization, system classification and criticality tailor the template as needed.

The same template could also be utilized as Data Integrity summary or Traceability where instead of impact and Mitigation, an objective evidence could be attached summarizing that the system meets the Data Integrity Requirements.

S. No.	Question	Response (Yes, No, N/A)	Impact	Mitigation Plan
Security and Access Control				
1.	Is the system access controlled through unique login credentials?			
2.	Is there a process defined and documented for user access control?			
3.	Are user accounts to the system reviewed periodically?			
4.	Are different user level access defined and documented?			
5.	Does the system have capabilities to perform the following? 1. Detection of incorrect credentials 2. Lockout of user accounts upon multiple incorrect attempts 3. Password expiration 4. Obscure Passwords during entry			
6.	Is the system time cannot be changed by anyone else except Administrators?			
Data Access and Review Process				
7.	Does the system prevent unauthorized modifications to the source data files stored within the Instrument?			

For any questions, please contact Loganathan.k@zifornd.com

S. No.	Question	Response (Yes, No, N/A)	Impact	Mitigation Plan
8.	Does the system prevent deletion of source data files?			
9.	Does the system prevent any modification or deletion to audit trail files (if they are separate)?			
10.	Are there any intermediate locations before the files are processed and reviewed? If Yes, are those locations controlled and verified for unauthorized modifications and deletions?			
11.	Is the source data review process defined and documented?			
12.	Are e-signatures utilized for review and approval within the Instrument Software? If yes, does it conform with 21 CFR Part 11 Requirements?			
13.	Does the system interface with LIMS or any other software for processing and approvals? If yes, does the integrations are validated for data accuracy and security?			
Audit Trail				
14.	Does the system provide Audit Trail capabilities?			
15.	Has the Audit Trail been tested as part of Qualification Package and does it demonstrate conformance to 21 CFR part 11 requirements?			
16.	Is the audit trail review (business and functional) process defined and documented?			
17.	Does the functional audit trail review been documented based on the frequency set?			

COMPLETED RISK ASSESMENT EXAMPLES

For any questions, please contact Loganathan.k@zifornd.com

S. No.	Question	Response (Yes, No, N/A)	Comments	Mitigation Required?	Mitigation Plan
Security and Access Control					
1	Is the system access controlled through unique login credentials?	No	High Risk – Impacts the Data Access Control	Yes	Upgrade the software to have unique individual accounts instead of shared accounts
2	Is there a process defined and documented for user access control?	Yes	N/A	N/A	N/A
3	Are user accounts to the system reviewed periodically?	No	Medium – Periodic review of user account is required to ensure only authorized users have access to the system.	Yes	Update the Procedure (SOP) to include the periodic review process.
4	Does the system have capabilities to notify the Administrators when there are multiple unauthorized attempts?	No	The system does not offer any automated capabilities. As part of periodic review, the system audit logs will be reviewed for unauthorized access attempts and appropriate actions will be taken accordingly (if needed).	No	None

COMPLETED DATA INTEGRITY SUMMARY EXAMPLES

S. No.	Question	Response (Yes, No, N/A)	Comments	Objective Evidence
1	Is the system access controlled through unique login credentials?	Yes	N/A	Refer Qualification Package for Instrument A, Change Number #xxx
2	Are e-signatures utilized for review and approval within the Instrument Software? If yes, does it conform with 21 CFR Part 11 Requirements?	N/A	All the review and approval process happen within LIMS and hence e-signature within the instrument is not utilized.	N/A
3	Are user accounts to the system reviewed periodically?	Yes	Periodic review results are stored within the Access Management System	Refer SOP XYZ – Use, Maintenance and Administration of Instrument A

End of Document