RISK ASSESSMENT PROTOCOL

FOR

COMPUTER SYSTEM OF

STABILITY-PC

System Name	**Stability -PC**
System ID	
Location	**Quality Assurance**
Effective Date	

RISK ASSESSMENT FOR COMPUTER SYSTEM OF STABILITY PC

System Name: Stability-PC **System ID:**

TABLE OF CONTENTS

RISK ASSESSMENT FOR COMPUTER SYSTEM OF STABILITY PC

System Name: Stability-PC **System ID:**

1. PRE-APPROVALS:

The signature listed below indicates the preapproval of this Risk assessment. This approval is joint responsibility of listed functional areas.

DOCUMENT DEVELOPMENT	SIGN / DATE
Name : _____ **Designation** : _____	

DOCUMENT REVIEW AND APPROVAL (M/S ……)
Sign / Date : _____ **Name** : _____ **Designation** : _____ **Engineering**
Sign / Date : _____ **Name** : _____ **Designation** : _____ **IT**
Sign / Date : _____ **Name** : _____ **Designation** : _____ **Quality Assurance**

DOCUMENT APPROVAL (M/S ……..)
Sign / Date : _____ **Name** : _____ **Designation** : _____ **Quality Assurance**

RISK ASSESSMENT FOR COMPUTER SYSTEM OF STABILITY PC

System Name: Stability-PC **System ID:**

2. SIGNATURE OF EXECUTOR:

All the executer involved in this document have to sign within prescribed format given below.

M/s ……

Name	Designation	Signature	Initial	Date

M/s ……

Name	Designation	Signature	Initial	Date

3. REVISION HISTORY:

Date	Supersedes	Reason for Revision

4. OBJECTIVE:

The objective of risk assessments is to analyze the risk of utilization of the Computer System of STABILITY-PC. To identify the possible areas of risk, where the existing laid down appropriate controls or measures requires further strengthening. To suggest suitable solutions (action plan) to mitigate or minimize the risk and review the risk and monitor controls of the system.

5. SCOPE:

The scope of the risk assessment exercise is to establish documentary evidence to assure that the manufacturing process is capable to produce the quality meeting pre-determined specifications using process control system with cGMP and GxP related risk. The scope of the risk assessment shall be limited to the process control system being installed at Validation of Hardware and Software system of computer system (STABILITY-PC) after modification. The Validation of Hardware and Software system of STABILITY-PC for modification shall be considered for the evaluation of the risk.

6. SYSTEM DESCRIPTION:

Computer system of STABILITY-PC defines the controlling of Stability chamber connected to the system. The CS software of stability chamber is a communication software for data management. The operator interface is carried out by CS screen. The CS is used to feed required parameters and set points in the system during operation. The system is connected to data server for printing and data backup. The system is secured by IT through password only within the system.

7. ROLE AND RESPONSIBILITY:

The validation team comprising of representative from each of the following departments should be responsible for overall compliance with this validation plan.

Department	Responsibilities
Validation Agency (…….)	➢ To collect the necessary data for Risk assessment activities. ➢ To prepare and execute the Risk assessment in coordination with engineering, validation and Quality Assurance team. ➢ Comply with regulatory / Guidelines / Standards / validation plan requirements throughout the validation life cycle. ➢ To submit Risk assessment for approval.
Engineering (M/s. ……)	➢ To provide the necessary data for Risk assessment activities. ➢ To review and approve the Risk assessment.
IT (M/s. ……)	➢ To provide the necessary data for Risk assessment activities. ➢ To review and approve the Risk assessment.
Quality Assurance (M/s. …….)	➢ . To provide the necessary data for Risk assessment activities. ➢ To review and approve the Risk assessment.
Quality Assurance (M/s. ……)	➢ To approve and authorized the Risk assessment

8. REFERENCES:

The publication listed below form part of this reference documents. Each publication shall have latest revision in effect on the date of this document is approved for execution.

GAMP 5	Good Automated Manufacturing Practices, Version 5, Guideline Document for Automated Systems from International Society of Pharmaceutical Engineering
21 Code of Federal Regulations (CFR), Part 210	Current Good Manufacturing Practice in Manufacturing, Processing, Packing, or Holding off Drugs; General
21 Code of Federal Regulations (CFR), Part 211	Current Good Manufacturing Practice for finished Pharmaceuticals
21 Code of Federal Regulations (CFR), Part 11	21 Code of Federal Regulations (CFR), Part 11Electronic Records, Electronic Signatures, Final Rule Electronic Submissions; Establishment of Public Docket, Notice
ICH Q9	International Conference of Harmonization (ICH) quality risk assessment Q9
EU GMP	Laying down the principles and guidelines of GMP in respect of medicinal products for human use.
WHO	Appendix 5, validation of computerized systems.

9. DOCUMENTATION PROCEDURE:

- Qualification activities will be performed as defined in the approved document.
- All documentation will be completed during the execution of the qualification.
- Recording of information will be made in permanent ink.
- Fill out complete information in the verification table provided.
- Do not keep any space blank. Mark blank space with a single line throughout the appropriate space with mentioning NA (Not Applicable) and put initial and date.
- Correct the mistakes by drawing a single line through the incorrect data, recording the correct information and then initialing and dating the change.

10. QUALIFICATION COMPLETION AND APPROVAL:

- Verify that all tests required by qualification are completed and attached.
- Verify that all amendments and discrepancies are documented, approved and attached.
- If all items in the qualification for the Computer System of STABILITY-PC have been reviewed and found to be acceptable, sign the corresponding block in the qualification completion and approval form.

11. ACCEPTANCE CRITERIA:

- Installation completion as per manufacturer's recommendations & cGMP requirements.
- The supply of all necessary documentation from manufacturer.
- The system is operating as intended and is under state of control.
- Operational features meet system requirements and system specifications.

12. RISK ASSESSMENT APPROACH:

The risk assessment should be done as per principle of failure mode, effects and criticality analysis. Risk assessment consists of the identification of hazards and the analysis and evaluation of risk associated with exposure to those hazards. Quality risk assessments begin with a well-defined problem description or risk question. When the risk in question is well defined, an appropriate risk assessment tool and the types of information that will address the risk question will be more readily identifiable. Hence the risk assessment will answer to the three following questions;

1. What might go wrong? (Risk identification/ unwanted event)
2. What are the consequences? (Severity / Impact)
3. What are likelihood (Probability and Frequency) it will go wrong, and the ability to detect it?

12.1 Identification of Risk (Unwanted Events):

This is the first stage of risk assessment which would answer the question "What might go wrong "including identifying the possible consequences on the quality of product and safety, health and environment. This would provide for the further steps in the quality risk assessment process.

12.2 Classification of Impact (Severity):

To identify severity or impact on product quality. The basic of rating are as under.

High: The effects are severe; very significant GMP non-compliance. Direct impact of data integrity.

Medium: The effects are moderately severe; Significant GMP non-compliance. An indirect impact of data integrity.

Low: The effects are not severe; Minor GMP non-compliance. Negligible impact of data integrity.

12.3 Classification of likelihood of Occurrence:

Classification of likelihood of occurrence shall be considered as under

Low: The negative event is unlikely to occur. Very less occur

Medium: The negative effect may occur. Records or regular basis.

High: The negative event is likely to occur. Frequently occur.

12.4 Classification of Risk Class:

The risk class for each risk scenario identified has been evaluated as a combination of severity and likelihood as reported in the below table.

		Likelihood		
		Low	**Medium**	**High**
Severity	**High**	**2**	**1**	**1**
	Medium	**3**	**2**	**1**
	Low	**3**	**3**	**2**

(High-1, Meduim-2 & Low-3)

Severity = Impact on product quality and data integrity (Or other harm)

Likelihood = Likelihood of the fault occurring.

Risk Class = Severity x Likelihood.

12.5 Classification of Risk Related to Probability of Detection:

The purpose of this phase has been to identify if the risk event could be recognized or detected (Detectability) by other system controls. The Detectability of a risk has been evaluated.

Detection	Criteria for Evaluation
Low	May overlook fault or failure possibly cannot be detected (No technical solution up to now)
Medium	Failure may be missed (Manual Control, Routine Work with Statistical Control)
High	Failure Can and Will be Detected (Using Statistical Tools).

12.6 Risk Priority Evaluation:

By combining the risk class with the detectability, it is possible to prioritise the fault conditions associated with each risk scenario based upon those areas of greatest vulnerability.

The matrix below provides the model to evaluate the risk priority.

		Detectability		
		Low	Medium	High
Risk Class	1	**High**	**High**	**Medium**
	2	**High**	**Medium**	**Low**
	3	**Medium**	**Low**	**Low**

Detectability = Likelihood that the fault will be noted before harm occur.

Risk Priority = Risk Class x Detectability.

12.7 Acceptability of Risk:

The risk priority rank, high or medium shall be considered unacceptable and existing control measures shall be considered insufficient. Recommended mitigation action shall be re-evaluated to meet its acceptance limit.

The risk priority rank low shall be considered acceptable. Current control measures shall be considered adequate. However, additional controls may be recommended for further strengthening existing system. Risk assessment forms for identified risk should be completed.

13. RISK REVIEW:

As risk assessment is an ongoing part of the quality assessment process. The output results of the risk assessment process will be reviewed if any major change is proposed in the system. The quality assessment process will be analyzed for a possible effect of any planned activity (results of product review, inspections, audits, change control) or unplanned (like root cause from failure investigations). The risk review might include reconsideration of risk acceptance decisions.

14. REPORT GENERATION:

The risk assessment report shall be made as per the documents sequence.

Risk Assessment annexure will be generated once all the risk assessment activities are finished. This will be a base document during the ongoing evaluation wherein the data will be reconfirmed or changed as per the requirement. These changes will come as a revision to the base document and will be approved by all concerned department.

15. DISCREPANCIES HANDLING DURING COMPUTER SYSTEM QUALIFICATION:

- In case of discrepancy observed during qualification, document in the defined column in each table and document the details of the observation in the discrepancy log sheet.
- Inform to engineering IT, QC and Quality Assurance about discrepancy.
- Investigate the discrepancy and ensure the possible impact.
- If discrepancy does not have potential to impact on operation as well as performance of the system, close the discrepancy with proper justification.
- The engineering IT, QC and QA will decide whether discrepancy is acceptable or not.
- If discrepancy is acceptable, provide conclusion and recommendation if any into respective column.

16. DISCREPANCY AND CORRECTIVE ACTION FORM:

Protocol Reference	
Discrepancy Number	

DISCREPANCY:

Describe the Discrepancy	
Reported by	Date

CORRECTIVE ACTION:

Describe corrective action taken (Attach additional sheets if necessary)	
Reported by	Date

DISPOSITION ACTION :

Acceptable?	Yes	No	
Discussion			
Approved by			Date

COMPLETION:

Completed by	Date

17. ABBREVIATION:

Abbreviations	Description
GMP	Good Manufacturing Practices
QA	Quality Assurance
SOP	Standard Operating Procedure
NA	Not Applicable
ICH	International Conference of Harmonization

18. ATTACHMENT SUMMARY:

Attachment No.	Description

19. RISK ASSESSMENT SUMMARY & CONCLUSION:

Compiled by: _____ **Date:**_____

20. POST APPROVALS:

The signature listed below indicates the post approval of this RISK assessment. This approval is joint responsibility of listed functional areas.

DOCUMENT DEVELOPMENT	SIGN / DATE
Name : _____ **Designation** : _____	

DOCUMENT REVIEW AND APPROVAL (M/S ……)
Sign / Date : _____ **Name** : _____ **Designation** : _____ **Engineering**
Sign / Date : _____ **Name** : _____ **Designation** : _____ **IT**
Sign / Date : _____ **Name** : _____ **Designation** : _____ **Quality Assurance**

DOCUMENT APPROVAL (M/S ……..)
Sign / Date : _____ **Name** : _____ **Designation** : _____ **Quality Assurance**