Instrument Name	Computer System
System ID.	.....
System Used For	High Pressure Liquid Chromatography
Make	Waters
HPLC ID.	
Application Software Type	Chromatographic☑ Non Chromatographic ☐
Application Software	Empower
Software Version	3.0
Make	Waters
System Type	New System☐ Existing system ☑
Location	Instrument Room

1.0 CONTENTS:

2.0 OBJECTIVE:

According to GMP guidelines, the quality status of Computer System (Hardware and Software) based control system used in Company must be traceable from the qualification documentation and records of the operational practice. Control system should be qualified and demonstrate the compliance with GAMP requirements.

Risk based qualification approach is adopted in order to determine the risk criteria and its measures of risk criteria.

3.0 RESPONSIBILITIES:

Risk Assessment Responsibilities are defined in following way.

3.1 QUALITY ASSURANCE (QA):

Following are the activities of QA:

- To provide quality assurance expertise in the execution of the risk assessment.
- To monitor risk assessment process with regulations and established standards
- To approve risk assessment report.

3.2 ENGINEERING /IT/ PRODUCTION/QC:

Following are the activities of Engineering, Information Technology, Quality Control Production Department:

- Assuring that selected system requires documents are available.
- Providing tools for data collection and archiving.
- Participate and Review of risk assessment report.

3.3 VALIDATION AGENCY:

Following are the main responsibilities of Validation Agency:

- Identifying risk scenarios and its Measures.
- Ranking of the risk scenarios.
- Preparation of risk reports.

4.0 RISK ASSESSMENT PROCESS

System used in facility is commercially available and purchased. Commercially available Instruments, Hardware and software have already been tested by the vendors . Therefore, simpler the risk analysis approaches are used for the commercial off-the-shelf systems.

The basis for the risk assessment will be the requirements specification. These documents are used to identify the system functions and their sub-functions, including the dependencies between them. In absence of formal User Requirement Specification (URS) and Functional Specification (FS), following strategy shall be considered to identify prospective URS and FS.

General list of features provided by system shall be reviewed. This information can be obtained from available user manual provided by vendor; if developed in-house, the URS and technical specification documents may be used. Derive basic features expected out of system and consider them as requirement specification.

Steps for Risk assessment:

1. Perform Initial Risk Assessment and determine System Impact
2. Identify Functions with Impact on patient safety, Product quality and Data Integrity
3. Perform Functional Risk Assessments and identify controls
4. Implement and verify Appropriate controls
5. Review Risks and Monitor Controls
6. Take Corrective and preventive action if existing control measure is not adequate to mitigate the identified risk.

4.1 IDENTIFYING GMP RISK:

The risk Identification is to access those risks associated with the control system operation in regulatory environment **"What can go wrong"?**

System functions, parameters should be evaluated and identified whether they represent a risk when assessed against a series of GxP criteria.

Following types of risks are mainly identified during risk assessment process but not limited:

- System access control
- Abnormal user operation performed at the time of system / software operation
- System hardware or Software failure.
- Power and communication failure of Control system or software.
- Improper training and unavailability of SOP's.
- Configuration of Process Set parameter.

4.2 IDENTIFYING GXP RISK SCENARIOS:

Having determined that a particular function may have a GxP risk associated with it, the assessment should proceed to identify the various risk scenarios i.e. the events that identify the risks associated with use of the system / software.

4.3 ASSESSING THE LIKELIHOOD OF AN ADVERSE EVENT:

Determine the likelihood (frequency or probability) of an adverse event occurring. User should consider the likelihood of the adverse event occurring per a quantity of transactions, and assigning a value to that estimate. Ranking of likelihood methods are defined as follows:

Probability of failure	Justification of Probability	Ranking
Very High: Adverse event occurs during every alternate.	Lack of operation and other critical SOP's	10
	Lack of Users Training and User Guide	9
High: Generally associated with adverse event similar to previous operation	Operational or system failure due to non- availability of system control	8
	Lack of Access control and/or unstable utilities	7
Medium: Generally associated with adverse event which occurs occasionally.	Error due to Human intervention like Wrong selection/enter operation set parameters	6
	Minor electrical or partial system failure	5
	Failure of Software or Hardware	4
Low: Failure is low during operation, which is totally system controlled in place.	Visual alarm/warning message mechanism in place. Failure reduces due to preventive maintenance. Users are trained with SOP's and various user guidelines.	3
	User access control with users Training	2
Remote: Failure is unlikely, no failure ever associated due to tested system control in place.	System control in place like interlock	1

4.4 ASSESSING THE SEVERITY OF IMPACT:

Risk Assessment requires not only the identification of the immediate effects of the risk but also affects the long-term impact on the business. These effects must be taken into account considering a wide variety of issues including impact on regulatory compliance, financial impact, Product Quality, Patient safety. The impact of risk occurring may be described as follows:

Probability of Effect	Possible Impact	Ranking
Hazardous (without warning)	System will completely disturb and/or non compliance with government regulation, product failure condition occurred	10
Hazardous(warning)	System will completely disturb and/or non compliance with government regulation, product failure condition occurred with warning message.	9
Very High	Major disruption to Product/Process and 100 % product/process scrapped. Total production cycle will be disturbed.	8
High	Minor disruption to Product/Process. <100 % product/process scrapped and corrected out by the process.	7
Medium High	Due to this type of adverse event post process are affected and may be required to 100 % reprocess/rework.	6
Medium	Due to this type of adverse event post process are affected and may required to minor correction.	5
Low	Adverse event occurs during execution of operation and can be correct by resetting of the system parameters.	4
Very Low	Adverse event occurs during execution of operation and can be correct by resetting of the system minor parameter.	3
Minor	Adverse event occurs during execution and will not affect the current operation it‘s kind of warning for the preventive action.	2
None	No Effect	1

4.5 ADVERSE EVENT DETECTION (DETECTIBILITY):

Identify if the adverse event can be recognized or detected by other means in the system. Adverse event having high probability of detection, may not cause a serious threat because it can be recognized quickly and suitable corrective action taken to mitigate its impact. If an adverse event has a low probability of detection, then the risk condition needs to be seriously considered for review of the design or the implementation of alternative procedures to avoid the event.

Probability of Detection	**Possible Detection control (s)**	**Ranking**
Almost Impossible	System will not detect any how and no known control(s) is available	10
Very Remote	System or operator will detect failure mode while fault is manually track down in the system.	9
Remote	System or operator will detect failure mode after wrong operation occurred and system is completely stop due to adverse event.	8
Very Low	System or operator will detect fault mode while executing next stage of system operation.	7
Low	System or operator will detect fault mode while starting next stage of system operation.	6
Medium	Operator will observe the minor abnormal system operation/control parameters.	5
Medium High	Operator will observe the multiple abnormal system operation/control parameters.	4
High	System will display the alarm message after the immediate next step of operation	3
Very High	System will display the relevant alarm message of the fault.	2
Almost High	System will display specific alarm message of the fault.	1

4.6 CALCULATION OF OVERALL PRIORITY (RISK PRIORITY NUMBER):

Overall priority is calculated using multiplication of the all three assessment ranking and decided based on following table:

Likelihood x Severity x Detection = RPN

Over all Priority RPN (Risk Priority Number):

Overall priority	Overall priority calculation result
Low	≤ 60
Medium	≤ 180
High	≥ 181

5.0 ABBREVIATIONS:

Short form	Abbreviated form
GxP	Generic acronym for pharmaceutical regulations, Good Manufacturing Practice (GMP), Good Laboratory Practice (GLP) & Good Clinical Practice (GCP)
GAMP	Good Automated Manufacturing Practice
ID No.	Identification Number
QA	Quality Assurance
SOP	Standard Operating Procedure
URS	User Requirement Specification
FS	Functional Specification
CSV	Computer System Validation
RPN	Risk Priority Number
GMP	Good Manufacturing Practices

6.0 REFERENCE DOCUMENTS REQUIRED FOR VALIDATION:

1. Standard operating procedures
2. System User Requirement Specification
3. System Design/Configuration Qualification documents
4. System History Record
    a. Instrument Calibration Records.
    b. Instrument Qualification
    c. Previous Change Control documents
5. Design Documents
    a. System operation manual
    b. List of system components as part of system
    c. Specification & installation manuals
    d. Vendor Test Reports.

7.0 APPROVAL PAGE:

Department	Name	Designation	Signature	Date
Prepared by: M/s.				
ENGINEERING				
Reviewed by: M/s.				
QUALITY ASSURANCE				
Reviewed by: M/s.				
ENGINEERING				
Reviewed by: M/s.				
IT DEPARTMENT				
Reviewed by: M/s.				
QUALITY CONTROL				
Approved by: M/s.				
QUALITY ASSURANCE				